IT Insight SECURITY

#13 AGOSTO 2023

O ESTADO DA NAÇÃO

... em cibersegurança

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

O ESTADO DA NAÇÃO

... em cibersegurança

START

TALENTO E REGULAMENTAÇÃO NA CIBERSEGURANÇA

ANCHOR

A SEGURANÇA DAS PLATAFORMAS DE IA É UM DESAFIO CRESCENTE PARA AS ORGANIZAÇÕES

NEWS

COVERAGE

EXPERT

SÉRGIO MARTINHO, LUSITANIA SEGUROS

NUNO NEVES, ANF

EDUARDO MAGRANI, CCA

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

BROWSE S.LABS

S.LABS

arcserve®

As empresas não compreendem bem as suas responsabilidades no que respeita à segurança dos dados na cloud

Bravantic® // Evolving Technology

O Estado da Cibersegurança em Portugal: desafios emergentes e estratégias de proteção

cipher a PROSEGUR company

Criando um plano para o sucesso

paloalto® NETWORKS

Habilitar o negócio e a segurança em conjunto: o valor do SASE

redShift

Estado da Nação: o impacto é real

S21SEC Cyber Solutions by Thales

Cibersegurança industrial:
Riscos e estratégias de mitigação

SECURNET ALWAYS ONLINE | ALWAYS SECURE

A (ciber)maturidade

SOPHOS Cybersecurity delivered.

O cibercrime afeta cada vez mais a administração pública

visionware

Ciberterrorismo e ameaças cibernéticas:
como defender (o Estado de) uma Nação?

Westcon

Melhorar a ciber-resiliência organizacional

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.

O ransomware aumentou 70% na Administração Pública no decorrer de um ano.

Atue contra as ameaças com um serviço gerido por especialistas

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: sophos.com/mdr

SOPHOS

230714 PTBR (PC)

TALENTO E REGULAMENTAÇÃO NA CIBERSEGURANÇA

RUI DAMIÃO

Ao falar com profissionais de cibersegurança – seja em entrevistas, pequenos encontros ou mesas-redondas – e questionar quais são os principais desafios com que têm de lidar – para além das ciberameaças em si –, a resposta é quase sempre a mesma: escassez de recursos e *compliance*.

Sobre as ciberameaças já todos sabemos qual é a realidade: são cada vez maiores, quase todos os dias há uma nova vulnerabilidade descoberta e é preciso mitigar, tanto quanto possível, o impacto que essa – e todas as outras que ainda não foram efetivamente resolvidas – possa ter.

Mas a escassez de recursos é um tema cada vez mais habitual entre os profissionais de cibersegurança. Esses recursos são, naturalmente, financeiros e humanos. Se o IT, de um modo geral, sente a falta de recursos humanos, qualquer área mais especializada dentro de um IT mais generalizado terá mais problemas; em cibersegurança não é exceção.

Como foi referido na mesa-redonda que é a capa da edição deste mês, as organizações portuguesas – sejam elas os clientes finais ou os integradores que fornecem o serviço – têm de lidar com a concorrência nacional e estrangeira pelos recursos nacionais, o que dificulta manter os recursos – que nem sempre são valorizados – ligados à organização.

Com a introdução de várias regulamentações a nível europeu que impactam, de forma mais ou menos direta, a cibersegurança, os profissionais da área têm de olhar para o ponto em que estão, o ponto onde têm de passar a estar num determinado período e qual o caminho a definir.

Em 2022, a IT Security realizou a sua primeira mesa-redonda dedicada ao Estado da Nação de Cibersegurança. Este ano voltámos a realizar um fórum sobre o mesmo tema onde 11 profissionais ligados à cibersegurança partilharam a sua visão sobre os temas mais importantes dentro da área.

Para o ano vamos voltar a realizar. Em julho, mês em que muitos governos mundiais fazem o seu próprio Estado da Nação, a IT Security vai voltar a olhar para o estado da cibersegurança no país, sobre o que se passou este ano. Será o talento e a legislação ainda um tema em cima da mesa? ◀

redShift

Especialistas em *Transformação* Digital

Aceleramos a transformação digital do seu negócio, com a implementação de soluções tecnológicas inovadoras.

Cibersegurança e Redes

Gestão de Informação

Low Code

Cloud & Centro de Dados

Outsourcing Especializado

Saiba como podemos
ajudar a sua empresa

A SEGURANÇA DAS PLATAFORMAS DE IA

É UM DESAFIO CRESCENTE PARA AS ORGANIZAÇÕES

HENRIQUE CARREIRO

A inteligência artificial está a tornar-se cada vez mais ubíqua, com sistemas de IA a serem utilizados numa vasta gama de aplicações, desde carros autónomos até diagnósticos médicos. No entanto, o crescente uso da IA também está a aumentar os riscos de segurança informática.

Um novo relatório da ENISA, "*A multilayer framework for good cybersecurity practices for AI*", alerta que o uso indevido da IA se tornará uma ameaça significativa nos próximos anos. O relatório identifica uma série de vulnerabilidades que podem ser exploradas para comprometer sistemas de IA, incluindo:

- **Dados maliciosos:** os sistemas de IA podem ser comprometidos se forem treinados em dados maliciosos, como imagens ou texto que foram alterados para enganar o sistema;
- **Ataques de negação de serviço**: os sistemas de IA podem ser sobrecarregados com ataques de negação de serviço, que podem impedir que funcionem corretamente;

• **Ataques de malware**: os sistemas de IA podem ser infetados por malware, que pode ser usado para roubar dados ou controlar o sistema;
• **Ataques de engenharia social**: os sistemas de IA podem ser enganados por agentes maliciosos que se fazem passar por pessoas confiáveis.

O referido relatório da ENISA também identifica uma série de medidas que podem ser tomadas para melhorar a segurança da IA, incluindo:

• Melhorar a qualidade dos dados utilizados para treinar sistemas de IA;
• Desenvolver sistemas de IA que sejam resistentes a ataques de negação de serviço;
• Desenvolver sistemas de IA que sejam resistentes a malware;
• Educar os utilizadores sobre os riscos de segurança da IA.

PROTEGER AS INFRAESTRUTURAS DE IA

Muito se tem falado, desde há alguns anos, na utilização da IA em cibersegurança, especialmente em duas vertentes. A primeira é no seu uso por parte dos atacantes, para melhor identificação e caracterização dos alvos. O outro, é no lado da defesa, já que só com o uso de IA é possível combater ataques cada vez mais sofisticados e otimizados, quando não gerados, por IA.

Tem-se falado menos na segurança das próprias infraestruturas de suporte a IA, talvez porque os riscos que comportam são, alegadamente, idênticos aos que podem ser esperados noutras áreas aplicacionais. Mas esta é, claramente, uma aproximação insuficiente. Não apenas a natureza do código de IA é diferente da de sistemas tradicionais – nomeadamente por ser francamente menos auditável – como a própria segurança tem de começar nos dados usados para treinar os sistemas. Por outro lado, as infraestruturas também têm uma arquitetura diferente, nomeadamente por serem muito mais dependentes de GPU do que qualquer outro sistema tradicional.

Em geral, estamos a falar de sistemas recentes, com muita tecnologia que é dominada por muito pouca gente dentro das organizações, com código que tem estado a evoluir a ritmo de atualizações semanais, em particular se estivermos a falar de sistemas LLM baseados em código aberto e auto-hospedados. Em muitos casos, não estão ainda interiorizadas boas práticas de engenharia de software e de operações. Definidas sim, até poderão estar, mas em muitos casos as equipas não tiveram ainda tempo, ou não geraram ainda a massa crítica, ou não sentiram a premência, para as colocarem em prática. O que significa que os sistemas de IA que muitas organizações poderão estar a implementar, desde os *chatbots* até outras mais próximas do núcleo do negócio, poderão estar vulneráveis a riscos não necessariamente identificados, menos ainda salvaguardados.

É por isso que recomendações com as agora apresentadas pela ENISA podem ser de grande utilidade. A ENISA, como outras organizações internacionais com semelhante missão, estão cientes do que há para fazer e estão a investir significativamente nesta codificação de boas práticas e elaboração de *checklists*. Avisadas andarão as organizações que procurem preparar-se – usando estes e outros materiais de idêntica natureza – para o que inevitavelmente virá a acontecer. *Secure by design* não tem sido a preocupação principal dos criadores de sistemas de IA, mas rapidamente, mais do que certamente esperamos, vai ter de passar a ser. ◀

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

UE ANUNCIA NOVO ACORDO SOBRE TRANSFERÊNCIAS DE DADOS PARA OS EUA

A EU-U.S. Data Privacy Framework foi, ainda assim, contestada.

A União Europeia assinou um novo acordo sobre a privacidade dos dados pessoais dos cidadãos europeus para o outro lado do Atlântico. De acordo com a Comissão Europeia, a *EU-U.S. Data Privacy Framework* tem um nível adequado de proteção de dados pessoais e abarca os padrões de todos os Estados-membros, para que as empresas o possam usar nas transferências de dados, sem necessitar de adicionar medida de segurança extra.

Joe Biden, presidente dos EUA, assinou uma ordem executiva em outubro para implementar o acordo, depois de chegar a um acordo preliminar com a presidente da Comissão Europeia, Ursula von der Leyen, num esforço para resolver a batalha sobre a segurança dos dados dos cidadãos da UE que as empresas de tecnologia armazenam nos EUA.

"Os dados pessoais podem agora fluir livremente e em segurança do Espaço Económico Europeu para os EUA sem quaisquer outras condições ou autorizações", disse o Comissário Europeu da Justiça, Didier Reynders. ◀

CISA ADICIONA FALHA NO ANDROID À LISTA DE VULNERABILIDADES EXPLORADAS

A falha, descoberta em 2021, está a ser ativamente explorada e permite ganhar acesso a informação sensível em dispositivos Android.

A CISA ordenou as agências governamentais norte-americanas a corrigir uma falha de alta severidade no Arm Mali GPU kernel driver, tendo-a adicionada à lista de vulnerabilidades ativamente exploradas e endereçada nas atualizações de segurança do Android deste mês.

A falha – CVE-2021-29256 – permite aos atacantes escalar para privilégios root e ganhar acesso a informação sensível no dispositivo Android através de operações na memória GPU.

Na atualização de segurança deste mês, a Google corrigiu outras duas vulnerabilidades no Android, nomeadamente uma falha de severidade média no Arm Mali GPU driver. ◀

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

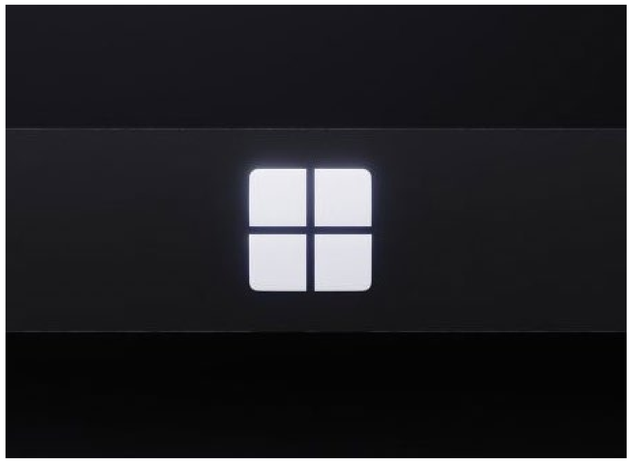
Helping your business **grow faster**

Portugal · Espanha · Irlanda · Holanda · Brasil · EUA

www.noesis.pt

MICROSOFT FAZ ALTERAÇÕES NO SISTEMA DE SIGNING KEY

A Microsoft anunciou mudanças no sistema que foi explorado por cibercriminosos para aceder a contas de email de duas dúzias de organizações.



A Microsoft anunciou que vai fazer alterações ao sistema signing key que foi explorado por cibercriminosos chineses no último mês para conseguir ter acesso a contas de email e espiar duas dúzias de organizações – incluindo agências governamentais.

O cibergrupo infiltrou-se nas contas através de tokens de autenticação – que são utilizados para validar a identidade de quem está a pedir acesso ao recurso, neste caso, o email – forjados. O grupo cibercriminoso utilizou signing key de consumidores inativos para criar tokens.

