IT Insight SECURITY

#15 DEZEMBRO 2023

AS AMEAÇAS INTERNAS

Building What's Next in Cybersecurity

Complex connectivity. Mountains of data. An expanding cloud environment. And always-evolving cybercriminals. That's why we create, disrupt and innovate, ensuring the world is ready for whatever the future holds. See how we can help your organization move forward with confidence. See how We've Got Next.

paloaltonetworks.com

WE'VE GOT NEXT

paloalto® NETWORKS | Cybersecurity Partner of Choice

COVER

BRAVE NEW WORLD

IT·SECURITY CONFERENCE

TRANSFORM

RISK

▼ AI ACT

CHAT

▼ NUNO PERRY,
GOV. REGIONAL DA MADEIRA

EXPERT

▼ CRISTIANE DIAS

BLUE TEAM

▼ BALWURK

HPE aruba networking

SAIBA O QUE O SASE UNIFICADO PODE FAZER POR SI

O SASE Unificado que a HPE Aruba Networking lhe propõe é uma estrutura de TI que combina funções de rede e segurança numa única plataforma que liga de forma segura todos os utilizadores, dispositivos e aplicações em toda a força de trabalho distribuída globalmente.

Conheça o poderoso SASE unificado da HPE Aruba Networking e fique a saber tudo o que pode fazer pela sua organização.

Saiba mais em https://www.go2event.pt/aruba-sase/

BROWSE S.LABS

S.LABS

arcserve®

Os ataques de ransomware estão a crescer em custo e frequência: 5 medidas que as organizações devem tomar para se protegerem

balwurk cyber security

A Gestão do Risco no contexto da Segurança Aplicacional

cipher
a Prosegur company

Desbloquear sinergias através de uma Gestão Integrada de Riscos

CSO chief security officers

Gestão Integrada de Risco

HPE aruba networking

SASE Unificado: conectividade e segurança modernas para a empresa digital

ONE IDENTITY by Quest

Gerir as identidades e os acessos para proteger as organizações

paloalto® NETWORKS

Estratégias de gestão de riscos de cibersegurança

SECURNET
ALWAYS ONLINE | ALWAYS SECURE

2023: Odisseia no ciberespaço

SOPHOS

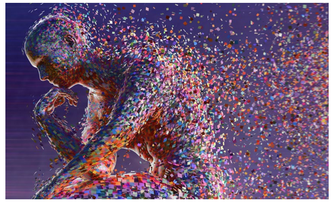
Ameaças internas: a face oculta das ameaças empresariais

VARONIS

Os seus dados estão à prova de insiders? Cinco passos para manter os seus segredos seguros

S.LABS

S.Lab ou Security Labs é a marca da área de conteúdo patrocinado / Branded Content da IT Security. Com o objectivo de desenvolver ideias dos nossos parceiros, mais difíceis de traduzir em formato publicitário, o S.labs trabalha os conceitos de marcas ou produtos em diferentes formatos como artigos, vídeos, webinars, podcasts, conferências, entre outros.



DIAMOND

"Em termos de grande crescimento está a cibersegurança e a IA nos próximos anos"

PLATINIUM

“É necessário rever a forma como as redes são desenhadas”

“Uma das grandes lacunas é a capacidade de responder com rapidez suficiente”

GOLDEN

Como conseguir a “imutabilidade de dados”

A convergência entre cibersegurança e network

“A segurança está no caminho crítico do negócio digital”

“É preciso entender a diferença entre cibersegurança e ciber-resiliência”

“Ameaças mais profundas às organizações vêm de vulnerabilidades conhecidas há muito tempo”

A transparência é a “chave” da Purple Team

SILVER

Soluções de cibersegurança tradicionais são “peças de puzzle que não encaixam”

O panorama mundial de ataques DDoS

Lenovo entrega portátil a leitor da IT Security

Oramix organiza almoço executivo

“As medidas que estão aplicadas são fundamentais, mas se calhar não são suficientes”

“Com uma superfície de ataque tão grande, teremos sempre um sistema vulnerável”

“Os ataques não são uma questão de ‘se’, são uma questão de ‘quando’”

As soluções de MFA são mais económicas e resolvem grande parte dos erros humanos”

Limite os danos que os insiders podem causar com a Plataforma de Segurança de Dados Nº 1.

- A maioria das empresas tem controlos de segurança em todo o lado, exceto nos seus dados, pelo que os insiders e os atacantes que contornam o perímetro podem infligir danos enormes.
- Um utilizador comprometido ou um insider mal-intencionado pode causar danos duradouros.
- A Varonis audita a atividade, envia alertas e garante por exemplo que cada funcionário só tenha acesso aos dados de que realmente necessita.

Descubra porque a Varonis está classificada como nº 1 no Gartner Peer Insights para gestão de riscos internos. **Obtenha a sua Avaliação de Risco de Dados gratuita em https://info.varonis.com/en/data-risk-assessment**

A TODOS OS LEITORES, OBRIGADO

RUI DAMIÃO

No passado dia 12 de outubro, a IT Security voltou a realizar a sua conferência e, para todos os que marcaram presença, só temos uma palavra: obrigado.

Quando começámos a preparar a edição deste ano, sabíamos que queríamos receber mais leitores do que na primeira edição, mas não sabíamos a quantidade de pedidos que íamos ter e que esgotaram o evento semanas antes do mesmo acontecer.

A partir daí, o que queríamos era ter o melhor programa e os melhores oradores possíveis. Sou suspeito, é certo, mas considero que conseguimos atingir precisamente isso. Tivemos oradores de vários setores de atividade, inclusive fora de Portugal, que partilharam a sua experiência, o seu conhecimento e os desafios que enfrentam – e como os ultrapassam – para melhorar a cibersegurança das suas organizações e que acabam por proteger os dados não só das organizações em si, mas também dos seus clientes (que somos todos nós).

Como disse na abertura da IT Security Conference, a adesão dos leitores mostra que a cibersegurança está na ordem do dia e ainda bem que assim o é. É um tema que tem de estar na ordem do dia porque diz respeito a todos, aos nossos dados, às nossas infraestruturas críticas que, sem elas, não conseguimos viver.

No questionário de satisfação que realizámos tivemos uma resposta bastante positiva que nos dá vontade de continuar a trazer – seja em eventos, nas edições que publicamos de dois em dois meses ou diariamente no *website* – os tópicos mais relevantes para os CISO, os CSO e outros responsáveis de cibersegurança e segurança de informação. Recebemos, também, várias sugestões que queremos pôr em prática para que o evento seja o melhor para todos os que marcam presença.

Para o ano pretendemos fazer mais. A terceira edição da IT Security Conference já tem data marcada – 10 de outubro de 2024 – e toda a equipa vai trabalhar com o mesmo entusiasmo para que a edição do próximo ano tenha, pelo menos, o mesmo sucesso que este ano teve.

Assim, resta-me agradecer, uma vez mais, a todos os leitores. Encontramo-nos no dia 10 de outubro do próximo ano!

xMDR

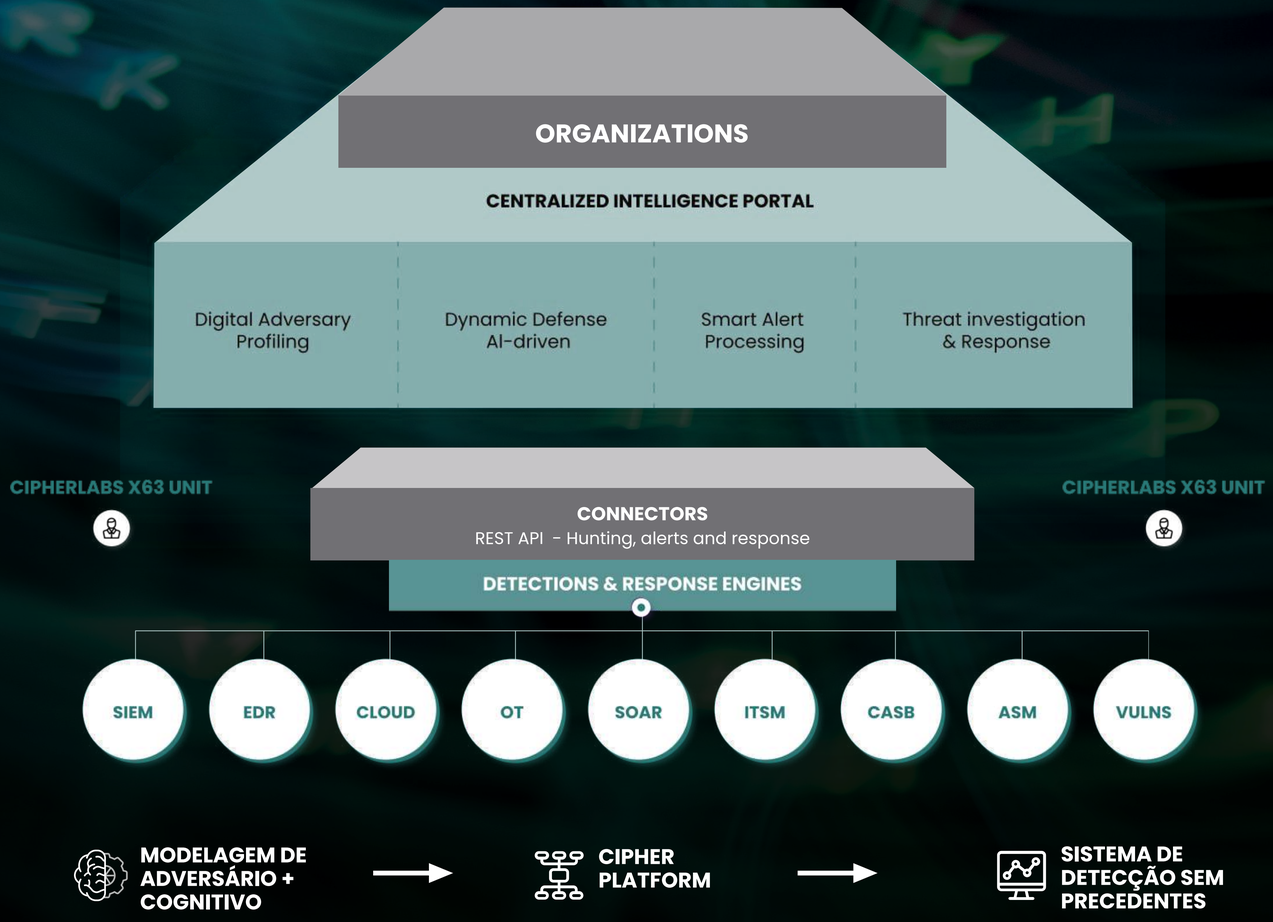
powered by cipher
a Prosegur company

Modelagem digital do adversário e aplicação de processos cognitivos

xMDR é a plataforma de serviços de segurança cibernética desenvolvida pela Cipher para responder aos problemas de visibilidade, fragmentação da tecnologia e escassez de profissionais que impedem a melhoria contínua da postura de cibersegurança das empresas.

Com o **xMDR** você obtém:

- Diminuição de falsos positivos abaixo de 1%
- Alertas de alto valor com a capacidade de antecipar incidentes
- Retorno do investimento com implantações ágeis em poucas horas



Fale conosco: **contato@cipher.com**

www.cipherxmdr.io cipher ciphersec ciphersec

AGI
E CIBERSEGURANÇA

HENRIQUE CARREIRO

A chegada iminente da inteligência artificial geral (AGI), como foi, de alguma forma recentemente prenunciada pelo drama de mudanças organizacionais na OpenAI, representa uma faca de dois gumes para o domínio da cibersegurança. Embora a AGI prometa revolucionar a deteção e a resposta aos ataques informáticos, suscita simultaneamente grandes preocupações quanto a uma potencial utilização indevida e quanto a consequências imprevistas. À medida que nos aventuramos neste território desconhecido, é fundamental avançar com passos seguros.

Por um lado, os sistemas de cibersegurança alimentados por AGI podem dar início a uma era transformadora de mitigação de ameaças. A sua capacidade de analisar grandes quantidades de dados poderá permitir a identificação de anomalias, padrões e comportamentos indicativos de ciberataques, permitindo neutralizar as ameaças antes de se materializarem em danos irreversíveis. Além disso, a capacidade de adaptação e aprendizagem contínuas da AGI poderá equipar-nos para nos mantermos à frente das táticas e técnicas em constante evolução utilizadas por agentes malévolos.

Mas, por outro lado, o poder da AGI tem potencial imenso para uma utilização indevida. Nas mãos, por exemplo, de agentes ao serviço de estados à margem da comunidade internacional, a AGI pode ser utilizada como arma para criar ciberataques capazes de causar danos generalizados. Os *deepfakes*, por exemplo, gerados por AGI, podem ser utilizados para espalhar a desinformação e manipular a opinião pública. Além disso, os sistemas de armas autónomos, alimentados por AGI, poderão constituir uma ameaça existencial para a humanidade (imagine-se o resultado de cruzar robots como os da Boston Dynamics com sistemas que disponham de AGI).

Dada a dualidade inerente aos futuros sistemas AGI, é imperativo estabelecer orientações e quadros éticos claros para garantir o seu desenvolvimento e implementação responsáveis. Estes quadros devem abordar questões fundamentais como a transparência e a responsabilização, o controlo e a supervisão humana, a beneficência e a não maleficência, bem como a não discriminação e a equidade.

A transparência e a responsabilização, nomeadamente, são essenciais para garantir que o desenvolvimento e a utilização dos sistemas AGI sejam objeto de escrutínio público. Os criadores de sistemas AGI devem ser transparentes quanto às suas capacidades e limitações e devem ser responsabilizados pelas suas ações. O controlo e a supervisão humana são fundamentais para evitar que os sistemas AGI funcionem de forma autónoma, podendo ter consequências catastróficas.

Teremos também de estar preparados para cenários em que esta tecnologia caia em mãos onde tais preocupações não sejam prioritárias. Não é difícil imaginar um conjunto de estados -- ou organizações -- que possam chegar a sistemas AGI e onde as questões de utilização responsável sejam consideradas de somenos importância. Ou seja, estamos entre dois caminhos que já se conhecem, por exemplo, dos casos de desenvolvimento de armas avançadas: por um lado, a responsabilidade na criação; por outro, a preparação para cenários em que rivais não tenha igual preocupação.

À medida que navegamos nas águas desconhecidas da AGI, é imperativo proceder com cautela e discernimento. Embora a AGI tenha um potencial imenso para melhorar as nossas capacidades de cibersegurança, apresenta simultaneamente riscos significativos. Ao aderir a princípios éticos e ao promover um desenvolvimento responsável, podemos aproveitar o poder da AGI para melhorar a sociedade -- sem nunca deixar de considerar, e estarmos ao mesmo tempo preparados, para o que outros, menos escrupulosos, possam estar a congeminar. ◀

noesis
an Altia Company

DARKTRACE

Detete todas as ciberameaças à sua empresa em apenas 4 semanas

Peça a sua avaliação gratuita
de Darktrace Enterprise Immune System

- 4 Semanas de utilização de solução de Cyber AI, sem custos
- Proteção dos colaboradores e organização contra ameaças de segurança
- Ação imediata sobre qualquer ameaça ou vulnerabilidade
- Tecnologia líder mundial assente em Machine Learning

Saiba mais

Helping your business **grow faster**

Portugal · Espanha · Irlanda · Holanda · Brasil · EUA

www.noesis.pt

CISA DESCREVE ESFORÇOS DE CIBERSEGURANÇA ASSENTES EM IA

A CISA detalha os seus esforços para promover a utilização da IA em cibersegurança e orienta as organizações de infraestruturas críticas na adoção da tecnologia.

A agência de cibersegurança norte-americana, a CISA, publicou um documento com os detalhes dos seus esforços na promoção da utilização da Inteligência Artificial (IA) com o objetivo de melhorar a segurança e apoiar as organizações de infraestrutura crítica na adoção desta tecnologia.

O *Roadmap to AI* da CISA está alinhado com a estratégia nacional de IA dos Estados Unidos e promove a utilização benéfica destas ferramentas no aperfeiçoamento das capacidades de cibersegurança. O documento descreve os esforços da agência na proteção dos sistemas de IA contra ameaças, procurando visar que esta tecnologia seja utilizada pelos cibercriminosos para ameaçar as infraestruturas críticas. ◀

PALAVRA-PASSE MAIS UTILIZADA EM PORTUGAL É "ADMIN"

Estudo revela quais são, atualmente, as palavras-passe mais utilizadas pelos portugueses, com "admin", "123456" e "user" a figurarem nos três primeiros lugares da lista.

Em 2023, "admin" foi a palavra-passe mais utilizada pelos portugueses, tal como revelado pelo quinto estudo anual NordPass.

As conclusões do estudo não representam em absoluto o uso de palavras-passe em todo o mundo, uma vez que os investigadores analisaram uma amostra de palavras-passe extraída de fontes de acesso público, incluindo fontes da dark web.

Segundo a NordPass, as 20 palavras-passe mais comuns em Portugal são:

1. admin
2. 123456
3. user
4. 123456789
5. 12345678
6. password
7. 12345
8. benfica
9. graciete10
10. merda123
11. Oliveira11
12. diogo123
13. Password
14. jorge123456
15. 1234567890
16. catarina
17. qwerty
18. xandrito
19. portugal
20. benfica91 ◀

arcserve®

Data Protection. Disaster Recovery. Data Management.

Livre-se de Ransomware

Com a plataforma de Resiliência de Dados da Arcserve

arcserve® OneXafe®

SPX ShadowProtect

ShadowXafe

OneXafe Solo

Cloud Services

SaaS Backup

UDP

Appliances

Seguro. Acessível. Otimizado.

arcserve.com

VULNERABILIDADE NO ZIMBRA EXPLORADA PARA CORROMPER EMAILS GOVERNAMENTAIS

Equipa de analistas da Google indicou que uma vulnerabilidade no Zimbra descoberta este ano está a ser explorada em várias campanhas para corromper emails pertencentes a governos.

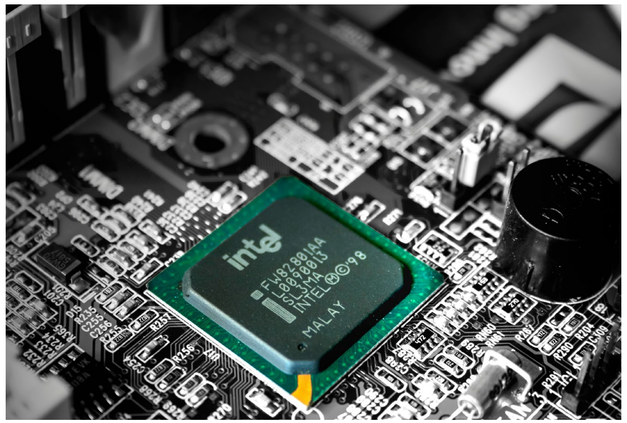
O Threat Analysis Group da Google revelou que uma vulnerabilidade *zero-day* no Zimbra Collaboration Suite foi explorada no início deste ano para "roubar" informação de emails de organizações de governos de vários países.

A vulnerabilidade (CVE-2023-37580) foi tornada pública durante o mês de julho e a Zimbra notificou os seus clientes para a mesma. A falha permite que um atacante execute código malicioso através do envio de emails que contenham URL específicos contra a organização alvo. Para que a vulnerabilidade seja explorada com sucesso, o utilizador tem de carregar no código malicioso enquanto estão autenticados numa sessão do Zimbra.

O grupo de análises de ameaça em questão revelou que assistiu à primeira campanha que explora esta vulnerabilidade a 29 de junho, quase um mês antes da correção ter sido lançada. ◀

INTEL CORRIGE VULNERABILIDADE GRAVE QUE AFETA CPU

A Intel corrigiu uma vulnerabilidade de alta gravidade que afeta CPU em desktops, dispositivos móveis e servidores.



A Intel corrigiu uma vulnerabilidade de alta gravidade que afeta unidades centrais de processamento (CPU) nos seus produtos *desktop*, móveis e servidores.

O sucesso da exploração deste bug – rastreado como CVE-2023-23583 e com o nome de código Reptar – poderá permitir aos cibercriminosos a obtenção do acesso de nível superior ao sistema, conseguindo chegar às informações confidenciais e até causar o *crash* da máquina. A vulnerabilidade tem a pontuação de gravidade CVSS de 8,8 em 10.

De acordo com uma investigação da Google sobre a vulnerabilidade, o Reptar é capaz de manipular instruções de software ao adicionar um prefixo redundante, podendo levar a um comportamento imprevisível do sistema e resultar numa falha do mesmo. Verificou-se um aumento do número de vulnerabilidades que afetam CPU em sistemas de hardware, segundo a Google. ◀

Os cibercriminosos de ransomware conectam-se quando as equipas se desconectam.

90% dos ataques de ransomware ocorrem fora do horário de trabalho. Contar com o serviço de deteção e resposta geridas (MDR) 24/7 da Sophos é uma parte essencial da estratégia de segurança de uma empresa.

Sophos Managed Detection and Response

O Sophos MDR é um serviço de segurança gerida que se adapta às suas necessidades e lhe permite atingir os seus objetivos de segurança e de negócio, sendo compatível com as suas ferramentas de cibersegurança existentes.

Saiba mais em: https://www.sophos.com/en-us/products/managed-detection-and-response

SOPHOS

230918 PTBR (MP)

ALIADOS DA NATO APOIAM CRIAÇÃO DE CENTRO COOPERATIVO PARA COMBATER ATAQUES

Os delegados da aliança expressaram apoio à resposta coletiva contra ciberataques, como a criação de um Centro Cibernético da NATO, durante a Cyber Defence Conference.

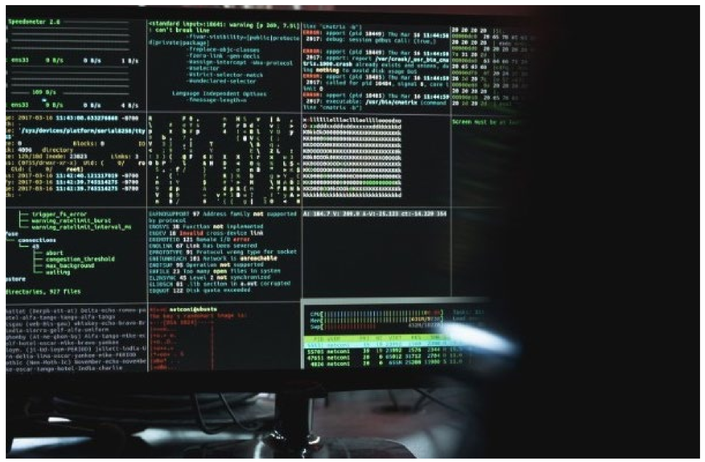
Os delegados da NATO reuniram-se na primeira edição da Cyber Defence Conference, que decorreu na cidade de Berlim. O evento assinala a crescente aceitação entre os aliados de que são necessários novos métodos para enfrentar os ciberataques para além da resiliência.

Aliados como a Alemanha, a anfitriã da conferência este ano, e o Reino Unido, o anfitrião do próximo ano, disseram que apoiavam a criação de um "NATO Cyber Centre" (Centro Cibernético da NATO), durante os discursos de abertura e o painel de discussão.

A missão concreta deste órgão não ficou clara, particularmente se este existiria para desenvolver as competências cibernéticas entre aliados, para criar uma consciência partilhada sobre aquilo que está a acontecer no ciberespaço, ou se seria um comando de nível tático para operações combinadas. ◀

REMCOS É A PRINCIPAL AMEAÇA CONTRA ORGANIZAÇÕES PORTUGUESAS

No mês de outubro, o Remcos tornou-se na ameaça mais dominante em Portugal, seguido pelo NJRat e pelo FormBook, que, apesar de perder alguma força, continua a ser a terceira ameaça mais prevalente.



A Check Point publicou o Índice Global de Ameaças relativamente a outubro de 2023. No mês passado, o *Remote Access Trojan* (RAT) NJRat, que é conhecido por visar agências governamentais e organizações em todo o Médio Oriente, subiu quatro lugares do sexto para o segundo lugar no *ranking* global. Entretanto, os investigadores relataram uma nova campanha de malspam que envolveu o avançado RAT AgentTesla. O setor da Educação continuou a ser o mais visado.

Em Portugal, em outubro de 2023, o malware mais dominante foi o Remcos, que afetou 2,57% das organizações portuguesas. Em termos de setores, também houve alterações no primeiro lugar: o setor das Finanças/Bancário foi a principal indústria atacada no mês passado. ◀

cso
chief security officers

O EQUILÍBRIO ENTRE A DISPONIBILIDADE E O RISCO É A CHAVE PARA A SEGURANÇA DA INFORMAÇÃO

CONHECIMENTO - ÉTICA - RIGOR

www.cso.pt | info@cso.pt

RETALHO TEM CADA VEZ MENOS CAPACIDADE PARA TRAVAR CIBERATAQUES EM CURSO

Estudo indica que apenas 26% das organizações de retalho conseguiu impedir os cibercriminosos de encriptar os seus dados num ataque de ransomware.

A Sophos partilhou as conclusões do seu relatório de investigação sobre o setor do retalho, "*The State of Ransomware in Retail 2023*" e descobriu que, no ano passado, apenas 26% das organizações de retalho foram capazes de interromper um ataque de ransomware antes que os seus dados fossem encriptados. Este é o valor mais baixo do setor nos últimos três anos – um declínio de 34% em 2021 e de 28% em 2022 –, o que sugere que as empresas de retalho têm cada vez menos capacidade de deter ataques de ransomware em curso.

A investigação concluiu que, para as organizações de retalho que pagaram o resgate, os custos médios de recuperação (não incluindo o próprio pagamento do resgate) foram quatro vezes superiores aos custos de recuperação das organizações que utilizaram cópias de segurança para recuperar os seus dados (três milhões de dólares versus 750 mil dólares). ◀

MICROSOFT VAI IMPLEMENTAR POLÍTICAS DE MFA PARA ACEDER A PORTAIS DE ADMINISTRAÇÃO

A Microsoft planeia implementar brevemente políticas de aplicação de MFA para acesso aos seus portais de administração, como Microsoft Entra, Microsoft 365, Exchange e Azure.

A Microsoft começará em breve a implementar políticas de acesso condicional que exigem a autenticação multifator (MFA) dos administradores para aceder aos portais de administração da empresa, como Microsoft Entra, Microsoft 365, Exchange e Azure.

A empresa anunciou que implementará também políticas que vão exigir MFA por utilizador em todas as aplicações de cloud. Uma política exigirá MFA para *logins* de alto risco, que estará disponível apenas para clientes do Microsoft Entra ID Premium Plano 2.

As políticas em questão, geridas pela Microsoft, serão adicionadas de forma gradual no modo '*report-only*' aos locatários elegíveis do Microsoft. Após a implementação chegar ao locatário, os administradores terão 90 dias para as rever e decidir se desejam ativá-las ou não. ◀

balwurk cyber security

Shift Left, Secure Right.

Your strategic partner for Application Security!

Our expertise empowers businesses to apply security by design principles within their software development lifecycle.

OUR SERVICES | *Application Security & GRC*

- DevSecOps
- Penetration Testing
- Vulnerability Check
- Cloud Security
- Education & Culture
- Maturity & Gap Analysis
- Governance & Compliance
- Risk Management

balwurk.com
mail@balwurk.com

GRUPO NORTE-COREANO UTILIZA MALWARE PARA MACOS EM ATAQUES

Investigadores de segurança descobriram um novo malware para MacOS e Windows associado ao grupo Lazarus, da Coreia do Norte.

O grupo norte-coreano Lazarus estará a utilizar um novo malware para MacOS e Windows em ataques recentes, indicam investigadores de cibersegurança. Num dos ataques, engenheiros de blockchain numa plataforma de compra e venda de criptomoedas foram alvo de uma aplicação Python desenhada para fornecer acesso inicial.

Como parte do ataque, o grupo Lazarus fez-se passar por membros da comunidade blockchain num canal público no Discord, convencendo as vítimas a descarregar um arquivo que continha um código malicioso.

No final do processo de várias fases, era executado um novo malware para MacOS chamado KandyKorn na máquina da vítima, permitindo aos ataques ter acesso ao sistema e exfiltrar dados.

Depois de instalado, o malware espera para que o servidor *command-and-control* envie comandos para permitir a recolha de informação, listar diretórios e processos, descarregar e carregar ficheiros e exfiltrar dados. ◀

88% DOS PORTUGUESES RECEIAM SER VÍTIMAS DE FRAUDE DIGITAL

A grande maioria dos portugueses receia ser alvo de algum tipo de fraude digital e é a favor de haver mais verificações nas suas transações, bem como do recurso a biometria e IA.

De acordo com o novo estudo do SAS, a esmagadora maioria dos portugueses (88%) tem receio de cair vítimas de algum tipo de fraude digital. Enquanto 66% dos 13.500 consumidores inquiridos, oriundos de mais de 15 países, consideram que as empresas deveriam fazer mais para os proteger, 60% mostra-se mais cauteloso sobre o assunto e 51% estão menos dispostos a partilhar os seus dados pessoais.

Em Portugal, 29% dos inquiridos acreditam que já foram alvos de algum tipo de fraude pelo menos uma vez, enquanto 62% afirmam ter sofrido uma tentativa de fraude no último ano, de acordo com o estudo "*Faces of Fraud*".

O furto de dados bancários é o tipo de fraude mais comum, seguido pelo furto de dados pessoais e pelas situações em que os consumidores são induzidos a pensar que foram os vencedores de um prémio financeiro. ◀

SECURNET

ALWAYS ONLINE | ALWAYS SECURE

MAIS DE 20 ANOS DE EXPERIÊNCIA, COM A SEGURANÇA NO ADN

info@securnet.pt

PORTO +351 224 673 094
LISBOA +351 213 622 204
*Chamada Rede Fixa Nacional

SIGA-NOS EM:

www.securnet.pt

ALWAYS ONLINE | ALWAYS SECURE

EUROPA É DAS REGIÕES COM PIOR SEGURANÇA DE PASSWORDS

Apesar de haver algumas melhorias na segurança de passwords a nível mundial, a Europa Meridional, onde se localiza Portugal, ocupa um dos últimos lugares no relatório da Dashlane.

No seu segundo relatório anual sobre o estado global de segurança das *passwords*, a Dashlane revela que houve ligeiras melhorias do "*Password Health Score*" a nível mundial. No entanto, a região da Europa Meridional, que inclui Portugal, registou uma das piores pontuações.

A análise baseou-se em dados anónimos e agregados e teve em consideração os hábitos de cibersegurança de mais de 19 milhões de utilizadores e 22 mil organizações clientes da Dashlane.

As conclusões do relatório indicam uma pequena melhoria da segurança de passwords em comparação com o ano passado, sendo que a pontuação do "*Password Health Score*" aumentou, em média, quase dois pontos em todas as regiões do mundo. No entanto, todas continuam a integrar a categoria de "necessita de melhoria", correspondente a pontuações entre 60 a 90. ◀

SOLARWINDS É PROCESSADA POR REGULADORES DOS EUA APÓS ATAQUE EM 2020

A Securities and Exchange Commission avança com um processo contra a SolarWinds por fraude e falhas de controlo interno após um ciberataque russo em 2020.

A SolarWinds Corp e um executivo sénior estão a ser processados pela Securities and Exchange Commission (SEC) dos Estados Unidos na sequência de uma violação do software da empresa numa campanha massiva de ciberespionagem russa em 2020.

Os reguladores da SEC anunciaram "acusações contra a empresa de software SolarWinds Corporation, com sede em Austin, Texas, e o seu diretor de segurança da informação, Timothy G. Brown, por fraude e falhas de controlo interno relacionadas com riscos e vulnerabilidades de cibersegurança supostamente conhecidos".

O processo sucede um ataque russo, em 2020, em que os cibercriminosos utilizaram software da SolarWinds para violar 632 mil endereços de e-mail do Departamento de Justiça e do Pentágono, como parte integrante do ciberataque MOVEit. ◀

Bravantic® // Evolving Technology

bluechip

IBM® Gold Partner

Insegurança é uma questão de prefixo

/ Cybersecurity

A segurança dos sistemas de informação é de extrema importância para as organizações, especialmente com a crescente digitalização dos negócios e com o aumento de ciberataques, a Cibersegurança tornou-se essencial. Em resposta a isso, temos à disposição soluções personalizadas para o ecossistema de cada organização. As nossas ofertas vão desde Security Consultancy, Compliance Regulatório, Gestão de Risco, Security Awareness, Security Assessment, SOC, Resposta a Incidentes.

Descubra toda a nossa expertise em
www.bravantic.com

Siga-nos em

COVER

QUANDO AS AMEAÇAS JÁ ESTÃO DENTRO DAS ORGANIZAÇÕES

POWERED BY:
paloalto NETWORKS

POR RUI DAMIÃO

NEM SÓ DE AMEAÇAS EXTERNAS VIVEM AS ORGANIZAÇÕES. OS COLABORADORES – DE FORMA INTENCIONAL OU POR NEGLIGÊNCIA – TAMBÉM PODEM SER UMA AMEAÇA À CIBERSEGURANÇA DAS EMPRESAS.

Quem anda no mundo da cibersegurança sabe que não é apenas através de sistemas extremamente complexos, atacantes superinteligentes e métodos complicados que se ataca uma organização. Por vezes, o simples carregar de uma ligação num simples email coloca em xeque toda a empresa.

Na larga maioria das vezes, carregar numa ligação não é uma ação intencional para colocar em risco toda a organização, mas sim uma desatenção ou uma falta de cultura de ciberhigiene que, na verdade, ameaça a operação da empresa.

Mas há também quem, intencionalmente, rouba informação da empresa, seja por desacordo com a própria empresa, seja por uma motivação financeira. Todas estas ameaças são tão importantes quanto o tal sistema extremamente complexo e os tais métodos sofisticados que, eventualmente, encontram uma brecha na organização para roubar tais informações confidenciais.

Paulo Pinto, Business Development Manager da Fortinet Portugal, relembra que uma ameaça interna "é um tipo de ciberataque provocado por um indivíduo que trabalha para uma organização ou tem acesso autorizado às suas redes ou sistemas".

Rui Duro, Country Manager da Check Point Software Technologies em Portugal, explica que as ameaças internas "podem ser intencionais, como um ataque deliberado, ou não intencionais, como neglicência ou erro humano que resulta em exposição não autorizada de informações".

David Grave, Security Director da Claranet Portugal, diz que, quando se fala de ameaças internas, fala-se de qualquer tipo de atividade maliciosa provocada por um membro de uma organização, onde se incluem "funcionários ou ex-funcionários que podem aceder, divulgar ou roubar informações confidenciais".