O ciberataque terá começa a 15 de maio e a Microsoft referiu anteriormente que o grupo "explorou um problema com o token de validação", não se tendo alongado sobre a vulnerabilidade específica que foi explorada. No final da última semana, a Microsoft publicou no seu blog e explicou um pouco mais o que aconteceu e qual foi a resposta ao incidente. ◀

APPLE LANÇA ATUALIZAÇÃO URGENTE PARA SISTEMAS OPERATIVOS IOS

De acordo com a Apple, a vulnerabilidade zero-day já foi ativamente explorada.

A Apple lançou uma atualização de software urgente para os seus sistemas operativos iOS e iPadOS e alertou que já foi detetada uma exploração zero-day. A vulnerabilidade detetada foi rastreada como CVE-2023-37450.

O lançamento do iOS 16.5.1 e iPadOS 16.5.1 surge no seguimento do processo de "respostas rápidas de segurança" que a empresa adotou e é agora adotado pela segunda vez. Segundo um comunicado da tecnológica de Cupertino, citado pela SecurityWeek, a falha de segurança foi observada no WebKit, um motor de browser utilizado pelos dispositivos Apple, como no Safari, Mail ou AppStore.

"O processamento de conteúdo da Web pode levar à execução arbitrária de código. A Apple está consciente de um relatório de que esse problema pode ter sido explorado ativamente. O problema foi resolvido com verificações aprimoradas", disse a Apple. ◀

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

MAIS DE 200 MIL SITES DO WORDPRESS EXPOSTOS POR FALHA EM PLUGIN

Plugin Ultimate Member, utilizado por mais de 200 mil sites no WordPress, tem uma vulnerabilidade crítica que está a ser explorada por atacantes.

Mais de 200 mil sites do WordPress estão expostos a ataques depois de ter sido descoberta uma vulnerabilidade crítica no plugin Ultimate Member. A vulnerabilidade (CVE-2023-3460) tem uma criticidade de 9.8 em dez e permite a atacantes adicionar novas contas de utilizadores ao grupo de administradores.

O plugin foi criado para tornar mais fácil o registo e login de utilizadores nos sites, podendo adicionar perfis, definir *roles*, criar campos personalizados e diretórios de membros, entre outros.

Alguns utilizadores deste plugin observaram a criação de contas e reportaram o problema na última semana, mas, ao que tudo indica, os ataques a este plugin terão começado no início de junho.

Neste momento, quem tem este plugin instalado deverá rever todas as contas de administrador do site e identificar eventuais contas rogue. ◀

DISPOSITIVOS MÓVEIS SÃO CADA VEZ MAIS OS ALVOS PREFERIDOS PARA CIBERATAQUES

Com um número crescente de empresas e trabalhadores dependentes deste tipo de dispositivos, o número médio de amostras únicas de malware móvel cresceu 51% em 2022.

Os dispositivos móveis são cada vez mais um alvo entre os ciberatacantes. Os dados revelados pelo '*Global Mobile Threat Report*' de 2023 da empresa Zimperium demonstram que as ameaças surgem em vulnerabilidades nos serviços que são incorporados em aplicações nos sistemas Android e iOS.

Em 2022, o número médio de amostras únicas de malware móvel cresceu 51%, num total de 77 mil amostras encontradas todos os meses. 23% das amostras de aplicações Android e 24% das amostras de aplicações iOS enviadas a repositórios públicos eram maliciosas.

Como consequência, o número de dispositivos comprometidos quase triplicou, com uma média de quatro links de phishing maliciosos acedidos por dispositivo.

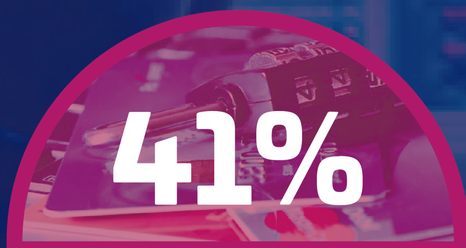
Em 2022, a maioria das empresas viu os seus trabalhadores (58%) a utilizarem mais estes dispositivos, em comparação com 2021. ◀

MDR

Serviço de Monitorização e Resposta que combina a visibilidade da infraestrutura fornecida pelo SIEM e as capacidades de deteção e resposta da plataforma EDR. Concebido para se alinhar com as necessidades do cliente, **respondendo a incidentes de forma automática**.

38%

É o crescimento dos ciberataques globais durante 2022 em comparação com 2021



41%

Dos incidentes de segurança ocorridos em 2022 envolveram phishing, malware ou ransomware.

43%

Dos ataques tiveram como alvo as PME, onde a segurança é menos robusta.

Que vantagens oferece?

Alinhado com as necessidades e pontos críticos da empresa.

Monitorização global com recurso a múltiplas tecnologias.

Ferramenta exigida em vários regulamentos e normas, como DORA y NIS2

Resposta automatizada a incidentes e resposta forense a incidentes críticos.

Evolução e inovação alinhadas com a maturidade do cliente.

Enriquecido com Threat Intel da S21sec.

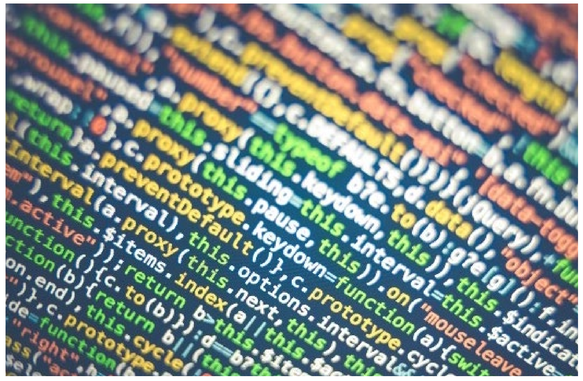
Solicite uma chamda com um ***Especialista da S21sec***

+351 220 107 120 marketing@s21sec.com www.s21sec.com

S21 SEC
Cyber Solutions by Thales

REGISTADOS NOVOS ATAQUES DO EMOTET NO SUL DA EUROPA

Desde o seu ressurgimento no final de 2021, a família de malware Emotet lançou múltiplas campanhas de spam e, desde 2022, a maioria dos ataques detetados por uma empresa de cibersegurança visaram os países do sul da Europa e Japão.



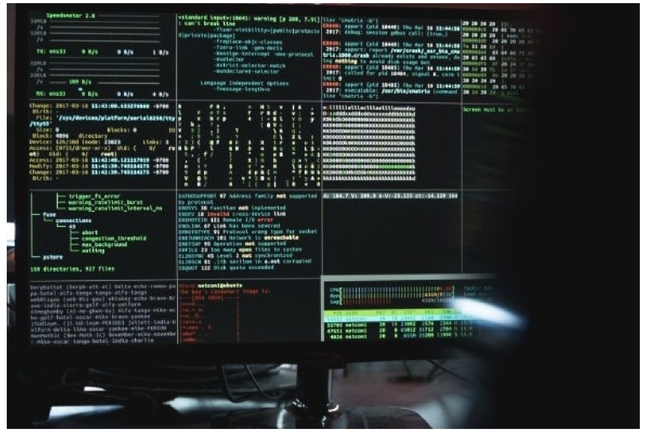
A Eset revelou as mais recentes atividades do infame Emotet desde o seu regresso à paisagem das ciberameaças no final de 2021.O Emotet é uma família de malware ativa desde 2014, operada por um grupo cibercriminoso conhecido como Mealybug ou TA542.

Embora tenha começado como um trojan bancário, o Emotet evoluiu mais tarde para uma rede de dispositivos online infetados com malware – ou botnet – tornando-se numa das ciberameaças mais prevalentes em todo o mundo.

Em janeiro de 2021, o Emotet foi alvo de um *takedown* limitado, em resultado de um esforço internacional e colaborativo de oito países, coordenado pela Eurojust e Europol. No entanto, o Emotet voltou ao ativo em novembro de 2021 com várias campanhas de spam, que terminaram abruptamente em abril de 2023. ◀

MAIORIA DAS EMPRESAS INDUSTRIAIS ATINGIDAS POR RANSOMWARE SOFRERAM ENCRIPTAÇÃO DOS DADOS

Estudo revela que dois terços das empresas industriais veem os seus dados encriptados após um ataque de ransomware e que esta é a taxa de encriptação mais elevada dos últimos três anos.



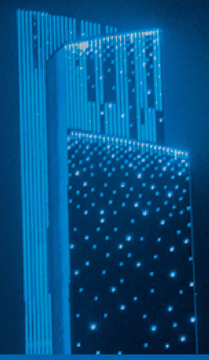
A Sophos lançou um novo relatório de investigação, "*The State of Ransomware in Manufacturing and Production 2023*", dedicado ao setor da produção industrial. A empresa concluiu que os criminosos encriptaram dados com sucesso em mais de dois terços (68%) dos ataques de ransomware contra este setor.

Esta é a maior taxa de encriptação registada nos últimos três anos e está em linha com uma tendência de mercado mais ampla de os atacantes conseguirem encriptar dados com mais frequência.

No entanto, em contraste com outras indústrias, a percentagem de empresas do setor da produção industrial que utilizou cópias de segurança para recuperar dados aumentou, para 73% contra 58% no ano anterior. Apesar deste aumento, o setor continua a ter uma das taxas de recuperação de dados mais baixas. ◀

visionware

Challenging an Unsafe World



LEALDADE

DISCRIÇÃO

DEDICAÇÃO

SOBRE

A nossa missão é contribuir para o Sucesso dos nossos clientes, aumentando a sua cultura e maturidade em Segurança da Informação.

SERVIÇOS

- CYBERSECURITY
- CYBER DEFENSE OPERATIONS - SOC & CSIRT
- FORENSIC INVESTIGATIONS
- PRIVACY & LEGAL — GDPR | RGPC | WHISTLEBLOWING
- ETHICS & CORPORATE COMPLIANCE
- STRATEGIC INTELLIGENCE
- PROFESSIONAL SERVICES
- TRAINING | VISIONWARE ACADEMY

SCAN ME

VISIONWARE.PT

visionwaresi

geral@visionware.pt

+351 225 323 740

PORTUGAL Porto | Lisboa

CABO VERDE Praia | Mindelo

ANUNCIADOS PRIMEIROS ORADORES DA IT SECURITY CONFERENCE

Fique a conhecer os primeiros oradores confirmados para a conferência organizada pela IT Security, que terá lugar em Lisboa a 12 de outubro.

No dia 12 de outubro de 2023, em Lisboa, a IT Security realiza a segunda edição da sua conferência que vai cobrir os principais conteúdos relacionados com o ecossistema de cibersegurança. *Pode pedir o seu voucher gratuito para a IT Security Conference*.

A IT Security já anunciou os primeiros oradores que vão marcar presença na conferência de 12 de outubro. Lino Santos, Coordenador do Centro Nacional de Cibersegurança, fará o *keynote* de abertura e Luís Morais, Chief Information Security Officer na Galp, também irá subir ao palco da IT Security Conference. João Camões, da Secretaria-Geral de Economia, José Alegria, da Altice, e Paulo Moniz, da EDP, vão participar na mesa-redonda "Como Aumentar a Ciber-Resiliência das Organizações" e Aurélio Blanquet, da EE-ISAC, Pedro Rodrigues, do Banco de Portugal, Rafael Aranha, da REN, e Dinis Fernandes, da Cybersafe, sobem ao palco para a mesa-redonda "Serviços Críticos e Operações de Segurança".

Também já estão confirmados na IT Security Conference Margarida Leitão Nogueira, da DLA Piper, Nuno Neves, da Associação Nacional de Farmácias, e Joaquim Godinho, da Universidade de Évora, assim como Paulo Vieira, da Palo Alto Networks, Paulo Rio, da HPE Aruba Networking, Vasco Sousa, da Arcserve, David Grave, da Claranet, Rui Barata Ribeiro, da IBM Portugal, Luís Lança, da Logicalis, João Manso, da Redshift, Rui Antunes, da Cisco, Paulo Pinto, da Fortinet, João Arriaga, da SealPath, Pedro Monteiro, da Varonis, e Bruno Castro, da VisionWare.