Aaron Bugal, Field CTO APJ da Sophos, explica que, ainda que "haja muitas circunstâncias diferentes possíveis, qualquer pessoa pode ser uma ameaça interna" numa organização.

AS AMEAÇAS (INTERNAS) COMUNS

Rui Duro, da Check Point, diz que, neste momento, há uma "variedade de ameaças internas que podem comprometer a segurança dos ativos digitais" e, como tal, "é importante reconhecer a importância de estar sempre um passo à frente desses desafios". Estas ameaças dizem respeito a acesso não autorizado, a phishing interno – que leva à divulgação inadvertida de informações confidenciais –, ao furto de dados, à negligência, ao malware interno e à privacidade e conformidade.

David Grave, da Claranet, separa os tipos mais comuns de ameaças internas em três categorias: furto de dados, acesso não autorizado e erro humano. "No caso do roubo de informações confidenciais sobre os negócios, os clientes e os funcionários, pode causar grande prejuízo à organização, passando ideias, números financeiros, contactos de clientes e projetos a concorrentes, por exemplo. Já o acesso não autorizado a sistemas e redes, normalmente protagonizado por funcionários mal-intencionados, pode resultar na "navegação" por áreas restritas de uma rede, na instalação de software malicioso ou na utilização de credenciais roubadas, comprometendo os sistemas. Por fim, a execução de ações incorretas, atitudes de negligência ou a falta de formação dos colaboradores podem comprometer a segurança dos dados e da rede da organização", afirma David Grave.

Para além das ameaças intencionais e não intencionais, Paulo Pinto, da Fortinet, acrescenta ainda as ameaças maliciosas, que são "uma forma de ameaça interna intencional que pretende causar danos para benefício pessoal ou como um ato de vingança. As ameaças maliciosas de pessoas com informação privilegiada têm como objetivo a fuga de

PAULO PINTO, FORTINET PORTUGAL

> AMEAÇA INTERNA "É UM TIPO DE CIBERATAQUE PROVOCADO POR UM INDIVÍDUO QUE TRABALHA PARA UMA ORGANIZAÇÃO OU TEM ACESSO AUTORIZADO ÀS SUAS REDES OU SISTEMAS"
>
> PAULO PINTO, BUSINESS DEVELOPMENT MANAGER DA FORTINET PORTUGAL

RUI DURO, CHECK POINT SOFTWARE TECHNOLOGIES EM PORTUGAL

> “A FALTA DE CONSCIENCIALIZAÇÃO DOS FUNCIONÁRIOS SOBRE PRÁTICAS SEGURAS, A NEGLIGÊNCIA EM SEGUIR POLÍTICAS DE SEGURANÇA E A ILITERACIA CIBERNÉTICA SÃO FATORES-CHAVE”,
>
> RUI DURO, COUNTRY MANAGER DA CHECK POINT SOFTWARE TECHNOLOGIES EM PORTUGAL

dados sensíveis, o assédio a diretores de empresas, a sabotagem de equipamentos e sistemas empresariais ou o roubo de dados para tentar progredir nas suas carreiras. Muitas destas ameaças maliciosas têm motivações financeiras, uma vez que os colaboradores roubam dados da empresa para os vender a hackers, organizações terceiras ou empresas rivais”.

Aaron Bugal, da Sophos, refere que “a fuga e a perda de dados são riscos muito comuns que as empresas enfrentam – sobretudo quando se trata de algum informador a causar danos. Em muitos casos, as fugas e perdas podem acontecer acidentalmente – por exemplo, através da utilização da opção 'responder a todos' a uma mensagem de email de origem externa, ou da perda de um computador portátil não encriptado, ou de um dispositivo de armazenamento em massa com dados relevantes, e que podem depois ser encontrados por qualquer pessoa”.

OS FATORES INTERNOS QUE MAIS CONTRIBUEM

David Grave considera que alguns dos fatores que levam os colaboradores a tornarem-se ameaças internas incluem “a falha na implementação de políticas e procedimentos de segurança da informação, incluindo a falta de atualizações de software e hardware, recursos e formação. Por outro lado, a implementação de políticas de segurança muito restritivas, que os funcionários consideram invasi-

vas, pode levá-los a contorná-las, muitas vezes por falta de conhecimento. O sentimento de descontentamento, de insatisfação ou mesmo um simples descuido por parte de funcionários também dá origem a comportamentos intencionais contra a organização".

Paulo Pinto, por sua vez, relembra que, "como em qualquer outra relação, a dinâmica colaborador-entidade empregadora muda com o tempo. Pequenos ressentimentos e queixas podem acumular-se e transformar-se em rancores contra a empresa e/ou a equipa de liderança", como o não cumprimento de promessas, a desvalorização do trabalho ou não ouvir sugestões.

Para Aaron Bugal, é claro que "as pessoas" são o principal fator de ameaça interno nas organizações. "Os colaboradores, tanto antigos como atuais, são o maior risco interno para qualquer organização. São as pessoas que normalmente clicam em emails de phishing, inserem dispositivos USB aleatórios nos ativos da empresa e configuram mal ou não fazem a manutenção correta dos ativos digitais que têm em sua posse, entre outras possibilidades, aumentando a superfície de ataque e gerando oportunidades para que algo mau aconteça", explica.

Rui Duro destaca o comportamento humano e a gestão inadequada dos recursos internos como os principais fatores que aumentam a ameaça interna das organizações. "A falta de consciencialização dos funcionários sobre práticas seguras, a negligência em seguir políticas de segurança e a iliteracia cibernética são fatores-chave", diz o executivo, acrescentando que "a má gestão de acessos e privilégios, a ausên-

DAVID GRAVE, CLARANET PORTUGAL

cia de uma monitorização efetiva das atividades dos utilizadores e a falta de uma cultura organizacional centrada na segurança, podem criar vulnerabilidades internas significativas".

MELHORES PRÁTICAS PARA DETETAR AMEAÇAS

Paulo Pinto alerta que, "se as organizações souberem como identificar as táticas e ferramentas" que uma pessoa infiltrada utiliza para atacar, então "podem detetar o ataque tão cedo quanto possível e tomar medidas para o atenuar", como *backdoors*, hardware ou software que permite o acesso remoto, palavras-passe alteradas ou alterações não autorizadas a firewalls e ferramentas antivírus. No entanto, além dos sinais mais técnicos, é importante ter atenção aos indicadores humanos, como "o mau humor constante no local de trabalho ou queixas incessantes, que podem ser precursores de uma ação de 'lobo solitário' por parte de um colaborador para prejudicar a empresa a partir do interior".

Aaron Bugal assume que "esta é a questão mais difícil de resolver e implementar", uma vez que as organizações "têm de conseguir alcançar o equilíbrio delicado entre educar os colaboradores e desenvolver uma atitude e cultura positivas no sentido de serem ciber-resilientes. Para além disso, também têm de implementar processos claramente articulados para ajudar a manter e difundir esta cultura, e selecionar as tecnologias mais adequadas às pessoas e aos processos para reduzir as ameaças e minimizar os riscos".

> "HÁ VÁRIAS PRÁTICAS QUE PERMITEM ANTECIPAR E/OU DETETAR AMEAÇAS INTERNAS COM RELATIVA RAPIDEZ, DEPENDENDO DA SUA NATUREZA E DA FORMA COMO ESTÃO DISSIMULADAS", COMO MONITORIZAÇÃO DE ATIVIDADES SUSPEITAS, CONTROLO DE ACESSO E AUDITORIA INTERNA DOS SISTEMAS.
>
> DAVID GRAVE, SECURITY DIRECTOR DA CLARANET PORTUGAL

Para Rui Duro, é importante implementar práticas e soluções avançadas para fazer o reconhecimento prévio de ameaças, como monitorização contínua, gestão de identidade e acesso, soluções de prevenção de ameaças avançadas, políticas de segurança claras e atualizações regulares.

David Grave, diz, também, que "há várias práticas que permitem antecipar e/ou detetar ameaças internas com relativa rapidez, dependendo da sua natureza e da forma como estão dissimuladas", como monitorização de atividades suspeitas, controlo de acesso e auditoria interna dos sistemas.

PRIVACIDADE E MONITORIZAÇÃO

Aaron Bugal, da Sophos, explica que é preciso existir "uma delimitação clara entre a vida privada e a vida profissional de um colaborador, e os ativos da empresa atribuídos a um colaborador devem ser apenas isso: ativos da empresa. Realizar atividades pessoais nos dispositivos da empresa deve ser aceitável, sendo que o bom senso dos colaboradores deve prevalecer quando têm de decidir ao que vão aceder e o que vão fazer num dispositivo que não lhes pertence. Como tal, se pretendem manter a privacidade das suas atividades pessoais, devem recorrer a dispositivos e redes alternativos, tendo de compreender que os ativos da empresa podem ser monitorizados por esta".

> SE ADOTARMOS UMA ABORDAGEM DE CIMA PARA BAIXO PARA MANUSEAR MELHOR AS INFORMAÇÕES QUE GERAMOS E/OU EXTRAÍMOS DOS NOSSOS CLIENTES, E AS ARMAZENARMOS EM SEGURANÇA E SEM ACESSO FÁCIL, DESENVOLVEREMOS UMA CULTURA NA QUAL AS INFORMAÇÕES DEVEM SER SEMPRE PROTEGIDAS, E TEREMOS SEMPRE PRESENTE UMA ATITUDE PROTETORA EM RELAÇÃO AO TRATAMENTO DE DADOS".
>
> AARON BUGAL, FIEDL CTO APJ DA SOPHOS

AARON BUGAL, SOPHOS

Já Rui Duro diz que o equilíbrio entre a privacidade dos colaboradores e a necessidade legítima de monitorizar atividades suspeitas será "um dos desafios mais complicados e, ao mesmo tempo, impor-

tantes para as organizações". Assim, as empresas precisam de ter políticas transparentes, princípios de necessidade, anonimização de dados, ferramentas de monitorização contextual e formação de consciencialização em cibersegurança e ciberhigiene.

Para David Grave, da Claranet, é importante estabelecer "políticas claras de privacidade e segurança" e fornecer formação adequada aos colaboradores. No entanto, acima de tudo, é preciso ter informação transparente sobre os seus direitos e expectativas. "É importante que as empresas realizem uma revisão das suas políticas e sistemas de segurança da informação, verificando a conformidade com as leis relevantes e as políticas internas", diz.

Paulo Pinto defende, também, que é necessário manter "uma comunicação transparente e aberta com os colaboradores" para que "não sejam levantadas questões éticas e morais entre a privacidade do colaborador e a segurança da empresa" e, também, do próprio trabalhador. "É importante que os colaboradores percebam a importância desta monitorização para prevenir e mitigar possíveis ataques", acrescenta.

MITIGAR AS AMEAÇAS INTERNAS

Para mitigar as ameaças internas, diz Rui Duro, da Check Point, "é essencial adotar uma abordagem abrangente que englobe políticas, tecnologia e cultura organizacional", estabelecendo políticas de segurança claras e comunicando-as de forma eficaz. Depois, também é necessário monitorizar as atividades dos utilizadores através de ferramentas especializadas e realizar avaliações periódicas de risco que permitem a identificação e a correção proativa de vulnerabilidades. Por fim, a resposta a incidentes deve ser ágil, com planos bem definidos e testados regularmente.

Já David Grave aponta quatro práticas que considera necessárias para as organizações mitigarem as ameaças internas: adoção de uma cultura de segurança da informação; definição de políticas claras de segurança da informação; implementação de sistemas de controlo de acesso; e monitorização e auditoria regulares dos sistemas de IT.

Aaron Bugal indica que é necessário "gerir as expectativas relativamente à forma como as informações internas são tratadas. Esta questão é de importância crucial neste momento, e é um sinal de que muitos governos estão a definir e a fazer cumprir os regulamentos e as leis de proteção de dados. Se adotarmos uma abordagem de cima para baixo para manusear melhor as informações que geramos e/ou extraímos dos nossos clientes, e as armazenarmos em segurança e sem acesso fácil, desenvolveremos uma cultura na qual as informações devem ser sempre protegidas, e teremos sempre presente uma atitude protetora em relação ao tratamento de dados".

Por último, Paulo Pinto, da Fortinet, diz que é necessário formar os colaboradores, implementar ferramentas que possam monitorizar o comportamento e as atividades dos utilizadores, segmentar a rede, implementar um processo de *data loss prevention*, reforçar o *identity and access management* e utilizar *multifactor authentication* e, por fim, utilizar tecnologias de engano e *honeypots*. No entanto, relembra, "não existe uma poção mágica que acabe com as ameaças internas". ◀

paloalto NETWORKS

ESTRATÉGIAS DE GESTÃO DE RISCOS DE CIBERSEGURANÇA

NA BASE DA CIBERSEGURANÇA ESTÁ A NECESSIDADE DE COMPREENDER OS RISCOS E COMO MINIMIZÁ-LOS. QUANDO FALAMOS DE RISCO NO MUNDO DAS TI'S, FALAMOS PRINCIPALMENTE DE DADOS, UTILIZANDO TERMOS COMO: PRIVACIDADE DE DADOS, EXFILTRAÇÃO DE DADOS E PERDA DE DADOS. MAS O RISCO EM CIBERSEGURANÇA ENVOLVE MAIS DO QUE APENAS PROTEGER DADOS.

Foto de Philipp Katzenberger na Unsplash

Proteger dados e bloquear vulnerabilidades conhecidas são boas táticas para a cibersegurança, mas essas atividades não são as únicas que os CISOs devem considerar. O que muitas vezes falta é uma abordagem mais abrangente à gestão de riscos e uma estratégia que considere mais do que apenas dados.

Hoje em dia, qualquer empresa consome e gera dados, mas também possui uma infinidade de dispositivos, incluindo dispositivos IoT, que muitas vezes não estão sob a supervisão ou controlo direto das equipas de TI. Embora a perda de dados seja um risco, também o são as interrupções de serviço, especialmente porque os dispositivos IoT e OT continuam a desempenhar papéis críticos. Para uma operação de cuidados de saúde, por exemplo, uma falha num dispositivo médico pode levar a consequências de vida ou morte.

DESAFIOS NA GESTÃO DE RISCOS DE SEGURANÇA

As técnicas de ataque estão sempre a mudar e as configurações dos dispositivos estão em constante mudança. Ou seja, a gestão de riscos não é estática.

Há uma série de desafios na gestão de riscos de segurança, entre os quais o tamanho e a complexidade do parque de TI e IoT. Os CISOs de hoje podem facilmente ficar sobrecarregados com informações e dados provenientes de um volume crescente de dispositivos. Juntamente com o volume, há uma grande

variedade de dispositivos, cada um com a sua superfície de ataque. A complexidade de gerir uma gama diversificada de políticas, dispositivos e controlos de acesso numa empresa geograficamente distribuída, não é uma tarefa trivial.

UMA ESTRATÉGIA MELHOR PARA GERIR RISCOS DE SEGURANÇA

A gestão de riscos de segurança não é uma tarefa única ou uma ferramenta única. É uma estratégia que envolve vários componentes-chave que podem ajudar os CISOs a eliminar lacunas e a estabelecer melhor as bases para resultados positivos.

Garantir visibilidade. Em primeiro lugar, as organizações precisam saber o que possuem. A gestão de ativos de TI e IoT não envolve apenas saber quais os dispositivos geridos que existem, mas também conhecer os dispositivos IoT não-geridos e compreender quais os sistemas operativos e versões das aplicações que estes utilizam.

Monitorização contínua. O risco não é estático e a monitorização também não deveria ser. A monitorização contínua de todas as mudanças, incluindo quem está a aceder à rede, onde os dispositivos estão a ligar-se e o que as aplicações estão a fazer, é fundamental para gerir riscos.

Foco na segmentação de rede. A redução do risco no caso de um potencial incidente de segurança pode muitas vezes ser alcançada reduzindo o "raio de explosão" de uma ameaça. Com a segmentação de rede, onde diferentes serviços e dispositivos são executados apenas em segmentos específicos de uma rede, a superfície de ataque pode ser minimizada e podemos **evitar dispositivos IoT invisíveis e não-geridos** como trampolins para ataques a outras áreas da rede. Assim, em vez de uma exploração num sistema impactar toda a organização, o impacto pode ser limitado apenas ao segmento de rede que foi atacado.

Priorizar a prevenção de ameaças. Tecnologias de prevenção de ameaças, como proteção de endpoint e rede, também são componentes fundamentais de uma estratégia eficaz de gestão de riscos de segurança. Da mesma forma é importante para a prevenção de ameaças ter a configuração de política correta e um acesso com menos privilégios implementados em endpoints, incluindo dispositivos IoT e tecnologias de proteção de rede, para evitar a ocorrência de possíveis ataques.

A execução desta estratégia pode ser alcançada recorrendo à Inteligência Artificial e técnicas de Machine Learning e Automação. Com o crescente volume de dados, tráfego de rede e dispositivos, simplesmente não é possível para qualquer ser humano, ou mesmo grupo de seres humanos, acompanhar. Com Automação baseada em Machine Learning, é possível identificar rapidamente todos os dispositivos de TI, IoT, OT e BYOD para melhorar a visibilidade, correlacionar atividades na monitorização contínua, recomendar as políticas corretas para acesso com menos privilégios, sugerir configurações otimizadas para a segmentação de rede e adicionar uma camada extra de segurança com prevenção proativa de ameaças.◀

arcserve®

OS ATAQUES DE RANSOMWARE ESTÃO A CRESCER EM CUSTO E FREQUÊNCIA:

5 MEDIDAS QUE AS ORGANIZAÇÕES DEVEM TOMAR PARA SE PROTEGEREM

OS ATAQUES DE RANSOMWARE CONTINUAM A AFETAR AS ORGANIZAÇÕES E OS CUSTOS SÃO ASSOMBROSOS.

Um inquérito recente a mais de 1.100 decisores de TI em PMEs revelou que 50% tinham sido alvo de ataques, com 35% a serem solicitadas um resgate acima de cem mil dólares, e a 20% um valor entre um e dez milhões de dólares.

Apesar dos milhares de milhões gastos em ferramentas de cibersegurança, as empresas estão ainda mal preparadas para os ataques de *ransomware*. Apenas 23% dos inquiridos disseram que estavam muito confiantes na sua capacidade de recuperar dados perdidos em caso de ataque de *ransomware*.

Entretanto, a superfície de ataque continua a expandir-se com as organizações a adotarem tecnologias como IoT, Inteligência Artificial, e o 5G a gerarem cada vez mais dados – dados esses que podem ser comprometidos e sequestrados por atacantes. Daí que as empresas necessitem de fortalecer as suas estratégias de recuperação de desastre, sistemas de *backup*, e soluções de imutabilidade de dados para prevenir a perda de dados críticos.

Este inquérito revelou que 92% das organizações estão a realizar investimentos adicionais para se protegerem contra ataques de *ransomware*, mas para a maioria das empresas, não é uma questão de se os dados forem comprometidos; é uma questão de quando.

Eis cinco medidas que as organizações podem tomar hoje para reduzirem a sua exposição ao *ransomware* e evitarem perdas avassaladoras.

1: EDUCAR OS COLABORADORES

É essencial investir na formação dos colaboradores para que possam reconhecer um ataque de *ransomware* e evitá-lo. O *ransomware* pode disfarçar-se de

muitas maneiras e os colaboradores devem aprender a escrutinar todos os *links* e não abrir anexos de e-mails não solicitados.

2: FOCAR NA CURA TANTO COMO NA PREVENÇÃO

As empresas continuam a investir fortunas em soluções de cibersegurança como *firewalls* de nova geração e sistemas de deteção e resposta avançados (XDR) concebidos para prevenir ataques. Porém estas mesmas empresas são, ainda assim, vítimas de *ransomware* e forçadas a pagar um elevado preço por isso.

É tempo das empresas deixarem de se focar exclusivamente na prevenção e investirem igualmente em medidas de cura como *backup* & recuperação e *storage* para imutabilidade de dados que lhes permitam recuperar rapidamente os seus dados e evitem pagar o resgate.

Encriptar os seus dados sensíveis é altamente recomendado, porque impede os atacantes de os ler e explorar ainda mais.

3: ACRESCENTE UM EXTRA À RESILIÊNCIA DOS SEUS DADOS

Muitas empresas planeiam uma estratégia e negligenciam os seus testes. É o equivalente a uma equipa de futebol desenhar uma estratégia sofisticada de defesa, mas nunca se dar ao trabalho de treiná-la. Todas as empresas deveriam testar os seus *backups* e respetivos planos de recuperação regularmente para garantir que efetivamente conseguem restaurar os seus dados e sistemas se sofrerem um ataque ou desastre natural.

4: SAIBA QUAIS SÃO OS SEUS DADOS MAIS CRÍTICOS

Os dados não têm todos o mesmo valor. Se está preocupado com custos, saiba que não tem que guardar todos os dados no mesmo local. Procure soluções de *storage* que lhe ofereçam opções com *data tiering*, porque estas permitem-lhe colocar dados menos importantes em armazenamentos mais baratos.

5: IMPLEMENTE UM PLANO DE RECUPERAÇÃO DE DESASTRE

Apesar de todas as medidas preventivas que tome, vai precisar de estar preparado para a possibilidade de um dia sofrer um ataque. Assim sendo, deverá realizar os *backups* tão frequentemente quanto o necessário – idealmente a cada 15 minutos para os dados críticos. Terá que verificar se todo o seu ambiente está a ser guardado, incluindo os seus colaboradores remotos e quaisquer aplicações SaaS que utilize, como o Microsoft 365.

Uma boa solução de recuperação de desastre será ainda fácil de testar, para poder validar que os seus objetivos de tempo de recuperação são cumpridos. Pode parecer óbvio, mas é aqui que muitas das soluções falham redondamente. A sua solução de recuperação de desastre deve conseguir recuperar sempre e em tempo útil para voltar a operar o seu negócio o quanto antes.

NOTA FINAL

Nao há uma defesa perfeita contra *ransomware*. Uma abordagem multi-camada inclui educar os colaboradores, investir em soluções de *backup* & recuperação fiáveis e ter imutabilidade dos dados entregue por uma solução desenhada para esse efeito, bem como um plano de recuperação de desastre robusto. É desta forma que as organizações podem estar um passo à frente desta ameaça e proteger os seus dados e negócios. ◀

SOPHOS

por Chester Wisniewski,
Director, Global Field CTO, Sophos

AMEAÇAS INTERNAS: A FACE OCULTA DAS AMEAÇAS EMPRESARIAIS

ATUALMENTE, AS EMPRESAS ENFRENTAM MUITAS AMEAÇAS – E, COMO AS QUE VÊM DO EXTERIOR SÃO A SUA PRINCIPAL PREOCUPAÇÃO, SOBRETUDO O *RANSOMWARE*, ESQUECEM-SE MUITAS VEZES DE CONSIDERAR AS AMEAÇAS INTERNAS, QUE PODEM SER IGUALMENTE DEVASTADORAS. DE FACTO, DEDICAM MUITO MENOS TEMPO A AVALIAR AS MEDIDAS DE SEGURANÇA INTERNA DO QUE EXTERNA.

As fontes das ameaças internas são diversas e muitas vezes difíceis de detetar. Podem ser o resultado de negligência ou mesmo malícia. Embora difíceis de medir, a verdade é que já afetaram muitas empresas.

O QUE LEVA AO APARECIMENTO DESTAS AMEAÇAS?

Intencionais ou não, as ameaças internas são inúmeras. Por exemplo, quando um colaborador se esquece de uma USB com informações críticas num local público, está a negligenciar o cumprimento das regras. Algo assim pode ser trágico, uma vez que existe o risco de roubo ou exposição pública de informações e tal pode levar a uma violação dos regulamentos


CHESTER WISNIEWSKI, DIRECTOR, GLOBAL FIELD CTO, SOPHOS

oficiais impostos pelos organismos governamentais (geralmente RGPD, PCI e HIPPA).

Contudo, as ameaças internas também podem ser desencadeadas intencionalmente – um colaborador pode, por exemplo, aperceber-se que os controlos são relaxados, e assim decidir roubar informações confidenciais impunemente.

Em geral, há três motivos principais para as ameaças internas: vingança, ganância e falta de atenção.

Os dois primeiros incluem, por exemplo, atos intencionais e acidentais, e são mais suscetíveis de ocorrer na sequência de um despedimento ou demissão – variando consoante o tipo de empresa. No caso do setor da defesa, pode tratar-se de corrupção ou espionagem; já no setor das TIC, o roubo de dados comerciais está mais generalizado. Os colaboradores que vendem produtos e soluções podem guardar os contactos dos seus clientes e os programadores podem roubar o código fonte da empresa.

Geralmente, as fugas de dados por ameaças internas ocorrem quando informações sensíveis se tornam "impossíveis de controlar", quando deveriam ser classificadas como confidenciais. A informação torna-se pública e pode ser consultada por pessoas cuja posição não o deveria permitir. Muitas vezes, as empresas veem-se confrontadas com este tipo de fuga por descuido, inadvertência ou falta de jeito – como a perda de dispositivos móveis, USBs ou a exposição pública de repositórios armazenados na cloud. Um exemplo clássico resulta da utilização dos campos "Para" e "CC" ao enviar um email para vários destinatários externos, em que as informações de identificação pessoal são expostas a todos eles; uma situação que poderia ser facilmente evitada utilizando o modo "BCC".

Por último, a destruição de dados é também uma ação típica, impedindo o acesso a informações críticas, o que pode afetar diretamente a capacidade operacional da empresa. Muitas razões podem levar a tais atos, mas a principal continua a ser o facto de os dados serem geralmente armazenados com pouca segurança, o que permite que demasiadas pessoas acedam a informações que nada têm a ver com as suas tarefas – e que possam, assim, roubar dados sensíveis por vingança, mas também destruí-los ou mesmo tentar conseguir dinheiro pela sua devolução.

QUAL A MELHOR FORMA DE RESPONDER A ESTAS AMEAÇAS?

Implementar uma estratégia de prevenção contra ameaças internas é difícil pois, uma vez lançado o ataque, a antecipação e o controlo já não são possíveis. É, por isso, a formação para a correta utilização e compreensão dos sistemas e processos internos da empresa, que pode contribuir muito para evitar fugas acidentais de dados.

Para além disso, pode ser útil recorrer a várias soluções e ferramentas, como sistemas de gestão de ficheiros e documentos; ou a ZTNA, que limita o acesso das pessoas apenas às ferramentas/serviços/aplicações necessárias; e as ferramentas de Prevenção de Fugas de Dados (DLP). Os sistemas XDR e as *firewalls* também podem ser muito úteis, porque permitem a implementação da DLP, e ao mesmo tempo registam o acesso e o movimento de dados, facilitando o trabalho forense de compreender as falhas e as suas consequências. ◀

VARONIS

OS SEUS DADOS ESTÃO À PROVA DE INSIDERS?

CINCO PASSOS PARA MANTER OS SEUS SEGREDOS SEGUROS

UM INCIDENTE OCORRIDO EM JUNHO DO ANO PASSADO NO PENTÁGONO, NO QUAL UM JOVEM GUARDA DE 21 ANOS, JACK TEIXEIRA, SUPOSTAMENTE DIVULGOU INFORMAÇÕES SENSÍVEIS NAS REDES SOCIAIS PARA MELHORAR A SUA IMAGEM SOCIAL, ESTÁ A REACENDER A DISCUSSÃO SOBRE A PROTEÇÃO DE DADOS CONTRA INVASORES MALICIOSOS. DESDE A SERPENTE NO JARDIM DO ÉDEN (A "INVASORA" ORIGINAL) ATÉ SNOWDEN, MANNING, WINNER E AGORA JACK TEIXEIRA, BASTA UM ELEMENTO PROBLEMÁTICO PARA MUDAR O CURSO DA HISTÓRIA.

O acesso à informação, e o facto de haver acesso excessivo a dados sensíveis em geral, é um tema comum que une os invasores. Robert Litt, ex-Advogado Geral do Gabinete do Diretor de Inteligência Nacional, avaliou o seguinte: "Após as divulgações, deve haver uma revisão profunda sobre a partilha de informações, número de pessoas com autorizações de segurança, implementação de políticas existentes em relação à 'necessidade de saber' e da monitorização de sistemas com acesso restrito".

As ameaças internas são os riscos mais difíceis de prevenir dentro de uma empresa e podem causar danos enormes. O Pentágono provavelmente fez tudo certo dentro dos seus limites físicos e digitais. Jack Teixeira trabalhava numa

área que atua com informações sensíveis – ou SCIF [Sensitive Compartmented Information Facility, na sigla em inglês], que "protege contra vigilância eletrónica e suprime divulgações de dados". Isso significa que nenhum dispositivo USB entrava ou saía, nada podia ser enviado para a internet e nenhuma transmissão podia ocorrer. Ainda assim, nenhum desses controlos de perímetro ajudou contra esta ameaça.

ANATOMIA DE UM ATAQUE INTERNO

Então, o que aconteceu de errado? O colaborador tinha acesso amplo a dados sensíveis que, teoricamente, ele não precisava. Apesar da agitação na indústria no que diz respeito ao conceito de *zero trust*, este caso parece ser uma falha no modelo de "necessidade de saber" e/ou uma quebra no monitorização de sistemas que usam informações sensíveis ou confidenciais.

Em muitas organizações, o foco frequentemente está na proteção dos limites em vez de proteger o alvo em si — os dados internos.

Imagine esta conversa entre um CEO e uma equipa de segurança de TI encarregada de proteger dados sensíveis:

CEO: Nós atualizamos os nossos sistemas?
Equipa de segurança de TI: Claro. Os criminosos explorariam vulnerabilidades se não o fizéssemos.

CEO: Treinamos os nossos colaboradores utilizando tentativas simuladas de *phishing*?
Equipa de segurança de TI: Sim, treinamos os colaboradores porque eles recebem emails de *phishing* a toda a hora.

CEO: Mantemos software de segurança nos dispositivos de todos?
Equipa de segurança de TI: Sim, porque, depois de serem alvo de *phishing*, o software nos dispositivos ajuda a bloquear o *malware* que os atacantes tentam instalar.

CEO: Bloqueamos dispositivos USB e *uploads* em massa?
Equipa de segurança de TI: Sim, isso facilita os *insiders* para roubarem os dados.

CEO: Bloqueamos e monitorizamos os nossos dados mais importantes?
Equipa de segurança de TI: Não.

Não é estranho que as organizações tenham tantos controlos onde o risco não está localizado? Afinal, os bancos não focam mais no que entra pelas portas e janelas do que em quem e o que entra e sai do cofre, caso contrário, o dinheiro receberia a mesma segurança que as canetas.

Se Jack Teixeira não tivesse acesso a tantas informações sensíveis desde o início, os danos potenciais poderiam ter sido inexistentes ou muito reduzidos, e contidos muito mais rapidamente. O Pentágono poderia ter falhado no perímetro, mas ninguém conheceria o nome de Jack Teixeira se os dados tivessem sido mantidos seguros desde o início.

ENCONTRE UM EQUILÍBRIO ENTRE ACESSO E SEGURANÇA

Trancar o cofre no mundo digital é, obviamente, um grande desafio. Mais dados sensíveis são armazenados em mais lugares a cada dia e a colaboração

exige equilibrar produtividade e segurança. Os dados só têm valor se puderem ser partilhados.

Se restringir completamente ou for muito rígido quanto ao acesso aos dados, eles tornam-se um recurso "congelado". A comunidade de inteligência aprendeu isso após restringir a partilha de informações entre várias agências governamentais antes do fatídico 11 de setembro de 2001, quando houve o ataque ao World Trade Center. Se as demais restrições, os ativos de informação podem rapidamente tornar-se um passivo, como visto no recente incidente no Pentágono.

Como é que pode equilibrar acesso e segurança? Aqui estão cinco passos que pode seguir para verificar o quão preparado está para um invasor malicioso ou um atacante externo que comprometa a conta ou o computador de um criminoso:

- Faça um inventário das regras que possui para proteger dados sensíveis.

- Definiu quando e como excluir, isolar ou bloquear dados sensíveis?

- Verifique se pode fazer cumprir essas regras manualmente ou com automação.

- Compreenda o quão facilmente pode detetar violações dessas regras.

- Procure regras que devam ser criadas, refinadas ou aplicadas de forma mais eficaz.

Se está apenas a começar, considere fazer um inventário dos seus dados para ver onde os utilizadores armazenam dados sensíveis e com quem os partilham.

Se a sua empresa for como a maioria das organizações, os seus colaboradores acedem a dados sensíveis a partir de qualquer lugar, de muitos dispositivos, em aplicações e repositórios de dados conectados à nuvem — o oposto de um SCIF. Com um perímetro tão distribuído e imprevisível, faz ainda menos sentido alocar a maioria dos seus recursos de segurança lá, pois não temos ideia de onde os ataques se vão originar.

No entanto, sabemos para onde os criminosos irão. O seu negócio pode não estar a lidar com inteligência ultrassecreta, mas é provável que tenha informações que alguém deseje. E é aí que faz sentido concentrar os recursos escassos.

Proteger informações com base na necessidade de conhecimento e monitorar de perto esses dados em busca de sinais de atividade incomum pode ajudar a reduzir os danos que os invasores podem causar e torná-los mais fáceis de identificar. Criminosos externos que assumem o controlo do computador ou a conta de um colaborador (e efetivamente se tornam "insiders") precisam de se esforçar muito mais para aceder aos dados desejados, dando às soluções de monitorização mais chances de os apanhar.

Não importa se está a lidar com segredos militares ou comerciais, ou se os seus colaboradores trabalham num SCIF, num prédio ou em casa — priorizar os seus controlos nos dados protege-os melhor de ataques internos ou externos. Como diz o ditado popular, vai matar dois coelhos com uma cajadada. ◀

QUALQUER ORGANIZAÇÃO ESTÁ SEMPRE EXPOSTA AO RISCO E GERIR O MESMO DA MELHOR MANEIRA É IMPERATIVO PARA A SAÚDE DA ORGANIZAÇÃO

POR RUI DAMIÃO

GERIR O RISCO (QUE ESTÁ SEMPRE À ESPREITA)

O ambiente de negócio é cada vez mais dinâmico. As organizações têm de lidar com novas ferramentas, novas oportunidades e, também, novos riscos que vão aparecendo à medida que o negócio evolui.

Gerir o risco é, assim, imperativo para as organizações que pretendem avançar o seu negócio com as menores preocupações possíveis. Uma abordagem

integrada da gestão de riscos traz vários benefícios para as organizações, mas, também, desafios que os líderes têm de enfrentar.