A IT Security Conference realiza-se a 12 de outubro n'O Clube – Monsanto Secret Spot, em Lisboa. Pode pedir o seu voucher no site da conferência. A Palo Alto Networks, a HPE Aruba Networking, a Sophos, a Arcserve, a Cato Networks, a Claranet, a IBM, a Logicalis, a Redshift, a S21sec, a Cisco, a Cybersafe, a Dell Technologies, a Fortinet, a SealPath, a Varonis, a VisionWare, a WatchGuard, a Lenovo, a Balwurk, a Divultec, a LG, a Westcon, a Arrow e a Ingecom são parceiras do evento, enquanto o Centro Nacional de Cibersegurança é parceiro institucional. ◀

xMDR

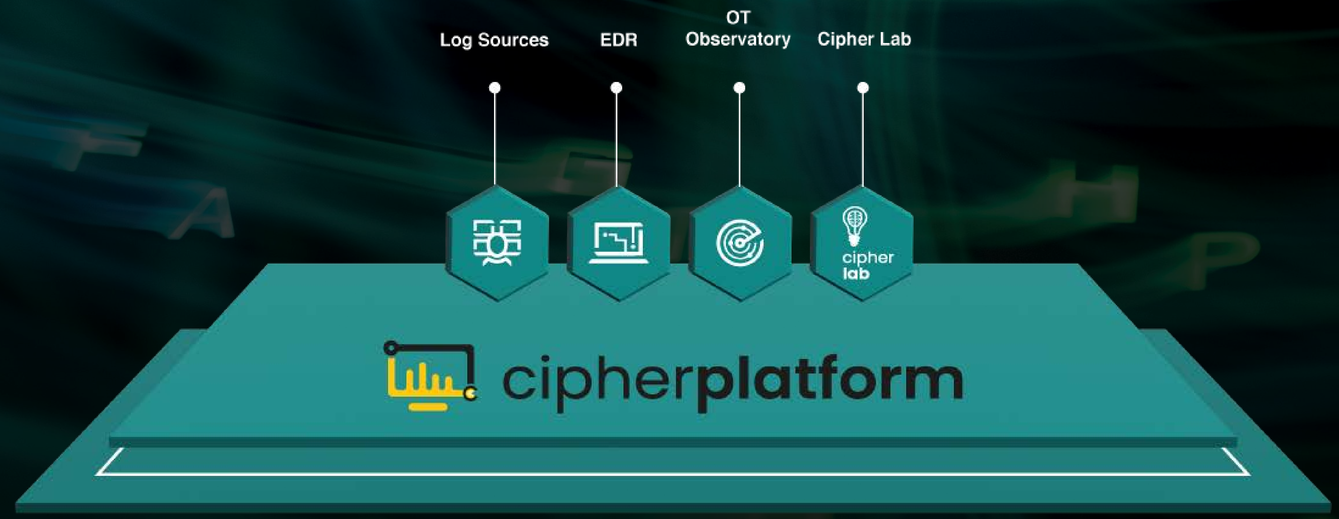
powered by cipher
a Prosegur company

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



MODELAGEM DE ADVERSÁRIO + COGNITIVO → CIPHER PLATFORM → SISTEMA DE DETECÇÃO SEM PRECEDENTES

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

www.cipherxmdr.io cipher ciphersec ciphersec

paloalto NETWORKS

HABILITAR O NEGÓCIO E A SEGURANÇA EM CONJUNTO:

O VALOR DO SASE

A SEGURANÇA COSTUMA SER CONSIDERADA UMA APÓLICE DE SEGURO. MAS NÃO FALAMOS DAS FORMAS ATRAVÉS DAS QUAIS AS NOSSAS ESCOLHAS DE SEGURANÇA PODEM REALMENTE VIABILIZAR OS NEGÓCIOS E EXPANDIR O QUE É POSSÍVEL DENTRO DAS ORGANIZAÇÕES. A SEGURANÇA PODE SER UMA FERRAMENTA PARA RESILIÊNCIA E INOVAÇÃO.

Aprender a maximizar o valor que a segurança pode oferecer geralmente vem de algumas fontes importantes: a primeira delas é olhar para dentro da nossa organização e estabelecer um alinhamento entre decisores para entender as necessidades e os fluxos de trabalho dos negócios.

Entrevistar decisores dentro das várias unidades de negócio dentro da organização para entender as suas necessidades é um primeiro passo e muito importante. O conhecimento adquirido permite decisões mais informadas e ajuda a implementar tecnologias de segurança que suportam e até aceleram o sucesso da organização. O segundo passo, consiste em adquirir conhecimento sobre os desafios que as organizações externas que foram vítimas de ataques tiveram de enfrentar.

MUITO MAIS DO QUE O “SEGURO” DE SEGURANÇA PARA A CAPACITAÇÃO DO NEGÓCIO

Os decisores nas organizações que adotam a antiga abordagem de “segurança como apólice de seguro” continuam a olhar para a cibersegurança como um custo. A realidade, porém, é que os investimentos em cibersegurança também podem ser um importante método de redução de custos para as organizações, protegendo o valor do negócio.

Para isto acontecer, é necessário pensar que a cibersegurança é um investimento que vai muito além do custo de compra.

O que acontece se a organização for atacada e não estiver segura? Quais os custos intangíveis que a organização economiza – associados a tudo, desde a implementação até à gestão ou se fizerem escolhas sensatas na hora de inves-

tir em cibersegurança. Algumas soluções modernas de cibersegurança capacitam as organizações de uma forma que vai muito além da continuidade do negócio. Uma delas é o SASE.

SASE NÃO É APENAS SOBRE SEGURANÇA

Fundamentalmente, o SASE fornece duas coisas principais: conectividade e segurança. No lado da conectividade, a implementação do SASE fornece formas de trabalhar remotamente altamente resilientes. A peça de segurança é que o SASE fornece segurança integrada profundamente incorporada nas mesmas tecnologias que fornecem os recursos de conectividade. Portanto, o SASE não trata apenas de fornecer ferramentas de segurança aos utilizadores corporativos, mas também de criar formas de trabalhar com segurança.

Hoje, é possível ter colaboradores que trabalham remotamente utilizando o seu *laptop* ligado por meio de uma arquitetura SASE usando o Prisma Access da Palo Alto Networks. Com esta nova abordagem as equipas de TI oferecem suporte aos colaboradores que trabalham remotamente, sem a necessidade de grandes quantidades de hardware a serem instaladas e implementadas para cada utilizador.

Além de apoiar os colaboradores que trabalham em casa, o SASE também ajuda a capacitar as filiais das empresas. Anteriormente, as empresas tinham um modelo em que as filiais transferiam o tráfego para o data center mais próximo. Como resultado, todas as aplicações SaaS críticas estavam a passar pelo data center para aceder à Internet.

Se houvesse algum problema com o data center ou em algum ponto entre a filial e o data center, isso poderia significar um problema. Sem mencionar o fato de que o desempenho das aplicações na filial era frequentemente degradado. Com um modelo SASE, as filiais podem aceder às aplicações diretamente na cloud, com total segurança.

INTRODUZIR O SASE NO NEGÓCIO

Conseguir que a nossa organização invista na adoção de um modelo de SASE, não pode ser apenas através da explicação das tecnologias que estão por trás deste modelo. Essa abordagem é a mesma da "velha" apólice de seguro.

Devemos introduzir o tema sem sequer falar sobre tecnologia. É pois, importante fazer uma abordagem para referir que qualquer utilizador, a partir de qualquer localização, independentemente do método de conectividade, independentemente da aplicação a que está a tentar aceder e independentemente de onde esta reside (cloud privada ou pública, SaaS), combinando tudo isto numa única politica entregue a partir da cloud, torna possível a qualquer colaborador ter uma experiência ótima de utilização, sem latências, de forma absolutamente segura.

Não há dúvida de que através da adoção de um modelo de SASE, o negócio passa a ser mais resiliente e mais bem-sucedido. Durante a pandemia, através do SASE, garantimos segurança, conectividade remota e a continuidade do negócio. ◀

A VOZ DOS CISO

Depois do sucesso da primeira edição, a IT Security Conference 2023 já tem data marcada: a 12 de outubro, em Lisboa, onde voltam a estar em destaque os temas mais relevantes relacionados com o ecossistema da cibersegurança.
A IT Security Conference 2023 será uma oportunidade para explorar as tecnologias mais inovadoras que impactam um grande número de indústrias, para além da partilha de conhecimentos entre CISO, CSO, diretores de segurança e diretores de IT com responsabilidade de cibersegurança. **As inscrições já abriram, reserve o seu lugar**.

PARCEIROS:

Diamond: paloalto NETWORKS

Platinium: HPE aruba networking; SOPHOS Cybersecurity delivered.

Golden: arcserve; CATO NETWORKS; claranet; IBM; LOGICALIS Architects of Change; redShift; S21sec Cyber Solutions by Thales

Silver: CISCO; cybersafe; DELL Technologies; FORTINET

Silver Exhibition Partner: sealpath; VARONIS; visionware; WatchGuard; Lenovo

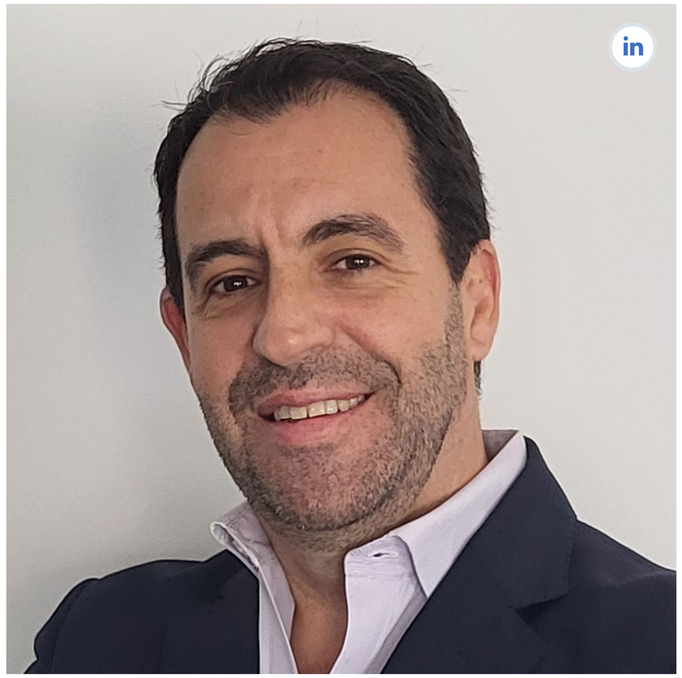
VAD Partners: balwurk; DIVULTEC; LG Life's Good; Westcon; ARROW; Ingecom

Institutional Partners: CNCS Centro Nacional de Cibersegurança PORTUGAL

por Paulo Neves,
Sales & Vendor Director Networking
& NGS na Westcon

MELHORAR A CIBER-RESILIÊNCIA ORGANIZACIONAL

A IMPORTÂNCIA DA CIBERSEGURANÇA É CADA VEZ MAIS EVIDENTE NA SOCIEDADE ATUAL. COM O CRESCENTE AVANÇO TECNOLÓGICO E A DEPENDÊNCIA DAS EMPRESAS EM RELAÇÃO À INTERNET E AOS SISTEMAS DIGITAIS, A PROTEÇÃO DE DADOS E INFORMAÇÕES TORNOU-SE UMA AÇÃO DE EXTREMA IMPORTÂNCIA.



Nesse contexto, uma das prioridades da **Westcon** – Distribuidor global de valor com um portefólio de fabricantes de tecnologia líderes no mercado – através da sua equipa de Next Generation Solutions (NGS), e em colaboração com os seus parceiros tecnológicos como integradores, MSSPs, etc., é apresentar aos clientes soluções inovadoras e líderes de mercado que abrangem todas as medidas e práticas eficientes adotadas para proteger sistemas, redes e dados contra ameaças, como vírus, *malware*, *ransomware*, *hackers* e outras formas de ataques. A proteção dessas informações é essencial para evitar a perda das mesmas assim como para evitar avultados prejuízos económicos.

Além da importância da cibersegurança em geral, é essencial entender as soluções específicas que cada fabricante oferece para proteção contra as ameaças atuais. Atualmente contamos com os principais fabricantes de soluções de segurança desde XIoT/OT, NGAV, EndPoint Proteccion, xDR, Identidade e Acesso, cloud e AI.

A **Claroty** é uma empresa especializada em segurança Healthcare (Medigate), industrial e de infraestrutura crítica. Os seus produtos visam proteger sistemas contra as ameaças atuais em ambientes XIot/OT, com foco em setores como saúde, energia, indústria e transportes.