BENEFÍCIOS

Duarte Caldas, Data & AI Partner Technical Specialista da IBM Portugal, refere que, cada vez mais, "as empresas precisam de ter a capacidade de reconhecer e gerir quer riscos, quer desafios de conformidade". Com o "aumento dramático de utilizadores ativos" que as empresas estão a testemunhar, as organizações estão a utilizar "ferramentas com recursos inconsistentes". Diz Duarte Caldas que "estes utilizadores precisam de soluções que integrem o poder da Inteligência Artificial (IA) e soluções baseadas nas melhores práticas da gestão de risco integrada: flexíveis na adaptação às mudanças regulatórias, mas simples o suficiente para utilizadores funcionais sem grande esforço de formação".

Uma abordagem integrada à gestão de riscos ajuda, assim, as organizações "a simplificar processos, melhorar a tomada de decisão e fornecer uma visão abrangente dos potenciais riscos, levando a uma mitigação de riscos mais eficaz".


DUARTE CALDAS, IBM PORTUGAL

Bruno Castro, Fundador & CEO da VisionWare, relembra que uma abordagem integrada à gestão de riscos se concentra "na avaliação de riscos no contexto mais amplo da estratégia empresarial" o que, "por si só", já "é vantajoso na medida em que atua como uma estrutura que garante que os principais riscos são compreendidos e considerados em conjunto com outros riscos, e não de forma isolada". Esta visão holística, explica, facilita o processo de

"ESTES UTILIZADORES PRECISAM DE SOLUÇÕES QUE INTEGREM O PODER DA INTELIGÊNCIA ARTIFICIAL (IA) E SOLUÇÕES BASEADAS NAS MELHORES PRÁTICAS DA GESTÃO DE RISCO INTEGRADA: FLEXÍVEIS NA ADAPTAÇÃO ÀS MUDANÇAS REGULATÓRIAS, MAS SIMPLES O SUFICIENTE PARA UTILIZADORES FUNCIONAIS SEM GRANDE ESFORÇO DE FORMAÇÃO

DUARTE CALDAS, DATA & AI PARTNER TECHNICAL SPECIALISTA DA IBM PORTUGAL

tomada de decisão – já que permite ter uma maior compreensão dos riscos –, assim como da conformidade com as diferentes regulamentações.

Outro benefício, refere, é, "sem dúvida, o aumento da resiliência e eficiência operacional, já que permite às organizações, identificar e mitigar proativamente os riscos, evitar interrupções nos processos de negócios e assim minimizar potenciais perdas financeiras".

Fábio Ribeiro, Sales Engineer da WatchGuard Portugal, defende que "a adoção de uma abordagem integrada à gestão de riscos é vital para fortalecer a postura de cibersegurança de uma organização", uma vez que permite ter uma visão holística e abrangente dos riscos de segurança. Esta estratégia "facilita a identificação e avaliação proativa de riscos, desde ameaças externas até vulnerabilidades internas, e promove uma resposta coordenada e eficaz a incidentes de segurança".

Ao mesmo, permite uma "alocação mais eficiente de recursos de segurança e assegura a conformidade com regulamentações, resultando numa melhor proteção contra ataques informáticos e numa postura de segurança mais robusta em todos os níveis da organização".


BRUNO CASTRO, VISIONWARE

> "SEM DÚVIDA, O AUMENTO DA RESILIÊNCIA E EFICIÊNCIA OPERACIONAL, JÁ QUE PERMITE ÀS ORGANIZAÇÕES, IDENTIFICAR E MITIGAR PROATIVAMENTE OS RISCOS, EVITAR INTERRUPÇÕES NOS PROCESSOS DE NEGÓCIOS E ASSIM MINIMIZAR POTENCIAIS PERDAS FINANCEIRAS".
>
> BRUNO CASTRO, FUNDADOR & CEO DA VISIONWARE

DESAFIOS PARA OS LÍDERES

Bruno Castro indica que um dos grandes desafios que os líderes têm de enfrentar é o equilíbrio entre "as múltiplas necessidades inerentes à segurança da informação numa organização, perante o cenário atual de riscos". O fundador e CEO da VisionWare

diz que "existe todo um conjunto de ameaças a ter em conta, externas e internas, e o CISO e o CSO têm o desafio de acompanhar a evolução e a inovação dessas mesmas ameaças para garantir que as defesas estão atualizadas, são eficazes, abordando os riscos de forma proativa".

"É ainda importante alinhar as estratégias de cibersegurança e de gestão de riscos com os objetivos de negócios, isto é, garantir que as medidas de segurança além de protegerem a organização contra ameaças, também estão alinhadas com as metas e a continuidade dos negócios", explica Bruno Castro. "Outro desafio reside na avaliação e comunicação de riscos. Avaliar e comunicar efetivamente os riscos para as partes interessadas é crucial". Por fim, "um desafio a ter em conta e, simultaneamente, uma meta é criar uma cultura de segurança, crucial para gerir riscos externos e internos".

Fábio Ribeiro relembra que os Chief Information Security Officers e os Chief Security Officers enfrentam "desafios notáveis no contexto da gestão integrada de riscos, marcado pela complexidade e pela evolução constante das ameaças". Assim, a principal dificuldade reside "em manter a segurança num cenário que está em constante modificação, exigindo uma resposta ágil e adaptável. A integração de informações de segurança provenientes de diversas fontes para uma análise de risco coesa e abrangente também representa um desafio considerável, requerendo habilidades técnicas avançadas e uma gestão eficaz de recursos".

Para Duarte Caldas, os líderes de segurança das organizações enfrentam desafios na necessidade de colaboração entre departamentos, acompanhando a evolução das ameaças e garantindo uma "comunicação perfeita" entre vários domínios de segurança. Os CISO e CSO precisam de "ter *insights* sobre questões sistémicas em controlos, processos e conformidade para áreas dinâmicas, como o risco cibernético. Isto exige que os sistemas tenham uma biblioteca ligada de itens de conformidade de potenciais riscos que possam ser visualizados em diferentes dimensões de negócio".

GERIR O RISCO EM TEMPO REAL

No atual ambiente de cibersegurança – que é cada vez mais complexo –, as organizações estão a adaptar-se a gerir o risco em tempo real. Fábio Ribeiro refere que as empresas estão a implementar tecnologias avançadas, como inteligência artificial e sistema de monitorização contínua, para detetar e dar uma resposta rápida a ameaças emergentes. Ao mesmo tempo, é preciso uma análise profunda e específica da segurança dos endpoints, um "aspeto essencial na gestão de riscos eficaz".

Duarte Caldas, da IBM Portugal, diz que as organizações estão a adotar uma gestão de riscos em


FÁBIO RIBEIRO, WATCHGUARD PORTUGAL

tempo real através da adoção de soluções de "monitorização contínua, integração de inteligência de ameaças e mecanismos de resposta automatizados para identificar e lidar rapidamente com ameaças emergentes".

Já Bruno Castro diz que "um indício positivo é que cada vez mais organizações reconhecem" a necessidade de gerir em tempo real o risco das organizações e muitas acabam por contratar um serviço de SOC. "Implementar ou adquirir um serviço de SOC é atualmente uma solução essencial para as empresas lidarem com a gestão de risco em tempo real. Um SOC compreende monitorização contínua 24/7, o que permite a deteção precoce de ameaças e, por consequência, uma resposta imediata a incidentes para mitigar ameaças, reduzir o tempo de resposta e o impacto dos ataques. Disponibiliza ainda a proteção dos dados e ativos, ao garantir que uma organização fica menos vulnerável a ciberataques e é uma garantia da continuidade dos serviços através de estabilidade operacional e recuperação rápida da cujo foco é minimizar as consequências de um ciberataque a longo prazo", explica.

Outra necessidade que as organizações devem apostar, refere o representante da VisionWare, é o investimento em treino e formação contínua dos colaboradores e, também, em testes de intrusão e simulação de ataques, que pretendem "reduzir os riscos associados a atividades humanas e fortalecer a primeira linha de defesa contra ameaças". ◀

> OS CHIEF INFORMATION SECURITY OFFICERS E OS CHIEF SECURITY OFFICERS ENFRENTAM "DESAFIOS NOTÁVEIS NO CONTEXTO DA GESTÃO INTEGRADA DE RISCOS, MARCADO PELA COMPLEXIDADE E PELA EVOLUÇÃO CONSTANTE DAS AMEAÇAS".
>
> FÁBIO RIBEIRO, SALES ENGINEER DA WATCHGUARD PORTUGAL

balwurk cyber security

por Paulo Rosado,
CEO Balwurk

A GESTÃO DO RISCO NO CONTEXTO DA SEGURANÇA APLICACIONAL

ESTATISTICAMENTE O NÚMERO DE VULNERABILIDADES RELACIONADAS COM SOFTWARE CONTINUA A AUMENTAR DE ANO PARA ANO E AS EMPRESAS TÊM DE GANHAR A CAPACIDADE DE GERIR OS RISCOS ASSOCIADOS A ESTE DESENVOLVIMENTO PARA CONTINUAREM A INOVAR DE FORMA RÁPIDA E COM PRODUTOS MAIS SEGUROS.

Hoje, podemos afirmar que o software ganhou o dom da ubiquidade. Nesta sociedade digital em que vivemos, desde o momento em que acordamos até que nos deitamos (e por vezes até durante a noite com pulseiras de monitorização), são dezenas, os pequenos programas com os quais interagimos numa base diária. Sem nos apercebermos, por detrás de cada uma destas aplicações, existem milhares de linhas de código com instruções que os computadores executam, para que nos seja apresentada a informação de que precisamos. Dependendo da sua complexidade estas aplicações podem interagir ou integrar com outras para enriquecer ou agregar mais conteúdo para enriquecer a informação

No domínio das aplicações corporativas desenvolvidas à medida passa-se exatamente o mesmo, independentemente do modelo em que operam (em cloud ou on-premises), mais uma vez milhares de linhas de código traduzidas em instruções, vão tratar grandes conjuntos de dados com diferentes níveis de criticidade onde podem estar dados pessoais ou dados relativos à saúde financeira da organização.

Estatisticamente o número de vulnerabilidades relacionadas com software continua a aumentar de ano para ano e as empresas têm de ganhar a capacidade de gerir os riscos associados a este desenvolvimento para continuarem a inovar de forma rápida e com produtos mais seguros. – Acontece que na sua maioria, o desenvolvi-

PAULO ROSADO, CEO DA BALWURK

mento das aplicações corporativas, não seguem ainda um padrão com base em princípios de segurança desde a conceção (também conhecido por movimento *shift left*), aumentando assim o risco da existência de vulnerabilidades no código ou na infraestrutura que suporta as aplicações e respetivos processos de negócio. – A União Europeia está a preparar um novo regulamento semelhante ao RGPD para produtos com elementos digitais, conhecido como **Cyber Resilience Act** (CRA), que tem como objetivo, o reforço das regras de cibersegurança no desenvolvimento de produtos de hardware e software.

A gestão do Risco no desenvolvimento de software é uma ferramenta essencial para identificar, avaliar e mitigar ameaças desde o início ao fim de um projeto. A sua quantificação (Risco = Probabilidade x Impacto), nem sempre é fácil calcular em projetos desta natureza, dada a falta de histórico para o cálculo de probabilidades, e de recursos especializados que ajudem a definir valores que façam sentido para a probabilidade de ocorrência. Neste sentido utilizar no processo de Gestão do Risco valores tangíveis mais fáceis de obter, ajuda a que este seja mais objetivo e fácil de operacionalizar com as diferentes equipas.

Com base na nossa experiência em projetos realizados por exemplo na área da Banca, a **Modelação de Cenários de Ameaças** (Threat Modeling) tem-se revelado um processo muito eficaz no Levantamento de Riscos (de acordo com a ISO 27005 o Levantamento de Riscos, compreende a Identificação, Análise e Avaliação do Risco) numa fase inicial do desenvolvimento.

MODELAÇÃO DE CENÁRIOS DE AMEAÇAS

Este processo é acima de tudo colaborativo e requer o envolvimento de diferentes participantes como o *Product Owner* que traz a visão e necessidades do negócio, a equipa de Arquitetura, de Desenvolvimento, e de Segurança da Informação (podendo existir outras de acordo com a complexidade do projeto). De acordo com uma das maiores referências na área da modelação de ameaças (**Adam Shostack**), este processo tem como objetivo responder a 4 questões:

1. O que é que estamos a desenvolver?

a. Definição do âmbito
b. Criação de Diagramas de Arquitetura

2. O que é que pode correr mal?

a. Criação dos cenários e Identificação de Ameaças
b. Identificação do contexto legal e regula-mentar

3. O que vamos fazer a esse respeito?

a. Avaliação de Risco
b. Mitigação e aplicação de controlos de segurança

4. Realizámos um bom trabalho?

a. Validação das medidas de segurança aplicadas

A realização deste processo fornece um conjunto de dados relevantes, por exemplo a severidade das vulnerabilidades, o nível de ameaça e o nível de exposição às ameaças identificadas, que podem depois ser utilizados em lugar do valor de Probabilidade no cálculo do Risco.

Para além deste enquadramento sumário, existem outros benefícios, nomeadamente a atribuição de valores concretos aos cenários de ameaças identificados, que envolvam por exemplo uma violação de dados, ou incumprimento de outros requisitos legais ou regulamentares.

Em conclusão, uma organização ao incorporar a modelação de ameaças no Ciclo de Vida do Desenvolvimento de **Software**, pode tomar de forma proativa decisões informadas sobre os riscos e a postura de segurança geral das suas aplicações. ◀

por Ricardo Dionísio,
EMEA GRC Manager at Cipher,
a Prosegur company

DESBLOQUEAR SINERGIAS ATRAVÉS DE UMA GESTÃO INTEGRADA DE RISCOS

NOS COMPLEXOS TEMPOS QUE CORREM, AS ORGANIZAÇÕES LIDAM COM UMA INFINIDADE DE RISCOS QUE EXIGEM UMA ABORDAGEM HOLÍSTICA E INTEGRADA. A GESTÃO INTEGRADA DE RISCOS (INTEGRATED RISK MANAGEMENT, DORAVANTE DESIGNADA POR IRM) SURGE COMO UMA ABORDAGEM ESTRATÉGICA CONCEBIDA PARA INTEGRAR AS VÁRIAS DISCIPLINAS DE GESTÃO DE RISCO, FORTALECENDO A RESILIÊNCIA DE UMA ORGANIZAÇÃO CONTRA OS DIVERSOS RISCOS A QUE SE ENCONTRA EXPOSTA.

A **IRM** representa uma mudança de paradigma na gestão de riscos, transcendendo os tradicionais silos de gestão de risco e procurando assim criar uma *framework* mais unificada (ou pelo menos alinhada). Na sua essência, a IRM é uma abordagem estratégica que harmoniza a gestão de risco no âmbito de cibersegurança, continuidade do negócio, privacidade/proteção de dados, gestão do risco empresarial e de outros domínios. Mas antes de avançarmos para o todo, é importante garantirmos que compreendemos as principais peças deste puzzle.

A **Cibersegurança** é uma peça crítica na proteção das organizações contra um largo espetro de ameaças digitais. A Gestão de Risco no âmbito da

Cibersegurança procura gerir o risco de quebra de confidencialidade, de integridade e indisponibilidade da informação. Esta envolve uma postura pró-ativa, envolvendo tecnologia, processos e pessoas para criar um mecanismo de defesa robusto. Desta forma, permita à organização compreender quais os controlos de segurança a priorizar, de forma a trabalhar para uma melhor prevenção, deteção e resposta às ciberameaças.

A **Continuidade de Negócio**, atualmente a evoluir para resiliência organizacional, passa cada vez mais pela realização de avaliações de risco e aplicação de medidas preventivas. Para além da vertente preventiva, mantém-se a importância das medidas de recuperação, contingência e realização de testes regulares para garantir que as operações críticas podem persistir mesmo face a perturbações.

A **Privacidade/Proteção de Dados** é um aspeto fundamental para o qual as organizações têm vindo a trabalhar para cumprirem com a regulamentação nacional e internacional, assim como as expectativas das partes interessadas na proteção dos dados pessoais. Em matéria de privacidade/proteção de dados, a gestão de risco avalia as práticas suscetíveis de provocar um risco elevado para os direitos e liberdades dos titulares dos dados pessoais.

Por último, embora seja possível cobrir mais vertentes de risco na IRM, a **Gestão de Riscos Empresariais** (ERM) desempenha um papel crucial no fornecimento de uma visão transversal dos riscos ao nível empresarial. Aborda não só os riscos financeiros, como também os riscos operacionais, estratégicos, reputacionais e de conformidade.

A principal mais-valia da Gestão Integrada de Riscos reside nas sinergias obtidas pelo alinhamento e integração de diversas práticas de gestão de riscos. Ao eliminar os silos e promover a colaboração entre a cibersegurança, a continuidade do negócio, a privacidade/proteção de dados e a gestão do risco empresarial, é expectável que a organização possa alcançar:

- **Visão holística dos riscos**: a IRM fornece uma visão abrangente e holística dos riscos, permitindo que as organizações compreendam e realizem uma gestão dos riscos em vários domínios de forma integrada;
- **Alocação eficiente de recursos**: otimiza a alocação de recursos, evitando redundâncias e garantindo que os esforços sejam concentrados nos riscos mais críticos;
- **Melhor tomada de decisão**: melhora a tomada de decisões ao fornecer uma compreensão mais completa da natureza interconectada dos riscos, permitindo escolhas informadas e estratégicas;
- **Reforço da resiliência**: aumenta a resiliência organizacional, considerando e preparando-se para potenciais perturbações provenientes de uma variedade de fontes, incluindo ameaças de cibersegurança, disrupções que afetem a continuidade do negócio, entre outras;
- **Melhor colaboração**: fomenta a colaboração e a comunicação entre diferentes departamentos e equipas, quebrando silos e promovendo uma compreensão partilhada dos riscos. ◀

CSO chief security officers

por Jorge Miranda,
Executive Manager da CSO

GESTÃO INTEGRADA DE RISCO

A GESTÃO INTEGRADA DE RISCO (GIR) É CONSTITUÍDA POR PESSOAS, PROCESSOS TECNOLÓGICOS E NÃO TECNOLÓGICOS E RESPETIVOS CONTROLOS DE GESTÃO DE RISCO UTILIZADOS NUMA ORGANIZAÇÃO.

O objetivo é aumentar a visibilidade e facilitar o processo de decisão face ao risco garantindo que a organização gere o mesmo proativamente e não reativamente. Esta postura revela-se fundamental para o sucesso do negócio, evitando crises económicas e financeiras.

A crescente complexidade, âmbito, processo de decisão e inexistência de GIR em ambiente de desmesurado crescimento e o aumento em número e complexidade dos processos de negócio na organização gera grandes dificuldades e ineficiências abrindo assim a necessidade de abordar este tema de forma coordenada e organizada.

O esforço de mitigação do risco de forma não integrada revela-se na maioria dos casos infrutífera e frustrante. A abordagem GIR revela-se eficiente no controlo, visibilidade e monitorização do risco.

De forma a começar a implementação de um sistema GIR devemos elencar e descrever, como coordenar as decisões para mitigação do risco, qual o valor acrescentado para a organização ao implementar um sistema de GIR, quais são as potenciais perdas se o risco não for gerido, como pode um sistema GIR mitigar risco minimizando perdas e maximizando proveitos.

Existem muitos benefícios diretos numa abordagem GIR e que passam por capacidade de mitigar risco associado a incidentes/acidentes com dados, agiliza a utilização de metodologias que permitem definir, implementar, avaliar a qualidade dos dados,


JORGE MIRANDA, CSO

prover a organização de ferramentas de recuperação de acidentes/incidentes e simultaneamente manter os níveis mínimos de operação, eficácia na identificação e mitigação do risco alinhado com a estratégia empresarial, permite a gestão centralizada do risco oferecendo uma clara visão sobre a sua envolvência, toma em linha de conta os eventos externos à organização contribuindo assim para uma avaliação mais realista do risco, as áreas de atuação estão perfeitamente descritas tendo como base identificação, análise, avaliação, controlo, informação, comunicação e monitorização, fácil visibilidade das oportunidades de melhoria, risco bem caracterizado e processo de decisão eficaz em relação à disponibilidade de recursos.

As organizações passam por grandes desafios na implementação de um GIR e que passam por uma vertente empresarial e outra técnica das quais se destacam na primeira vertente a necessidade de patrocínio da administração, avaliação correta dos custos de operação, responsáveis dos dados, normas regulações e legislação já na segunda vertente destaco a identificação, qualidade e consistência dos repositórios de dados, a solução de GIR deve ser confiável escalável e flexível, o risco interno e externo dos dados envolvidos que muitas vezes estão inconsistentes e/ou sem interesse.

Um sistema GIR eficaz deve ser planeado tendo em consideração uma abordagem sistemática tipo "silo" que permite eficazmente integrar e coordenar o risco inerente aos processos de negócio da organização indo assim de encontro às expetativas e desempenho pretendido. As principais linhas orientadoras que se devem ter em consideração são o mapeamento, inter-relações de risco entre processos, desenho dos processos de negócio, criação da matriz de risco efetiva sem redundâncias. Os riscos devem ser racionalizados e priorizados e aceites por todos os intervenientes no GIR, riscos avaliados com grandes "scores" devem ser relacionados a processos de melhoria continua requerendo sempre avaliação e adequação tecnológica. O alinhamento com novos "standarts" e respetivas revisões devem ser adaptadas ao GIR e preferencialmente nestes processos de revisão substituir controlos manuais por automatizados.

A implementação de uma solução tecnológica de GIR deve ser analisada tendo em consideração as necessidades de cada organização, no entanto o processo de decisão deve ter em linha de conta a pré-existência ou não de um sistema, experiência de utilização, suporte técnico, manuais/tutoriais. As funcionalidades disponibilizadas são muito importantes e das quais devem constar avaliação do risco/mitigação, base de dados de conformidade, análise/relatórios, facilidade de integração. ◀

SECURNET
ALWAYS ONLINE | ALWAYS SECURE

por Ofélia Malheiros,
Governance, Digital and Security Advisor

2023: ODISSEIA NO CIBERESPAÇO

ASSISTIMOS AO IRROMPER DUMA NOVA SOCIEDADE, A SOCIEDADE 5.0, ESTA SOCIEDADE UTILIZA O CIBERESPAÇO, SERVIÇOS DIGITAIS EM LARGA ESCALA, TOMA DECISÕES AUTOMATIZADAS BASEADAS NA INFORMAÇÃO, USA DISPOSITIVOS HÍBRIDOS E EXPERIÊNCIAS IMERSIVAS.

É uma sociedade com novos desafios, riscos, responsabilidades e funções vitais. Uma dessas novas funções vitais é a gestão do ciber-risco integrada com as decisões estratégicas de negócio, fulcral para as organizações acentes em operações digitais.

A crescente importância na sociedade da "segurança e gestão de risco" é demonstrada pelo crescimento sustentado deste mercado nos últimos anos, a nível internacional e nacional e da sua tendência de crescimento futuro.

OPERAÇÕES NO CIBERESPAÇO: ALTERAÇÃO DO RISCO

A digitalização das operações permite acelerar a entrega de novos serviços e produtos, incrementa valor para o negócio e para a sociedade, mas aumenta a dependência da informação, de serviços e de plataformas de terceiros, presentes no ecossistema organizacional. Tomem-se como exemplo os repositórios de desenvolvimento e bibliotecas de código aberto, os sensores ligados a plataformas *cloud* e o processamento de grande volume de informação no ciberespaço, incluindo a utilização de plataformas de *augmented business analytics/intelligence*.

Estas dependências - da informação e do ecossistema de Parceiros no ciber--espaço - podem, não sendo corretamente geridas, incorporar novas vulnerabilidades e aumentar a superfície de exposição a ameaças, levando ao incremento do ciber-risco. O novo contexto de operações está a ser usado pelos cibercriminosos para explorar vulnerabilidades na cadeia de fornecimento, proporcionando pedidos de resgate em ecossistemas alargados.

GESTÃO DE RISCOS (DES)CONHECIDOS?

Atualmente, o risco de ameaças cibernéticas é uma das principais preocupações dos gestores de risco, assim como as falhas na cadeia de fornecimento. Segundo o Global cybersecurity outlook do World Economic Forum, as áreas com maior influência na estratégia de ciber-risco nos próximos dois anos serão a Inteligência Artificial e *Machine Learning*, a maior adoção de *cloud* e os avanços na gestão de identidades/acessos.

E você conhece e gere os seus ciber-riscos? Fazendo o paralelo com "2001 odisseia no espaço", os tripulantes apercebem-se da alteração de riscos com origem no computador HAL e tomam medidas para os controlar. No entanto, a capacidade do HAL ler os lábios era sua desconhecida, permitindo ao computador realizar ações com danos irreversíveis para os humanos.

Com a evolução das operações para o ciberespaço e do panorama geopolítico é relevante tomar consciência da alteração dos riscos, dos novos riscos e geri-los! São cruciais medidas adequadas na gestão do ciber-risco, uma vigilância apertada face à evolução da superfície de ameaças e de novas técnicas maliciosas.

Neste contexto, é importante encontrar um Parceiro que acrescente valor pela partilha de informação da sua rede alargada de *intelligence* das tendências de ameaças e ataques, que aplique boas práticas e tenha *know-how* no contexto das vulnerabilidades em processos de transformação digital. Que o suporte nas medidas para uma correta gestão dos seus riscos conhecidos, mas também explicite os riscos até então para si desconhecidos. Estas são claramente mais--valias que se devem procurar num bom Parceiro.

JORNADA DA SEGURANÇA DIGITAL

No caminho da segurança digital, o objetivo é gerir o ciber-risco alinhado com a estratégia e os objetivos de negócio, conhecendo o ecossistema digital a que se pertence. O que deve ser concretizado?

- Uma **estratégia de segurança digital** que governe o risco, otimize a segurança e privacidade da informação no seu ecossistema digital, com responsáveis de risco bem definidos;
- **Identificar, analisar, avaliar e tratar transversalmente os riscos/oportunidades** no ecossistema digital, com prioridades alinhadas ao negócio;
- Consolidar **indicadores** com base nos processos e tecnologia;
- **Monitorizar os riscos/oportunidades** no cumprimento da legislação e normas da organização.

Face ao elevado impacto para o negócio da adoção de processos e tecnologia digital, as medidas a implementar devem ser decididas ao nível estratégico, permitindo alinhar a inovação, novas fontes de negócio, a cibersegurança, regulamentação e manter a vantagem competitiva.

Em resumo, a gestão do ciber-risco deve ser o resultado da integração dos riscos e das oportunidades aos diversos níveis da organização. ◀

RUI DAMIÃO

"A CAPACIDADE DE CONTER A AMEAÇA É O NOSSO PAPEL ENQUANTO SERVIÇO DE CIBERSEGURANÇA"

NUNO PERRY

CISO DO GOVERNO REGIONAL DA MADEIRA

NO PALCO DA IT SECURITY CONFERENCE 2023, NUNO PERRY, CISO DO GOVERNO REGIONAL DA MADEIRA, FOI ENTREVISTADO EM DIRETO, FALOU DO ATUAL AMBIENTE DE CIBERSEGURANÇA QUE AS ORGANIZAÇÕES VIVEM, ASSIM COMO O RECENTE ATAQUE QUE O SERVIÇO DE SAÚDE DA MADEIRA SOFREU.

Como é que olha para o ambiente de cibersegurança atual?

Interpretando de alguma forma aquilo que ouvimos cá hoje, é um ambiente complexo, pode até ser um lugar-comum, mas aqui com talvez dois grandes drivers.

Primeiro, a conflitualidade internacional, os conflitos geopolíticos que vamos assistindo no mundo – como a questão da Ucrânia e mais recentemente o conflito israelo-palestiniano – despoletou um conjunto de ações no ciberespaço. Pelo menos, o número de atores do cibercrime disparou em número e, certamente, em ações. Por outro lado, temos o cibercrime clássico que tem a motivação financeira e continua a ter um grande espaço de atuação e de motivação.

Às vezes, as fronteiras são difusas, mas há claramente estas duas vertentes. Às vezes são contratados como atores de ações de nível de Estado e de nível estratégico, mas são talvez estes dois – o contexto da conflitualidade e o contexto da cibercriminalidade – que marcam o mundo atual.

Por outro lado, a emergência das tecnologias que têm as suas buzzwords, como a inteligência artificial, a computação quântica, não esquecer o 5G, o IoT, entre outros, são as principais questões que modelam o nosso ciberespaço.

O Nuno trabalha no Governo Regional da Madeira. Em termos de cibersegurança, quais são as especificidades de trabalhar num governo regional e como é que a entidade em si olha para o tema?

O Governo Regional é uma entidade política de dimensão e responsabilidade territorial. Quais são as diferenças? Um território insular, descontinuado do território continental, que levanta questões da sua resiliência comunicacional, capacidade de ter ligação à Internet, às redes de comunicações internacionais, dependente dos cabos submarinos, neste caso de um cabo nacional, que liga Açores, Madeira e o continente e de um cabo que foi um investimento do Governo Regional, o EllaLink, em que temos um ramal de ligação do cabo que liga Fortaleza a Sines, para nos dar exatamente essa capacidade, termos alguma redundância, alguma capacidade alternativa em caso de acontecer algum problema.

O Governo Regional tem total superintendência num conjunto de setores da sociedade e tem a responsabilidade: por um lado, daquilo que é o trabalho garantido dentro da organização da administração pública regional, a segurança das suas infraestruturas, sistemas, dados; e, por outro lado, tem de se preocupar, em termos da sociedade em geral, que as suas empresas e que o tecido social esteja também dentro de parâmetros de cibersegurança que sejam aceitáveis.

Ainda dentro da administração pública, é uma administração pública como a nacional. Portanto, tem administração direta, indireta, setor empresarial, com todas as nuances e vicissitudes e complexidade que comportam essa situação.

É muito importante também referir outra diferença, que é a autonomia política, que significa que a capacidade de decisão autónoma da região pode não acompanhar a capacidade de decisão política nacional, e há diferenças, até porque os impactos são também diferentes.

Num cenário, por exemplo, de um ataque à rede elétrica nacional, isso não afeta, salvo por contaminação do agente atacante, mas a rede não tem impacto nas regiões autónomas; são entidades absolutamente diferentes, redes fisicamente segregadas. Há diferenças e a capacidade de decisão própria também faz esta diferenciação entre aquilo que é trabalhar em ciber no ambiente de um governo regional.

Considerando aquilo que o Nuno disse, nomeadamente de ser um território insular, quais são as principais preocupações na cibersegurança?

Em termos macro, aquela primeira que eu referi há pouco, mas já endereçada, a questão das interligações. Em relação às ameaças propriamente ditas, vamos acompanhar aquilo que é um território ligado à Internet, e aí já ultrapassamos aquilo que é o físico e o geográfico; estamos dentro do ciberespaço, suscetíveis a todas as ameaças que existem. Aí, diria que não há grande diferença.

Há um tema que é quase impossível não escapar, que é o ciberataque que o Serviço de Saúde da Madeira sofreu. O que é que pode partilhar sobre este ataque?

Em primeiro lugar, dar uma nota muito rápida sobre o ecossistema, como é que funciona, até porque os serviços de cibersegurança que dirijo foi criado em 2020, tem três anos e é um serviço com um grau de maturidade ainda muito inicial, literalmente inicial. Fizemos aqui um trabalho de avaliação usando o Quadro Nacional de Referência para saber a segurança, portanto, estamos no nível inicial.

Por outro lado, como referi também, a organização do Governo Regional tem os estabelecimentos públicos, empresariais, e, no caso, o setor de saúde é um estabelecimento público-empresarial, sobre o qual nós, serviços de cibersegurança, não temos visibilidade técnica; não tenho capacidade, nem alarmística para verificar o que está a passar nesse setor.

É o IT do SESARAM, do Serviço Regional de Saúde, que faz esse trabalho, mas nós temos alguma capacidade própria, alguma experiência em resposta a situações mais difíceis, a situações de crise, e somos o ponto de contacto do Centro Nacional de Cibersegurança na região. É nessa qualidade que vamos em auxílio, em complemento ao incidente que o Serviço Regional de Saúde sofreu.

EM RELAÇÃO ÀS AMEAÇAS PROPRIAMENTE DITAS, VAMOS ACOMPANHAR AQUILO QUE É UM TERRITÓRIO LIGADO À INTERNET, E AÍ JÁ ULTRAPASSAMOS AQUILO QUE É O FÍSICO E O GEOGRÁFICO; ESTAMOS DENTRO DO CIBERESPAÇO, SUSCETÍVEIS A TODAS AS AMEAÇAS QUE EXISTEM

Isso foi muito bom até porque permitiu à equipa da entidade dedicar-se quase totalmente a lidar com o problema que tinha em mãos, deixando a componente administrativa e a gestão comunicacional para o exterior com o C-Level, neste caso com nível político.

O ataque foi um ataque de ransomware com o grupo Rhysida – que, segundo as informações públicas, também impactou Gondomar – e teve um impacto global. O Serviço Regional de Saúde da Madeira, ao contrário do Serviço Nacional de Saúde, está total-

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

mente integrado. Os hospitais e os centros de saúde estão debaixo de um IT único, um centro de dados e uma infraestrutura de comunicações únicas, que é excelente do ponto de vista da higiene, da limpeza e da maturidade que ele já tem em termos de IT, mas também tem um nível de risco correspondente a essa circunstância, que significa que, se eu afetar um ponto desta infraestrutura, vou impactar todo o resto.

Novamente numa região insular, isto do ponto de vista do impacto societal e daquilo que pretende a Diretiva NIS prevenir, nomeadamente daquilo que são as entidades agora importantes ou essenciais, é muito relevante porque não temos alternativa. Se o serviço de saúde não está no seu funcionamento normal ou com níveis de qualidade diferenciados, não é fácil logisticamente transferir os doentes para outro território; não se ataca aqui o Garcia da Horta e do outro lado da ponte há três hospitais alternativos. Isto tem outro grau de relevância.

Os processos, como devem calcular, são muito recentes e ainda estão sob processos de investigação, mas não seria nada de estranho e expectável, até porque o modo de operação do grupo é conhecido: daquilo que deriva da engenharia social, do comprometimento de credenciais, dos acessos exploratórios e da persistência dentro das redes e depois, em determinada altura, o lançamento da execução do *payload* e, depois, a expansão da encriptação da infraestrutura. Isto não é nada, é um *playbook* comum e não fugiu sem entrar em outro tipo de detalhe a estes pormenores.

Sobre a resposta também posso dar uma nota que foi interessante. Entre as fantásticas qualidades da equipa técnica que lá estava e a dedicação das pessoas,

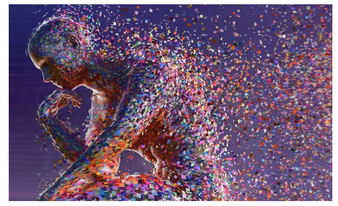
muitas vezes ficam cansadas na monitorização, mas ficam muito cansadas nas respostas aos incidentes porque querem dar o melhor que têm da sua capacidade técnica para ajudar a sua organização a recuperar. Foi uma lição fabulosa da dedicação dos meus colegas.

É esse o nosso papel enquanto Serviço de Cibersegurança: ajudar na contenção, identificar o vetor, identificar o paciente zero, preparar um plano de recuperação e extinguimos aí a nossa missão. No dia 17 [de setembro], para mim, o paciente saiu dos intensivos e foi entregue ao seu respetivo dono, terminando o meu papel em termos de missão. A abordagem foi criar uma infraestrutura limpa, uma infraestrutura verde em paralelo com a infraestrutura afetada,

> OS HOSPITAIS E OS CENTROS DE SAÚDE ESTÃO DEBAIXO DE UM IT ÚNICO, UM CENTRO DE DADOS E UMA INFRAESTRUTURA DE COMUNICAÇÕES ÚNICAS, QUE É EXCELENTE DO PONTO DE VISTA DA HIGIENE, DA LIMPEZA E DA MATURIDADE QUE ELE JÁ TEM EM TERMOS DE IT, MAS TAMBÉM TEM UM NÍVEL DE RISCO CORRESPONDENTE A ESSA CIRCUNSTÂNCIA

garantindo logo de início, tendo com grau de certeza muito elevado que tínhamos um processo clínico preservado, aquilo que são os dados clínicos, dando-nos algum *leverage*, alguma capacidade de não termos de lidar com temas mais complexos, nomeadamente com a relação com o atacante. A partir daí, sobre essa rede verde, sobre essa rede protegida, ir levantando serviços gradualmente, ir gerindo o potencial de haver contaminações, que é um processo também muito complicado.


IT·SECURITY
CONFERENCE
LISBOA
2023
OCT 12
conf.itsecurity.pt



LINO SANTOS:

"O VILÃO NÃO É O NÚMERO DE INCIDENTES, É O IMPACTO DECORRENTE DESSES INCIDENTES"

A 2.ª EDIÇÃO DA IT SECURITY CONFERENCE ESTREOU-SE COM O KEYNOTE DE LINO SANTOS, COORDENADOR DO CNCS, QUE IDENTIFICOU O BOM, O MAU E O VILÃO DA CIBERSEGURANÇA EM PORTUGAL

POR RITA SOUSA E SILVA

A 2.ª edição da IT Security Conference, que decorreu no passado dia 12 de setembro, n'O Clube Secret Spot Monsanto, arrancou com a subida ao palco de Lino Santos, Coordenador do Centro Nacional de Cibersegurança (CNCS), que apresentou o panorama da cibersegurança em Portugal, em três diferentes segmentos: o bom (aspetos positivos), o mau (aspetos críticos) e o vilão (ameaças).

"A base para nós conseguirmos definir o que é que está a correr bem e o que é que está a correr mal não é de todo percecionada", começa Lino Santos. Todos os anos, o CNCS produz um conjunto de relatórios que mede os mesmos indicadores, o que permite compreender a sua "evolução ou a não evolução" ao longo do tempo, possibilitando "orientar os nossos instrumentos" e "desenvolver as políticas públicas de uma forma mais focada".

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

O BOM

"Temos uma melhor perceção dos utilizadores e a atenção relativamente ao tratamento dos seus dados pessoais", aponta o Coordenador do CNCS. Em 2021, 71% dos utilizadores afirmaram gerir o acesso aos seus dados de algum modo, representando um aumento de 3% comparativamente a 2020.

Atualmente, existe uma maior oferta de formação especializada na área de cibersegurança, com um total de 25 cursos superiores, sendo que, em 2022, registaram-se mais três cursos em relação a 2021. A procura tem acompanhado a oferta, verificando-se um aumento no número de alunos inscritos nestes mesmos cursos.

Ao longo do tempo, a administração pública (AP) tem vindo a adotar cada vez mais medidas de cibersegurança. "Eu diria que aqui há um reflexo bastante importante daquilo que é o investimento que as várias áreas governativas estão a fazer na sua transição digital, com recurso a financiamentos europeus", constata Lino Santos.

O "crescimento da cultura de cibersegurança para um *report* dos incidentes" pelas PME é outro ponto positivo do panorama português, refere. Das empresas que sofrem incidentes, 81% afirmaram reportar a alguma autoridade em 2021, tendo em conta que a média da União Europeia (UE) é de 54%. "Isso ajuda-nos a trabalhar, ajuda-nos a identificar problemas e ajuda-nos a ajudar outras organizações", sublinha o profissional do CNCS.

Observou-se também uma melhoria da cooperação através de Centros de Análise e Partilha de Informação (ISAC), existindo seis consoladas em 2023. "São instrumentos que nos permite, por um lado, fazer alerta rápido às organizações e, por outro, com este efeito de rede, melhorar as competências e maturidade das organizações menos experientes quando estão num grupo onde existem organizações mais experientes", explica.

Por fim, Lino Santos destaca a crescente atenção da UE à cibersegurança, que tem "liderado esta senda regulatória das novas tecnologias e da segurança da informação de uma forma que é exemplar para o resto do mundo", com o desenvolvimento da NIS 2 e da lei da IA, por exemplo.

O MAU

No que aos aspetos críticos diz respeito, Lino Santos começou por identificar a falta de recursos especializados no mercado, assim como o elevado custo associado, e a "grande" rotatividade dentro das organizações. "Apesar do aumento do número de inscritos em cursos relacionados com cibersegurança, a demanda por parte das organizações, sejam públicas ou privadas, continua a ser muito elevada e o caudal que as universidades disponibilizam não é de todo suficiente", alerta. "Temos que apostar na requalificação de pessoas".

A esmagadora maioria dos profissionais da área de cibersegurança (84%) são homens, existindo poucas mulheres no setor.

Além disto, existe "uma insipiente inovação na área da cibersegurança seja dentro das organizações,

> “A BASE PARA NÓS CONSEGUIRMOS DEFINIR O QUE É QUE ESTÁ A CORRER BEM E O QUE É QUE ESTÁ A CORRER MAL NÃO É DE TODO PERCECIONADA”

seja na criação de novos produtos ou até da própria indústria de cibersegurança, que não está ao nível dos nossos congêneres europeus". Neste sentido, é notável uma falta de investimento do desenvolvimento de produtos e serviços em cibersegurança, existindo somente uma patente por 94 publicações científicas em Portugal entre 2017 e 2021.

Cursos superiores especializados à parte, o CNCS verificou uma pouca presença de disciplinas de cibersegurança nos cursos superiores de Ciências Informáticos, sendo que esta temática foi explorada em apenas 44% dos cursos em 2022. Lino Santos defende que "criar uma cultura de cibersegurança no nosso país significa introduzir o tema em todas as áreas do saber e significa introduzir o tema desde os graus de ensino mais baixos, ou seja, desde o ensino básico".

"Há uma pouca atenção das organizações para as competências básicas de cibersegurança", refere o Coordenador do CNCS, considerando insuficientes as ações de sensibilização obrigatórias. "Do número de incidentes que nós tratamos, 53% - mais de metade dos incidentes - o que é explorado não é o sistema informático. O que é explorado é o fator humano", completa, reforçando a importância do investimento nas competências digitais dos funcionários.

O VILÃO

O vilão da cibersegurança – tanto em Portugal como no mundo – é claro: "o vilão não é o número de incidentes; o vilão é o impacto decorrente desses incidentes que têm tendência a aumentar". Para Lino Santos, o caminho para combater os incidentes passa pelo foco "mais na prevenção e menos na reação".

O Coordenador do CNCS destaca que os incidentes têm tendência a aumentar "por causa do ransomware e por causa dos ataques de negação de serviço". O impacto sentido nas organizações decorrente de ataques de ransomware é "traumático", reforça. "Todas as semanas temos uma ou duas PME, um ou dois municípios que param completamente" durante uma semana e, em alguns casos, até um mês até à recuperação de serviços essenciais.

O DESAFIO

Lino Santos termina o seu keynote com uma mensagem positiva. "Nós estamos a viver um momento muito importante da cibersegurança em Portugal", indicando iniciativas como NIS 2, QNRCS, Guião para a Gestão de Riscos, MOOC, Panorama e ENSC 3.0.

No mês passado, o CNCS viu "duplicado o nosso quadro de pessoal", revela o Coordenador. "Temos as condições para fazer mais e melhor", finaliza.

ENISA:

"OLHAR PARA A NIS 2 COMO UMA OPORTUNIDADE DE MELHORARMOS A CIBERSEGURANÇA DAS ORGANIZAÇÕES"

O CYBERSECURITY EXPERT DA ENISA APRESENTOU OS PRINCIPAIS DESAFIOS LEVANTADOS PELA NIS 1 E QUAIS AS MAIS-VALIAS CRIADAS PELA DIRETIVA NIS 2

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

POR MARTA QUARESMA FERREIRA

Ricardo Figueiredo, Cybersecurity Expert da European Union Agency for Cybersecurity (ENISA), levou até ao palco da 2.ª edição da IT Security Conference o tema da nova Diretiva NIS 2.

A sucessora da NIS 1 nasceu num contexto de eventos disruptivos, como foi o caso da pandemia da COVID-19, da transformação digital e das questões de geo-política e soberania digital entre China, EUA e União Europeia. No contexto de ameaças, "vemos tudo a mudar rapidamente, com mais impacto, mais ativo, algo que nos preocupa diariamente", começa por explicar Ricardo Figueiredo.

A proposta da NIS 2 surge assim naquele que é considerado o maior pacote legislativo à escala europeia, onde se pode encontrar também o Cybersecurity Act, a Nova Estratégia da União Europeia para a Cibersegurança, iniciativas setoriais (DORA) e a reformulação dos mecanismos e dos instrumentos de financiamento ao nível da cibersegurança.

O Cybersecurity Expert considera que o ponto de partida para compreender a nova diretriz passa por avaliar o que "correu bem e o que correu menos bem na diretiva NIS 1". Um dos grandes problemas, destaca, estava relacionado com âmbito de aplicação da Diretiva, admitindo a dificuldade na sua gestão, que acabou por "criar muitas divergências". Em causa estava a falta de consideração no âmbito da diretiva de determinados setores críticos; por outro lado, na transposição para a legislação nacional, os Estados-Membros tiveram a liberdade de "identificar os operadores de serviços essenciais que efetivamente iriam estar abrangidos", o que levou a que cada Estado-Membro identificasse o seu operador, criando elevadas divergências a nível europeu.

A questão da supervisão foi outro dos pontos referidos por Ricardo Figueiredo, uma vez que um dos pilares da NIS estava relacionado com "a partilha da informação e com a cooperação entre os Estados-Membros" que funcionava numa base voluntária e que nunca chegou a acontecer.

NOVIDADES DA NIS 2

O âmbito de aplicação da nova Diretiva é agora mais alargado. "Vamos ter mais do dobro dos setores a 'caírem' dentro do âmbito da Diretiva NIS e dentro destes setores muito mais empresas", graças a um novo critério de dimensão.

Uma das outras alterações elencadas está relacionada com a designação antiga, que desaparece, com as entidades a serem classificadas como "entidades essenciais" e "entidades importantes". Há ainda um "reforço do foco na componente de gestão de risco", acrescenta Ricardo Figueiredo.

Em suma, as empresas de média ou grande dimensão estarão abrangidas pela nova Diretiva NIS, com um regime de supervisão específico no caso de serem classificadas como "entidades essenciais" ou "entidades importantes"; por outro lado, ao nível da gestão de risco, existirão "o mínimo de medidas de segurança técnica e organizativa" a serem observadas. De acordo com o Cybersecurity Expert da ENISA, será também encorajada a aplicação de normas internacionais e de certificação e será ainda exigida a demonstração da aplicação de políticas de controlo de segurança de informação implantadas nas organizações. No fim, e numa ótica de gestão de risco, a NIS 2 traz a responsabilização do *Board* por não *compliance*.

Ricardo Figueiredo sublinha que é necessário "ver a NIS 2 como uma oportunidade de melhorarmos a cibersegurança nas nossas organizações e contribuir para aumentar a resiliência dos setores críticos".

A nova Diretiva passa a compreender 15 setores. As entidades passarão a ser classificadas entre "importantes" e "essenciais" de acordo com os critérios da União Europeia para classificação de organizações. As empresas que tenham mais de 50 colaboradores e mais de 10 milhões de euros de volume de negócios passam a estar abrangidos pela NIS 2.

Atualmente, os Estados Membros encontram-se a fazer a transposição da NIS 2, que deverá estar concluída até 17 de outubro de 2024. A lista de entidades abrangidas no âmbito desta nova Diretiva terá de ser apresentada em abril de 2025

POR RITA SOUSA E SILVA

LUÍS MORAIS:

"AO TRABALHAR COM PROJETOS DE INOVAÇÃO, VÃO TRAZER RISCO PARA DENTRO DA ORGANIZAÇÃO"

O KEYNOTE DE LUÍS MORAIS, CISO DA GALP, ABORDOU COMO APLICAR A CIBERSEGURANÇA NA INOVAÇÃO E A INOVAÇÃO NA CIBERSEGURANÇA NA PREVENÇÃO E COMBATE DE CIBERAMEAÇAS.

Luís Morais, CISO da Galp, apresentou na 2.ª edição da IT Security Conference a relação complexa, mas simbiótica entre as equipas de cibersegurança e o departamento de inovação dentro de uma organização, com o objetivo de fortalecer a capacidade de proteção e combate contra incidentes.

CIBERSEGURANÇA NA INOVAÇÃO

"Vamos ser sinceros: se isto fosse o secundário, os tipos da inovação e os tipos da cibersegurança nunca se sentavam na mesma mesa para almoçar", brinca Luís Morais, retratando o cenário atual da cibersegurança e inovação dentro das organizações. "Os tipos da inovação olham para a cibersegurança como os tipos que estão sempre a dizer que não", enquanto as equipas de cibersegurança veem as de inovação como "adolescentes que querem fazer tudo sem seguir as regras e vamos ter que os controlar".

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

O caminho para a resolução desta relação complexa passa pelo diálogo entre os dois departamentos de modo a compreender a perspetiva um do outro, acredita o CISO da Galp. As equipas de inovação devem perceber que aquilo que "funciona em laboratório nem sempre funciona na vida real, principalmente porque o laboratório não tem os agentes de ameaça que nós temos todos os dias a atacar as nossas redes". Por outro lado, as pessoas da cibersegurança devem compreender "aquilo que são os requisitos da organização, onde é que a organização quer ir estrategicamente e suportar a organização nesse desenvolvimento".

"A organização tem de perceber que, ao trabalhar com projetos de inovação, eles vão trazer risco para dentro da organização", sublinha Luís Morais, considerando este um dos "fatores-chave na mudança do *mindset*".

A experiência das equipas de cibersegurança da Galp, conta Luís Morais, tem assentado em desempenhar o papel de "parceiros do negócio", trabalhando intimamente com o departamento de inovação "desde o dia zero, tentando implementar princípios de ciber-resiliência *by design*".

O objetivo é garantir que as soluções de inovação são efetivamente seguras e que "nos permitem reagir e responder no caso de haver uma intrusão nessa tecnologia" através do controlo dos dados utilizados em conjunto com "uma aproximação em *sandbox*".

O "*drive*" da implementação de projetos de inovação deverá passar por "começar a implementar estes projetos em âmbitos controlados do ponto de vista tecnológico, do ponto de vista dos dados que acedem e ir aumentando progressivamente esses dados à medida que nós percebemos que a tecnologia é funcional, que tem retorno de investimento e que vai ser usada".

Por outro lado, isto permite às equipas de cibersegurança "ir testando os mecanismos e controlos que temos que aplicar em cima daquela tecnologia, que é nova, que nós não conhecemos e que, portanto, não podemos utilizar as mesmas técnicas de sempre para a desenvolver".

INOVAÇÃO NA CIBERSEGURANÇA

Não obstante, a relação simbiótica entre inovação e cibersegurança tem proporcionado um conjunto de tecnologias que permitem às equipas de *cyber* "ser um bocadinho mais capazes de responder às ameaças que temos diariamente".

A automação e orquestração tem sido benéfica para a cibersegurança, visto que possibilita "tirar a atenção dos meus analistas que estão a lidar com incidentes de segurança, focá-los naquilo que é essencial e ter muito maior produção do ponto de vista de cibersegurança e de gestão de incidentes com os mesmos recursos humanos", bem como "mantê-los interessados e motivados".

Outros exemplos são as tecnologias de machine learning, IA e *Threat Intel Sharing*, juntamente com a *behaviour analytics* de pessoas, sistemas e redes. O *Continuous Cyber Risk Management* é uma ferramenta utilizada que funciona como "um sistema imunitário", identificando as fragilidades dentro do ecossistema e corrigindo-as de forma quase automática, possibilitando uma "melhor capacidade de gestão do dia a dia".

Por fim, Luís Morais destaca o fator humano como um dos maiores riscos na ocorrência de incidentes, sendo importante a formação das equipas. Na Galp, a capacitação das pessoas, explica, é feita através da gamificação e *adaptive learning*, que permite avaliar os pontos em que estão menos confiantes e, posteriormente, dar prioridade precisamente a estas temáticas.

MARGARIDA LEITÃO NOGUEIRA:

"TENDÊNCIA REGULATÓRIA EUROPEIA "COMPORTA IMPACTO ECONÓMICO E OPERACIONAL PARA ENTIDADES"

A TENDÊNCIA REGULATÓRIA NO ESPAÇO EUROPEU FOI A TEMÁTICA ABORDADA NO KEYNOTE DE MARGARIDA LEITÃO NOGUEIRA, PARTNER DA DLA PIPER, NA 2.ª EDIÇÃO DA IT SECURITY CONFERENCE.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

POR RITA SOUSA E SILVA

Margarida Leitão Nogueira, Partner da DLA Piper, debruçou-se sobre a tendência regulatória europeia sobre cibersegurança e o seu impacto nas organizações.

A advogada identificou os principais fatores de risco que estão "na base do aumento do risco em matéria de cibersegurança e, portanto, do aumento dos ciberataques". A adoção massiva do trabalho remoto durante o período pandémico impulsionou "os acessos às redes e sistemas de informação a partir do exterior das organizações" e "o processo de transição digital".

Esta transição digital nas organizações ocorreu "de forma repentina" e "sem que tivessem sido adotadas as medidas de segurança necessárias". De igual modo, no que diz respeito às tecnologias emergentes, como a IoT, "nem sempre são ponderados devidamente os riscos associados" e "aplicadas as soluções técnicas necessárias".

O "contexto geopolítico complexo" tem contribuído para o crescimento dos riscos. "Sabe-se que alguns dos agentes que levam a cabo ciberataques são agentes estatais que visam, por um lado, a recolha de informação e, por outro, perturbar setores-chave da economia", afirma.

Neste sentido, a União Europeia sentiu a necessidade de "criar novos requisitos e obrigações legais para as organizações no sentido da proteção das suas redes e sistemas", assim como de "estender a abrangência de alguns dos requisitos já existentes a novos setores". Em particular, a advogada destacou a diretiva REC, referente à resiliência das entidades críticas; o Regulamento de Ciber-Resiliência, que vai impor requisitos a produtos com elementos digitais; a Diretiva NIS 2, que visa "garantir o elevado nível comum de cibersegurança"; e o Regulamento DORA, que aborda a resiliência operacional digital do setor financeiro.

DIRETIVA NIS 2

Em vigor desde janeiro, a NIS 2 deverá ser transposta para os estados-membros até outubro do próximo ano. Quando comparada com a diretiva anterior, a NIS 2 vem trazer uma "maior abrangência dos setores e entidades", como a indústria de gestão de resíduos, dos serviços postais e do fabrico de dispositivos médicos.

A diretiva introduz a "distinção entre entidades essenciais e entidades relevantes", a melhoria da gestão de risco e o estabelecimento de prazos de notificação de incidentes.

"Responsabilizam-se órgãos de direção e de gestão das entidades" em caso de infração, que devem não só "implementar medidas de gestão de risco", mas também "supervisionar a sua implementação". Já a criação da Rede Europeia de Organizações de Coordenação de Cibercrises visa "uma maior partilha de informação e cooperação entre todos os estados-membros".

REGULAMENTO DORA

Tratando-se de um regulamento e não de uma diretiva, o DORA "não necessita de transposição" e, a partir de 2025, "é aplicável diretamente em todos os estados-membros, sem prejuízo de legislação que venha a ser aprovada".

O regulamento aplica-se a entidades financeiras e empresas tecnológicas que prestam serviços de TIC a entidades financeiras, tendo como objetivo "harmonizar e criar requisitos uniformes para a resiliência e segurança das redes e sistemas de informação" do setor.

O DORA inclui a implementação de medidas de gestão de riscos, de "conteúdo específico conforme legalmente previsto" em contratos entre entidades financeiras e prestadores de serviços de TIC e de testes de resiliência.

Facilita ainda a partilha de informação entre estas entidades, "desde que tenha como objetivo reforçar a resiliência operacional digital", e estabelece obrigações relativas à gestão e reporte de incidentes.

REGULAÇÃO "COMPORTA DESAFIOS"

"A tendência regulatória europeia tem vindo a impor uma maior exigência a todas as organizações no que respeita ao cumprimento de obrigações e requisitos legais", refere Margarida Leitão Nogueira. "Esta exigência comporta desafios, comporta um impacto económico e operacional para as entidades abrangidas muito significativo".

"É fundamental investir-se em cibersegurança enquanto pilar essencial do desenvolvimento do negócio", sublinha. "Uma preparação adequada pode ser determinante".

CRISTIANE DIAS:

A CIBERSEGURANÇA É "RESPONSABILIDADE DE TODA A ORGANIZAÇÃO E NÃO APENAS DAS TI"

O KEYNOTE DE CRISTIANE DIAS MOSTROU AO PÚBLICO DA IT SECURITY CONFERENCE 2023 COMO FOMENTAR A CIBER-RESILIÊNCIA DAS ORGANIZAÇÕES, COM FOCO NO PROCESSO DE RESPOSTA A INCIDENTES.

POR RITA SOUSA E SILVA

Cristiane Dias, Head of CyberSecurity no setor de utilities brasileiro, levou até ao palco da 2.ª edição da IT Security Conference o seu conhecimento sobre o reforço da resiliência cibernética das organizações, com especial enfoque no processo de resposta a incidentes.

"Ao longo da minha carreira, eu já sofri três incidentes cibernéticos em três empresas diferentes", arranca Cristiane Dias. "O que tinha de comum nas três empresas era que o básico não era seguido".

"Nos três incidentes não existia o conceito de MFA em todos os ambientes, não existia o conceito de mínimos privilégios e muitos ambientes estavam sem atualizações por conta de ausência de janela de manutenção pela área de operações", revela.

É com base na sua experiência de defesa contra atividades cibercriminosas que Cristiane Dias centrou o seu keynote no processo de recuperação no período

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

> AS EQUIPAS TÉCNICAS TÊM UMA VONTADE MUITO GRANDE DE FAZER TUDO, MAS QUEM FAZ TUDO AO MESMO TEMPO NÃO CONSEGUE CONCLUIR

pós-incidente, dividido em duas fases principais: a "fase tática" e a "fase estratégica".

FASE TÁTICA

No que à fase tática diz respeito, a "primeira coisa a determinar" é o "impacto", uma vez que uma empresa "não consegue mitigar um incidente se não sabe [que] ativos foram impactados". Desta forma, é "importantíssimo determinar a presença do atacante", sendo que este poderá estar a "rodar scripts" sem o conhecimento das organizações.

A criação de "um plano de restauração", onde são delegadas "exatamente as responsabilidades aos teams", é um passo importante do processo de recuperação. "Não adianta fazer tudo ao mesmo tempo", afirma. "As equipas técnicas têm uma vontade muito grande de fazer tudo, mas quem faz tudo ao mesmo tempo não consegue concluir".

"Defina os responsáveis e documente as ações", acrescenta Cristiane Dias, onde está deverá estar estipulada a "timeline" dos eventos. Um erro frequente no pós-incidente é "não [saber] exatamente a data e a hora que aquela atividade foi executada".

FASE ESTRATÉGICA

"Mantenha o negócio informado", alerta Cristiane Dias. A profissional revela que, no primeiro incidente que enfrentou, "ficámos dez dias indisponíveis", enquanto no ataque seguinte, já numa organização diferente, "ficámos uma semana". Por sua vez, "na última empresa, ficámos 23 horas indisponíveis".

O "sucesso na defesa contra o último incidente" assenta em dois fatores-chave: "lições aprendidas e um plano de comunicação eficiente". "As equipas não se conseguem focar num plano de resposta a incidentes se a todo o momento o telefone das equipas não para de tocar com alguém a querer saber quando o sistema vai voltar", alerta.

Neste sentido, a profissional revela que "uma das coisas que funcionou bem foi a cada hora nós tínhamos um comité de comunicação para o negócio", em que era dado o "*status* da última hora das ações do team em relação à resposta ao incidente".

Criar "pares para validação" e formalizar "uma ocorrência nos órgãos locais" são outras ações destacadas. "Se as empresas não formalizarem, o governo não tem como ter consciência da quantidade de incidentes cibernéticos que ocorrem no país", acrescenta.

Cristiane Dias ressalva também a importância de realizar "o *report* final do incidente", com informações sobre "quais foram as ações, quem foram os teams que executaram tais ações, quais os planos de mitigação, qual o *downtime* de cada sistema".

LIÇÕES APRENDIDAS

Aprender com os incidentes é uma etapa fundamental para fomentar a ciber-resiliência das organizações. Relativamente à vertente tática, "não adianta chegar, criar um comité de crise, [recuperar] a empresa em 23 horas, se não tem uma governança depois disso porque vai ser novamente atacado", adverte.

É importante também criar "*playbooks*, *workbooks* e casos de uso aderentes ao seu negócio" para o SOC e o MSS. "Nas três empresas, duas delas tinham um SOC de empresas grandes", explica Cristiane Dias. "Nenhum dos dois SOC identificou a presença do atacante que já estava pelo menos há 15 dias. Nós tínhamos a falsa sensação de que estávamos seguros".

Validar a estrutura de DevSecOps, estender o processo de table top "a todos os níveis", adotar os conceitos de DRP e *threat hunting* para ter conhecimento sobre "o que os criminosos na deep, na dark web estão a falar da sua empresa", bem como realizar testes e explorações externas *blackbox* "a cada três meses" e "sempre que subir um novo sistema" devem ser procedimentos frequentes das organizações, segundo Cristiane Dias.

"Reforce o processo de *hardening* e *baseline* de segurança", recomenda também Cristiane. "Durante os três incidentes, o que tínhamos em comum é muitas GPO a rodar na camada de AD e algumas conflituando entre elas", o que contribuía para a "falsa sensação de segurança porque uma estava a anular a outra".

Nos ambientes legados, "crie o conceito de segregação", que é "fundamental para que os sistemas core business não fossem atacados e conseguíssemos voltar em 23 horas, por conta da segregação de OT com IT".

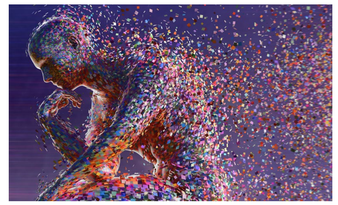
É ainda necessário reforçar "os controlos com os teams internos", uma vez que "a grande maioria das vulnerabilidades vem de teams com privilégios elevados que não tratam essas credenciais de forma adequada".

No que diz respeito à vertente técnica, Cristiane Dias indica que é necessário atualizar "o mapa de risco da organização" e reforçar "o plano de adequação curto, médio e longo prazo", criando uma "*timeline* com investimentos para isso".

Além disto, é essencial compreender que o conceito de segurança é uma "responsabilidade de toda a organização e não apenas da TI", sendo importante criar "programas de consciencialização de todos os níveis".

A criação de "metas departamentais de segurança", ligadas à "participação de lucros", e alinhar a cibersegurança "com a estratégia de negócio" são outras ações apontadas pela profissional. "Não existe uma empresa 100% segura", enfatiza.

Antes de concluir o seu keynote, Cristiane Dias deixa uma mensagem para o público: "o crime cibernético é extremamente organizado. Que nós CISO e líderes de segurança também tenhamos esse mindset de união, de compartilhamento de informações, respeitando a confidencialidade de cada empresa".



BRIGADEIRO-GENERAL PAULO VIEGAS NUNES:

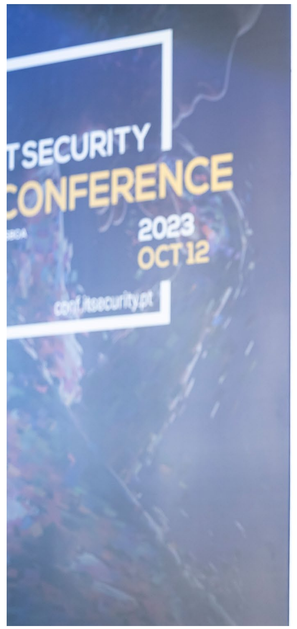
DAR PODER DE DECISÃO À MÁQUINA

"É O CABO BOJADOR DE PODERMOS LIDAR COM A IA"

A CONFERÊNCIA ENCERROU COM OS INSIGHTS DO BRIGADEIRO-GENERAL PAULO VIEGAS NUNES, PRESIDENTE DO SIRESP, SOBRE A FRAGMENTAÇÃO E DESCONTINUIDADE NA ERA DIGITAL, IMPULSIONADA PELA SUPERIORIDADE DE INFORMAÇÃO E PELA GUERRA COGNITIVA.

POR RITA SOUSA E SILVA

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



A última sessão da conferência ficou a cargo do brigadeiro-general Paulo Viegas Nunes, presidente do SIRESP. A sua apresentação incidiu sobre a superioridade de informação e a guerra cognitiva cuja "interligação provoca a fragmentação e descontinuidade estratégica".

Nos últimos anos, tem-se observado uma nova "dinâmica que se tem vindo a acentuar" na era digital, assente na "construção do mundo que se autoalimenta quase autofagicamente".

"As dependências tecnológicas que se vão mantendo e estruturando criam vulnerabilidades", constata o brigadeiro-general. "Vulnerabilidades essas que ameaçam e comprometem a resiliência das organizações, mas também dos Estados".

O ambiente de informação "junta" os domínios do "ambiente físico, informacional e cognitivo", permitindo assim "interligar simultaneamente todos os instrumentos do poder e todos os domínios operacionais". A Internet é uma esfe-

ra "multidomínio", afetando "não só o ambiente de informação, mas outros ambientes físicos onde a sua intervenção ou ligação se estabelece".

SUPERIORIDADE DE INFORMAÇÃO

Atualmente, vivemos em "sistemas e conflitos híbridos", onde coexistem "uma dinâmica civil com uma dinâmica militar". Isto está intrinsecamente ligado ao conceito de guerra híbrida, ou seja, a "guerra que não tem forma definida" e é "multiforme, dinâmica e permanente".

Dois dos principais vetores da guerra híbrida situam-se no ciberespaço: "os ciberataques" e "a guerra de informação ou media". Perante o desenvolvimento tecnológico, emerge sempre uma questão central: "porque é que nós avançamos para a tecnologia?". A resposta é clara. "Avançamos porque queremos ter vantagem", sublinha.

Num ambiente competitivo, o "centro de gravidade é a obtenção da vantagem no domínio da informação", ou seja, "a tal superioridade da informação". Cada ator procura "preencher o seu ambiente de informação até ao limite daquilo que necessita para a sua operação" e, muitas vezes, "entra em competição com outros atores" que têm o mesmo objetivo.

"Quando existe conflito, competição ou confrontação, nós temos duas vontades diferentes, com interesses muitas vezes antagónicos, em que um ator se confronta com o outro", aponta. Quem tem superioridade é o ator que "tiver o seu ambiente de informação mais preenchido para as necessidades operacionais".

PIRÂMIDE COGNITIVA E CICLO DE DECISÃO

É neste contexto que Paulo Viegas Nunes reforça a necessidade de olhar para a pirâmide cognitiva. "Nós temos capacidade e possibilidade de atuar em vários domínios", refere.

A intervenção na pirâmide cognitiva passa pela: guerra dos sinais, correspondente ao domínio físico, que "os militares normalmente designam por guerra eletrónica"; guerra da informação, "ou seja, a lógica estruturante, a guerra da sintaxe"; e guerra cognitiva.

Além disto, o presidente do SIRESP apresentou o ciclo de decisão, designado *OODA-loop* – observar, orientar, decidir e agir – que traz consigo "a decisão em rede". A interrupção do ciclo de decisão leva à sua ineficiência, o que "significa a ineficiência da decisão".

"Cada um dos ciclos de decisão tem um tempo. Esse tempo, se for mais rápido por um ator do que por outro, dá vantagem em termos operacionais", explica. "Se eu conseguir ser tão rápido quanto o tempo que um ator demora a observar, a orientar e até a decidir, eu intervenho sobre a realidade antes de ele poder, com a decisão dele, intervir-se ele próprio sobre a realidade".

Isto significa que "a realidade com que ele vai intervir já é diferente daquela que ele observou e orientou", ou seja, "entrámos dentro do ciclo de decisão de um adversário". Neste caso, a superioridade "já não é de informação, é de decisão".

> “SE TIVERMOS UMA FORÇA QUE COMBATE, ELA NECESSITA DE DESENVOLVER SINERGIAS PARA SE PROTEGER”

A introdução da Inteligência Artificial (IA) na equação torna o processo ainda mais “assimétrico”. Esta tecnologia “molda dados” e “molda a informação que alimenta o decisor”. Desta forma, “não só é um problema de tempo, mas é um problema de conteúdo de informação que alimenta o decisor”.

CIBERSEGURANÇA COMO FORÇA COMBATENTE

A Internet é “a zona de interesse para todas estas entidades poderem trabalhar”. Neste sentido, não basta assegurar “o funcionamento normal sem intervenção” dos sistemas de informação e de comunicações. É imperativo garantir a “resiliência do ciberespaço que intersecta todos estes sistemas” – aquilo que se designa “a garantia da missão”.

“Se tivermos uma força que combate, ela necessita de desenvolver sinergias para se proteger”, sublinha o brigadeiro-general, ou seja, precisa de "uma força de proteção que salvaguarde e dê resiliência à atuação operacional”.