A **CrowdStrike** é líder em proteção de *endpoints* e deteção de ameaças. A sua plataforma utiliza inteligência artificial e machine learning para identificar e bloquear ameaças avançadas em tempo real.

A **Okta** é uma plataforma de gestão de identidade e acesso, que oferece soluções para gerir de forma segura as identidades e os acessos dos colaboradores, clientes e parceiros às aplicações e sistemas das empresas.

A **Vectra** é uma empresa especializada em soluções de deteção e resposta a ameaças internas na rede – NDR (Network Detection and Response). A suas soluções utilizam inteligência artificial para identificar anomalias de comportamento e atividades maliciosas dentro da rede.

A **Zscaler** é líder em segurança na nuvem que oferece proteção avançada para redes, aplicações e dados, independentemente da localização do utilizador. Utiliza um sistema de filtragem em cloud para bloquear ameaças e garantir o acesso seguro aos recursos digitais.

Estes fabricantes representam uma pequena amostra do vasto leque de soluções de segurança disponíveis na **Westcon** e no mercado global. Cada um deles oferece abordagens e tecnologias diferentes, mas todos têm como objetivo comum garantir a segurança digital das empresas e organizações. Em conclusão, a cibersegurança é de extrema importância nos dias atuais devido aos riscos e ameaças cada vez mais sofisticados encontrados na internet e às consequências que daí advêm.

Contacte a nossa equipa de NGS da Westcon – *ngs.pt@westcon.com* para saber como podemos ajudar a proteger o negócio dos seus clientes, contando para isso com as principais soluções de fabricantes líderes, como a **Claroty**, **CrowdStrike**, **Okta**, **Vectra** e **Zscaler**, essenciais para garantir uma proteção eficiente e abrangente contra ataques cada vez mais sofisticados.

Na **Westcon**, apoiamos os parceiros a atingir todo o seu potencial. Somos apaixonados por proporcionar sucesso empresarial e crescimento. Começamos com um alinhamento estratégico: queremos compreender e fazer crescer o seu negócio. As nossas equipas acompanham todos os passos com uma grande vontade e capacidade de apoiar e aumentar as suas oportunidades. Garantimos saber responder, em qualquer momento, aos desafios diários apresentados pelas operações no canal e temos orgulho em combinar confiança com empreendedorismo, tudo em prol do sucesso dos nossos fabricantes e parceiros.

Partner Success. It's what we do.

Westcon

Garantimos proteção eficiente e abrangente contra ataques cada vez mais sofisticados.

Conheça o nosso portfolio de NGS:

CLAROTY · CROWDSTRIKE · okta · VECTRA · zscaler

Partner Success.
It's what we do.

ngs.pt@westcon.com

ESTADO DA NAÇÃO

Como vai a cibersegurança em Portugal?

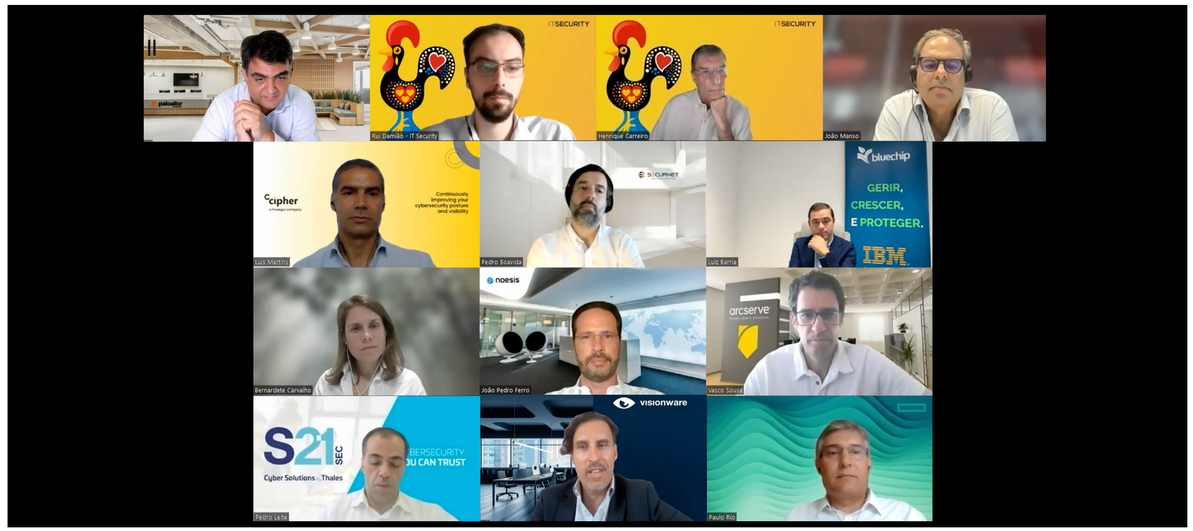
POR RUI DAMIÃO

PARA ONDE CAMINHA A CIBERSEGURANÇA? COMO É QUE AS ORGANIZAÇÕES SE ESTÃO A ADAPTAR AOS NOVOS DESAFIOS? É SOBRE ESTES TEMAS, E PARA AVALIAR O ESTADO DA CIBERSEGURANÇA EM PORTUGAL, QUE A ARCSERVE, A BLUE CHIP, A CIPHER, A HPE ARUBA NETWORKING, A NOESIS, A PALO ALTO NETWORKS, A REDSHIFT, A S21SEC, A SECURNET, A SOPHOS E A VISIONWARE PARTILHAM A SUA VISÃO SOBRE COMO EVOLUEM AS ORGANIZAÇÕES NACIONAIS.

É inegável que a cibersegurança é uma necessidade para todas as organizações, seja de que tamanho forem. Essa perceção tem crescido nos últimos anos, muito por causa dos ciberataques que ocorreram junto de grandes empresas no início de 2022 e que trouxeram para a perceção pública de que um problema de cibersegurança pode acontecer a todos.

Nesta mesa-redonda, os 11 participantes – representantes de algumas das principais empresas prestadoras de serviços e produtos de cibersegurança – mencionam que as organizações nacionais ainda têm um caminho a percorrer, mas que têm estado a ganhar terreno em comparação com as suas congéneres europeias.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



COMPARANDO PORTUGAL COM OUTROS PAÍSES EUROPEUS, COMO ESTÁ O CONTEXTO DA CIBERSEGURANÇA?

João Manso, CEO, Redshift: "Portugal tem feito um esforço muito grande. Olhando para a Europa, a nossa visão é de que Portugal está a recuperar terreno em algumas áreas de alguns setores, principalmente na indústria, nas telecomunicações, na banca e nos seguros. Em Espanha, por exemplo, as PME estão muitíssimo pior do que Portugal, mas se olharmos para o setor do governo, do Estado, Portugal ainda continua muito atrás em relação à grande maioria dos países, especialmente comparativamente aos do norte da Europa"

Paulo Vieira, Country Manager, Palo Alto Networks: "A maturidade subiu bastante no ano passado com os problemas todos de cibersegurança que o país sofreu. O mercado mais pequeno começou a notar e a sentir que tem de investir e dar um passo no sentido certo, mas ainda temos um caminho longo para fazer. Julgo que toda esta componente de leis ajuda a ter esta perceção do que é que é a cibersegurança e a sua necessidade. Acho que demos passos muito grandes em 2022 e continuamos a dá-los em 2023"

Pedro Leite, Chief Operating Officer, S21sec: "O investimento em cibersegurança durante 2023 rondará os 219 mil milhões de dólares, um aumento de 12,1% em relação a 2022 e também se prevê um aumento em Portugal à volta dos 10%. O país, em termos de investimento, está a acompanhar o investimento a nível europeu, mas também tem aqui um caminho para recuperar. Também verificamos que a perceção de risco aumentou em relação a 2022; as empresas, face aos incidentes que tivemos, têm mais noção de que isto também as pode afetar"

JOÃO MANSO, REDSHIFT

"A REGULAÇÃO QUE TEM ESTADO A SURGIR TEM SIDO PARTICULARMENTE IMPORTANTE, PRINCIPALMENTE PARA MOTIVAR AS EMPRESAS"

BRUNO CASTRO, VISIONWARE

"ACREDITO QUE O PRÓXIMO MINDSET EM TERMOS DE DECISÕES NESTA ÁREA É SER CAPAZ DE NÃO OPTAR PELA COMPONENTE DE PRODUTO AS IS, MAS SER CAPAZ DE ADOTAR MODELOS DE GOVERNAÇÃO"

Paulo Rio, Network and Security Consulting, HPE Aruba Networking: "Há um forte investimento feito pelas organizações portuguesas nos últimos anos; depende da fonte que consultemos, mas estamos a falar de 150 milhões em Portugal que representará o mercado de cibersegurança. Há quem fale que, em dois ou três anos, esse número possa chegar ou ultrapassar os 300 milhões, o que é um reflexo de que as organizações estão a fazer um esforço e um investimento contínuo e progressivo na área"

Luiz Barria, Industrial Cybersecurity Evangelist, Blue Chip: "Quando falamos de Portugal em matéria de cibersegurança, é preciso ter em consideração três competências: regulatória, tecnológica e pessoas. Quando falamos de regulamentação, Portugal tem-se destacado e vemos isso nos últimos dois anos onde Portugal definiu a sua matéria de ciberespaço. Dentro de um relatório que saiu em 2021, Portugal – entre 182 países – saiu do seu 28.º lugar e foi para 14.º, ou seja, destacou-se na questão de regulamentação"

COMO SENTEM A MATURIDADE DAS ORGANIZAÇÕES E DAS EMPRESAS PORTUGUESAS?

Bruno Castro, Founder & CEO, VisionWare: "Houve um *boost* dado pela pandemia que veio dar uma alteração completamente drástica a este mundo cibernético e o que temos vindo a ver são os mesmos tipos de ataque com morfologias diferentes; são as mesmas usurpações de identidade através de roubo de credenciais, por exemplo. Cada vez mais vejo a camada de gestão a querer saber, a estar envolvida, a conhecer os riscos, as opções em cima da mesa e, quando estamos em cenários de desastre, estarem envolvidos diretamente na sala de crise"

Pedro Boavida, Diretor Técnico, Securnet: "Sentimos que tem havido uma grande evolução na maturidade das organizações portuguesas; há uma maior consciência e perceção e já passámos a fase de que os problemas só acontecem aos outros. Por outro lado, os ciberincidentes são reconhecidos como um dos maiores riscos para o negócio. Há também uma maior capacitação por parte das organizações, seja por via dos imperativos legais ou até por relações com parceiros de negócio onde surgem exigências de conformidade"

João Ferro, SOC and Cybersecurity Specialist, Noesis: "Antes, se calhar, passávamos um bocadinho entre os pingos da chuva, mas hoje, como os ataques são mais transversais, estamos no epicentro do furacão. Em termos de impacto, já estamos com uma média extremamente alta em comparação com o que acontece no resto da Europa e isto é preocupante. Por outro lado, segundo um estudo do Eurostat, Portugal encontra-se em quarto lugar em termos da utilização de documentação e processos e utilização de boas práticas, o que é bom, mas valem o que valem"

PEDRO BOAVIDA, SECURNET

QUAIS SÃO AS NOVAS TECNOLOGIAS QUE ESTÃO A SER MAIS PROCURADAS PELAS ORGANIZAÇÕES NACIONAIS? EM 2023, QUAL SENTEM QUE É O TIPO DE PRODUTO QUE AS EMPRESAS PORTUGUESAS MAIS INVESTEM?