Tal como a nível militar, as organizações têm de ter um pensamento semelhante. A cibersegurança desempenha o “papel de força combatente”, ou seja, “é o instrumento de proteção de todos os outros domínios”.

“Qualquer atividade de uma organização que viva num ambiente de informação precisa de cibersegurança”, reforça. “Não é só porque é desejável, é porque é fundamental e absolutamente estruturante da sua atividade”.

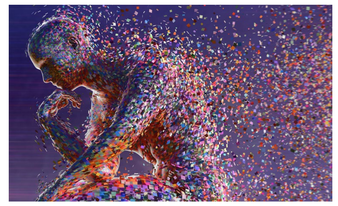
DIREITOS DE DECISÃO DA IA

O caminho que está a ser percorrido com a IA passa por “mimetizar determinado tipo de ações até um ponto perigoso, em que vamos dar direitos de decisão à máquina porque é mais eficiente a máquina agir” com estes. Isto significa dar-lhe “autonomia da ação”.

Para Paulo Viegas Nunes, este é “o Cabo Bojador de nós podermos lidar com a IA”. “Quando transferirmos direitos de decisão para a máquina, nós perdemos direitos de decisão”, sendo que esta é “muito mais eficiente e rápida”. Desta forma, a IA “favorece a superioridade cognitiva”.

É “por estas razões” que surgem “a fragmentação e a descontinuidade estratégica, porque nós não conseguimos deixar de atuar multidomínio, e atuar multidomínio exige um sincronismo permanente”.

“A resposta a isto é sinergias, cooperação multinível, interagência nacional e internacional”, conclui. “Se falharmos neste trabalhar em rede de forma colaborativa, vamos perder esta batalha, porque a rede é muito mais rápida e a forma de decisão em rede supera largamente a decisão autónoma”.



COM O APOIO DA CLARANET

CIBERINTELIGÊNCIA:

A FERRAMENTA "TOTALMENTE DIFERENCIADORA" QUE ALIA A ANÁLISE DE DADOS E A SEGURANÇA

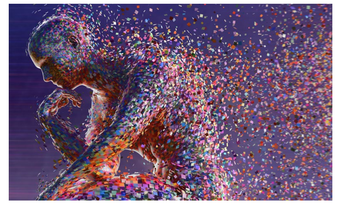
A PRIMEIRA MESA-REDONDA DO DIA CONTOU COM A PARTICIPAÇÃO DE UM LEQUE DIVERSIFICADO DE PROFISSIONAIS DAS MAIS DIVERSAS ÁREAS – UNIVERSO SONAE, UNIVERSIDADE DE ÉVORA, CIIWA E CLARANET – PARA DEBATER O CONCEITO DE CIBERINTELIGÊNCIA E O SEU PAPEL NA ESTRATÉGIA DE SEGURANÇA DAS ORGANIZAÇÕES.

POR MARTA QUARESMA FERREIRA

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

Como é que podemos definir a ciberinteligência? Foi com este mote que arrancou a primeira mesa-redonda da 2.ª edição da IT Security Conference, com o tema "A necessidade de ciberinteligência".

Coube a Paulo Lima, Head of IT da Universo Sonae, partilhar a sua perspetiva, entendendo a ciberinteligência como a "capacidade de levar à ação", que passa por conseguir "extrapolar algo, ou que nos alerte para alguma coisa, ou que nos alerte para alguma tendência", passando dos dados para a ação de forma automatizada. Para Mário Filipe, Responsável de Segurança de Informação da Universidade de Évora, os dados ganham outra dimensão quando colocados numa perspetiva académica. "A nossa forma de encarar a ciberinteligência é recolher o máximo de informação", com automatização



que, neste caso, está mais dependente da intervenção manual.

Para David Grave, Cybersecurity Director da Claranet, a adoção de ferramentas como a ciberinteligência é "totalmente diferenciadora", uma vez que há necessidade de recolha de dados, com a diminuição de uma investigação que leva apenas algumas horas.

"Do mundo do *intelligence*, do mundo das informações, há uma parte específica que é respeitante à ciber", justificou Rogério Bravo, Membro CIIWA e Coordenador de Investigação Criminal da PJ. Desta coleção de dados fazem parte "indicadores de ataques, indicadores de comprometimento, tudo o que sejam dados que digam respeito à organização e que tenham uma origem eletrónica".

Do ponto de vista da Universo Sonae, Paulo Lima explicou que a empresa olha para a estratégia de segurança como uma "estratégia com vários níveis". A ciberinteligência, referiu, é colocada como pilar desta mesma estratégia que culmina depois em ação. No final do dia, defendeu, o objetivo passa por "aumentar a confiança dos utilizadores e dos clientes. Se for bem gerida no dia-a-dia pode ser, inclusivamente e na minha opinião, um fator de competitividade, distintivo para as organizações".

PAULO LIMA, UNIVERSO SONAE

MÁRIO FILIPE, UNIV. ÉVORA

Da perspetiva da Universidade de Évora, Mário Filipe fala numa "mudança de paradigma", com a segurança a tornar-se uma preocupação na instituição de ensino superior. "Os nossos docentes e alunos chateiam-se porque às vezes eu envio um email a avisar 'não devem fazer isto'" porque, prossegue, "eles têm mais do que fazer do que estar preocupados com segurança".

"Temos de ser militares, temos de assumir que existe doutrina e temos de a seguir", sublinhou Rogério Bravo, que alertou para a necessidade de pensar na segurança para além dos quatro pilares – tecnologias, pessoas, processos e segurança física. "É preciso perceber que dentro desses processos existe precisamente esse desenho e adoção e temos de

ROGÉRIO BRAVO, CIIWA


DAVID GRAVE, CLARANET

assumir a existência dessa doutrina e desses quatro pilares", acrescentou.

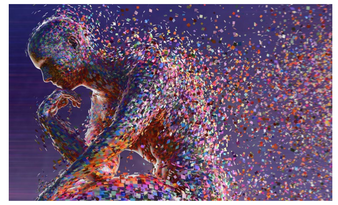
David Grave defendeu que, em termos estratégicos, as organizações terão de adotar a cibersegurança. "Nós estamos a observar um potencial disruptivo da adoção do AI para os bons", afirma, acrescentando que a atual realidade demonstra que as ferramentas de IA à disposição para defesa "são manifestamente superiores às ferramentas de inteligência artificial que existem para o ataque". Entre os principais problemas para o utilizador comum, enumerou o Cybersecurity Director da Claranet, estão a produção de conteúdo, o texto, a qualidade de texto, os *deepfakes* de voz e vídeo.

Levar a ideia às organizações de que necessitam de colocar a cibersegurança como um assunto prioritário nas suas agendas tem-se revelado, por vezes, um desafio. Para Paulo Lima, o primeiro passo passa por fazer mais trabalho junto da Academia, assim como manter a formação e os testes realizados aquando da entrada dos colaboradores na organização. É ainda necessário incentivar à sensibilização contínua ao longo do tempo dentro da empresa.

No caso do contexto do ensino superior, a maior dificuldade nesta questão passa pela entrada anual de centenas de novos estudantes que trazem consigo dispositivos que aumentam os riscos. "Temos de conseguir chegar não só aos alunos de informática, que vão trabalhar em cibersegurança, mas a todos os alunos", afirmou Mário Filipe.

Para Rogério Bravo os relatórios de análise situacional, divididos pelos quatro pilares já abordados, revestem-se de uma importância e nova dimensão ao oferecerem uma visão geral e potenciam o awareness junto dos C-Level sobre as necessidades da organização ao nível da cibersegurança.

"Há aqui dois níveis que estamos a ver de falhas de informação: na Academia e na entrada dos utilizadores, como é que nós vamos formar as nossas pessoas para estarem a um nível que nós consideramos aceitável de cibersegurança e de conhecimento para trabalharem connosco", elencou David Grave, que aponta para a existência de um "*gap* de comunicação entre o IT e o C-Level".



COM O APOIO DA DELL TECHNOLOGIES

CIBER-RESILIÊNCIA:

"O CISO NÃO PODE SER O PEDRO E O LOBO: TEM QUE SER PARANOICO, MAS CONTIDO"

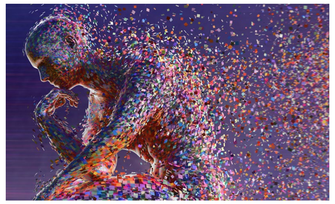
A SEGUNDA MESA-REDONDA DO DIA REUNIU PROFISSIONAIS DA ALTICE, DA EDP, DA SECRETARIA-GERAL DA ECONOMIA E DA DELL TECHNOLOGIES PARA DISCUTIR COMO AUMENTAR A CIBER-RESILIÊNCIA DAS ORGANIZAÇÕES

POR RITA SOUSA E SILVA

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

A segunda mesa-redonda da 2.ª edição da IT Security Conference contou com a participação de José Alegria, da Altice, Paulo Moniz, da EDP, João Camões, da Secretaria-Geral da Economia, e Bruno Mendes, da Dell Technologies. O tema, moderado por Rui Damião, diretor da IT Security, incidiu sobre a ciber-resiliência das organizações e as estratégias que impulsionam o seu aumento.

Saber recuperar em caso de desastre é crucial para qualquer organização. Bruno Mendes, Senior Sales Executive da Dell Technologies, começou por enquadrar o conceito de ciber-resiliência, caracterizando-a como "a capacidade de, independentemente do que acontecer no vosso ecossistema, seja ele qual for, terem uma capacidade real de recuperar informação em tempo útil".



JOSÉ ALEGRIA, ALTICE

PAULO MONIZ, EDP

Muitas vezes, a ciber-resiliência é abordada como uma temática exclusivamente tecnológica, mas Paulo Moniz, Director de Information Security and IT Risk da EDP, sublinha que esta "deve existir de cima a baixo, desde a parte mais tecnológica, desde as operações, desde o desenvolvimento das aplicações até aos serviços de negócio".

Neste sentido, é necessário "pensar a resiliência ao nível do negócio" em dois pontos centrais. Em primeiro lugar, Paulo Moniz destaca que o momento em que "fazemos aqueles famosos *business impact analysis*" e "dizemos assim 'quanto tempo é que esta aplicação pode estar em baixo de forma a não ter um prejuízo de X?'", referindo-se ao RPO e ao RTO. "É nesse momento que realmente devemos alertar e acho que essa consciência acaba por ser natural, que existem processos alternativos para quando essas aplicações ou esses sistemas estão em baixo".

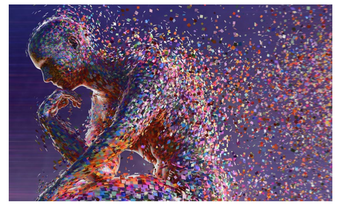
O segundo ponto para levar a ciber-resiliência para os processos de negócio é "o momento dos exercícios", em que "devemos ser o mais real possível e tentar simular situações onde os processos e os serviços do negócio são realmente afetados e, depois, acaba por se pensar em soluções alternativas".

CINCO PILARES DA "DOUTRINA ATIVA"

José Alegria, CISO da Altice, afirma que o CISO, "para convencer e evangelizar quem tem o dinheiro e quem manda, tem de criar um instrumento linguístico", que designa de "doutrina", assentando em cinco pilares.

Primeiramente, o "pilar essencial" é a governança, que consiste em "explicar às pessoas respetivas, a todos os níveis o que é que é necessário", esclarece José Alegria. "Sem governança não há *budget* sustentável, não há meios, não há direção".

Seguem-se duas dimensões "inibidoras": a "prevenção ativa", que é composta por superfície externa, superfície interna, *supply chain* e pessoas; e a "proteção ativa", que remete para quando não foi possível "inibir que um ataque se materializasse",



mas “pelo menos ficou contido” e “não se propagou excessivamente”.

Já a quarta dimensão “é uma que tem sido uma vergonha para a nossa profissão”: “não consigo inibir, não consigo conter, mas pelo menos detetei a tempo e horas e contrarespondi em tempo útil”. O CISO da Altice reforça que “a maior parte dos ataques que apareceram nos jornais foram detetados post factum”, sendo “fácil detetar um ataque quando a empresa está nas couves”.

Por fim, o quinto pilar é “saber recuperar a entidade”, nomeadamente o Active Directory.

“O CISO não pode ser o Pedro e o lobo”, remata José Alegria. “Ele tem que ser paranoico, mas contido, em silêncio, e tem de fundamentar a sua discussão com a comissão executiva com números, com métricas, com um sistema analítico sólido”.

ELEVAR O CONHECIMENTO

João Camões, Chefe da Divisão de Estruturas de Comunicações e Segurança da Secretaria-Geral da Economia, realça a necessidade de adotar uma “estratégia multi-facetada”, começando por, em primeiro lugar, realizar “uma avaliação das lacunas do conhecimento” e, “a partir desses resultados, ter programas de formação personalizados e imersivos”.

JOÃO CAMÕES, SEC. GERAL DA ECONOMIA

BRUNO MENDES, DELL

“Passar a cibersegurança para a ordem do dia” é um passo importante para elevar o conhecimento sobre a ciber-resiliência, consistindo em “não criar eventos nem formações que são atos isolados, mas ter um processo contínuo de aprendizagem”. Para João Camões, isto é algo que “não acontece na cultura organizacional de muita das nossas organizações, quer sejam privadas quer sejam públicas”.

Relativamente ao estado da ciber-resiliência na administração pública, revela que existem “dificuldades naturais porque temos vários procedimentos que ainda são mais ou menos arcaicos”. A “falta de cultura organizacional e uma falta de cultura cívica” aplicada às temáticas de ciber-resiliência é um “problema” entre organizações públicas e privadas.

COM O APOIO DA FORTINET

ZERO-TRUST E SASE:

A ERA DE "NÃO CONFIAR CEGAMENTE NO UTILIZADOR"

A ASSOCIAÇÃO NACIONAL DAS FARMÁCIAS, O BANCO CTT, A CUF E A FORTINET JUNTARAM-SE NA TERCEIRA MESA-REDONDA DA IT SECURITY CONFERENCE 2023 PARA DEBATER A TEMÁTICA DE ZERO-TRUST E SASE

POR RITA SOUSA E SILVA

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

As sessões de tarde da 2.ª edição da IT Security Conference arrancaram com uma mesa-redonda sobre zero-trust e SASE, onde profissionais de diversos setores – Associação Nacional das Farmácias, Banco CTT, CUF e Fortinet – se juntaram para discutir as principais vantagens e desafios da adoção destas tecnologias pelas organizações.

Paulo Pinto, Securing Cloud and Business Transformation da Fortinet, ficou a cargo de enquadrar o conceito de zero-trust, que considera ter sido impulsionado por dois fenómenos: "um foi a desmaterialização do posto de trabalho e o outro foi a desmaterialização da computação".

Atualmente, qualquer colaborador "tanto pode estar em casa, como pode estar num escritório em Espanha, como pode estar em viagem". Esta mobilidade urge um maior controlo do utilizador "que está a aceder aos recursos da organização, que tipo de dispositivo está a usar, se é dele ou se não é, se está numa zona pública".

É perante a "infinidade de conexões" que surge o Zero Trust Network Access (ZTNA) como "um proxy que faz a ligação entre esta mobilidade do utilizador do dispositivo aos sítios onde quer chegar, aos tais software-as-a-service", explica Paulo Pinto.

As tecnologias de zero-trust e SASE podem ser essenciais na estratégia de segurança das organizações num cenário laboral em contínua transformação. "Antes, tinha 10-15% da minha organização que se ligava por VPN e agora tenho 100% da organização, porque em quase todos os sítios temos modelos híbridos de trabalho ou modelos de teletrabalho", afirma Carlos Silva, Diretor de Segurança e Proteção de Dados do Banco CTT. "A utilização destas tecnologias vem claramente reduzir o risco para as organizações".

Nuno Neves, Chief Security Officer da ANF, sublinha o "conceito de não ser binário" do zero-trust. "Eu tenho um utilizador, ele autenticou-se e não é por isso que agora tem acesso a tudo o que teria. Consigo pôr uma série de condições, mais uma série de requisitos", explica. "Passo a não confiar cegamente que aquele utilizador é correto e vai fazer aquilo que é suposto".

Em particular, o setor da saúde exige "outro tipo de cuidados em que não podemos pôr certo tipo de informação em provedores externos, tanto por motivos legais como por motivos de ética", reforça Miguel Gonçalves, CISO da CUF.

MULTICLOUD E ZERO-TRUST

A vasta panóplia de opções de cloud e de múltiplos modelos de serviço é "um desafio adicional" e, ao mesmo tempo, "um *driver*", constata Carlos Silva. "Cada um tem um cloud provider e temos vários serviços em várias clouds. Muitas vezes nem sequer sabemos bem em que cloud é que estão".

Para Carlos Silva, é fundamental garantir duas características: a "observabilidade do que está a acontecer", ou seja, "não me interessa ter uma consola que sirva para ver a minha cloud A, outra para ver a cloud B ou cloud C", sendo necessário "ter isto num único sítio"; e, por outro lado, a "componente de

MIGUEL GONÇALVES, CUF

PAULO PINTO, FORTINET

gerir os utilizadores que acedem a esses serviços".

"Em multicloud ou em ambientes totalmente distribuídos em que o conceito de perímetro deixa de existir, não faz qualquer sentido não termos implementado uma estratégia de zero-trust", acrescenta.

O zero-trust "vale para tudo", segundo Nuno Neves, contribuindo para fortalecer a segurança dos ambientes cloud ou multicloud. "O facto de nós termos numa só cloud ou em várias clouds, mas mantermos nós o controlo sobre os utilizadores, sobre os acessos e sobre quem é que acede ao quê, porquê, de onde, com que condições, acho que é fundamental".

Miguel Gonçalves acredita que "a falta de recursos" é um "grave problema". O CISO acrescenta que, "se não tivermos algo que faça essa gestão por nós, tínhamos de ter uma equipa gigante. Temos de agarrar naquilo que a tecnologia nos pode oferecer para nos ajudar a fazer essa gestão".

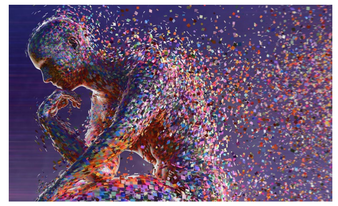
Existe ainda "muita falta de maturidade nas companhias portuguesas" relacionada com o mapeamento dos perfis de utilizadores, de acordo com Miguel Gonçalves. "Sem termos esses perfis bem mapeados, esse trabalho de consultoria feito, não há zero-trust que resista", defende.

Paulo Pinto reforça que "não se trata só da questão operacional, trata-se da questão de poder demonstrar compliance em tempo real nas diversas operações que fazem".

MUDAR MENTALIDADES TOP-DOWN

A adoção das tecnologias zero-trust e SASE exige uma mudança de mentalidades, onde a maior resistência é sentida "no topo", refere Carlos Silva.

Explicar aos executivos superiores – quem "banca a festa" – "a ideia de que a partir de agora nós não confiamos em nada nem em ninguém, nem na nossa própria rede interna" é um "desafio". No entanto, "a partir do momento em que consiga pôr os principais responsáveis, administradores, diretores, team leaders, todo o resto da organização vai atrás e vai aceitar como sendo um benefício para todos".



COM O APOIO DA CYBERSAFE

SERVIÇOS CRÍTICOS E OPERAÇÕES DE SEGURANÇA:

"A CIBERSEGURANÇA NÃO PODE SER VISTA COMO O BOMBEIRO DA EMPRESA"

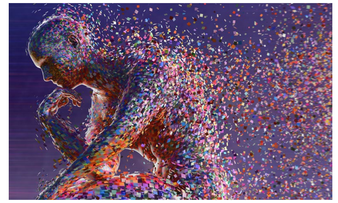
A CIBERSEGURANÇA AO NÍVEL DOS SERVIÇOS CRÍTICOS E DAS OPERAÇÕES DE SEGURANÇA TEVE EM DESTAQUE NA ÚLTIMA MESA-REDONDA DA IT SECURITY CONFERENCE 2023, QUE CONTOU COM A PARTICIPAÇÃO DO BANCO DE PORTUGAL, DA REN, DA EE-ISAC E DA CYBERSAFE.

POR MARTA QUARESMA FERREIRA

A última mesa-redonda da IT Security Conference 2023 teve como tema "Serviços Críticos e Operações de Segurança" e contou com as visões e experiências de Pedro Rodrigues, Head of Cybersecurity and IT Compliance do Banco de Portugal, Rafael Aranha, Head of Cybersecurity da REN, Aurélio Blanquet, Secretary General EE-ISAC e Dinis Fernandes, Executive Manager da Cybersafe.

Ao nível da regulação, Rafael Aranha começou por explicar que a REN opera em Portugal sob um conjunto de regulamentos – NIS1, Regulamento de Segurança da Anacom, ENTSO-E - que garantem a "segurança do abastecimento e a segurança do mercado elétrico". O aparecimento da diretiva NIS 2 contribuiu para complementar a responsabilidade de gestão de risco e a área da formação. "Felizmente tem aparecido alguma regulação, mas as regulações têm de casar umas com as outras", alerta o Head of Cybersecurity, considerando, no entanto, que existe aqui um desafio na forma como as regulações se relacionam umas com as outras.

Da experiência de Dinis Fernandes, a regulação tem-se revelado como um "catalisador e um simplificador" para que os Conselhos de Administração e Direções das empresas tenham os mesmos objetivos ao nível da cibersegurança. "Quando temos o mesmo objetivo aparece o *budget* para fazer projetos, aparece a vontade para as várias áreas interagirem", constata. No que à NIS 2 diz



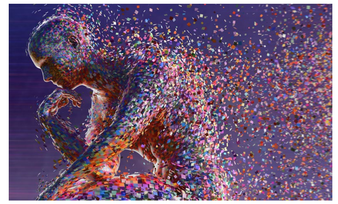
PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

respeito, o Executive Manager olha para a diretiva como um 'empurrão' para que cada vez mais setores cumpram os requisitos exigidos e aumentem, assim, a sua cibersegurança.

Sobre a NIS 2, e no âmbito da sua aplicação ao nível dos serviços e infraestruturas críticas, Aurélio Blanquet destaca e reforça também a importância do alargamento da diretiva para outros setores, assim como dentro do âmbito de aplicação em cada um dos setores. "A cibersegurança passou a fazer parte da mesa do *board*, mas é um movimento recente, deixou de ser um tema de IT, mas não é uma coisa muito sentida pelo negócio, e vai ter de passar a ser porque a NIS 2 assim o impõe", remata o Secretary General da EE-ISAC, a associação sem fins lucrativos estabelecida em Bruxelas que se destina à partilha de informação e análise de informação sobre segurança, com o objetivo de criar uma comunidade para troca de informações. Desta forma, a NIS 2 vem também alavancar a necessidade de aumentar a partilha e a cooperação ao nível europeu, dentro de cada setor e intra-setores, assegura Aurélio Blanquet, antevendo que a nova diretiva leve ainda as empresas a assumirem o treino e a sensibilização necessária dos seus recursos.

PROTEÇÃO EM SERVIÇOS CRÍTICOS E A CIBERSEGURANÇA PARA LÁ DA RESPOSTA A INCIDENTES

Ao nível da cibersegurança e da proteção de infraestruturas críticas, Pedro Rodrigues defende que é "essencial ter na raiz a identificação do que



são os sistemas críticos, como é que os vamos proteger e isso implica sempre algum nível de isolamento", esclarecendo que a exposição nos sistemas críticos não deverá ser igual aquela observada nos sistemas públicos. O Head of Cybersecurity and IT Compliance do Banco de Portugal relembra que as equipas de cibersegurança das organizações não devem perder de vista aquilo que são os ativos/sistemas críticos.

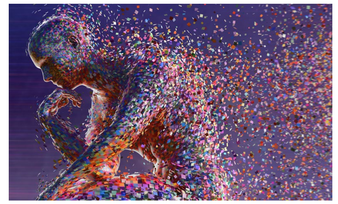
"A cibersegurança não pode ser vista como o bombeiro da empresa", frisa Rafael Aranha, que acrescenta que a cibersegurança necessita de ser "transversal aos processos de negócios", não podendo "ser vista como uma área vertical de uma empresa" ou como uma área de gestão de incidentes.

PEDRO RODRIGUES, BANCO DE PORTUGAL

RAFAEL ARANHA, REN

O PAPEL DA IA NA DEFESA DAS ORGANIZAÇÕES

Com toda a atenção de que tem sido alvo, a inteligência artificial pode, na perspetiva de Pedro Rodrigues, "ajudar a atingir um objetivo de otimização e de funcionamento muito mais eficiente do ponto de vista da defesa". É necessário criar ambientes de testes, perceber as mais-valias, escolher o use case para resolver. Porém, o Head of Cybersecurity considera que as infraestruturas críticas podem não ser o "ambiente certo" para este tipo de testes com IA, sendo necessário escolher bem o use case e ganhar confiança nas ferramentas. "Vai potenciar as nossas capacidades defensivas e vai-nos aproximar um pouco daquilo que são as capacidades ofensivas com as quais temos de lidar todos os dias", reitera.



TENDÊNCIAS AO NÍVEL DE OPERAÇÕES DE SEGURANÇA

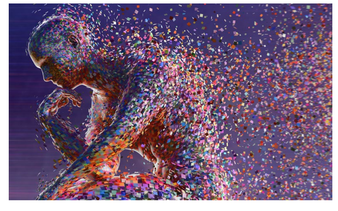
A trabalhar em centros de operações de segurança (SOC) desde 2007, Dinis Fernandes tem assistido a uma evolução nesta ferramenta. "Nos últimos dois anos as operações de segurança mudaram mais do que nos últimos 15. Há esta dificuldade que toda a gente conhece com a falta de analistas de segurança, falta de pessoas qualificadas", indica o Executive Manager que, por outro lado, destaca o número crescente de alertas que os SOC recebem. Os problemas elencados têm provocado o surgimento de alguns produtos, entre eles a introdução de ferramentas XDR e MDR, que acrescentam ao SOC uma capacidade de reposta a incidentes, alargando o ambiente e atuação do mesmo.

AURÉLIO BLANQUET, EE-ISAC

DINIS FERNANDES, CYBERSAFE

COOPERAÇÃO COMO FERRAMENTA NA RESPOSTA A INCIDENTES

A encerrar a mesa-redonda, Aurélio Blanquet destaca a partilha de informação como essencial na melhoria da resposta individual a incidentes de segurança. "Além da defesa, no sentido da deteção, da resposta e da recuperação a incidentes, o next step é, pelo menos, não estarmos um passo atrás daquilo que é a comunidade que nos tenta agredir, é começarmos a pensar em cibersegurança preventiva", defende, concluindo que cada um deve "trabalhar em prol do grupo para que depois, no retorno, cada um de nós possa trabalhar melhor para si mesmo".



" EM TERMOS DE GRANDE CRESCIMENTO ESTÁ A CIBERSEGURANÇA E A IA NOS PRÓXIMOS ANOS"

PAULO VIEIRA, COUNTRY MANAGER DA PALO ALTO NETWORKS, TROUXE À IT SECURITY CONFERENCE 2023 UMA APRESENTAÇÃO SOBRE O IMPACTO DA IA NA CIBER-RESILIÊNCIA DAS ORGANIZAÇÕES.

A manhã da 2.ª edição da IT Security Conference, que teve lugar no dia 12 de setembro, contou com os insights de Paulo Vieira, Country Manager da Palo Alto Networks, sobre o impacto da Inteligência Artificial (IA) no setor da cibersegurança, particularmente na ciber-resiliência das organizações.

"Acho que estamos num ponto de viragem no mercado da cibersegurança", começou por dizer Paulo Vieira, dando início à sua apresentação executiva sobre Machine Centric for Human Augmentation.

Paulo Vieira destaca como preocupante a "galopante" rapidez dos cibercriminosos na execução de ataques nos últimos anos: "entre o tempo de entrada para dentro da infraestrutura e o tempo de exfiltração, em 2021, contámos com 44 dias; em 2022, 30 dias; em 2023, 5 dias e, neste momento, estamos em horas".

Cada vez mais são publicadas notícias sobre o potencial da IA no cenário de

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

PAULO VIEIRA, PALO ALTO NETWORKS

ciberameaças, refere, possibilitando o aumento da velocidade das atividades maliciosas para quase em tempo real e expandindo a sua abrangência. Apesar dos esforços da União Europeia (UE) e dos Estados Unidos em implementar guidelines jurídicas sobre a utilização das tecnologias de IA, "não existe legislação ainda" e, mesmo assim, "os maus não vão seguir as guidelines".

Neste contexto, com a sua apresentação, Paulo Vieira visa dotar a audiência com a capacidade de responder a três diferentes questões: como é que as organizações conseguem melhorar a sua ciber-resiliência? Como é que a IA vai conseguir melhorar essa ciber-resilência? E quais são alguns exemplos práticos da IA em cibersegurança?

COMO É QUE AS ORGANIZAÇÕES CONSEGUEM MELHORAR A SUA CIBER-RESILIÊNCIA?

Atualmente, as organizações estão a sentir "um gigante salto em termos de superfície de ataque, um overload de dados, o nosso ponto de trabalho espalhado por todo o lado, problemas de supply chain e a parte de compliance", retrata Paulo Vieira o panorama da cibersegurança.

> "EU NÃO CONHEÇO NENHUM CLIENTE QUE ESTEJA SATISFEITO COM O SEU SIEM".

Para o Country Manager da Palo Alto Networks, uma organização só tem conhecimento do seu nível de ciber-resiliência se o conseguir efetivamente medir. "Há uma pergunta que eu faço em muitas reuniões de board e de direção: qual é o tempo que vocês demoram a detetar e qual é o tempo que vocês demoram a resolver um problema de segurança?", conta. "A maior parte das vezes não sabem responder. Se não conseguimos responder, não conseguimos medir. Se não conseguimos medir, não conseguimos melhorar".

Em Portugal, o mean time to detect (MTTD), em média, está nos 287 dias, explica Paulo Vieira, reforçando que este facto representa "287 dias que os maus estão dentro da vossa infraestrutura e vocês não sabem", dirigindo-se a uma plateia de profissionais de cibersegurança.

Neste sentido, o colaborador da Palo Alto Networks apresentou os quatro níveis de maturidade de ciber-resilência de uma organização, sendo que o primeiro remete para ações reativas e manuais, assente em políticas díspares. "Somos bombeiros, não temos noção e estamos a tentar fazer melhor com aquilo que temos", refere.

No segundo nível, "começamos a ter uma política mais orientada", com um framework de segurança parcialmente integrado, mas ainda "sem qualquer tipo de integração ainda com várias peças". Por sua vez, o terceiro assenta numa ciber-resiliência res-

ponsiva, onde existe uma melhor integração e visibilidade e "começamos a ter governança".

O quarto e último patamar "já está automatizado, já conseguimos integrar as peças todas e conseguimos tirar valor acrescentado de todas", com base numa ciber-resiliência proativa. "Obviamente que existem muito poucas empresas que conseguem estar no quarto estado", conclui Paulo Vieira, revelando que a maioria das organizações se encontram no primeiro ou segundo nível.

COMO É QUE A IA VAI CONSEGUIR MELHORAR ESSA CIBER-RESILÊNCIA?

O Country Manager da Palo Alto Networks considera que "a IA está na rampa de lançamento em todo o lado", motivado especialmente pelo investimento empregue nesta tecnologia. "Em termos de grande crescimento está a cibersegurança e a IA nos próximos anos".

Paulo Vieira explica de que modo a IA pode melhorar a ciber-resiliência das empresas, como prevenir de forma precisa as ameaças em tempo real, automatizar as operações de segurança e mitigar situações de fraude em tempo real, assim como reduzir a superfície e impacto de um ataque.

Por outro lado, a IA possibilita a mitigação dos riscos das organizações, impulsionando a proatividade das próprias plataformas, a consolidação com parceiros estratégicos orientados por IA e a redução dos custos operacionais. Além disto, as tecnologias de IA permitem "começar a consolidar e proativamente identificar problemas de compliance em tempo real".

QUAIS SÃO ALGUNS EXEMPLOS PRÁTICOS DA IA EM CIBERSEGURANÇA?

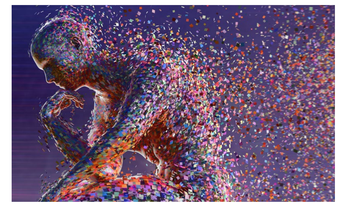
"Eu não conheço nenhum cliente que esteja satisfeito com o seu SIEM", revela Paulo Vieira, referindo que esta é uma tecnologia existente há mais de duas décadas.

Atualmente, existe um trabalho manual repetitivo no setor de cibersegurança, onde o analista é "o centro do mundo", cujas funções passam pela deteção, investigação e resposta e pela analítica, tendo ainda "um chapéuzinho de automação em cima", que é a "componente que não funciona". Para Paulo Vieira, "isto leva a uma atrição gigante neste mercado em que ninguém quer trabalhar nele".

"Nós temos que inverter esta pirâmide", defende o profissional da Palo Alto Networks. "Temos que introduzir toda a parte de automação a fazer o trabalho pesado, introduzir toda a parte analítica de IA e ML, fazer toda a parte de deteção, investigação e resposta, e o analista só tem que tomar a decisão de barra ou não barra".

"Começar a pôr robôs a fazer esse trabalho que os humanos vão ter mais dificuldade e mais trabalho para fazer", conclui. Um exemplo é o XSIAM da Palo Alto, concebido com IA, que reimagina o SOC. Pegando no caso de um cliente, Paulo Vieira, mostra que 86 incidentes são automatizados sem intervenção humana e apenas 16 são manuais, necessitando de intervenção humana para tomar uma decisão.

"O grande problema neste momento são os dados", aponta Paulo Vieira, destacando que, no XSIAM, 73% dos dados estão a ser automatizados no exemplo demonstrado.



HPE aruba networking

“É NECESSÁRIO REVER A FORMA COMO AS REDES SÃO DESENHADAS”

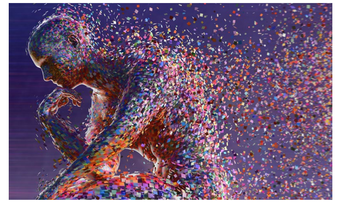
A APRESENTAÇÃO DE PAULO RIO, NETWORK AND SECURITY CONSULTING DA HPE ARUBA NETWORKING, DEBRUÇOU-SE SOBRE COMO A REDE DE EDGE, COMPLEMENTADA COM SERVIÇOS EM CLOUD, PODERÁ FORTALECER A SEGURANÇA DAS ORGANIZAÇÕES.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

PAULO RIO, HPE ARUBA NETWORKING

Na 2.ª edição da IT Security Conference, a apresentação executiva de Paulo Rio, Network and Security Consulting da HPE Aruba Networking, focou-se em Edge to Cloud Security, explicando como é que a rede de Edge poderá ajudar a melhorar os níveis de segurança das organizações, assim como de que forma é que estas infraestruturas podem ser complementadas com serviços em cloud.

Face ao “arsenal de controlos de segurança” que as empresas têm a seu dispor, existem uma variedade de ferramentas que atuam em diferentes camadas. Em particular, Paulo Rio realça a componente de rede, que desempenha “um papel estratégico porque se situa precisamente na intersecção entre o tráfego dos endpoints e dos workloads”, situando-se numa posição privilegiada para que “as equipas de governance que definem as políticas de segurança possam fazer enforcement nesse ponto estratégico da infraestrutura”.



Um desenho adequado das infraestruturas, acompanhado pela capacitação das ferramentas e motores de segurança nesta camada, possibilitará "reduzir a superfície de ataque a que a infraestrutura está sujeita", "conter as ameaças" e "limitar os ataques de movimento lateral".

REDESENHAR AS REDES

O primeiro "ingrediente" no desenho de uma infraestrutura de rede segura assenta nos atributos de segurança. No entanto, este "não pode ser visto uma maneira isolada", considerando apenas a segurança, uma vez que, se uma organização abdicar de outros "atributos de qualidade", "poderemos estar a comprometer o nível de segurança final da infraestrutura de rede".

Neste sentido, Paulo Rio destaca dois pontos adicionais necessários para uma arquitetura de rede. A "capacidade avançada de gestão e desejavelmente simplicidade" é indispensável, visto que a sua ausência significa que "provavelmente as equipas de operação ficarão com o ónus de operar redes complexa", o que poderá "comprometer o nível de segurança".

O segundo aspeto identificado é a "a flexibilidade e agilidade que essas redes de Edge devem proporcionar às organizações". Ao longo do tempo, as redes e os próprios negócios vão sofrendo transformações e, com isso, "as necessidades e os desafios que as organizações sentem vão sendo crescentes".

Atualmente, as organizações enfrentam um número de "desafios constantes", particularmente a "problemática da mobilidade" e o "crescimento de novos dispositivos a ligarem-se à rede, como é o caso de IoT". Por outro lado, a tendência é a movimentação em parte ou total dos workloads das empresas para a cloud, afirma o profissional da HPE Aruba Networking. "Todo este processo transformativo obviamente traz desafios às organizações, mas também traz oportunidades".

Desta forma, perante as ameaças crescentes e as transformações que as organizações vão enfrentando, Paulo Rio acredita que "é necessário rever a forma como as redes são desenhadas".

Redesenhar as redes implica a sua divisão em três camadas: a camada de acesso, "onde os utilizadores e os workloads se ligam"; a camada intermédia, que serve de gateway e onde é feita a interface com os serviços de WAN, bem como onde residem os sistemas de routing e de firewall; e a camada cloud, onde estão "os serviços de valor acrescentados ou com maior exigências, que não têm normalmente a possibilidade de correr on prem e, por esse motivo, foram movimentados para a cloud".

No entanto, Paulo Rio considera que, em primeiro lugar, é essencial "tornar a segurança algo omnipresente, independentemente da camada em que estejamos a falar" e "dotar as infraestruturas de capacidades de gestão, monitorização,

automação, policy avançados". Este último assenta no fenómeno de migração dos serviços para a cloud, cada vez mais adotado pelas empresas, visando "tentar tirar partido da elasticidade que os ambientes cloud oferecem".

Com esta restruturação das redes, "todas as camadas passam a estar dotadas de capacidades e motores de segurança para fazerem a contenção das ameaças", explica. Do ponto de vista prático, existirão "vários ambientes que desejavelmente deverão ser geridos a partir de um ponto central, com uma única política de controlo de acessos".

SEGURANÇA ZERO TRUST E SASE

De acordo com Paulo Rio, existem duas abordagens relativas à adoção destas tecnologias: uma abordagem de monofabricante ou a combinação de vários fabricantes, que é a "realidade mais comum", sendo necessária a agilidade e flexibilidade da infraestrutura.

Relativamente à implementação de redes Zero Trust, o colaborador da HPE Aruba Networking explicou à audiência de que forma é que se pode potenciar as redes de acesso para proporcionar a microsegmentação.

"Quando falamos em Zero Trust, falamos em acessos controlados a cada dispositivo que aceda à infraestrutura", refere. Alguns exemplos referidos foram a microsegmentação em que o controlo é feito no ponto em que o dispositivo se liga, a centralização do tráfego de modo que esse controlo seja feito num ponto central, e a distribuição desse controlo entre os equipamentos que estão na infraestrutura.

Além disto, é essencial ter "a possibilidade de combinar várias formas de microsegmentação e eventualmente até conjugá-las", uma vez que as necessidades variam de organização para organização.

Para oferecer a capacidade de microsegmentação a data centers, Paulo Rio aponta não só o "controlo entre hosts físicos", mas também "a necessidade de fazer o controlo dos hosts que estão virtualizados". O contributo da infraestrutura de edge é o facto de permitir este "controlo fino e avançado do tráfego que flui entre workloads".

POLÍTICAS DE SEGURANÇA

Por fim, Paulo Rio reforçou a importância da aplicação das políticas de segurança nas infraestruturas de rede de uma organização. "É importante que as ferramentas de gestão que instrumentalizam e configuram a infraestrutura de rede tenham a capacidade de fazer e implementar políticas de segurança o mais mapeadas possível com as políticas formais que a organização definiu", sublinha.

Estas políticas de segurança, refere, são compostas por dois grandes "building blocks": o contexto e as condições de acesso; e, perante estas, é aplicado um conjunto de "enforcement profiles", que são os "motores de controlo que cada equipamento possui".

SOPHOS

" UMA DAS GRANDES LACUNAS É A CAPACIDADE DE RESPONDER COM RAPIDEZ SUFICIENTE"

CHESTER WISNIEWSKI, FIELD CTO APPLIED RESEARCH DA SOPHOS, REFORÇOU A IMPORTÂNCIA DO TEMPO NA DEFESA CONTRA CIBERAMEAÇAS NO PALCO DA 2.ª EDIÇÃO DA IT SECURITY CONFERENCE.

A expressão "um luxo a que não nos podemos dar" serviu de mote para a apresentação executiva de Chester Wisniewski, Field CTO Applied Research da Sophos, referindo-se à importância do tempo na deteção de ameaças e na resposta a incidentes.

"Os criminosos estão a tornar-se cada vez melhores e melhores a reduzir a quantidade de tempo necessária para fazer aquilo que fazem quando invadem as nossas redes e tentam roubar as nossas informações", afirma.

Na última década, observou-se uma mudança no panorama das ciberameaças, impulsionada particularmente pela especialização dos criminosos. "Há 10-15 anos, um grupo criminoso poderia ser composto por dois ou três indivíduos. Existiam muitas tarefas envolvidas e, como eles estavam a realizá-las todas, não eram muito eficientes nelas", relembra.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

CHESTER WISNIEWSKI SOPHOS

“UM DOS MEUS RECEIOS EM PAÍSES QUE TÊM SIDO MENOS VISADOS PORQUE OS CRIMINOSOS NÃO TÊM COMPETÊNCIAS PARA ESCREVER ATAQUES DE ENGENHARIA SOCIAL BEM ELABORADOS CONTRA OS NOSSOS UTILIZADORES, É QUE ESSA ÚLTIMA BARREIRA FOI REMOVIDA AGORA PORQUE ELES PODERÃO UTILIZAR ESTES MODELOS GRÁTIS”,

Atualmente, tudo pode ser everything-as-a-service, sendo que o nível de lucros obtidos com um ataque, especialmente de ransomware, aumentou substancialmente e, como consequência, “tudo começou a transformar-se numa especialização do lado criminoso”.

À medida que se especializam, os cibercriminosos estão cada vez mais "rápidos" e "eficientes". "Uma das grandes lacunas que estou a ver na nossa base de clientes é a capacidade de responder com rapidez suficiente", revela Wisniewski. As equipas "podem estar a receber os alertas, mas não conseguem responder aos alertas antes que o ataque já tenha causado danos suficientes".

Além disto, a Inteligência Artificial (IA) é cada vez mais uma ferramenta ao dispor dos cibercriminosos, que estão ativamente à procura de formas para a utilizar em ataques, assim como as organizações estão a tentar utilizá-la para fortalecer a sua defesa.

Um exemplo indicado por Wisniewski são os ciberataques em Portugal, nomeadamente ataques de engenharia social, que são frequentemente orquestrados em português do Brasil, sendo, por isso, “muito fáceis de serem detetados pelas pessoas”. No entanto, “com coisas como os LLM – IA generativa, ChatGPT –, os criminosos podem escrever um português perfeito em português do Brasil ou em português de Portugal. Já não é um desafio e já não parece o Google Tradutor”.

“Um dos meus receios em países que têm sido menos visados porque os criminosos não têm competências para escrever ataques de engenharia social bem elaborados contra os nossos utilizadores, é que essa última barreira foi removida agora porque eles poderão utilizar estes modelos grátis”, alerta Wisniewski, não sendo necessário qualquer pagamento para “começar a criar ataques mais especializados para todos no mundo”.

APRENDER COM OS ERROS

De acordo com um relatório da Sophos, as três ameaças mais preocupantes para os profissionais de segurança no ciberespaço são: a configuração incorreta de ferramentas de segurança; as ameaças zero-days; e a escassez de competências e expertise internas sobre cibersegurança.

No entanto, as ameaças mais comuns verificadas pela Sophos nos casos de resposta a incidentes não aparecem no topo da lista. “Ainda estamos a lidar com passwords roubadas, vulnerabilidades não corrigidas e ferramentas de acesso

remoto expostas", indica Wisniewski. "Os zero-days são algo com que vale a pena preocupar-se, mas não é como as pessoas estão a ser vitimizadas. Elas estão a ser vitimizadas pelas lacunas".

ATAQUES OCORREM FORA DE HORAS

Mais de 80% dos ataques ocorrem fora do horário laboral das organizações visadas, independentemente do país em que o incidente aconteceu, apresenta Wisniewski. Dos ataques que decorreram durante o horário de trabalho, muitos foram durante o fim-de-semana.

"Se não tem operações 24/7, é improvável que alguém observe um ataque inicial, quando os criminosos costumam ser mais barulhentos".

A média do tempo de permanência dos cibercriminosos está gradualmente a diminuir, apontou o profissional da Sophos. Há três anos, era de 13 dias, enquanto atualmente é de oito. Nos casos de ransomware, diminuiu de nove para cinco dias.

"No primeiro dia, tudo o que fizeram foi invadir algumas credenciais e vaguear pela rede", afirma. "No terceiro dia, estão a transferir os dados para as clouds, onde os criminosos os podem explorar, manter como reféns e extorquir. Se não conseguir expulsá-los da sua rede até ao quinto dia, é quando eles explodem a bomba e criptografam os dados".

Antes de dar a sua apresentação por terminada, Chester Wisniewski deixa um conselho aos profissionais de cibersegurança. "Têm de responder rapidamente e com conhecimento do que precisam de fazer", remata. "O tempo é essencial".

LOGICALIS
Architects of Change

"É PRECISO ENTENDER A DIFERENÇA ENTRE CIBERSEGURANÇA E CIBER-RESILIÊNCIA"

LUÍS LANÇA, CTO DA LOGICALIS, REFORÇOU A IMPORTÂNCIA DE SABER DISTINGUIR CIBERSEGURANÇA DE CIBER-RESILIÊNCIA.

Luís Lança, CTO da Logicalis, explicou a importância de saber distinguir cibersegurança de ciber-resiliência para proteger ativos críticos numa época marcada por ameaças cada vez mais avançadas.

A cibersegurança "não está a mudar ao ritmo suficiente", especialmente no advento de "um novo campo estratégico", a IA generativa. Luís Lança ressalva dois "pêndulos": por um lado, "a componente de weaponização", ou seja, a forma como os cibercriminosos utilizam esta tecnologia; e, por outro, "entender aquilo que podemos fazer de bom", centrado em saber remediar vulnerabilidades e melhorar o "conhecimento dos nossos SOC analysts para responder a incidentes e preveni-los".

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

LUÍS LANÇA, LOGICALIS

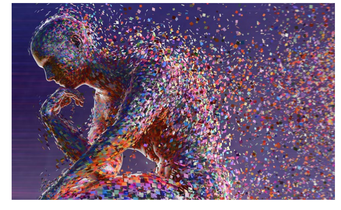
O fator-chave é reconhecer que cibersegurança e ciber-resiliência "não são iguais". "Quando foi feito um inquérito pelo World Economic Forum (WEF), 59% dos inquiridos disse que são sinónimos. Então há um trabalho a fazer: explicar dentro da organização a diferença entre as duas", sublinha.

"É importante entendermos que não podemos negligenciar um pós-ataque", afirma. "Nós temos de saber selecionar os dados que são críticos para uma rápida reposição das empresas em caso de ataque".

"Já temos um grande número que já está a pensar na resiliência", refere Luís Lança, ao analisar um relatório do WEF onde 53% das organizações afirmam ser "cyber resilient". No entanto, existe uma dificuldade dos decisores "top-level" em compreender a sua importância.

"Os CISO têm de estar no topo da mesa". Além disto, a conjugação do papel da resiliência com "segurança e outcome de negócio" é "fundamental".

redShift



“AMEAÇAS MAIS PROFUNDAS ÀS ORGANIZAÇÕES VÊM DE VULNERABILIDADES CONHECIDAS HÁ MUITO TEMPO”

A GESTÃO DA EXPOSIÇÃO CIBERNÉTICA TORNOU-SE FUNDAMENTAL PARA A ANTECIPAÇÃO E REDUÇÃO DE RISCOS, DIZ JOSÉ ALARCON, DA TENABLE E PARCEIRO DA REDSHIFT.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

Segundo José Alarcon, Country Manager Spain & Portugal da Tenable e Parceiro da RedShift, a gestão da exposição cibernética é essencial nos atuais ecossistemas convergentes de IT, OT, cloud e identity.

As organizações estão expostas a três tipos de riscos – operacional, financeiro e cibernético – que estão “todos integrados”, explica Alarcon. “Um risco cibernético pode colocar em perigo a nossa organização inteira”.

A superfície de ataque está a “aumentar dramaticamente”, existindo “muitos mais tipos de dispositivos e ameaças” que facilitam o alcance dos invasores. “Não é uma questão de se foi violado ou não, é de quando será violado. Em algum momento ou outro haverá uma violação”, garante.

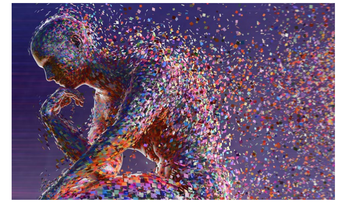
JOSÉ ALARCON, REDSHIFT

A “origem do problema” é o facto de um sistema poder ser comprometido “através de uma vulnerabilidade ou configuração incorreta”. É “impossível” que uma organização consiga “gerir potencialmente cem novas vulnerabilidades por dia útil”. “Não há analistas nas vossas equipas que consigam tratar disto”, adverte Alarcon.

“Muitas das ameaças mais profundas às nossas organizações vêm de vulnerabilidades conhecidas há muito tempo que simplesmente não foram tratadas corretamente”, afirma.

As organizações têm de “comunicar adequadamente” entre si e “ser capaz de mostrar à sua gestão onde está o efeito real no negócio”.

arcserve®



COMO CONSEGUIR A "IMUTABILIDADE DE DADOS"

VASCO SOUSA, TERRITORY ACCOUNT MANAGER DA ARCSERVE, LEVOU AO PALCO DA IT SECURITY CONFERENCE A TEMÁTICA DA PRESERVAÇÃO E IMUTABILIDADE DOS DADOS CRÍTICOS DE UMA ORGANIZAÇÃO.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

VASCO SOUSA, ARCSERVE

A apresentação de Vasco Sousa, da Arcserve, centrou-se em como preservar a integridade dos dados críticos de uma organização.

Vasco Sousa salientou a importância de trazer o conceito de "air gap" para as organizações, consistindo em "termos dados que estão completamente segregados para, numa última linha, poder vir a recuperá-los em caso de necessidade". O air gap físico remete para "onde de facto não há ligação nenhuma, é algo que está offline", enquanto o air gap virtual é "onde eu tomo algumas medidas de forma que estejam segregados esses dados".

Vasco Sousa forneceu três alternativas para conseguir a imutabilidade dos dados. As tapes configuram o "air gap físico" e "obrigam a ter rotinas de pegar nas tapes e levar para um cofre offline". Já o object lock significa que "aquilo que eu gravo não volta a ser passível de ser nem editado, nem rescrito, nem sequer apagado" e o recurso à cloud pode ser problemático quando "tenho volumes de dados muito grandes". O object-storage-on-prem possibilita "trazer para dentro do nosso data center as tecnologias de object lock".

Desenhar um plano de recuperação de desastres deverá passar pela definição dos conceitos de RPO, referente a "quantos dados é que eu estou disposto a perder", e de RTO, que é "o tempo que vou levar a recuperar se eu tiver uma falha neste momento".

De seguida, é necessário "catalogar a minha informação" e distinguir quais são os dados importantes.

Por fim, os "testes de verificação" são a "melhor" – aliás, a "única" – forma de "verificar que os backups estão passíveis de serem recuperados". Estes funcionam como um "simulacro", permitindo "formar as equipas para estarem preparadas para uma situação de um ciberataque" e descobrir "falhas de cobertura".

“A SEGURANÇA ESTÁ NO CAMINHO CRÍTICO DO NEGÓCIO DIGITAL”

RUI BARATA RIBEIRO, SECURITY SALES LEADER DA IBM, FOCOU-SE NA UTILIZAÇÃO DA SEGURANÇA PARA RENTABILIZAR AS ATIVIDADES DE UM NEGÓCIO.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

Rui Barata Ribeiro, da IBM, abordou a forma como a segurança pode ser utilizada para “suportar as atividades de negócio” e “monetizar a relação com os clientes”

Num estudo realizado pela IBM em 2022, 96% dos líderes de segurança identificaram um problema “na relação com os seus clientes que tem que ver com o processo da autenticação, o processo de criação de uma identidade de um cliente num portal”.

“O cliente digital online é frequentemente impiedoso e, uma vez que há uma grande oferta, é muito fácil para ele mudar de fornecedor”, alerta.

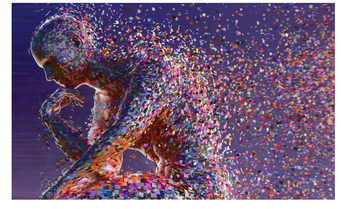
Atualmente, existe uma “relação direta entre a adoção digital e o nível de segurança percebido”. Para Rui Ribeiro, “a segurança está no caminho crítico do negócio digital”.

“Quanto mais um serviço for percebido como seguro, mais ele é adotado pelos clientes”, especialmente no que diz respeito ao mobile. “Quanto mais tiver a capacidade de passar segurança ao meu cliente final, mais eu tenho capacidade de vender”, sublinha.

As “grandes linhas mestras” da área de Consumer Identity Access Management são: “como introduzir a identidade nos meus processos de negócio; como verificar essa mesma identidade da forma menos intrusiva possível; e como criar uma arquitetura que me permita gerir o futuro aplicacional ou o futuro da tipologia de acesso dos utilizadores às aplicações”.

O elemento da privacidade dos dados dos utilizadores é essencial, sendo um dos principais motivos da não adoção destas tecnologias. “Se houver uma probabilidade de a pessoa ser impersonada negativamente, vai evitar a adoção de tecnologia”, realça.

CATO NETWORKS



A CONVERGÊNCIA ENTRE CIBERSEGURANÇA E NETWORK

A TRANSFORMAÇÃO DE SEGURANÇA E REDE NUMA ABORDAGEM SINGLE-VENDOR DE SASE FOI O TEMA APRESENTADO POR MARIANA NUNES, DA CATO NETWORKS.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

MARIANA NUNES, CATO NETWORKS

A apresentação de Mariana Nunes, EMEA Internal Channel Account Manager da Cato Networks, procurou "explicar como está a ser transformado o universo de network e cybersecurity baseado no conceito de SASE, apresentado pela Gartner há alguns anos".

Ouviu-se falar pela primeira vez de Security Access Service Edge (SASE) em 2019, quando a Gartner publicou um relatório que incidia sobre a "dificuldade que o mundo estava a passar com essa quantidade de produtos e como seria o futuro que é a convergência entre os dois mundos: network e cybersecurity".

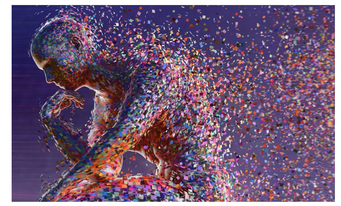
Neste sentido, Mariana Nunes explica que o conceito de SASE foi concebido com o intuito de "convergir todas as capacidades de SD-WAN, de cloud optimization, com todas as capacidades de cibersegurança que nós conhecemos, que hoje são múltiplos produtos, múltiplos vendors, e que vem criar dificuldade para a área de tecnologia".

Em 2022, a Gartner publicou uma outra investigação que não se centrava apenas em SASE, mas em "como ser um single-vendor, como entregar todas as capacidades de cibersegurança e todas as capacidades de network debaixo do mesmo guarda-chuva".

Recentemente, em agosto de 2023, foi lançado o "o tão querido quadrante mágico da Gartner", que "finalmente deu a patente para os nossos clientes e para as empresas em redor do mundo entenderem como é que o mercado funciona", refere.

No Magic Quadrant for Single-Vendor SASE, Mariana Nunes aponta que a Cato Networks é destacada com a posição de "challenger". "Um dos conceitos da Cato é a simplicidade", sublinha. "Não só vai conectar e assegurar, mas vai fazer isso de uma forma simples com uma consola de management".

S21SEC
Cyber Solutions by Thales



A TRANSPARÊNCIA É A "CHAVE" DA PURPLE TEAM

A APRESENTAÇÃO DE LUÍS CATARINO, OFFENSIVE SECURITY MANAGER DA S21SEC, DESTACOU OS DESAFIOS E VANTAGENS DA PURPLE TEAM.

Luís Catarino, da S21sec, abordou a estratégia de Purple Team nas organizações, identificando os seus desafios e vantagens.

A Purple Team "consiste numa abordagem colaborativa" entre a Red Team, cuja responsabilidade é a segurança ofensiva, e a Blue Team, que está encarregue da defesa, com o "objetivo principal" de "melhorar as capacidades de deteção e resposta".

DESAFIOS

O primeiro desafio da Purple Team é definir "qual é o momento mais apropriado" e a sua frequência, uma vez que "requer já uma elevada maturidade a nível de segurança".

As Red e Blue Teams são os recursos necessários, indica, reforçando a importância de "formar as equipas para que possam dar estas respostas e fechar este ciclo da melhor forma possível".

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

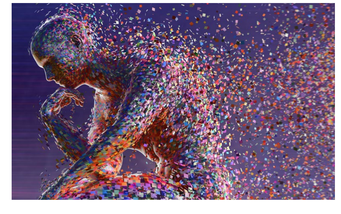
LUÍS CATARINO, S21SEC

Para o sucesso da Purple Team, a transparência é a "chave", sublinha, sendo essencial "que exista uma comunicação em tempo real, eficaz e que exista uma visibilidade total dos ataques por parte da Red Team e das deteções por parte da Blue Team".

VANTAGENS

Uma vantagem é ter "os incentivos alinhados", refere. "Se o ataque não foi bem-sucedido, temos aqui uma oportunidade de melhoria para a equipa que vai atacar. Se tivermos um ataque bem-sucedido, temos uma oportunidade de melhoria para quem está a defender".

Luís Catarino destaca ainda a melhoria da eficiência, bem como das métricas, permitindo ver "os ataques que foram detetados, os tempos de resposta, a informação forense disponível ou não disponível que temos nas nossas organizações".



visionware

“OS ATAQUES NÃO SÃO UMA QUESTÃO DE ‘SE’, SÃO UMA QUESTÃO DE ‘QUANDO’”

A ENTREVISTA A FILIPE CUSTÓDIO, PARTNER & BOARD MEMBER DA VISIONWARE, REFLETIU SOBRE AQUILO QUE UM SELO DE MATURIDADE DIGITAL EM CIBERSEGURANÇA SIGNIFICA PARA UMA ORGANIZAÇÃO.

Filipe Custódio, Partner & Board Member da VisionWare, subiu ao palco para uma entrevista sobre a importância dos selos de maturidade digital, após a organização se ter tornado “a primeira empresa privada com o selo Ouro”, na categoria de cibersegurança.

Os selos de maturidade digital, uma medida do Plano de Ação para a Transição Digital, “consistem em três categorias onde é possível as organizações privadas ou públicas se candidatarem a um grau de maturidade”: cibersegurança, sustentabilidade e acessibilidade.

“A cibersegurança é daquelas áreas que é muito difícil uma organização dizer que tem”, afirma Filipe Custódio. “É muito difícil alguém dizer ‘eu estou ciberseguro’ ou ‘eu tenho segurança nos meus sistemas de informação’. Eu estou seguro até ao dia em que tiver um ataque com sucesso. Os ataques não são uma questão de ‘se’, são uma questão de ‘quando’”

.

REQUISITOS EXIGENTES E DIFICULDADES

Um exemplo de um requisito para o nível Ouro de cibersegurança está relacionado com os ciberataques de phishing, nos quais “a segurança do meio humano é sempre a mais complicada e é aí que acontecem a maior parte dos ataques”.

O grau superior do selo de maturidade de cibersegurança “exige que as organizações façam exercícios de phishing à própria organização”, consistindo em “enviar mails a tentar enganar os próprios funcionários e que publique esses resultados internamente de uma forma didática”.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

FILIPE CUSTÓDIO, VISIONWARE

Para o Partner & Board Member da VisionWare, este critério foi "complicadíssimo" a nível jurídico. "Só para fazermos isto precisámos de algumas reuniões complicadas com os nossos advogados por causa do direito laboral", revela.

Filipe Custódio destaca três dificuldades na obtenção do selo Ouro: a dificuldade jurídica, considerando que "algumas medidas existem algum tipo de aconselhamento"; a aderência das pessoas devido a medidas que "exigem mudanças de comportamentos", apesar de isto não ter sido problemático para a VisionWare por ser "uma empresa bastante jovem"; e as dificuldades técnicas, uma vez que determinadas normas técnicas são "demasiado avançadas".

SELOS CONFEREM CONFIANÇA

Filipe Custódio destaca o conceito de 'supply chain security', o que significa que "a cibersegurança de uma organização é também influenciada pela cibersegurança dos seus fornecedores".

Neste contexto, a "confiança" dos clientes nas organizações é "fundamental". Mantê-la e impulsioná-la pode passar por encontrar "selos que possamos ter ou entidades autónomas que nos certifiquem de que fazemos tudo aquilo que é necessário para garantir a segurança dos nossos e dos dados dos nossos clientes".

"Quando alguém contrata serviços, está também a pôr a sua cibersegurança nas mãos desse fornecedor", refere. "A única forma de garantir que o fornecedor cumpre os mínimos requisitos de segurança é que ele tenha algum tipo de requisitos de maturidade".

O selo "dá alguma confiança acrescida sobre a consequência do ciberataque", destaca. Filipe Custódio menciona ainda um outro critério do selo de nível Ouro, que é a existência de "um SOC interno" e de "exercícios de resposta a incidentes de cibersegurança". "Isto mostra que a organização está preparada e responde adequadamente a estes desafios", reforça.

CONSELHOS AOS PARES

"A procura de níveis que certifiquem a vossa segurança interna deve ser o critério de sucesso da vossa função", aconselha, dirigindo-se a uma plateia de profissionais de cibersegurança. "Um bom CISO é aquele que analisa o nível de segurança da sua organização, planeia e diz 'daqui a dois anos quero a minha organização no nível superior'. O selo de maturidade digital pode ser a forma de certificar este nível".

Filipe Custódio sublinha também que "o suporte da gestão de topo é fundamental", cabendo "ao CISO saber comunicar isto convenientemente", pois poderá "haver resistência à mudança".

As organizações "devem ter como principal objetivo a mudança organizacional", conclui. "Não tanto o selo, mas conseguir mudar a organização para lá chegar e fazê-lo de uma forma estruturada e com sentido".

SOLUÇÕES DE CIBERSEGURANÇA TRADICIONAIS SÃO “PEÇAS DE PUZZLE QUE NÃO ENCAIXAM”

RUI ANTUNES, CYBERSECURITY SALES SPECIALIST DA CISCO, CENTROU A SUA APRESENTAÇÃO EXECUTIVA NOS ATUAIS DESAFIOS DO SETOR DE CIBERSEGURANÇA E NA RESPOSTA DO MERCADO.

Rui Antunes, da Cisco, focou-se nos desafios do trabalho híbrido e dos ambientes multicloud no setor de cibersegurança, bem como nas preocupações originadas pela resposta ‘patchwork’ do mercado.

Atualmente, os “os desafios da cibersegurança têm vindo a aumentar” e estão a tornar-se “cada vez mais complexos”. Para Rui Antunes, isto deve-se a um conjunto de fatores. No que aos utilizadores e dispositivos diz respeito, “destacaríamos os trabalhadores remotos, os dispositivos não corporativos que acedem à rede e os dispositivos de IoT”.

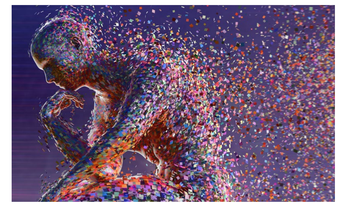
Ao nível das aplicações, refere “a public cloud e as aplicações SaaS”, acrescentando que, “se isso não bastasse, vemos um número maior de ataques cada vez mais sofisticados”.

Face aos crescentes desafios, o mercado “reagiu com soluções pontuais”, criando “para cada nova preocupação um novo produto”, suscitando consequentemente “preocupações adicionais”. Alguns exemplos apontados são a “má experiência para os utilizadores”, porque “têm de interagir com diversos softwares de segurança, diversos portais”, e a “complexidade de administração”.

As “falhas de segurança” foram o problema “mais grave” impulsionado pela ‘patchwork approach’ do mercado. “Essas soluções são como peças de puzzle que não encaixam uma nas outras e, no espaço entre elas, há lugar a serem exploradas por atacantes”, sublinha Rui Antunes.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

“A adoção de public cloud só veio agravar isto, porque cada public cloud tem os seus próprios controlos de segurança”, acrescenta.



sealpath

“AS MEDIDAS QUE ESTÃO APLICADAS SÃO FUNDAMENTAIS, MAS SE CALHAR NÃO SÃO SUFICIENTES”

JOÃO ARRIAGA, BUSINESS DEVELOPMENT MANAGER, CONSIDERA QUE PARA ALÉM DE CLASSIFICAR, É TAMBÉM NECESSÁRIO PROTEGER A INFORMAÇÃO DE ACESSOS MENOS PRÓPRIOS.

‘O futuro da classificação e segurança de dados’ foi o tema apresentado por João Arriaga, da SealPath.

Os dados empresariais são hoje partilhados sem controlo, muitas vezes à boleia do próprio negócio, o que potencia o risco de exfiltração e perda dos mesmos. “As medidas que hoje estão aplicadas são fundamentais, mas se calhar não são suficientes”, considera João Arriaga, que fala numa ausência do layer da proteção de dados, do conteúdo e acesso aos documentos e da sua classificação.

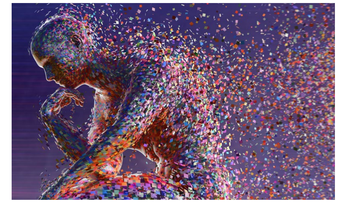
A SealPath estabelece quatro dimensões na classificação da informação: a sensibilidade e o nível de danos que pode causar à organização; os regulamentos; o tipo de dados; e disseminação.

A proteção da informação deve funcionar não só através da encriptação, mas também com uma camada de permissões nesta encriptação que vai permitir aos utilizadores lerem, escrevem ou imprimirem, independentemente do local onde se encontrem. “São proteções fundamentais”, reiterou João Arriaga, que destaca a necessidade de monitorização e autoria aos ficheiros protegidos.

Para a SealPath, é essencial classificar a informação para, desde logo, compreender o valor da mesma e saber onde se encontra; priorizar o que deve ser protegido; prevenir fuga de dados e aplicar a proteção adequada; otimizar a proteção de dados e facilitar a conformidade. Por outro lado, as aproximações teóricas, a utilização de etiquetas demasiado simples, o uso de demasiados níveis de classificação, a desvalorização de regras que as empresas têm de respeitar e a dependência excessiva da classificação por parte do utilizador estão entre as principais causas para a classificação de dados não funcionar.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

JOÃO ARRIAGA, SEALPATH



“AS SOLUÇÕES DE MFA SÃO MAIS ECONÓMICAS E RESOLVEM GRANDE PARTE DOS ERROS HUMANOS”

CARLOS VIEIRA, DA WATCHGUARD, CONCENTROU A SUA APRESENTAÇÃO NO CONCEITO DE IDENTITY THREAT DETECTION AND RESPONSE E NA SUA RESPETIVA APLICAÇÃO.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

A conferência contou com a presença de Carlos Vieira, Country Manager da WatchGuard, que se focou em Identity Threat Detection and Response (ITDR).

“As soluções de MFA são as soluções de segurança mais económicas e que resolvem uma grande parte dos problemas e dos erros humanos”, defende Carlos Vieira.

Segundo um estudo da Verizon, “em 2022, 74% das vulnerabilidades ao nível de data breach” derivam do “problema do fator humano”. 37% das empresas com mais de mil funcionários “são vulneráveis a este erro de fator humano”, enquanto nas organizações com menos de mil trabalhadores “falamos de 54%”.

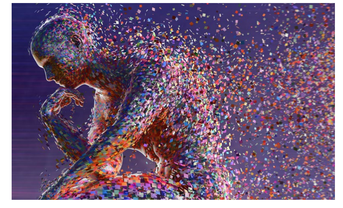
Para Carlos Vieira, o dado “mais interessante” é um que “nos afeta a todos nós”: em média, um colaborador tem cerca de 27 passwords para memorizar, sendo que “61% ao nível dos trabalhadores [as] reutilizam e, “no caso de acessos pessoais, reutilizamos 73%”. No período pós-pandémico, “55% das empresas vão adotar sistemas híbridos”.