Bernardete Carvalho, Territory Account Manager, Sophos: "É preciso perceber o contexto e voltar um bocadinho atrás. Foi muito importante a transformação digital que veio possibilitar aos utilizadores ter dinâmica, mas que traz a necessidade de assegurar os múltiplos acessos e recorrer a inúmeras ferramentas. Sabemos que o contexto atual – a complexidade das ameaças, escassez de recursos e *know-how* – obriga a uma abordagem à cibersegurança como um serviço que são especializadas por equipas com resposta 24/7"

"O PRODUTO MAIS PROCURADO É O 'BRAINWARE' PARA FAZER FUNCIONAR CORRETAMENTE TODA ESTA TECNOLOGIA EM QUE AS EMPRESAS TÊM INVESTIDO"

Vasco Sousa, Channel Account Manager, Arcserve: "As tecnologias visam responder a necessidades. Na minha componente – preservação dos dados –, a potencial perda de dados pode ser causada por atores externos e internos à organização. Vejo uma tecnologia que tem vindo a ser adotada em vários segmentos de mercado, uma busca por soluções de *backup* ou proteção de dados em plataformas SaaS, ferramentas que façam *backup* a dados como o 365 ou Salesforce, que há três anos eram raríssimas as organizações que se preocupavam com esses dados"

Luís Martins, VP Managing Director Portugal, Cipher: "O futuro será híbrido. Vai haver procura por novas soluções e produtos e, também, pelos serviços. Não há balas de prata que resolvem todos os problemas e não há soluções mágicas para endereçar todos os problemas que existem. Há é um conjunto – pessoas, tecnologias e processos – que podem ajudar a endereçar todas estas situações. Acredito que o mercado vai evoluir no sentido de procurar quer serviços, quer produtos que possam ajudar a colmatar vulnerabilidades"

Pedro Boavida, Securnet: "Podemos falar do EDR, XDR e muitas outras tecnologias, mas começam por ser, apenas, mais uma e depois vão sendo consolidadas no contexto das organizações. O produto mais procurado é o 'brainware' para fazer funcionar corretamente toda esta tecnologia em que as empresas têm investido. Na maior parte das vezes, a nossa relação com os clientes começa depois da venda"

Bruno Castro, VisionWare: "Acredito que o próximo *mindset* em termos de decisões nesta área é ser capaz de não optar pela componente de produto *as is*, mas ser capaz de adotar modelos de governação de segurança multidisciplinares que envolvem tecnologia e soluções, mas também a parte de *compliance* e privacidade. Outras abordagens numa visão 360° que, aí sim, se avalie uma solução de EDR ou firewalls como também se avalia a definição de procedimentos ou até planos de recuperação de desastres"

"NESTE MOMENTO, JÁ NÃO ESTAMOS A FALAR DE CIBERSEGURANÇA NUMA REALIDADE DISTANTE (...) QUE ESTÁ CONFINADO À BOLHA DA TI"

"O TEMPO MÉDIO DE UM ATAQUE DE RANSOMWARE PASSOU DE DOIS MESES PARA QUATRO MESES, O QUE MOSTRA A SOFISTICAÇÃO DESSES ATAQUES"

Pedro Leite, S21sec: "Sabemos que a maior debilidade do ponto de vista de segurança é o erro humano. Em função disso, há um denominador comum: há um investimento forte em gestão de identidade e de privilégios. As empresas estão a fazer um forte investimento no que diz respeito à identificação e autorização dos utilizadores. Acompanhado com isto, e devido à debilidade que os utilizadores têm, também sentimos que na parte de *endpoint* há uma procura muito grande de soluções como EDR porque é um dos principais vetores de ataque"

A UNIÃO EUROPEIA TEM LANÇADO, NOS ÚLTIMOS MESES, VÁRIAS REGULAMENTAÇÕES QUE IMPACTAM A CIBERSEGURANÇA E CIBER-RESILIÊNCIA DAS ORGANIZAÇÕES. COMO É QUE AS EMPRESAS SE ESTÃO A ADAPTAR A ESTAS DIRETIVAS? AS ORGANIZAÇÕES PORTUGUESAS ESTÃO A CAMINHAR O *COMPLIANCE*? EM QUE PONTO, DE UM MODO GERAL, É QUE ESTÃO?

Pedro Boavida, Securnet: "Existem imperativos legais, transposições de diretivas ou até outras obrigações regulamentares específicas do setor de atividade que acabam por colocar as organizações no caminho da conformidade. Para além das organizações que têm de se alinhar com estes imperativos legais, existem outras que voluntariamente querem estar neste caminho. Isto tudo é positivo; por um lado a sofisticação e a complexidade dos ataques aumentou muito a zona de perigo e estas obrigações legais ajudam, de certa forma, a reduzi-la"

LUÍS MARTINS, CIPHER

"A ESCASSEZ DE TALENTO É ALGO SENTIDO DE FORMA TRANSVERSAL, NÃO APENAS A NÍVEL NACIONAL, MAS A NÍVEL MUNDIAL. NÃO É UM TEMA EXCLUSIVO NOSSO"

Luiz Barria, Blue Chip: "Podemos fazer uma distinção entre o que é a cibersegurança e a ciber-resiliência. Dentro das regulamentações que têm de saído, podemos dizer que as empresas estão a reagir para isso, têm feito investimentos a nível processual – como políticas – para gerar evidências para auditorias internas e externas. As empresas estão a rever as suas políticas e estão mais ativas nesse ponto, para além de ter investido na aquisição de sistemas, de tecnologia"

Luís Martins, Cipher: "No aspeto das regulamentações, estamos a seguir um caminho, mas onde temos claramente dificuldades de chegar ao universo de pequenas e médias empresas que acabam por constituir a maior parte de organizações empresariais no país. A regulamentação é necessária, é positiva, traz uma série de mais-valias para as organizações e acredito que as organizações empresariais têm de olhar para estas regulamentações como uma mais-valia para o negócio e não apenas algo que têm de implementar"

João Manso, Redshift: "A regulação que tem estado a surgir tem sido particularmente importante, principalmente para motivar as empresas que são cobertas por essa regulação a terem de fazer investimentos. O envolvimento da camada C tem muito mais a ver com a necessidade de ter resposta e garantir que a sua organização é *compliant* com a regulação do que ser uma visão objetiva da necessidade de estar a intervencionar a parte mais tecnológica da organização"

A ESCASSEZ DE TALENTO É UM PROBLEMA PARA QUALQUER ORGANIZAÇÃO, ESPECIALMENTE EM CIBERSEGURANÇA. COMO SE PODE COMBATER ESTE PROBLEMA, SABENDO QUE AS ORGANIZAÇÕES TÊM DE CONTINUAR A PROTEGER AS SUAS INFRAESTRUTURAS E SISTEMAS?

Luís Martins, Cipher: "A escassez de talento é algo sentido de forma transversal, não apenas a nível nacional, mas a nível mundial. Não é um tema exclusivo nosso. No nosso contexto específico, e porque temos pessoas muito talentosas, acaba por haver um ataque – se assim se pode chamar – de outras entidades fora do nosso país aos nossos talentos onde, do ponto de vista salarial, têm outras condições que não existem em Portugal. A pandemia trouxe a aceleração da transformação digital e de pudermos trabalhar a partir de casa remotamente para outras geografias"

João Ferro, Noesis: "É de louvar e enfatizar que os profissionais portugueses na área de IT são reconhecidos a nível mundial e não menos os da área de cibersegurança. Este é um tema sensível e tem sido menos aligeirado pelo facto de se poder trabalhar remotamente que pode trazer benefícios de se conseguir fazer o *onboard* de pessoas que não estão só nos meios urbanos, mas também existem mais ofertas lá de fora, se calhar a ganhar outro tipo de vencimentos; acaba por ser um pau de dois bicos"

Bernardete Carvalho, Sophos: "A escassez de talento é uma preocupação e é transversal a todas as áreas, mas na cibersegurança é, realmente, um chavão. É importante perceber que esta escassez de recursos também é uma questão de custo e o tempo que pode levar a formar e capacitar o recurso. No contexto atual, os serviços geridos são a única forma de garantir alguma eficácia para gerir as ameaças mais complexas"

BERNARDETE CARVALHO, SOPHOS

"NINGUÉM QUER ASSUMIR A RESPONSABILIDADE DO IMPACTO DE UM CIBERATAQUE E É IMPORTANTE ESTARMOS TODOS CONSCIENTES"

Paulo Vieira, Palo Alto Networks: "No mercado onde trabalhamos vivemos um momento onde as empresas geram cada vez mais alertas, mais logs, com mais equipamentos a levar alertas para um único sítio. Um cliente que tenha dez mil logs diários hoje e amanhã tenha 20 mil, não vai passar de uma pessoa para duas; não funciona. A resposta é, cada vez mais, ter tecnologia que, de facto, consiga fazer essa triagem e análise e transformar alertas em incidentes e depois começar a utilizar automação, que vai ser a resposta para resolver esta escassez"

Paulo Rio, HPE Aruba Networking: "A falta de recursos pode ocorrer de uma forma literal de falta de recursos humanos e de competências desses recursos humanos, mas também na fadiga das equipas de operação que trabalham na análise dos dados. Depois, há a necessidade de ter uma resposta aos incidentes – quer na deteção quer na recuperação – que, mais uma vez, vai exigir recursos. A caracterização da falta de talentos desconstrói-se numa série de outras dificuldades. A automação e a orquestração têm um papel importante para aliviar as tarefas de forma parcial ou até total"

PAULO VIEIRA, PALO ALTO NETWORKS

COMO ESTÃO A EVOLUIR AS CIBERAMEAÇAS E COMO É QUE AS ORGANIZAÇÕES PORTUGUESAS ESTÃO A FAZER FRENTE ÀS MESMAS?

Pedro Leite, S2lsec: "O relatório de 2023 de riscos e conflitos traduz bem o que se passou em 2022 na componente das ameaças. O que diz o relatório é que os incidentes de segurança continuam a aumentar. As ciberameaças que estão a afetar o contexto nacional são muito idênticas ao que temos tido nos anos anteriores, como ransomware, phishing e burla online. Se olharmos para o relatório da IBM, o tempo médio de um ataque de ransomware passou de dois meses para quatro meses, o que mostra a sofisticação desses ataques"

"ESTAMOS A VER O ROUBO DE CREDENCIAIS A SER O VETOR NORMAL PARA ENTRAR PARA AS INFRAESTRUTURAS DOS CLIENTES"

"HÁ A NECESSIDADE DE TER UMA RESPOSTA AOS INCIDENTES – QUER NA DETEÇÃO QUER NA RECUPERAÇÃO – QUE, MAIS UMA VEZ, VAI EXIGIR RECURSOS"

Paulo Vieira, Palo Alto Networks: "Os ataques estão cada vez mais complexos e os atacantes estão cada vez mais estruturados. Estamos a ver o roubo de credenciais a ser o vetor normal para entrar para as infraestruturas dos clientes. As tecnologias têm de conseguir acompanhar este caminho porque temos de ser capazes de detetar que aquele email não é da Cláudia dos recursos humanos, mas é alguém a fazer-se passar pela Cláudia dos recursos humanos"

Paulo Rio, HPE Aruba Networking: "O número de incidentes é alarmante, mas o relatório do CNCS aponta que o número de incidentes reportados são mais de dois mil; o número de incidentes observados foram mais de 70 milhões. Obviamente que desses 70 milhões existem os incidentes que têm um impacto direto na disponibilidade. Mais alarmante é que a linha continua a ser crescente. Estamos muito longe de atingir o *plateau*; a defesa e o ataque não estão equilibrados. A defesa tem de fazer um trabalho maior do lado das organizações, dos fabricantes, dos integradores e dos reguladores"

João Manso, Redshift: "O problema que temos em Portugal é que parece que há um excesso de investimento em tecnologia, mas há lacunas na tecnologia. Queixamo-nos que não temos recursos, mas não valorizamos os recursos. Um exemplo: se tivermos de fazer manutenção num carro, não temos problema em pagar 50, 80, cem euros por hora ao técnico, mas, quando falamos de cibersegurança e se pedem 50, 60 por hora é muito, um exagero. Não se valoriza a necessidade e capacidade dos recursos. No lado da tecnologia, existe tecnologia a mais e mal implementada; compra-se tecnologia para resolver problemas sem se avaliar se aquela tecnologia é adequada às necessidades da organização"

Vasco Sousa, Arcserve: "O ransomware já cá está há bastante tempo e continua na linha da frente das ameaças. Vejo uma sensibilização cada vez maior para manter os dados protegidos. Os dados das organizações, em primeiro lugar, têm de estar seguros e, só depois, é que devem estar acessíveis. Isto passa por uma abordagem onde todos contribuímos para este objetivo final. Não se consegue ter uma abordagem de cibersegurança sem ferramentas, mas obviamente que isto tem de ser complementado com processos, com serviços e com formação e de forma contínua"

João Ferro, Noesis: "O paradoxo da cibersegurança está assente num racional que está invertido, em que o retorno e o investimento são muito díspares. Um custo de efetuar um ataque é irrisório em comparação com o custo para uma empresa tem de fazer em prevenção, que pode chegar às centenas de milhares de euros. Isto também contribui para haver cada vez mais atacantes e curiosos a experimentar. O cibercrime já vale mais do que o PIB da Suíça, por exemplo, e é uma área bastante aliciante com cada vez mais adeptos"

JOÃO FERRO, NOESIS

A CIBERSEGURANÇA É, HOJE, UM TEMA NA MESA DA ADMINISTRAÇÃO? COMO TEM ESTADO A EVOLUIR O ENVOLVIMENTO DA ADMINISTRAÇÃO NA CIBERSEGURANÇA?