De acordo com um inquérito da Gallup, “para os MSSP, 42% dos clientes preveem ‘outsourciar’ a parte de gestão de acesso a terceiros e 35% vão implementar soluções de MFA e de password management”.

“ITDR não é um produto, não é uma solução de segurança”, sublinha Carlos Vieira. “Acaba por ser uma subárea da parte de segurança”, que procede à “implementação de mecanismos de deteção, de investigação, de análises suspeitas, de IoA e IoC”.

CARLOS VIEIRA, WATCHGUARD

“Sem implementar uma política de ITDR e *zero--trust*, sem que haja uma monitorização constante, uma correlação constante, só per se utilizar estas ferramentas [de segurança] não nos vai resolver o problema”, destaca.



VARONIS

“COM UMA SUPERFÍCIE DE ATAQUE TÃO GRANDE, TEREMOS SEMPRE UM SISTEMA VULNERÁVEL”

PEDRO MONTEIRO, DA VARONIS, FALOU SOBRE A IMPORTÂNCIA DA ADOÇÃO DE UMA ESTRATÉGIA CENTRADA NA SEGURANÇA AUTOMATIZADA DE DADOS.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

PEDRO MONTEIRO, VARONIS

O enfoque da apresentação de Pedro Monteiro, Account Manager da Varonis, foi a importância de colocar a proteção de dados no centro da estratégia de segurança das empresas.

Pedro Monteiro referiu o exemplo de “um caso paradigmático do CISO do Twitter, que foi chamado ao Congresso norte-americano, onde houve um esclarecimento de que não era possível proteger os dados”. Isto deveu-se sobretudo ao facto de a empresa ter “crescido de tal maneira de forma incontrolável que não sabiam, primeiro, onde é que os tinham guardado e, depois, como os podiam proteger”.

Isto conduz a um “segundo problema”: o “acesso dos próprios funcionários” aos dados da organização.

“O mundo híbrido está cada vez mais caótico e está a crescer de um modo alucinante”, aponta. “Temos cada vez mais ferramentas que despoletam um conjunto de informações que nós temos de salvaguardar. Com uma superfície de ataque tão grande, obviamente teremos sempre um sistema vulnerável ou um funcionário mal-intencionado”.

O profissional refere que “conseguimos reativar infraestruturas, conseguimos por serviços em pé”, no entanto, “quando os dados são atacados, as coisas já são mais complicadas”.

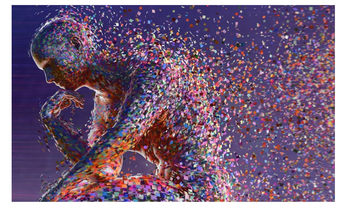
Desta forma, Pedro Monteiro acredita que “nós travamos uma batalha diferente daquela que os fabricantes tradicionais de segurança, porque nos focamos primeiro na segurança de dados e não depois”.

Existem três questões de clientes que motivam a Varonis a ter uma “componente de segurança mais ativa”: “se os meus dados estão em risco; se consigo detetar fugas de informação; e se estou compliant”.

oramix
EXPERT SERVICES

ORAMIX ORGANIZA ALMOÇO EXECUTIVO

A ORAMIX ORGANIZOU, NA SEGUNDA EDIÇÃO DA IT SECURITY CONFERENCE, UM ALMOÇO COM VÁRIOS CISO, NUMA OPORTUNIDADE PARA DEBATER E TROCAR EXPERIÊNCIAS SOBRE O TEMA DE RESPOSTA A INCIDENTES. VÁRIOS LEITORES DA IT SECURITY, PRESENTES NA CONFERÊNCIA, PARTILHARAM A SUA EXPERIÊNCIA COM A RESPOSTA A INCIDENTES DE CIBERSEGURANÇA E QUAIS OS PROCEDIMENTOS QUE UTILIZAM PARA RESOLVER OS PROBLEMAS QUE VÃO APARECENDO.



CLOUDFLARE

O PANORAMA MUNDIAL DE ATAQUES DDOS

O WORKSHOP CLOUDFLARE, POWERED BY V-VALLEY, ABORDOU O TEMA "RECENT CYBER ATTACK FIGURES BY INDUSTRY AND HOW IS CLOUDFLARE PROTECTING COSTUMERS".

Em paralelo com as sessões no palco, o workshop Cloudflare, powered by V-Valley, decorreu na Sala Jardim e centrou-se no cenário atual de ataques DDoS no mundo. A apresentação ficou a cargo de Juan Molina, Channel Solutions Enginner EMEA, e de Maria Sacau, Senior Account Executive Iberia.

A maioria dos ataques à camada de rede duram três horas (72.72%), com um bitrate de 500Mbps (42.53%) e de 1G-10Gbps (37.17%). As ameaças emergentes são os ataques DDoS de lavagem de DNS e o aumento de botnets de máquinas virtuais, segundo a CloudFlare.

Relativamente aos ataques L3/L4, as principais indústrias atacadas são a de TI e Serviços, onde 32,62% do tráfego é DDoS, a de Música (13,43%) e a de Broadcast Media (12,63%).

MARIA SACAU E JUAN MOLINA, CLOUDFLARE

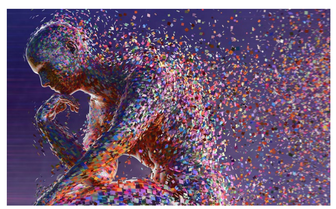
A nível nacional, 4,45% do tráfego originado em Portugal é tráfego de ataque DDoS L3/4, revela a CloudFlare.

Quanto aos ataques L7 (HTTP), a indústria de Gestão e Consultoria é a mais visada, sendo que 18,38% do seu tráfego é DDoS. Seguem-se as organizações sem fins lucrativos (17,60%) e o setor de Contabilidade (10,06%).

Os principais países mais atacados por DDoS L7 (HTTP) são a Palestina, onde 11.97% do seu tráfego é malicioso, São Cristóvão e Neves (10.29%) e Paquistão (7.33%). Os principais países de origem são Moçambique (19.2%), Egipto (13.5%) e Finlândia (12.1%).

Verifica-se o aumento dos ataques WAF, cuja execução real é geralmente realizada por bots. Para vencer o jogo, é essencial lutar com bots contra bots, acredita a Cloudflare.

A agenda dos líderes deverá centrar-se na redução do risco cibernético, numa força de trabalho híbrida segura, no controlo dos custos operacionais e na migração e gestão de clouds, recomenda a empresa.



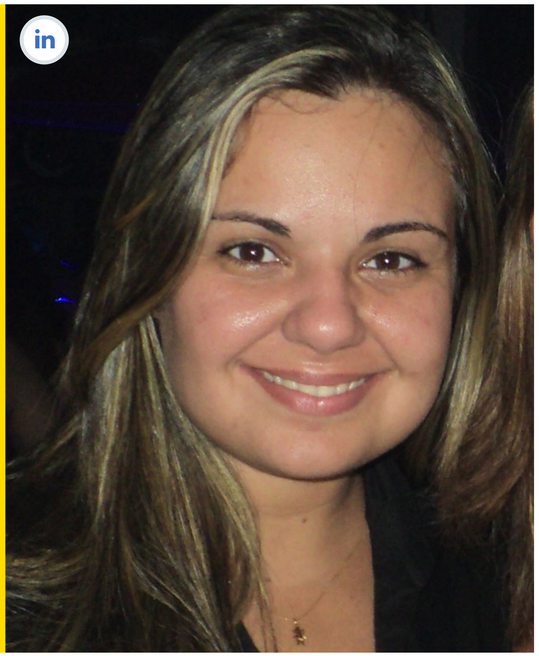
Lenovo

LENOVO ENTREGA PORTÁTIL A LEITOR DA IT SECURITY

NO FINAL DA IT SECURITY CONFERENCE, A LENOVO, REPRESENTADA POR RUI GOUVEIA, CHANNEL MANAGER, ENTREGOU A UM DOS PARTICIPANTES DA IT SECURITY CONFERENCE O PRÉMIO QUE FOI SORTEADO ENTRE OS LEITORES PRESENTES: UM LENOVO X1 CARBON GEN 11.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

XXXXXA (À DIREITA)



EXECUTIVA COM 27 ANOS DE ATUAÇÃO EM EQUIPAS DE INFRAESTRUTURA, PRIVACIDADE, GOVERNANÇA DE TI, SENDO 16 ANOS NA ÁREA DE CIBERSEGURANÇA EM LOGÍSTICA, SERVIÇOS, RETAIL E INDÚSTRIA. ESPECIALISTA EM SEGURANÇA DA INFORMAÇÃO NO INSTITUTO TECNOLÓGICO DE AERONÁUTICA, MINISTÉRIO DA DEFESA/COMANDO DA AERONÁUTICA, BRASIL. MBA SOBRE TRANSFORMAÇÃO DIGITAL NO MIT, EUA. PALESTRANTE EM CONFERÊNCIAS NO BRASIL E EXTERIOR.

POR CRISTIANE DIAS

OS DESAFIOS DE SEGURANÇA DA INFORMAÇÃO NA ERA DA INTELIGÊNCIA ARTIFICIAL

À MEDIDA QUE A INTELIGÊNCIA ARTIFICIAL (IA) SE TORNA MAIS OMNIPRESENTE, A SEGURANÇA DA INFORMAÇÃO ENFRENTA DESAFIOS SIGNIFICATIVOS.

A crescente adoção da IA no mundo moderno trouxe consigo inúmeros benefícios e avanços em diversas áreas, como medicina, indústria, automação, entre outras. No entanto, esta revolução tecnológica não está isenta de desafios e preocupações, especialmente quando se trata da Segurança da Informação. A integração da IA em sistemas e processos criou um ambiente propício para ameaças cibernéticas cada vez mais sofisticadas, tornando a proteção de dados e a privacidade

uma prioridade eminente. A IA apresenta desafios únicos neste campo, que vão desde vulnerabilidades cibernéticas até questões éticas e de privacidade.

A DUPLA FACE DA INTELIGÊNCIA ARTIFICIAL

A IA tem se destacado como uma das tecnologias mais promissoras dos últimos anos. Tem a capacidade de analisar grandes volumes de dados, identificar padrões complexos e tomar decisões com base nessa análise, o que a torna uma ferramenta poderosa em diversas áreas.

Por outro lado, tem mostrado o seu valor em várias aplicações, desde chatbots de atendimento ao cliente até diagnósticos médicos precisos e carros autónomos. No entanto, à medida que a IA se torna cada vez mais omnipresente, a preocupação com a Segurança da Informação também cresce.

Os desafios são variados e complexos, e algumas das principais preocupações incluem:

1. Ataques Cibernéticos Automatizados

A IA é frequentemente usada para melhorar a segurança cibernética, mas também pode ser usada por invasores para aprimorarem os seus ataques. A capacidade de aprendizagem e adaptação da IA a novos cenários torna-a numa ferramenta eficaz para identificar vulnerabilidades em sistemas de segurança e até mesmo desenvolver ataques personalizados.

A automação proporcionada pela IA torna os ataques cibernéticos mais eficazes e devastadores. Algoritmos de IA podem identificar vulnerabilidades em sistemas de segurança e lançar ataques de forma contínua e coordenada.

Outro ponto de preocupação são os ataques de phishing que usam IA para personalizar mensagens e adaptar o seu conteúdo com base nas características da vítima. Tal situação torna os utilizadores mais vulneráveis a ataques de Engenharia Social e são mais difíceis de detetar.

Vulnerabilidades em algoritmos de IA também podem ser explorados. Modelos de IA podem ser usados para manipular resultados, como classificação de conteúdo ou previsões.

2. Deepfakes e Manipulação de Mídia

A geração de deepfakes, que são vídeos e áudios manipulados com a ajuda da IA, apresenta uma ameaça significativa à Segurança da Informação e à reputação das pessoas e organizações. Esta tecnologia pode ser usada para criar conteúdo enganoso e prejudicial, minando a confiança na mídia e nas informações disponíveis.

A capacidade da IA de criar deepfakes convincentes, que podem enganar até mesmo olhos treinados, levanta sérias preocupações sobre a disseminação de informações falsas e a desinformação, o que provoca implicações significativas para a política, as eleições e a sociedade como um todo.

3. Violação de Privacidade

A coleta e análise de dados em larga escala por meio de algoritmos de IA levanta preocupações sobre a privacidade dos indivíduos. Empresas e governos podem usar IA para extrair informações pessoais, o que levanta questões éticas sobre como é que esses dados são armazenados e utilizados.

A divulgação não autorizada de informações pessoais representa uma ameaça significativa.

A proteção dos dados pessoais e sensíveis é fundamental e os vazamentos de informações podem ter sérias consequências para os indivíduos e as organizações.

4. Viés e Discriminação

Os algoritmos de IA são treinados com base em dados históricos, o que pode introduzir viés nos resultados. Isso significa que a IA pode perpetuar e amplificar preconceitos existentes, refletindo nos dados de treinamento, o que é uma preocupação significativa quando se trata de decisões importantes como contratações, empréstimos.

No âmbito de processos judiciais pode levar a decisões injustas e prejudiciais, agravando problemas sociais e éticos.

5. Ataques Adversariais

Os ataques adversariais são um dos desafios mais significativos da IA. Envolvem a manipulação de dados de entrada para confundir ou enganar um modelo de IA, o que pode resultar em erros graves, levando a decisões incorretas em sistemas autónomos como carros ou sistemas de segurança.

6. Responsabilidade e Ética

A tomada de decisões automatizada levanta questões de responsabilidade e ética. Quem é responsável por erros ou decisões incorretas em sistemas de IA? Como garantir que a IA é usada de maneira ética e para o bem da sociedade?

INICIATIVAS DE REGULAÇÃO EM TODO O MUNDO

Devido às crescentes preocupações em torno da Segurança da Informação e da IA, muitos países e organizações internacionais têm tomado medidas para regular o seu uso.

A União Europeia (UE) introduziu a Lei de Inteligência Artificial que estabelece diretrizes rigorosas para o uso de IA, que visam garantir a segurança, a ética e a transparência na sua utilização. Isso inclui requisitos de avaliação de riscos e proibições de usos específicos, como reconhecimento facial em tempo real para locais públicos.

Com o apoio da General Data Protection

OS ALGORITMOS DE IA SÃO TREINADOS COM BASE EM DADOS HISTÓRICOS, O QUE PODE INTRODUZIR VIÉS NOS RESULTADOS. ISSO SIGNIFICA QUE A IA PODE PERPETUAR E AMPLIFICAR PRECONCEITOS EXISTENTES REFLETINDO NOS DADOS DE TREINAMENTO, O QUE É UMA PREOCUPAÇÃO SIGNIFICATIVA QUANDO SE TRATA DE DECISÕES IMPORTANTES COMO CONTRATAÇÕES, EMPRÉSTIMOS.

Regulation (GDPR) da União Europeia, em vigor desde maio de 2018, diretrizes rígidas para a coleta, armazenamento e processamento de dados pessoais já são seguidas. Afeta empresas que operam na União Europeia e impõe multas significativas por violações de privacidade.

Nos Estados Unidos, a Federal Aviation Administration (FAA) implementou regulamentações para drones autónomos e a Food and Drug Administration (FDA) emitiu diretrizes para o uso de IA em dispositivos médicos.

Embora não tenham uma regulamentação federal de IA abrangente, alguns estados, como a Califórnia, estão a adotar medidas semelhantes à California Consumer Privacy Act (CCPA).

A CCPA confere aos residentes da Califórnia maior controlo sobre as suas informações pessoais e obriga as empresas a divulgarem as suas práticas de coleta e uso de dados.

Além disso, o Governo e o Congresso estão a considerar várias propostas para regulamentar a IA, abordando questões de ética, privacidade, transparência e segurança cibernética.

No Brasil, desde agosto deste ano, está em tramitação o Projeto de Lei sob número 2.338/2023 que regulamenta o uso de IA.

Uma das preocupações é a de que não haja conflito com a Lei Geral de Proteção de Dados (LGPD — Lei 13.709/2018) na regulamentação da Inteligência Artificial.

Inspirada na General Data Protection Regulation (GDPR), a Lei Geral de Proteção de Dados Pessoais (LGPD) entrou em vigor em 2020. Estabelece regras para a coleta e uso de dados pessoais no Brasil, protegendo a privacidade dos cidadãos.

Outras iniciativas como a União Internacional de Telecomunicações e Autorregulação da Indústria estão a trabalhar em padrões globais, reforçando o compromisso em criar diretrizes éticas para o desenvolvimento e uso da IA.

CONCLUSÃO

A Inteligência Artificial trouxe inúmeras vantagens e avanços, permitindo que máquinas realizem tarefas que antes eram exclusivas de seres humanos, como o reconhecimento de padrões, a análise de grandes volumes de dados e até mesmo a tomada de decisões complexas.

A preocupação central em relação à IA e Segurança da Informação está relacionada à capacidade das tecnologias de IA de serem usadas para fins maliciosos. Isso inclui o uso de IA para criar deepfakes convincentes, phishing mais sofisticado e até mesmo ataques cibernéticos automatizados. À medida que a IA se torna mais avançada, os riscos associados a essas atividades maliciosas aumentam significativamente.

A regulamentação da IA pode desempenhar um papel vital na mitigação dos riscos, mas é necessário um esforço contínuo por parte das empresas, governos e da sociedade em geral para garantir que a IA seja usada de maneira responsável e para o bem comum.

Num mundo cada vez mais impulsionado pela Tecnologia, a consciencialização e a confiabilidade dos utilizadores também desempenha um papel fundamental na aceitação da IA, promovendo uma adoção responsável e manutenção da Segurança da Informação.

Embora a IA continue a ser uma força impulsionadora da inovação, garantir segurança deve ser uma prioridade constante para que possamos colher os benefícios da IA sem comprometer a integridade dos nossos dados e a confiança pública. ◀

GERIR AS IDENTIDADES E OS ACESSOS PARA PROTEGER AS ORGANIZAÇÕES

A GESTÃO DE IDENTIDADES E ACESSOS É UM TEMA CADA VEZ MAIS IMPORTANTE NAS ORGANIZAÇÕES. TER A CERTEZA DE QUE O UTILIZADOR TEM ACESSO APENAS À INFORMAÇÃO QUE PRECISA É UMA NECESSIDADE PARA QUE A EMPRESA FUNCIONE DA FORMA MAIS SEGURA POSSÍVEL.

Gerir identidades digitais – seja de utilizador internos ou externos – tem de estar na lista de prioridades das organizações. Esta gestão tem de ser feito através de software que, automaticamente, dá ou revoga acessos dos utilizadores consoante a sua função.

Num pequeno-almoço executivo durante o mês de outubro, a IT Security e a One Identity juntaram representantes de organizações portuguesas de


JOÃO FERREIRA, BANCO DE PORTUGAL


RUI SOUSA GIL, JOSÉ DE MELLO CAPITAL


SÉRGIO TRINDADE, EPAL

vários setores de atividade para falar sobre o tema, dos desafios e das práticas que encontraram para gerir as identidades digitais dos colaboradores das suas entidades.

Antes de um debate com os presentes, Daniel Gaspar, Senior Sales Account Manager and Team Leader for Iberia da One Identity, apresentou a visão da empresa para este problema e para ter uma identidade de segurança unificada.

As soluções da One Identity permitem aumentar a segurança da organização enquanto se suporta a transformação digital da mesma, se permite auditorias, se aumenta a gestão de logs e aumenta a eficiência operacional.

Na visão da One Identity, uma das melhores maneiras de proteger as organizações em ambientes dinâmicos é passar de uma abordagem fragmentada para uma abordagem holística, através da unificação de processos anteriormente distintos e correlacionar as identidades para ter uma visibilidade de 360 graus.

A One Identity disponibiliza uma plataforma de segurança da identidade unificada que vai de encontro às necessidades das organizações, juntando soluções de Identity Governance and Administration (IGA), de gestão de acessos, de gestão de acessos privilegiados e gestão de Active Directory numa única solução end-to-end.

Sérgio Trindade, CIO e CDO, EPAL: "Temos contratação externa, fornecedores que nos dão apoio, e era extremamente difícil conseguir que estivessem ativos apenas quando faziam falta. O que fizemos foi centrar numa área para garantir que os acessos que eram dados, retirados e o próprio processo de autorização seguiam um padrão e uma política interna que garantisse que, efetivamente, isso acontecia do ponto de vista de identidade"

Carlos Silva, Diretor de Segurança e Proteção de Dados, Banco CTT: "Há algo que me faz confusão que é o Active Directory. É necessário, mas uma dor de cabeça em termos de segurança. É uma tecnologia com 30 anos, totalmente legada, sem segmentação de privilégios, muito pouco resiliente e, nos últi-


CARLOS SILVA,BANCO CTT


JOÃO PAULO CAVACO, INSPEÇÃO-GERAL DE EDUCAÇÃO E CIÊNCIA


PAULO MARTINS, SL BENFICA


JORGE FERNANDES, CISO

mos anos, todos os grandes ataques que existiram tiveram o Active Directory comprometido. Nesse sentido, devemos segregar em termos de utilizadores ao máximo"

João Paulo Cavaco, Head of the Communication and Information Systems Division, Inspeção-Geral de Educação e Ciência: "A segregação é essencial. O que tem de haver, depois, também são processos comuns para toda a gente que faz parte. Um dos caminhos feitos no sentido da concentração do problema acaba por criar um problema muito maior que não tem solução. Depois de concentrado, vai ser preciso dividir, sem dúvida nenhuma"

Paulo Martins, Diretor de TI & Operações, SL Benfica: "A segmentação tem de ser vista de várias perspetivas e cada empresa, cada entidade, tem de ver o seu enquadramento. Não há uma receita que diz que se deve fazer uma segmentação mais ou menos excessiva. Cada um tem de olhar para o seu ecossistema. Segmentar muito pode trazer problemas bem mais graves. É preciso perceber de que lado estamos a olhar. É preciso olhar para o todo e de uma forma estruturada. A receita não será igual para todos"

Jorge Fernandes, CISO: "Tem de haver um envolvimento das pessoas da área do negócio que sabem quem é que tem de ter acesso àquilo. Não é o IT que vai decidir quem é que tem acesso a esses processos. Se não houver esse envolvimento das pessoas ligadas ao negócio, isto sai ao contrário"

Rui Sousa Gil, Diretor de Tecnologias de Informação, José de Mello Capital: "Se tenho uma determinada pessoa, com um determinado perfil dentro de uma ferramenta de operação, não quero estar a gerir discretamente o acesso e a atribuição desse perfil. Quando tenho aquele automatismo que me é dado pelos Active Roads de integração entre o RH e a empresa, quero que todos os acessos e, para além disso, as autorizações nas aplicações e na infraestrutura sejam


DANIEL GASPAR, ONE IDENTITY


NUNO SILVA, UNIVERSIDADE LUSÍADA


MIGUEL BORGES, GALUCHO


JOSÉ GAMA, AUDITOR

completamente limpas no instante imediatamente a seguir à saída da pessoa da empresa"

Nuno Silva, IT Manager, Universidade Lusíada: "A parte académica é bastante diferente. Os alunos autenticam-se com o seu número de aluno próprio, gerem as suas passwords por regras mínimas que são definidas. O problema que temos é o acesso ao software; o aluno, durante as aulas e os laboratórios, tem de ter acesso a variados software e aí anda completamente perdido porque tem autenticações. Esse é o principal dilema"

Miguel Borges, IT Director, Galucho: "A gestão dos acessos é um problema grande porque, sendo uma unidade fabril com muitos departamentos internos das linhas de montagens, há muitos utilizadores que precisam de aceder a vários tipos de informação que está separada por toda a infraestrutura. Acho que o problema maior é a falta de clareza dos processos e o que é preciso, muitas vezes, e rever e refazer os processos para controlar, também, esse tipo de acesso"

José Gama, Auditor: "A minha visão tem a ver com os princípios da auditoria, que é o princípio do que é que espero encontrar num sistema, mais do que a forma de lá chegar. Existem empresas onde a relação do funcionário com os recursos humanos provoca a imediata suspensão dos privilégios que essa pessoa tem – seja em termos daquilo que pode fazer, onde é que pode fazer, como é que entra no trabalho. Isso é um reflexo totalmente automático"

João Ferreira, Administrador de Sistemas, Banco de Portugal: "As organizações normalmente funcionam com base em regras, mas têm dificuldades em cumpri-las e fazê-las cumprir. Procura-se criar processos e regras a uma boa prática de gestão de identidades e gestão de acessos, mas o conjunto de exceções a que normalmente somos confrontados, às vezes, distorce um bocado as coisas. Isso faz desencadear um conjunto de processos que levam à formação de uma identidade digital para essa pessoa e, em função do departamento, da função, uma série de fatores e variáveis, essa identidade é mais ou menos privilegiada, tem mais ou menos acessos, ganha acesso a mais ou menos aplicações" ◀

AI ACT: ALINHAR A INOVAÇÃO À CIBERSEGURANÇA

Foto de Andrea De Santis na Unsplash

POR RITA SOUSA E SILVA

A LEI DE IA DA UNIÃO EUROPEIA ENFRENTA O DESAFIO DE ASSEGURAR A SEGURANÇA SEM CORTAR AS PERNAS DA INOVAÇÃO. À MEDIDA QUE OS CIBERCRIMINOSOS APERFEIÇOAM A SUA ATIVIDADE COM A TECNOLOGIA, COLOCAR A CIBERSEGURANÇA NO CENTRO DA REGULAÇÃO DA IA TORNA-SE CADA VEZ MAIS IMPORTANTE.

Regular a Inteligência Artificial (IA) é uma corrida contra o tempo: quanto mais a elaboração de um enquadramento regulatório demora, mais rápido a tecnologia inovadora avança e mais alarmantes são as preocupações ligadas à segurança, privacidade e proteção de dados. Enquanto isso, os cibercriminosos – com menor ou maior experiência – aproveitam-se da facilidade de utilização da IA para realizar ataques cada vez mais sofisticados.

A União Europeia (UE) lançou a primeira pedra na regulamentação da IA, centrando-se sobretudo na mitigação dos riscos – e a cibersegurança é inegavelmente um deles. "Qualquer regulação de IA vai ter de olhar também para o tema da cibersegurança", afirma Eduardo Magrani, Consultor Sénior da área de Tecnologias, Media e Telecomunicações da CCA Law Firm.

Margarida Leitão Nogueira, Partner da DLA Piper, relembra a dicotomia inerente à IA em matéria de segurança cibernética. Por um lado, "a IA é suscetível de ter um papel essencial no que respeita ao reforço da cibersegurança das organizações e no combate ao cibercrime" e, por outro, "pode potenciar a sofisticação e disseminação de ciberataques, se utilizada com propósito malicioso".

Os legisladores europeus enfrentam um desafio crucial na produção da legislação pioneira sobre a IA: garantir a segurança digital sem travar a evolução tecnológica e a competitividade no espaço europeu.

LUZ VERDE DO PARLAMENTO

Em junho, o Parlamento Europeu deu luz verde à proposta do AI Act, assente nos princípios de segurança, privacidade e transparência. As regras seguem uma abordagem baseada no risco, estabelecendo obrigações para fornecedores e utilizadores de sistemas de IA.

"Não existe segurança garantida nas TIC, incluindo nos sistemas de IA", destaca a Agência Europeia

para a Segurança das Redes e da Informação (ENISA). "No entanto, uma avaliação de riscos permite tomar uma decisão informada sobre quais são as possíveis ameaças e vulnerabilidades e como minimizar o seu impacto".

O projeto de lei incide sobre os sistemas de IA classificados como sendo de risco inaceitável, que são considerados "uma ameaça para as pessoas" e, por isso, será proibida a sua utilização, assim como a sua colocação no mercado ou em serviço. Estes incluem a manipulação cognitivo-comportamental de pessoas ou grupos vulneráveis específicos, a pontuação social e os sistemas de identificação biométrica em tempo real e à distância.

Por sua vez, os sistemas de IA de risco elevado estão "sujeitos a requisitos exigentes por serem suscetíveis de colocar em causa a segurança ou direitos fundamentais", explica Margarida Leitão Nogueira. Estes dividem-se em duas categorias: aqueles que são utilizados em produtos abrangidos pela legislação da UE em matéria de segurança dos produtos; e aqueles que estão enquadrados em determinadas


EDUARDO MAGRANI, CCA LAW FIRM

áreas específicas que terão de ser registados numa base de dados da UE.

As tecnologias de alto risco "têm medidas muito específicas: garantia de explicabilidade dos algoritmos; maior transparência aos utilizadores; necessidades de auditorias, de relatórios de impacto", afirma Eduardo Magrani. Os utilizadores deverão receber das organizações que recorrem à tecnologia "informações mais detalhadas sobre que tipo de IA ou de algoritmo é aplicado, quais são os riscos atrelados,

> AS TECNOLOGIAS DE ALTO RISCO "TÊM MEDIDAS MUITO ESPECÍFICAS: GARANTIA DE EXPLICABILIDADE DOS ALGORITMOS; MAIOR TRANSPARÊNCIA AOS UTILIZADORES; NECESSIDADES DE AUDITORIAS, DE RELATÓRIOS DE IMPACTO",
>
> EDUARDO MAGRANI, CONSULTOR SÉNIOR DA ÁREA DE TECNOLOGIAS, MEDIA E TELECOMUNICAÇÕES DA CCA LAW FIRM

como é que controlam esses riscos". O advogado acrescenta que "as autoridades vão ser mais munidas com essas informações, então os utilizadores vão sentir-se mais empoderados para reivindicar os seus direitos".

A ENISA destaca o artigo 15.º da Lei da IA, que "propõe requisitos de cibersegurança para sistemas de IA de alto risco, a fim de garantir o *compliance*, identificar riscos e implementar as medidas de segurança necessárias". Neste sentido, "uma avaliação de risco de segurança deve ser realizada tendo em conta a conceção do sistema e a finalidade a que se destina".

Para Margarida Leitão Nogueira, "um dos aspetos relevantes constantes" do AI Act é a "garantia de solidez técnica e de resistência a ações maliciosas suscetíveis de pôr em causa a segurança dos sistemas de IA de risco elevado". Neste sentido, a proposta estabelece "que 'os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de acordo com o princípio da segurança desde a conceção e por defeito', devendo atingir um nível apropriado de cibersegurança durante o ciclo de vida".

Além disto, os responsáveis pela implementação dos sistemas de IA de risco elevado "estão obrigados a garantir a monitorização regular da eficácia das medidas de solidez e cibersegurança, bem como a respetiva atualização", acrescenta a advogada.

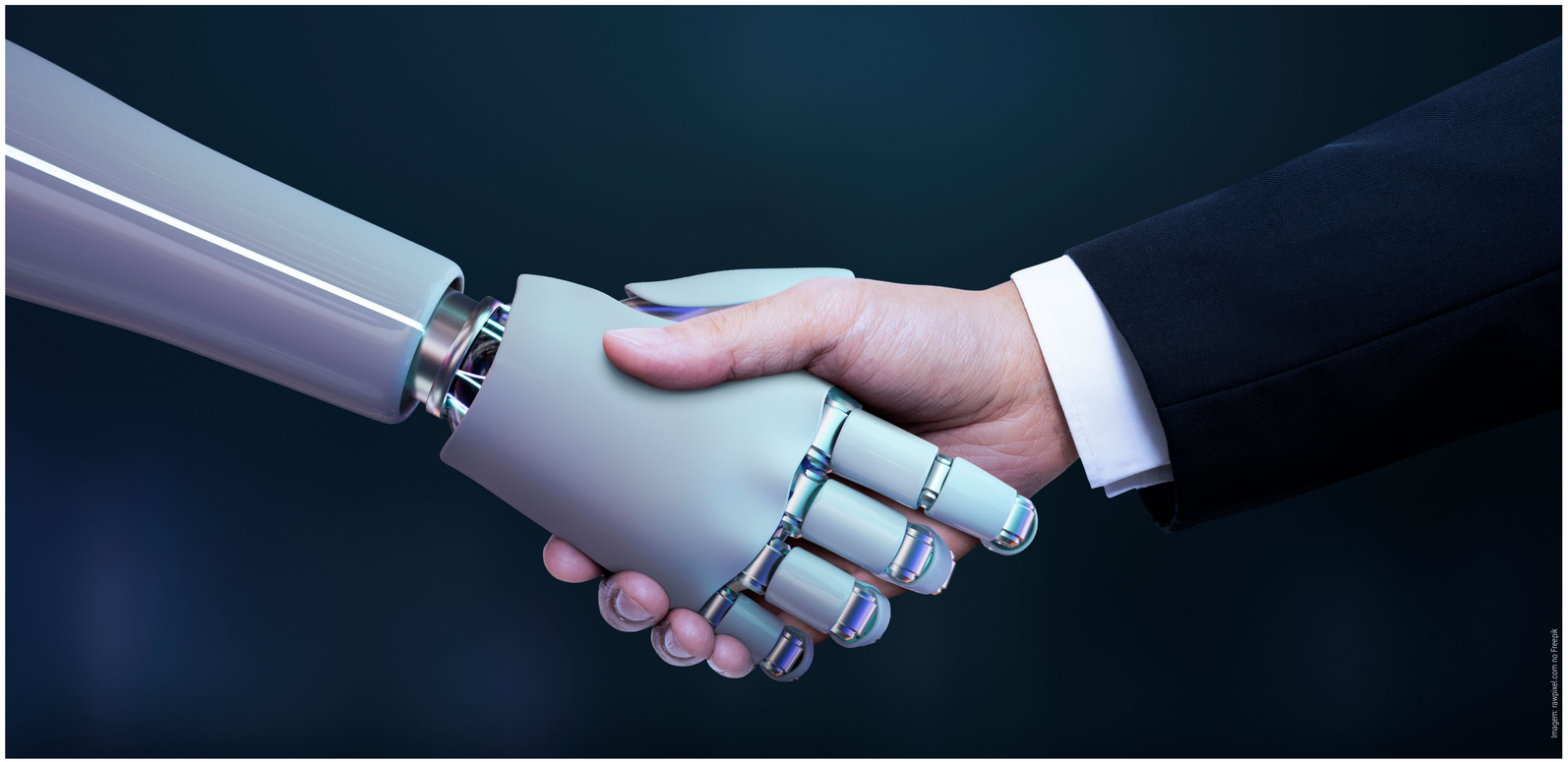
Já os sistemas de IA de risco limitado deverão cumprir requisitos mínimos de transparência de forma que os utilizadores tomem decisões informadas sobre a sua utilização.