Vasco Sousa, Arcserve: "Há uns anos não era assim e temos consciência disso. Neste momento, já não estamos a falar de cibersegurança numa realidade distante que se ouve falar dos fóruns de cibersegurança, que está confinado à bolha da TI. Todas as organizações já sofreram com o tema da cibersegurança. Mesmo nós, enquanto cidadãos, já sofremos com isso de forma direta ou indireta. Uma administração sabe que isto é uma realidade e a determinada altura – mais cedo ou mais tarde – vai recorrer ao departamento de TI e fazer a questão 'o que temos de fazer para que isto não aconteça ou que tenha o mínimo impacto'"

"É DE LOUVAR E ENFATIZAR QUE OS PROFISSIONAIS PORTUGUESES NA ÁREA DE IT SÃO RECONHECIDOS A NÍVEL MUNDIAL E NÃO MENOS OS DA ÁREA DE CIBERSEGURANÇA"

LUIZ BARRIA, BLUE CHIP

"AS EMPRESAS ESTÃO A REVER AS SUAS POLÍTICAS E ESTÃO MAIS ATIVAS NESSE PONTO, PARA ALÉM DE TER INVESTIDO NA AQUISIÇÃO DE SISTEMAS, DE TECNOLOGIA"

Bernardete Carvalho, Sophos: "A administração parece consciente da complexidade da cibersegurança, mas existe a necessidade de melhoria do investimento. Todo este contexto trouxe uma consciencialização crescente para se fazer uma nova abordagem à cibersegurança ou haver a necessidade para a revisão da estratégia e ser muito focada. Ninguém quer assumir a responsabilidade do impacto de um ciberataque e é importante estarmos todos conscientes e que a administração também esteja"

Luiz Barria, Blue Chip: "Podemos dizer que a administração precisa de conhecer aquilo que está ao seu redor, as pressões externas dos ataques e ameaças que aumentam cada vez mais. Quando a administração toma conhecimento disso e tenta antecipar, coloca a cibersegurança num radar que se chama gestão de risco e começa-se a preparar para eventuais situações. Essa preparação não é apenas para não acontecer; é em caso de acontecer. O aumento e a rapidez das ameaças fazem com que a cibersegurança tenha de estar no mapa da gestão de risco"

Bruno Castro, VisionWare: "O *mindset* mudou um bocadinho. Há alguma literacia digital, nomeadamente no que envolve a cibersegurança na camada C. Já não se olha para a cibersegurança como um custo, olha-se como um investimento. Ainda vejo pontualmente alguma frustração de se fazerem grandes investimentos e serem vítimas de ciberataque; depois é preciso justificar esse investimento e como é que se sofreu um ciberataque. Vejo, também, ao nível da governação o *top management* a estar envolvido"

arcserve®

AS EMPRESAS NÃO COMPREENDEM BEM AS SUAS RESPONSABILIDADES NO QUE RESPEITA À SEGURANÇA DOS DADOS NA CLOUD

MUITOS AINDA PENSAM QUE OS DADOS ESTÃO MAIS SEGUROS *ON-PREM*.

A COVID-19 levou as organizações a utilizar a cloud para uma gama mais alargada de casos de utilização, especialmente como meio de cópia de segurança dos dados. No entanto, apesar do aumento da utilização, a maioria das organizações ainda não está esclarecida sobre as suas responsabilidades em matéria de segurança e recuperação de dados.

Foto: Israel Andrade / Unsplash

Isto de acordo com um novo relatório da empresa de proteção de dados Arcserve, baseado numa sondagem a 709 decisores de TI de todo o mundo, que afirma que quase metade (48%) aumentou a adoção de serviços


Foto: rawpixel / Freepik

em cloud para a gestão de dados como consequência direta da pandemia de Covid-19.

A maioria (61%) utiliza a cloud para serviços de cópia de segurança, bem como para infraestruturas de TI (57%).

Ainda assim, os equívocos sobre a segurança dos dados que residem na *cloud pública* são galopantes. Quase metade dos inquiridos (44%) acredita que as cópias de segurança dos dados numa cloud pública não são tão seguras como as cópias de segurança *on-prem*, subindo para quase três quartos (69%) entre as organizações com mais de 1PB de dados.

Além disso, dois em cada cinco acreditam que manter estes dados seguros e recuperáveis é da responsabilidade do fornecedor de serviços em cloud, em vez de ser uma responsabilidade partilhada com o proprietário dos dados.

A conformidade, a falta de controlo sobre os dados e as preocupações com a segurança são os principais obstáculos a uma maior adoção da cloud, segundo o relatório.

"As empresas procuram cada vez mais os serviços na cloud como parte de uma estratégia de centro de dados híbrido para ajudar a gerir o custo e a complexidade dos seus ambientes de dados, que normalmente se tornaram ainda mais difíceis de gerir com a mudança para o trabalho remoto", disse Vasco Sousa, Channel Manager da Arcserve.

"É encorajador o facto de muitos planearem aumentar a segurança dos dados e fazer investimentos em cópias de segurança com os seus MSP. A experiência que os MSPs trazem para a mesa garantirá que essas organizações terão planos de proteção e recuperação de dados bem definidos e testados."

Saiba mais em: *www.arcserve.com/pt*

Bravantic // Evolving Technology

por Luiz Barria,
Industrial Cybersecurity Evangelist na Blue Chip Portugal

O ESTADO DA CIBERSEGURANÇA EM PORTUGAL: DESAFIOS EMERGENTES E ESTRATÉGIAS DE PROTEÇÃO

A SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO É UMA PREOCUPAÇÃO CADA VEZ MAIS PROEMINENTE PARA AS ORGANIZAÇÕES EM TODO O MUNDO, E PORTUGAL NÃO É EXCEÇÃO. COM A CRESCENTE DIGITALIZAÇÃO DOS NEGÓCIOS E O AUMENTO DOS CIBERATAQUES, A CIBERSEGURANÇA TORNOU-SE IMPRESCINDÍVEL PARA GARANTIR A CONTINUIDADE DE NEGÓCIO E PROTEGER OS ATIVOS DAS ORGANIZAÇÕES.

LUIZ BARRIA, BLUE CHIP PORTUGAL

Nos últimos **21 meses**, Portugal sofreu **9 mil ataques** cibernéticos, segundo o relatório CyberTrends. Os cibercriminosos estão a explorar diversas técnicas, como o phishing e o ransomware, dois tipos de ciberataques mais utilizados em organizações ou instituições portuguesas. Segundo report da IBM, Portugal foi o **terceiro país europeu mais afetado por ataques informáticos**, atrás apenas do Reino Unido e Alemanha.

As organizações portuguesas veem nestes últimos anos os ciberataques crescerem exponencialmente. O número médio semanal de ataques em Portugal aumentou no primeiro trimestre de 2023, segundo informações da Check Point Software, onde uma mesma organização foi atacada **1.065 vezes por semana, um número acima da média europeia**. As principais organizações alvo dos cibercriminosos pertencem às áreas de educação e saúde.

Diante dessas ameaças, é necessário que as organizações portuguesas adotem abordagens proativas para fortalecer a sua postura em Cibersegurança. Das iniciativas que já estão a ser adotadas no país vemos o papel do Estado, com a criação de centros de cibersegurança

e a implementação de políticas e regulamentações que incentivam a proteção dos ativos digitais, que estão alinhadas com as políticas da União Europeia, como a adoção do Cybersecurity Act, da NIS 2, o Digital Markets Act/Digital Services Act, entre outros. Além disso, a **colaboração entre as organizações e o Centro Nacional de Cibersegurança (CNCS)**, entre outras autoridades reguladoras desempenham um papel crucial na luta contra as ciberameaças e o aumento da segurança cibernética.

No entanto, enfrentar os desafios da cibersegurança não é tarefa fácil. Muitas organizações ainda lutam para equilibrar a segurança com a produtividade e a eficiência operacional. A implementação de soluções de segurança muitas vezes é vista como um obstáculo, pois pode restringir o acesso a determinadas aplicações e informações. Além disso, as preocupações com os custos envolvidos na elaboração de medidas de segurança também podem dificultar a adoção generalizada de práticas robustas de cibersegurança.

Outro desafio que se revela nestes últimos anos é o aumento do trabalho remoto, impulsionado nos últimos anos devido à pandemia de COVID-19. Embora o trabalho remoto ofereça benefícios em termos de redução da pegada ecológica, ele também apresenta grandes dificuldades em relação à cibersegurança, como, por exemplo:

– As redes domésticas, em geral, são menos seguras do que as redes corporativas;

– Os ambientes de trabalho remoto podem aumentar a superfície de ataque para cibercriminosos;

– Os funcionários que trabalham em computadores pessoais em casa podem não ter o mesmo nível de controlo sobre a gestão das atualizações dos seus próprios dispositivos, o que pode representar um risco para as organizações.

Portanto, as organizações necessitam de encontrar um equilíbrio maior entre a flexibilidade e a segurança, de modo que as práticas de segurança sejam seguidas por todos, mesmo fora do ambiente de escritório.

À medida que nos aproximamos do futuro, é essencial que as organizações em Portugal continuem a investir em soluções de cibersegurança adequadas e adotem uma abordagem proativa para enfrentar as ameaças em constante evolução. A colaboração entre o setor público e privado, a consciencialização sobre a segurança e a implementação de práticas robustas são fundamentais para garantir a proteção dos ativos digitais e a continuidade de negócio.

O estado da cibersegurança em Portugal enfrenta desafios emergentes, mas as estratégias de proteção estão a ser desenvolvidas para enfrentá-los. A cibersegurança é uma prioridade para as organizações, que investem em soluções personalizadas e colaboram com autoridades reguladoras. No entanto, o equilíbrio entre segurança e eficiência operacional, assim como os desafios do trabalho remoto, exigem atenção contínua. A implementação de medidas de segurança e a consciencialização sobre os riscos são cruciais para garantir um ambiente digital seguro e resiliente em Portugal. ◀

por Luís Martins,
VP Managing Director Portugal na Cipher,
a Prosegur company

CRIANDO UM PLANO PARA O SUCESSO

A CIBERSEGURANÇA DEVE AJUDAR AS ORGANIZAÇÕES A MONITORIZAR AS AMEAÇAS, EXERCER TEMPOS DE RESPOSTA EFETIVOS, FORTALECER A SEGURANÇA DE REDE E A PROTEÇÃO DE DADOS CRÍTICOS.

Uma boa estratégia centra-se na identificação proactiva de processos e controlos de segurança que impedem um ataque bem-sucedido. O objetivo das medidas reativas é minimizar o tempo de permanência do atacante quando a prevenção falha. Uma estratégia equilibrada entre abordagens ofensivas e reativas devem resultar num forte estado de ciberesiliência.

Segundo um estudo recente do Instituto Ponemon mais de metade dos inquiridos (52 por cento) dizem que os testes de segurança ajudam as organizações a fortalecer as defesas contra ciberameaças. A monitorização e os testes contínuos são importantes para superar os adversários. As ciberameaças com as quais as organizações são mais afetadas, o ransomware é o mais ofensivo em segurança (41%). Isto é seguido de perto pela engenharia social (40%) e a exploração das vulnerabilidades na cloud (39 por cento).

A Cipher disponibiliza a sua plataforma global de serviços de cibersegurança - xMDR. Este projeto inovador foi desenvolvido pela Cipher Labs para ajudar as empresas a proteger a sua pegada digital num

LUÍS MARTINS, CIPHER, A PROSEGUR COMPANY

momento em que o número de ameaças está em constante crescimento. A plataforma xMDR inclui Inteligência Artificial e Machine Learning para aumentar a sua cobertura a todas as potenciais superfícies de ataque nas redes empresariais, incluindo os recursos informáticos, a tecnologia operacional, a Internet of Things (IoT) e a computação baseada na cloud. Este sistema amplia outros serviços de segurança já geridos pela Cipher e complementa outros serviços, tais como Governance, Risk & Compliance, Red Team Services e outros serviços especializados.

A plataforma é uma evolução do sistema MDR (Managed Detection and Response). O "X" em xMDR significa "extended" - ampliado em português - e representa o salto tecnológico realizado para garantir a total resposta às diferentes exigências dos clientes em termos de serviço e inovação.

Alguns dos principais fatores diferenciadores residem na sua abordagem exclusiva à definição de perfis de adversários, na baixa taxa de falsos positivos e nos níveis de serviço (SLA) mais ambiciosos.

A plataforma xMDR oferece um modelo de negócio em que o cliente paga apenas pelo serviço concreto que necessita. Além disso, a entrega e o suporte da solução são localizados e oferecidos no idioma da própria empresa. ◀

redShift

por João Manso,
CEO na RedShift Consulting

ESTADO DA NAÇÃO: O IMPACTO É REAL

AO DIA DE HOJE NÃO RESTAM GRANDES DÚVIDAS RELATIVAMENTE AOS EFEITOS NEFASTOS QUE UM ATAQUE CIBERNÉTICO PODE ORIGINAR NAS ORGANIZAÇÕES. A SEGURANÇA DA INFORMAÇÃO DAS NOSSAS EMPRESAS, O SEU "OURO", É MUITAS VEZES NEGLIGENCIADA, FRUTO DE UMA FRACA POSTURA DE SEGURANÇA, POTENCIADA, NA GRANDE MAIORIA DAS VEZES, POR FALTA DE ESTRATÉGIA INSTITUCIONAL.

ESTÁ A CIBERSEGURANÇA AO ALCANCE DE TODAS AS ORGANIZAÇÕES?

A cibersegurança impõe desafios constantes, devido à forma dinâmica como surgem diariamente novas tecnologias, novas "facilidades" e cabe-lhe garantir mecanismos de utilização segura, monitorização contínua e uma capacidade tão robusta, capaz de resolver, tanto quanto possível, em caso de comprometimento. Os vetores de ameaça são variadíssimos e assumem fragilidades técnicas, humanas e/ou processuais. Se por um lado é crucial garantir a existência de tecnologia que permita monitorizar e mitigar tentativas de comprometimento, tão automaticamente quanto possível, por outro lado. todos os indivíduos, com a sua maior ou menor literacia de cibersegurança, são tendencialmente o alvo prioritário de quem ataca.

A expressão "Não há almoços grátis!" aplica-se mais uma vez e, neste contexto em particular, é cada vez mais evidente. A tecnologia envolvida carece de investimento, a operação interna, as organizações (Processos) carecem de investimento, as pessoas carecem de investimento ... E trata-se de um investimento contínuo, porque, conforme já foi referido, as "facilidades" surgem diariamente. É inegável que se trata de investimento que até há muito pouco tempo não vinha "orçamentado" e era quase encarado como um "desperdício" ou um "desporto para ricos".

JOÃO MANSO, REDSHIFT CONSULTING

O investimento em cibersegurança é não só importante, como imprescindível, para garantir a continuidade e resiliência das organizações. Há dados estatísticos avassaladores quanto a empresas (na sua maioria PMEs) que se viram obrigadas a fechar, tais foram os impactos do ataque. Os ataques de ransomware proliferam todos os dias, mas não são a única ameaça. A segurança da informação tem de deixar de ser encarada não como um custo isolado, mas sim parte da estrutura de operação.

O grande desafio é inevitavelmente identificar a capacidade (base) necessária para endereçar os mecanismos "mínimos" de segurança, de forma a mitigar os riscos de maior impacto para a organização.

3 PASSOS PARA A CAPACIDADE DE RESPOSTA A INCIDENTES

É um enorme desafio para um consultor de cibersegurança (que o seja verdadeiramente), em Portugal, clarificar conceitos que "atropelam" os decisores das empresas portuguesas. Mas também nesse prisma (e que é transversal à nossa sociedade) há que acabar com a massificação de especialistas em tudo e mais "um par de botas" (como é a cibersegurança).

Entrando num discurso mais técnico: fruto da dificuldade em explicar, traduzindo simplificadamente, o que é um SIEM, um EDR, um SOAR ... e que nenhum deles é um SOC, os decisores acabam por "investir" em tecnologia isolada que não se traduz, na maioria das vezes, num valor acrescentado ou mesmo numa real capacidade. A tecnologia vai e volta, a capacidade fica! E está assente na simbiose entre a aplicação da tecnologia aos processos próprios da organização e da prontidão dos seus colaboradores.

Como podemos caminhar para uma postura mais resiliente e mais capaz de fazer face a ameaças com as quais nos deparamos? Utilizando, tal como no futebol, o VAR. Mas aqui naturalmente este VAR terá outro significado.

VISIBILIDADE

Não protegemos o que não vemos! É um desafio constante, mas incontornável, garantir que conhecemos a nossa organização. Como é a nossa informação gerada, transportada, armazenada? Onde estão as fronteiras da minha organização? Que mecanismos tenho de monitorização (efetiva) do que se passa nos pontos nevrálgicos da minha rede, sistemas e equipamentos ligados? Que comportamentos preciso/tenho de detetar que me afetam diretamente o negócio?

A tecnologia ajuda, mas o conhecimento da organização impera neste processo.

AUTOMAÇÃO

Existindo uma validação e a certeza de que os processos estão consolidados e testados, há que fazer um empoderamento de tarefas (técnicas e não técnicas) de forma automatizada. Meios de comunicação/notificação, mecanismo de deteção e classificação, análise de indicadores ... o grande objetivo passa por focar o esforço humano nas tarefas de valor acrescentado.

REAÇÃO

É o desiderato final de uma capacidade de resposta a incidentes -garantir uma reação cabal e níveis de resposta/recuperação aceitáveis, face ao risco que o negócio pode acomodar.

Finalizar dizendo, e lançado o mote, que a postura de segurança de uma organização pode afetar uma cadeia infindável de outras que com ela "coabitam". Organizações mais seguras, Portugal mais seguro! ◀

S21SEC
Cyber Solutions by Thales

CIBERSEGURANÇA INDUSTRIAL
RISCOS E ESTRATÉGIAS DE MITIGAÇÃO

A DIGITALIZAÇÃO ACELERADA DOS SISTEMAS DE AUTOMAÇÃO E CONTROLO, O USO DE TECNOLOGIAS PADRÃO E O AUMENTO DA CONETIVIDADE COM OUTROS SISTEMAS, EXPÔS AS ORGANIZAÇÕES A RISCOS DE CIBERSEGURANÇA PARA OS QUAIS NÃO ESTAVAM PREPARADAS.

Com a chegada da Indústria 4.0, modificaram-se as formas de organização dos meios de produção, os processos foram dotados de maior inteligência e implementou-se um grande número de dispositivos para conseguir um maior controlo dos processos industriais. Nesta linha, está a ser implementado um maior número de sensores, atuadores, controladores, gateways para concentração de comunicações, etc. relacionados à IoT. Uma vez que tal número de dispositivos cria uma série de dados quase inatingíveis por algumas infraestruturas, é necessário o apoio em tecnologias que já foram amplamente utilizadas em ambientes IT, como tecnologia cloud ou o machine Learning.

Assim, o maior risco é a gestão do novo equipamento, tanto em termos de volume como da sua forma de funcionamento. Como referido anteriormente, o advento dos dispositivos IoT no mundo industrial significa que o número de dispositivos numa planta crescerá exponencialmente, em oposição ao modelo estático tradicional. O equipamento usado em ambientes industriais foi projetado sem se ter em conta a cibersegurança, revelando grandes falhas de segurança que podem paralisar a produção a qualquer momento.

Nos grupos de trabalho da norma de referência industrial, IEC 62443, já existe um foco em IoT e estão planeados novos documentos orientados para a segurança no âmbito da norma. No caso da S21sec, garantimos uma identificação adequada e uma gestão eficiente dos riscos de cibersegurança para as infraestruturas industriais. Contamos com boas práticas e regulamentações prestigiadas em metodologias e ferramentas líderes com a menor interferência possível nos processos industriais. Além disso, contamos com mais de 10 anos de experiência em projetos de cibersegurança industrial. Para funcionar na sua plenitude, deve haver uma colaboração total entre indústria, fornecedores tecnologia/cibersegurança e reguladores, caso contrário, não conseguiremos proteger adequadamente este novo modelo de trabalho.

É de salientar que ter um inventário atualizado de ativos em ambientes industriais, ou fazer um do zero, é um dos maiores desafios que uma empresa industrial pode enfrentar. Estes inventários de ativos são complexos de gerir, em parte devido às mudanças causadas pelo paradigma que descrevemos antes. Assim, ao ter um inventário atualizado de ativos em organizações industriais permite aumentar a velocidade de reação a ciberataques, executar projetos com maior complexidade como um redesenho de rede ou implementação de uma monitorização centralizada, controlar os fluxos de comunicação que possuem os dispositivos industriais e detetar problemas nos processos. Por outro lado, para detetar ativos industriais e completar o inventário, há que ter em conta que nem todos os ativos enviam frames ou pacotes para a rede e, portanto, algumas ferramentas não são capazes de os detetar. Por vezes, os dispositivos industriais só podem ser detetados quando arrancam ou são reiniciados.

Sobre as medidas a adotar, as empresas industriais, apesar de estarem conscientes de que o OT requer medidas de proteção específicas, não podem avaliar por si próprias quais as medidas a implementar e como implementá-las. Com isto, não estão a aplicar as melhores medidas de segurança e recorrem cada vez mais a especialistas em segurança para os ajudar a proteger todos os seus dispositivos conectados. No nosso caso são considerados 4 vetores nos nossos serviços de cibersegurança OT:

1. **Conheça os sistemas e automação e controlo melhor que o inimigo**. Isto através de inventário de ativos OT básico/avançado, avaliação Técnica de vulnerabilidades OT, teste de intrusão OT básico/avançado, GAP analysis e plano de ação de cibersegurança industrial, análise de risco e plano diretor de cibersegurança industrial;
2. **Afaste os potenciais atacantes das suas instalações industriais** com redesenho da arquitetura de segurança, desenvolvimento de políticas e procedimentos, implementação de soluções de segmentação de rede, implementação de soluções de acesso remoto seguro, implementação de soluções de proteção de dispositivos removíveis, implementação de soluções AntiMalware, curso de estratégias de defesa contra ciberataques industriais e curso sobre firewalls e IDS / IPS Industriais;
3. **Vigie o inimigo nos processos industriais** com implementação de soluções de deteção de anomalias, implementação de soluções de deception, implementação de soluções de SIEM e SOC OT;
4. **Enfrente o inimigo nos processos industriais** através de Red Team e Purple Team para OT, DFIR OT Pre Breach, implementação de soluções de backup e DFIR OT post breach (sob pedido);

Mais info em: *https://www.s21sec.com/pt/ciberseguranca-industrial-pt/* ◀

SECURNET
ALWAYS ONLINE | ALWAYS SECURE

por Pedro Boavida,
Diretor Técnico, Securnet

A (CIBER)MATURIDADE

NA CIBERSEGURANÇA, EM PORTUGAL E NÃO SÓ, HÁ UM CAMINHO LÓGICO A PERCORRER, COM PRIORIDADES QUE VARIAM EM FUNÇÃO DO SETOR DE ATIVIDADE E DE OUTRAS CARACTERÍSTICAS, MAS HÁ PRECEDÊNCIAS E SEQUÊNCIAS LÓGICAS QUE NÃO SE ALTERAM. É PRECISO COMEÇAR PELAS FUNDAÇÕES.

Um inquérito realizado a especialistas em gestão de risco[1] em Portugal, indicou que ciberincidentes são as ocorrências mais relevantes no TOP-3 de riscos para estes profissionais (47%), à frente das catástrofes naturais (37%), de disrupções na cadeia de fornecimento (30%), fogos, explosões e pandemias (todos com 27%).