Com a aprovação do Parlamento Europeu, os eurodeputados decidiram alargar a lista de proibições para incluir "utilizações intrusivas e discriminatórias da IA", como é o caso dos sistemas de identificação biométrica à distância, tanto em tempo real em espaços públicos como em diferido, e dos sistemas de categorização biométrica que utilizem características sensíveis (como género, raça, etnia, estatuto de cidadania, religião, orientação política).

São também proibidas as utilizações de sistemas de policiamento preditivo, bem como de reconhecimento de emoções na aplicação da lei, gestão das fronteiras, local de trabalho e nos estabelecimentos de ensino. Os eurodeputados classificam também como risco inaceitável a remoção não direcionada de imagens faciais da Internet ou de filmagens de videovigilância para criar bases de dados de reconhecimento facial.

Além disto, os fornecedores de modelos de base estarão incumbidos de avaliar e mitigar eventuais riscos, devendo registar estes modelos na base de dados da UE. Os sistemas de IA generativa que têm por base estes modelos, como o ChatGPT, terão de cumprir os requisitos de transparência com, por exemplo, a disponibilização aos utilizadores de resumos pormenorizados dos dados protegidos por direitos de autor.

"O ponto mais importante é entender que [o AI Act] não está sozinho", reforça Eduardo Magrani. Regulações como o RGPD, a NIS 2, o DORA e frameworks de segurança como o ISO e o NIST, refe-



re, "são complementares às determinações do AI Act e não podem ser esquecidas na fase de implementação, lembrando que essas entidades não têm de esperar o dano ocorrido".

ARMA DE CIBERCRIMINOSOS

Devido à sua fácil utilização, os cibercriminosos têm usufruído dos vários benefícios da IA – nomeadamente a capacitação de um maior número de utilizadores, incluindo os menos experientes – para realizar atividades maliciosas. As ferramentas de IA "podem fornecer análises melhores e mais rápidas dos sistemas investigados, ser usados em ataques de engenharia social ou apoiar a criação de malware personalizado", explica a ENISA.

De acordo com a Check Point, isto levou à criação de pequenos grupos de cibercriminosos capazes de encetar ciberataques mais sofisticados devido a esta tecnologia.

Os *deepfakes*, uma ferramenta de IA que possibilita a criação de gravações de voz e de vídeo falsas/manipuladas, são frequentemente utilizados para os atacantes se fazerem passar por celebridades, líderes políticos ou executivos de organizações.

Os grupos de ransomware estão a desenvolver novos métodos em que combinam a IA com ferramentas há muito estabelecidas, como dispositivos USB, para realizar ciberataques disruptivos, alerta a Check Point.

Em março, a Europol, a Agência da UE para a Cooperação Policial, alertou para o potencial uso indevido de ferramentas como o ChatGPT em três áreas específicas: os ataques de phishing, devido à sua capacidade de "redigir textos altamente realistas"; os cibercrimes, uma vez que os atacantes podem aproveitar-se da habilidade de "reproduzir padrões de linguagem para personificar o estilo de fala de indivíduos ou grupos específicos"; e a desinformação.

Com as mensagens de phishing aperfeiçoadas,

"UM DOS ASPETOS RELEVANTES CONSTANTES" DO IA ACT É A "GARANTIA DE SOLIDEZ TÉCNICA E DE RESISTÊNCIA A AÇÕES MALICIOSAS SUSCETÍVEIS DE PÔR EM CAUSA A SEGURANÇA DOS SISTEMAS DE IA DE RISCO ELEVADO".

MARGARIDA LEITÃO NOGUEIRA, PARTNER DA DLA PIPER

é cada vez mais difícil distingui-las de comunicações legítimas. Todos os dias, as marcas de empresas como a Amazon, a Microsoft e a Google são utilizadas para o furto de dados através de emails e SMS fraudulentos, destaca a Check Point.

"À medida que as capacidades dos LLM, como o ChatGPT, estão a ser ativamente melhoradas, a exploração potencial destes tipos de sistemas de IA por criminosos oferece uma perspetiva sombria", adverte a Europol. "Para um potencial criminoso com pouco conhecimento técnico, este é um recurso inestimável para produzir código malicioso".

INOVAÇÃO, COMPETITIVIDADE E SOBERANIA

Uma das maiores críticas ao AI Act é o entrave à inovação e a falta de competitividade. Recentemente, as maiores empresas da Europa – como a Siemens, Heineken, Renault e Airbus – manifestaram-se contra a regulação proposta pela UE, considerando que "comprometeria a competitividade e a soberania tecnológica da Europa sem efetivamente endereçar os desafios que estamos e estaremos a enfrentar".


MARGARIDA LEITÃO NOGUEIRA, DLA PIPER

"A Europa não se pode dar ao luxo de ficar à margem", reitera a carta aberta assinada por 163 executivos. Em vez de concentrar a regulação na IA generativa e implementar um "*compliance* rígido", os reguladores deveriam produzir uma lei que se limitasse aos "princípios amplos numa abordagem baseada em riscos", defendem.

Margarida Leitão Nogueira esclarece que as empresas europeias consideram a proposta "demasiado restritiva", podendo colocá-las "numa posição

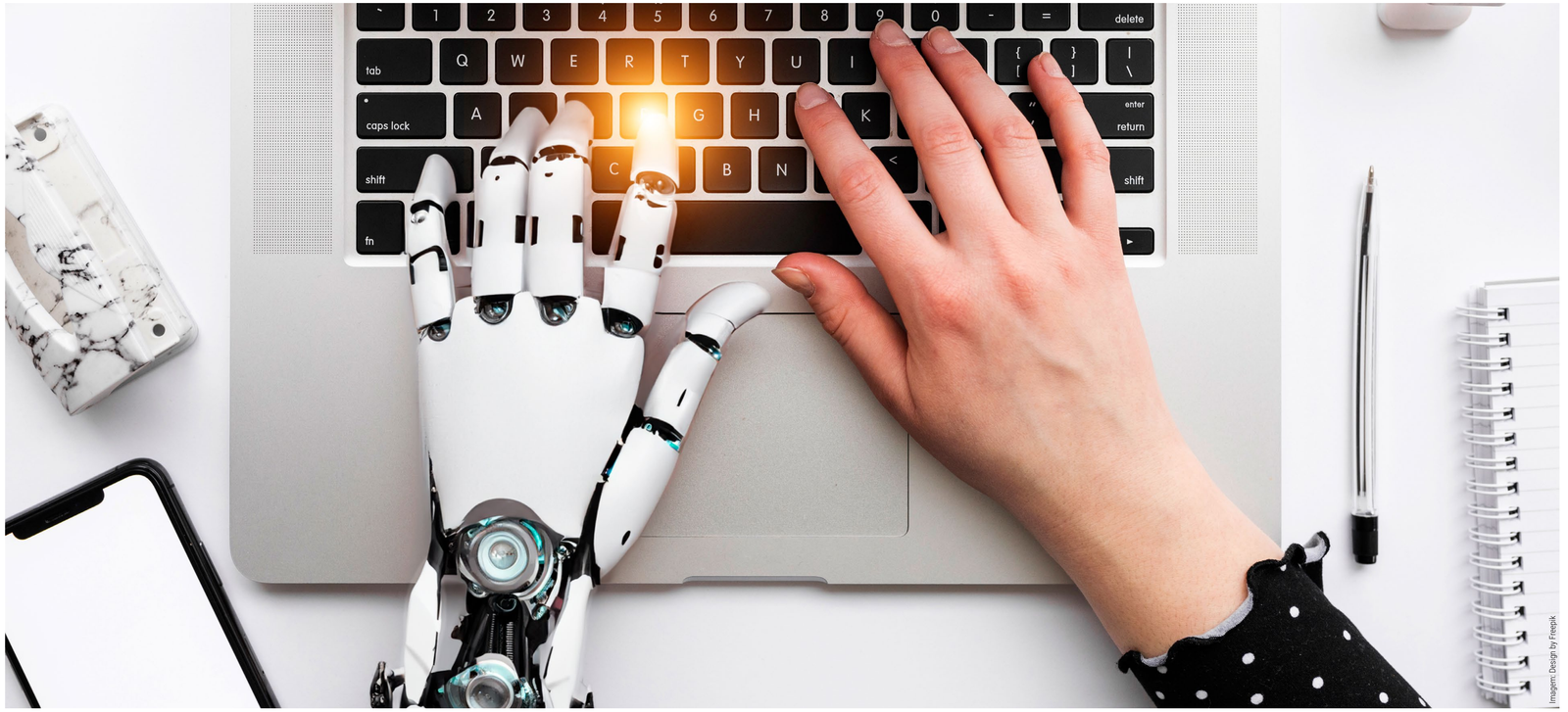


Imagem: Design by Freepik

de desvantagem, sobretudo face a concorrentes localizados nos Estados Unidos e China". Desta forma, é "determinante" a adoção de "soluções equilibradas e proporcionais de forma a não limitar a capacidade de inovação".

A questão da soberania tecnológica está "na ordem do dia", sendo que os ataques cibernéticos no conflito Ucrânia-Rússia "chamaram a atenção para o tema da cibersegurança ainda mais", segundo Eduardo Magrani. "Hoje, temos sistemas de *cloud computing* que não garantem uma hegemonia dos países e do bloco europeu que dependem da tecnologia de outras regiões", acrescenta. "Países como Alemanha e França vêm-se preocupando fortemente em como garantir a sua soberania digital em computação em nuvem".

Também os Estados Unidos alertaram que a proposta da UE prejudicará as pequenas empresas europeias, beneficiando somente as grandes organizações capazes de cobrir os elevados custos de compliance. O país acredita que o regulamento poderá ter consequências como a redução de produtividade e o desincentivo ao investimento.

O AI Act "terá um impacto económico e operacional significativo para as organizações", refere Margarida Leitão Nogueira, implicando "um maior esforço para pequenas empresas que não dispõe do mesmo nível de recursos financeiros e humanos". No entanto, o projeto de lei "prevê a necessidade de prestar particular atenção à redução dos encargos administrativos e dos custos de conformidade para as micro e pequenas empresas".

Eduardo Magrani sublinha a existência de um "*clash* geopolítico" sobre esta questão, uma vez que "os Estados Unidos têm uma abordagem muito mais afeita a riscos que a UE muitas vezes não está disposta", preferindo uma "legislação robusta, que crie mitigadores efetivos de risco antes de um produto ser colocado no mercado".

PRINCIPAIS DESAFIOS

Em outubro, a Reuters reportou a dificuldade dos legisladores europeus na chegada a acordo sobre o projeto de lei. Em particular, a falta de consenso tem incidido sobretudo a abordagem aos "modelos de base", refere Margarida Leitão Nogueira, considerada "demasiado restritiva" por alguns países europeus.

"Tínhamos um texto muito maduro já no início desse ano, mas foi atrasado por conta do impacto da IA generativa", afirma Eduardo Magrani. "A introdução no mercado de uma plataforma como o ChatGPT foi altamente disruptiva".

No final de novembro, a Alemanha, França e Itália chegaram a um acordo sobre a forma como a IA deve ser regulamentada, o que deverá acelerar as negociações a nível europeu. Num documento conjunto, os três países apoiaram a "autorregulação obrigatória através de códigos de conduta" para os modelos básicos de IA, mas opõem-se às "normas não testadas".

"Juntos sublinhamos que a Lei da IA regula a aplicação da IA e não a tecnologia como tal", escreveram no documento. "Os riscos inerentes residem na aplicação de sistemas de IA e não na própria tecnologia".

As três potências europeias afirmaram que a Europa precisa de um "quadro regulamentar que promova a inovação e a concorrência, para que os intervenientes europeus possam emergir e transmitir a nossa voz e os nossos valores na corrida global da IA", segundo escreve o POLITICO.

Prevê-se que o AI Act entrará em vigor no final de 2025 ou no início de 2026. Devido ao "rápido desenvolvimento tecnológico" e "ao cenário de ameaças cibernéticas em constante mudança", os estados-membros "poderão enfrentar desafios na implementação da lei", acredita a ENISA.

"Se, em termos gerais, o cumprimento dos requisitos legais em matéria de cibersegurança coloca, por si só, desafios às organizações, tais desafios são de complexidade acrescida no contexto da IA, face às respetivas especificidades e vulnerabilidades", refere Margarida Leitão Nogueira.

Um dos principais desafios, segundo Eduardo Magrani, é a necessidade de "uma mudança cultural" no seio das organizações, uma vez que a regulação trará "um nível de compliance muito alto e nem todas as entidades estão preparadas". Desta forma, é necessário "começar a trilhar a jornada do compliance em proteção de dados, em cibersegurança, em ética de IA".

Uma preparação adequada, ainda antes da aprovação da regulação, poderá ser chave para o cumprimento bem-sucedido das medidas legais aplicáveis. Desta forma, Margarida Leitão Nogueira indica um conjunto de medidas transversais que poderão ser adotadas pelas organizações: "definir um modelo de governo, políticas e procedimentos internos claros em matéria de IA; sensibilizar para uma utilização responsável dos referidos sistemas; criar canais de comunicação eficazes; definir equipas multidisciplinares capazes de monitorizar a conformidade legal dos IA". ◀

HPE aruba networking

SASE UNIFICADO: CONECTIVIDADE E SEGURANÇA MODERNAS PARA A EMPRESA DIGITAL

OS ARQUITETOS DE REDE, OS LÍDERES DE TI E OS PROFISSIONAIS DE SEGURANÇA DE HOJE ENFRENTAM DESAFIOS SIGNIFICATIVOS. O TRABALHO HÍBRIDO É A NOVA NORMA, O PERÍMETRO DE SEGURANÇA ESTÁ A DISSOLVER-SE E A MAIORIA DAS APLICAÇÕES MUDOU-SE PARA A CLOUD. ISTO SIGNIFICA QUE MUITAS ORGANIZAÇÕES ENFRENTAM RISCOS ACRESCIDOS, CUSTOS OPERACIONAIS ELEVADOS E UMA MÁ EXPERIÊNCIA DE UTILIZADOR. O SASE UNIFICADO RESOLVE ESTES DESAFIOS.

No último ano, muitos líderes de TI adotaram uma estrutura **SASE** (Secure Access Service Edge) para permitir uma ligação mais rápida e segura nas suas organizações.

O **SASE** converge as funções das soluções de rede e segurança num único serviço nativo da cloud que fornece conectividade e segurança consistentes a partir de qualquer lugar.

O **SASE** não é apenas uma tendência tecnológica; é um imperativo estratégico para as empresas modernas que procuram prosperar na era digital. No entanto, nem todas as soluções **SASE** são criadas da mesma forma. Alguns fornecedores de **SASE** oferecem várias soluções pontuais que são integradas de forma deficiente ou requerem alternância entre PoPs de diferentes fornecedores, o que pode gerar latência, problemas de desempenho e sobrecarga de gestão.

Por outro lado, existem soluções **SASE** que fornecem todas as principais capacidades da **SASE** a

partir de uma plataforma única e fortemente integrada - melhorando a postura de segurança, a eficácia, a experiência do utilizador e do administrador e a eficiência de custos.

Isto é o que chamamos de SASE Unificado. E para uma adoção mais simples e mais económica para o SASE, é o caminho a seguir.

O **SASE** Unificado combina os dois conjuntos de tecnologia - as redes SD-WAN e SSE - numa solução de fornecedor único que permite que as empresas obtenham ainda mais simplicidade, eficiência operacional e economia de custos. Uma abordagem unificada também permite maior agilidade e um processo de implementação mais rápido, aumentando o *time-to-value*.

A Gartner prevê que "até 2025, 50% das novas compras de redes SD-WAN vão ser ofertas de **SASE** de fornecedor único, em comparação com 10% em 2022.

MELHORE O DESEMPENHO DA REDE, A EFICIÊNCIA E A POUPANÇA DE CUSTOS

A tecnologia **SASE** da HPE Aruba oferece uma série de benefícios para as empresas que procuram melhorar a sua segurança, a conectividade e a eficiência da rede.

O **SASE** Unificado, que combina SD-WAN e SSE numa solução de um único fornecedor, pode ser implementado de uma forma rápida e fácil e permite-lhe definir o ritmo a que adiciona opções extras, à medida das suas necessidades.

AS FORÇAS MOTRIZES DA ADOÇÃO DO SASE

Antes de mais nada, porquê adotar o **SASE**? A resposta pode ser resumida em 3 simples afirmações:

1. **A segurança que antes era eficaz, agora já não é suficiente;**
2. **Redes que antes eram geríveis, agora já não são;**
3. **Soluções que antes funcionavam bem, agora já não o fazem.**

As arquiteturas tradicionais de rede e segurança que se baseavam principalmente na conectividade segura baseada no perímetro já não satisfazem as necessidades do ambiente empresarial moderno. A rápida adoção de serviços cloud, dispositivos móveis, IoT, OT e trabalho remoto/híbrido criou uma força de trabalho distribuída e dinâmica que necessita de acesso seguro e fiável a aplicações e dados em qualquer lugar, a qualquer hora e em qualquer dispositivo.

No entanto, embora as necessidades empresariais tenham evoluído, a utilização de soluções tradicionais de segurança de rede expõem as organizações a novos desafios e riscos de conectividade, tais como:

– **Aumento da superfície de ataque e da complexidade**: Com mais utilizadores, dispositivos, localizações e serviços cloud para proteger, a organização tem de lidar com mais pontos de entrada potenciais para os atacantes e mais ferramentas de segurança para gerir e atualizar. Para além disso, cada ponto de entrada (ou seja, utilizador ou dispositivo) tem acesso direto à rede empresarial, aumentando ainda mais o risco;

– **Má experiência do utilizador e diminuição da produtividade**: Com mais tráfego a ser reencaminhado através da VPN e da rede empresarial, os utilizadores sofrem com uma maior latência, perda de dados e limitações de largura de banda que afetam o seu desempenho e produtividade, para não falar da satisfação na utilização;

– **Custos operacionais elevados e ineficiências**: Com a proliferação de soluções de rede e de segurança para implementar, manter, atualizar e resolver problemas, a organização tem de gastar mais recursos e tempo na gestão da infraestrutura e na resolução de problemas.

Enfrentar estes desafios e riscos pode ser intimidante. No entanto, trabalhando juntos, os responsáveis de redes e segurança podem eliminar estes problemas utilizando uma estrutura **SASE**.

UM PODEROSO SASE UNIFICADO COM A HPE ARUBA NETWORKING

Se procura uma poderosa solução **SASE** de fornecedor único que proporcione acesso seguro e fiável a partir de qualquer lugar, o **SASE da HPE Aruba Networking** pode ser a sua resposta. Com a sua rede SD-WAN líder do setor e o premiado SSE, a HPE Aruba Networking propõe uma abordagem abrangente e unificada ao **SASE**, feita a pensar nas empresas distribuídas e dinâmicas de hoje.

Com a crescente procura de integração entre soluções de rede e segurança, a HPE Aruba Networking ajuda as equipas de TI a consolidar, simplificar e proteger a ligação dos seus negócios. Com a HPE Aruba Networking, as equipas de TI podem proporcionar controlos de segurança de WAN e cloud diretamente para a aplicação no edge da rede com o HPE Aruba Networking EdgeConnect e redes SD-WAN - em vez de encaminhar os dados pelo data center - enquanto o SSE garante que os controlos de segurança *zero trust* possam ser aplicados a todas as pessoas e dispositivos, independentemente de onde estes se conectem - *campus*, *branch*, em casa ou em movimento. ◀

O QUE PODE FAZER COM O SASE UNIFICADO?

- Simplifique a adoção da SASE trabalhando com um único fornecedor - menos gestão e maior comodidade para a sua equipa de TI;
- Unifique o SASE na medida certa, para a fase em que se encontra no seu percurso, com um modelo de licenciamento flexível que se adapta ao seu orçamento;
- Resolva o fraco desempenho das aplicações com o encaminhamento inteligente fornecido pela SD-WAN avançada - melhore a experiência do utilizador final;
- Provisione, configure e monitorize a sua rede e aplicações com facilidade;
- Reduza os custos removendo com segurança os firewalls das filiais, uma vez que a SD-WAN inclui NGFW e segmentação de ponta a ponta.

AS PRINCIPAIS ÁREAS DE NEGÓCIO DA ORGANIZAÇÃO - A SEGURANÇA APLICACIONAL E O GRC – COMPLEMENTAM-SE DE FORMA A GARANTIR A SEGURANÇA EM TODO O CICLO DE VIDA DO DESENVOLVIMENTO APLICACIONAL.

BALWURK:

"PRETENDEMOS APOIAR E CAPACITAR AS EMPRESAS NO MOVIMENTO DENOMINADO POR SHIFT LEFT SECURITY"

▶ MARTA QUARESMA FERREIRA

O nascimento da Balwurk cruza-se com a vontade dos sócios da Xpand IT em criarem uma empresa de cibersegurança que colmatasse falhas ao nível de segurança, nomeadamente no desenvolvimento de software por parte das organizações.

Considerada uma empresa irmã da Xpand IT, a Balwurk desenvolve, no entanto, o seu trabalho de forma independente, em duas áreas de negócio dis-

RICARDO RODRIGUES, BALWURK

tintas: Segurança Aplicacional e GRC. O objetivo é comum e passa por garantir a segurança, *by design* e *by default*, em todo o ciclo de vida do desenvolvimento aplicacional. A área de Segurança Aplicacional é complementada com os serviços de GRC, com respostas ao nível regulatório, de conformidade e de análise de risco.

"Pretendemos apoiar e capacitar as empresas no movimento denominado por Shift Left Security, que significa trazer a segurança enquanto requisito prematuramente para o processo de desenvolvimento de software, também conhecido por security by design", começa por explicar Ricardo Rodrigues, Head of Application Security & GRC da Balwurk.

Para além do Regulamento Geral sobre Proteção de Dados (RGPD), Ricardo Rodrigues considera que a proposta de criação do Cyber Resilience Act (CRA) a nível europeu é um dos grandes contributos para a evolução do negócio da Balwurk.

CLIENTES E ORGANIZAÇÃO DO NEGÓCIO

Ao nível das exigências dos clientes, o Head of Application Security & GRC da Balwurk aponta para "uma maior consciencialização das suas necessidades e exigência com o valor acrescentado na contratação dos serviços e produtos".

Tanto as unidades de Segurança Aplicacional como de GRC, e respetivo portfólio de serviços, estão construídos "para dar resposta adequada às necessidades das organizações, independentemente do nível de maturidade das mesmas".

"PRETENDEMOS APOIAR E CAPACITAR AS EMPRESAS NO MOVIMENTO DENOMINADO POR SHIFT LEFT SECURITY, QUE SIGNIFICA TRAZER A SEGURANÇA ENQUANTO REQUISITO PREMATURAMENTE PARA O PROCESSO DE DESENVOLVIMENTO DE SOFTWARE, TAMBÉM CONHECIDO POR SECURITY BY DESIGN"

> AS TENDÊNCIAS E AMEAÇAS IDENTIFICADAS "CONSTITUEM, EM SI, UMA VERDADEIRA OPORTUNIDADE DE MELHORIA PARA A QUAL A BALWURK ESTÁ TOTALMENTE DISPONÍVEL PARA CONTRIBUIR COM A NOSSA MISSÃO DE AJUDAR A CONSTRUIR UM MUNDO DIGITAL MAIS SEGURO".

Neste ponto, a Balwurk defende que o nível de maturidade das organizações, no que respeita à segurança aplicacional, "é tanto maior quanto mais cedo começarem a aderir ao movimento "Shift Left Security", apostando fortemente numa postura preventiva que diminui a reatividade, "investindo na transição do ciclo DevOps para o ciclo DevSecOps".

"Neste ciclo, o primeiro passo é o Planeamento, e nele incluímos os nossos serviços de 'Educação e Cultura', a par com o de 'Modelação de Ameaças'", esclarece Ricardo Rodrigues.

A "Educação e Cultura" para a segurança é "um serviço adaptado às reais necessidades das organizações, desenvolvendo conteúdos específicos para as equipas de desenvolvimento, procurando o envolvimento de todas as partes interessadas e participantes no ciclo de vida do desenvolvimento aplicacional e na integração operacional das mesmas, designadamente no ciclo DevSecOps".

No caso da "Modelação de Ameaças", o objetivo passa por "analisar a arquitetura na qual a solução aplicacional está inserida e todo o ecossistema envolvente, confrontando os requisitos funcionais da mesma com um conjunto pré-definido de cenários que ajudam a identificar possíveis ameaças de segurança e conformidade".

O AUMENTO DA IMPORTÂNCIA DA CIBERSEGURANÇA

A Balwurk tem acompanhado de perto os episódios de ciberataques em Portugal "com muita atenção". Presentes no mercado português desde janeiro de 2023, a organização tem procurado criar junto dos projetos dos clientes "uma verdadeira e consistente consciencialização, provando o real valor de retorno com os nossos serviços".

Ricardo Rodrigues considera que existe uma consciencialização cada vez maior para este tema a nível nacional. No entanto, há ainda dificuldade em "transformar essa consciência em resultados efetivos". As tendências e ameaças identificadas "constituem, em si, uma verdadeira oportunidade de melhoria para a qual a Balwurk está totalmente disponível para contribuir com a nossa missão de ajudar a construir um mundo digital mais seguro". ◀

SOPHOS AJUDA AUTOZITÂNIA A MITIGAR POSSÍVEIS CIBERAMEAÇAS COM SOLUÇÃO 24/7

MARTA QUARESMA FERREIRA

A IMPLEMENTAÇÃO DO SOPHOS MDR PERMITIU À AUTOZITÂNIA CONTAR COM UMA EQUIPA DE ESPECIALISTAS DA SOPHOS QUE MONITORIZA E NEUTRALIZA POSSÍVEIS AMEAÇAS, PERMITINDO QUE AS EQUIPAS DE IT DA ORGANIZAÇÃO SE FOQUEM NOUTRAS QUESTÕES

A Autozitânia procurava uma solução para prevenir possíveis ciberataques que pudessem pôr em causa a continuidade das operações e da qualidade do serviço prestado aos clientes.

De forma a reagirem às ameaças de forma célebre, a empresa de importação e distribuição de peças


VICTOR HUGO, INOVFLOW


BERNARDETE CARVALHO, SOPHOS

de automóveis optou pela implementação de um Centro de Operações de Segurança (SOC) externo.

"Apesar de na Autozitânia termos uma equipa de IT estruturada, o volume de projetos e solicitações a que a nossa equipa é exposta diariamente não se alinhava com uma gestão interna dos desafios da cibersegurança. Atualmente, entendemos que esta área obriga a uma atenção 24/7 e a um investimento sistemático na obtenção de conhecimento, que seriam impossíveis com os nossos recursos internos, e foi maioritariamente isso que nos fez decidir por externalizar", começa por explicar José Mendes, IT Manager da Autozitânia.

A SOLUÇÃO ENCONTRADA E A SUA IMPLEMENTAÇÃO

A escolha recaiu na solução Sophos Managed Detection and Response (MDR), apresentada pela Inovflow, com garantias de cobertura 24/7 ao nível da cibersegurança.

Para Victor Hugo, Business Developer da Inovflow, a implementação do Sophos MDR permitiu à Autozitânia "fazer uma avaliação ao estado da sua segurança para, posteriormente, e com as devidas medidas corretivas, alinhar o caminho em conjunto".

"A Sophos disponibilizou à Autozitânia uma equipa de especialistas dedicados e com experiência, que impede os ataques avançados e toma as medidas necessárias para neutralizar as possíveis ameaças antes que estas causem impacto nas operações e comprometam informação sensível", acrescenta Bernardete Carvalho, Territory Account Manager da Sophos.

Esta solução veio também ajudar a Autozitânia a agilizar a complexidade inerente ao recrutamento, formação e manutenção de equipas de analistas. "A

> "APESAR DE NA AUTOZITÂNIA TERMOS UMA EQUIPA DE IT ESTRUTURADA, O VOLUME DE PROJETOS E SOLICITAÇÕES A QUE A NOSSA EQUIPA É EXPOSTA DIARIAMENTE NÃO SE ALINHAVA COM UMA GESTÃO INTERNA DOS DESAFIOS DA CIBERSEGURANÇA. ATUALMENTE, ENTENDEMOS QUE ESTA ÁREA OBRIGA A UMA ATENÇÃO 24/7 E A UM INVESTIMENTO SISTEMÁTICO NA OBTENÇÃO DE CONHECIMENTO, QUE SERIAM IMPOSSÍVEIS COM OS NOSSOS RECURSOS INTERNOS, E FOI MAIORITARIAMENTE ISSO QUE NOS FEZ DECIDIR POR EXTERNALIZAR"
>
> JOSÉ MENDES, IT MANAGER DA AUTOZITÂNIA

tentativa de criar um centro de operações de segurança completo e a realidade de gerir a sua própria oferta de cibersegurança como serviço está simplesmente fora do alcance de praticamente todas as organizações de TI, e nisto o Sophos MDR pode ajudar", refere Bernardete Carvalho.

A implementação da solução ocorre de forma "rápida, fácil, *user-friendly*" e é totalmente administrada a partir da consola de gestão única e integrada - a Sophos Central.

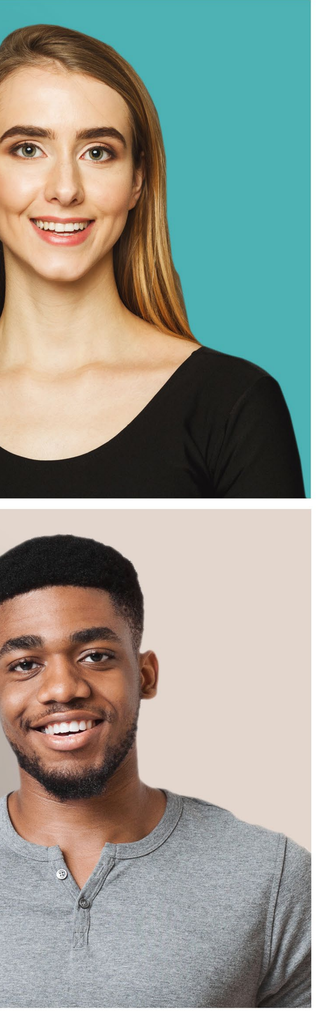
Entre as várias vantagens do Sophos MDR destacam-se: o serviço de deteção e resposta 24/7, 365 dias por ano; tempo de resposta médio de 38 minutos em resolução de incidentes; e relatórios semanais e mensais.

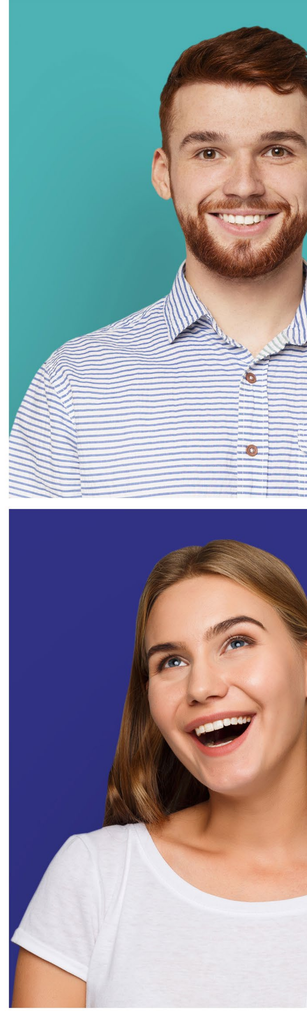
"Mesmo com muitas camadas de segurança, existe sempre a possibilidade de ocorrer um ataque, e nisto o Sophos MDR também é um bom apoio, devido à rápida reação e resolução", reitera Victor Hugo da Inovflow.

RESULTADOS QUE SE REFLETEM NO NEGÓCIO

"Já temos [Sophos] MDR há seis meses, e desde então contamos com uma equipa que está disponível 24 horas por dia, sete dias por semana para detetar qualquer possível ameaça à segurança da Autozitânia e, consequentemente, neutralizar e mitigar a mesma", explica José Mendes, IT Manager da Autozitânia. A organização optou por uma intervenção total da equipa técnica da Sophos, o que se tem refletido num "maior descanso" no que diz respeito à proteção dos dados e, como consequência, do próprio negócio.

A Autozitânia conta agora com uma equipa de IT dedicada às suas áreas, sem que ponha em risco a segurança da empresa, melhorando a produtividade das pessoas. "[A solução da Sophos] deu-nos também a garantia de que temos uma equipa altamente especializada e que nos acompanha 24/7, para evitar que o nosso foco deixe de estar onde deve estar: no *core* do nosso negócio", conclui José Mendes.





#15 DEZEMBRO 2023

OBRIGADO POR TER LIDO A

IT Insight SECURITY

Se ainda não é um leitor registado da IT Insight Security e para ter acesso a todo o nosso conteúdo registe os seus dados profissionais aqui

Conheça a política de privacidade da IT Insight Security aqui

IT Insight SECURITY

PUBLISHER: Jorge Bento
DIRETOR : Rui Damião - rui.damiao@medianext.pt
ANCHOR: Henrique Carreiro
REDAÇÃO: Marta Quaresma Ferreira, Rita Sousa e Silva
BUSINESS DEVELOPMENT:
Beatriz Salzedas - (+351) 910 788 082 - beatriz.salzedas@medianext.pt
João Calvão - (+351) 910 788 413 - joao.calvao@medianext.pt
MARKETING & EVENTS DIRECTOR:
Rosa Bento - rosa.bento@medianext.pt
MARKETING COMMUNICATIONS ASSISTANT:
Rita Rodrigues - (+351) 912 971 161 - rita.rodrigues@medianext.pt
ARTE E PAGINAÇÃO: Teresa Rodrigues
FOTOGRAFIA: Rui Santos Jorge
DESENVOLVIMENTO WEB: Global Pixel
COLABORARAM NESTE NÚMERO: Cristiane Dias

A REVISTA DIGITAL INTERATIVA IT INSIGHT SECURITY É EDITADA POR:
MediaNext Professional Information Lda.
PERIODICIDADE: Bimestral

CEO: Pedro Botelho

SEDE E REDAÇÃO: Largo da Lagoa, 7c, 2795-116 Linda-a-Velha, Portugal
TEL: (+351) 214 147 300 | **FAX**: (+351) 214 147 301

REGISTO E.R.C
Entidade Reguladora para a Comunicação Social nº 127602

Consulte aqui o Estatuto Editorial

IT Insight Security é membro de:

ASSOCIAÇÃO PORTUGUESA DE IMPRENSA

acepi ASSOCIAÇÃO PARA O COMÉRCIO ELECTRÓNICO E PUBLICIDADE INTERACTIVA

CIWA COMPETITIVE INTELLIGENCE & INFORMATION WARFARE ASSOCIATION

Editado por:

media NEXT