Um outro relatório, sobre "ameaças, risco e conflitos"[2], identificou como ameaças relevantes o *phishing*, *smishing* e *vishing*; *ransomware*; fraudes e burlas online; comprometimento de credenciais e a exploração de vulnerabilidades.

Paralelamente, calcula-se que Portugal seja o terceiro país europeu com mais ataques[3] (9%), depois de Reino Unido (43%) e Alemanha (14%). E algumas das notícias deste ano de 2023, na comunicação social e transversais a todos os setores, confirmam-no.

Mas afinal, quais são as nossas fragilidades?

Para medir fragilidades (e com isso ambicionar melhorar com objetividade) podemos recorrer a meios de diagnóstico que validam e quantificam as vertentes processuais, tecnológicas e humanas. Seja através de ferramentas que através de modelos permitem uma autoavaliação atribuindo pontuações e níveis (ENISA, FIRST, etc.), seja recorrendo a empresas especializadas (como a SECURNET) que o façam com base em referenciais como o SIM3, CREST, NIST, SOC-CMM, entre outros, nomeada-


PEDRO BOAVIDA, SECURNET

mente orientados a ramos de atividade específicos, de que o TISAX é exemplo, no setor automóvel.

E depois da avaliação? Mais tecnologia?

Depois da avaliação há quase sempre um caminho lógico a percorrer. Em função do setor, as prioridades podem variar. Mas, há precedências e sequências lógicas. É preciso começar pelas fundações, focados na gestão do risco, eficiência e resiliência.

Sem esquecer o mantra "prevenir, prevenir, prevenir", é necessário investir mais em **capacidade (leia-se conhecimento)** e nem tanto em ferramentas. É necessário rentabilizar o que (já) existe e nem sempre reforçar a teórica capacidade instalada obcecados por "hypes". Afinal, utilizamos quase sempre apenas uma pequena parte da tecnologia que possuímos.

Com alguma dose de imaginação, podemos até usufruir de serviços de informação gratuitos, com *blacklists* de IPs, domínios e *hashs* de ficheiros, integráveis nas soluções que já temos e ajudando a reduzir a superfície de ataque (e de atacantes).

Mesmo com *firewalls* de última geração, de fabricantes e reputação inquestionáveis, qual a percentagem de organizações que utilizam verdadeiramente todo o arsenal instalado para proteção de ataques de 5ª geração? Quantas firewalls estão a inspecionar o tráfego de HTTPS optando pela "eficácia" em detrimento do "desempenho"? Quantas *firewalls* têm todas as subscrições de proteção (antivírus, *antimalware*, *antibots*, IPS, etc.) ativadas, configuradas e ajustadas às suas realidades, em vez do tradicional "default"? E periodicamente analisados e revistos? Quantas organizações já olharam para os seus serviços de DNS?

Não bastam soluções EDR, XDR ou NDR que analisem comportamentos de dispositivos, utilizadores e o próprio tráfego na rede, um SIEM com múltiplas fontes e todas as outras soluções disponíveis no mercado se não for possível configurá-las devidamente ou se não for possível (por disponibilidade ou conhecimento) interpretar todas as informações que proporcionam, agindo depois em conformidade.

Aliás, será bom relembrar que atualmente a maioria dos ataques não derivam de "quebras nas tecnologias", mas de erros humanos, de utilização e de configuração, ambos com denominadores comuns de falta de conhecimento e de impreparação. Será também por tudo isto que vários analistas sugerem agora arquiteturas consolidadas e de um único fabricante, já que, para além de vantagens orçamentais, importará dominar essas tecnologias entre mãos, em vez de colmatar eventuais "falhas" com... mais tecnologia para aprender!

A ciber(maturidade)

Será também absolutamente necessário que a gestão de topo das organizações assuma a cibersegurança como uma obrigatoriedade. Que assuma que um pouco menos rápido e mais seguro é a opção, a única opção. Quantas organizações têm ativas funcionalidades de *sandboxing*, com emulação, testes, detonação e sanitização de ficheiros, assumindo como válida a pequena latência que estes fundamentais mecanismos de proteção introduzem? Quantas organizações aceitam que, usando um browser qualquer utilizador poderá (e deverá) aguardar um pouco até que a legitimidade desse site seja validada em tempo-real?

And last but not least, estar preparado para quando o "Dia D" chegar.

E a tudo isto, com equilíbrio entre desempenho e segurança, poderemos chamar... ciber(maturidade)!

[1] Fonte: Allianz Risk Barometer Results appendix 2022
[2] Fonte: CNCS, Relatório em 15 minutos, cibersegurança em Portugal. Dezembro 2022
[3] Fonte: X-Force Threat Intelligence Index 2023

SOPHOS
Cybersecurity delivered.

O CIBERCRIME AFETA CADA VEZ MAIS A ADMINISTRAÇÃO PÚBLICA

AS CAPACIDADES DE DETEÇÃO E RESPOSTA A AMEAÇAS DO SOPHOS MDR AJUDAM AS ENTIDADES A ESTAREM PREPARADAS.

Mais de metade (58%) das instituições governamentais foram afetadas por *ransomware* em 2021, vs 34% em 2020. Este aumento de 70% num ano demonstra a rápida aceleração das ciberameaças e do desafio que o setor público enfrenta.

De modo geral, a maioria dos gestores de TI no setor observou um aumento do volume (59%), da complexidade (59%) e do impacto (56%) dos ciberataques. Como os cibercriminosos continuam a utilizar a automação e o "malware como serviço", estes números só vão aumentar.

O impacto das ciberameaças no setor público é grave, tanto a nível financeiro como operacional. Em 2021, o custo médio de reparação de um ataque de *ransomware* foi de 660.000$, e quase metade (42%) dos dados encriptados não foram recuperados. O *ransomware* também afetou a capacidade de funcionamento da grande maioria (82%) das vítimas. Se os sistemas de TI não funcionam, a capacidade de uma agência governamental para prestar serviços críticos é gravemente prejudicada, o que pode, em última análise, afetar a segurança nacional, as

infraestruturas e a economia. A recuperação também é lenta: mais de 1/5 (21%) das vítimas demorou entre 1 e 6 semanas a voltar ao normal.

"As ameaças atuais exigem uma resposta coordenada e atempada. Infelizmente, demasiadas organizações estão em modo reativo, o que tem impacto nas prioridades da empresa, mas também tem um custo humano considerável. Eliminar as suposições e aplicar defesas baseadas em informações acionáveis permitirá que as equipas de TI se foquem em apoiar a empresa, em vez de tentarem apagar os fogos contínuos dos ataques ativos," diz **John Shier, CTO da Sophos**.

É seguro dizer que as soluções de cibersegurança, por si só, não impedem todos os ciberataques. Para não serem detetados por elas, os criminosos utilizam cada vez mais ferramentas legítimas, bem como credenciais e permissões de acesso roubadas, e exploram vulnerabilidades não corrigidas. Fazendo-se passar por utilizadores autorizados e explorando as fraquezas nas defesas, evitam ativar tecnologias de deteção automatizadas. A única forma de detetar e neutralizar os ataques de forma fiável é prestar atenção 24/7, com operadores especializados que utilizam diversos alertas de segurança e informações sobre ameaças em tempo real para identificar e travar as ameaças antes que causem danos.

No entanto, a complexidade dos ambientes operacionais modernos e a velocidade das ciberameaças tornam cada vez mais difícil para a maioria das organizações gerir sozinhas, e com êxito, a deteção e a resposta. Assim, lutam para acompanhar o ritmo de adversários bem financiados que inovam e industrializam continuamente a sua capacidade de escapar às tecnologias defensivas.

Um dos maiores riscos para as organizações são os adversários ativos, agentes de ameaças que adaptam as suas técnicas, táticas e procedimentos (TTPs) em tempo real, utilizando ações práticas para responder às tecnologias de segurança e defesa. Estes ataques, que muitas vezes resultam em incidentes devastadores de *ransomware* e violação de dados, são dos mais difíceis de travar.

Permitir que os defensores ultrapassem os atacantes nesta corrida exige uma abordagem abrangente, mas simples. Os serviços geridos de deteção e resposta a ameaças são fundamentais para fazer face à nova industrialização do cibercrime – tanto em organizações públicas como privadas –, uma vez que reduzem o risco e os custos associados aos incidentes de cibersegurança.

O **Sophos Managed Detection and Response (MDR)** oferece o apoio de uma equipa de especialistas que detetam e respondem a ciberataques direcionados, com um tempo médio de resposta de 38min (muito mais rápido do que a média das equipas internas). Protege centenas de agências governamentais, dando-lhes uma profundidade e amplitude de experiência sem precedentes sobre as ameaças que enfrentam. Com a sua extensa telemetria, constrói uma "imunidade comunitária", aplicando o que aprende com a proteção de um fornecedor a todos os clientes, reforçando as defesas. Para mais informações, visite *http://www.sophos.com/* ◀

visionware

por Bruno Castro,
Fundador & CEO da VisionWare.
Especialista em Cibersegurança e Análise Forense

CIBERTERRORISMO E AMEAÇAS CIBERNÉTICAS:
COMO DEFENDER (O ESTADO DE) UMA NAÇÃO?

O CIBERTERRORISMO E AS AMEAÇAS CIBERNÉTICAS SÃO UM PERIGO REAL E CRESCENTE PARA AS SOCIEDADES. NESTA ERA DIGITAL, ESTAMOS TODOS INTERLIGADOS, E COM ISSO, ADVÉM O RISCO DE ATORES MALICIOSOS UTILIZAREM A INTERNET, PARA ESPALHAR O MEDO E PERTURBAR A ORDEM, GERANDO O CAOS NAS SOCIEDADES MODERNAS. DESDE ROUBO DE IDENTIDADE A VIOLAÇÕES DE DADOS, PASSANDO PELA INTERRUPÇÃO DE SERVIÇOS VITAIS PARA AS COMUNIDADES, ESTAS AMEAÇAS PODEM TER IMPLICAÇÕES DE GRANDE ALCANCE PARA INDIVÍDUOS, EMPRESAS E GOVERNOS.

Nos últimos anos, a ameaça da cibercriminalidade tornou-se proeminente. A comunidade cibercriminosa está a visar cada vez mais os setores público e privado, sem grande distinção, roubando informação sensível e perturbando as operações de forma altamente disruptiva. Além disso, na VisionWare, temos comprovado toda a complexidade e polivalência dos recentes ciberataques, que podem ser utilizados para espalhar informação e propaganda errónea, resultando em agitação social, caos e instabilidade política.

O que observamos é que ninguém está a salvo. Nem mesmo as infraestruturas críticas (energia, telecomunicações, sistemas de transporte, saúde, etc.) dos países ocidentais, já bastante debatidas e cuja segurança exalta preocupações crescentes, tanto para os governos como para os cidadãos.

À medida que a tecnologia avança, o mesmo acontece com a sofisticação dos atores cibernéticos maliciosos. Estes, para além de continuarem a explorar vulnerabilidades aplicacionais ou tecnológicas, apostam cada vez mais na interligação das fraquezas do fator humano – isto é, na engenharia social – com o intuito de tornar o ciberataque mais eficaz e de menor tempo de atuação, sem-

pre com vista à obtenção de um acesso ilegítimo a identidades, e por aí em diante.

Para mitigar estas ameaças, governos e empresas privadas devem tomar medidas sérias e céleres para proteger as suas infraestruturas tecnológicas de suporte à atividade digital. Basta pensarmos na percentagem expressiva de infraestruturas críticas e/ou setores vitais, em Portugal, que estão nas mãos dos privados.

Os Estados europeus têm-se posicionado como moderadores, contudo, todos sabemos que os moderadores não ganham debates. A lógica é idêntica no âmbito da cibersegurança. É assim crucial, que governos e empresas trabalhem em conjunto, para partilhar informações e recursos, a fim de melhor detetar e responder de forma eficaz e preventiva a ameaças cibernéticas.

Temos assistido semanalmente – se não, diariamente - a uma intensificação e sofisticação de ciberataques na sociedade portuguesa. Estes ataques, transversais a quase todos os principais setores da nossa sociedade – telecomunicações, saúde, banca, transportes, educação -, têm causado muita turbulência, visto que, em certos casos, também tem implicado um impacto direto para o core business das 'vítimas', e por inerência, ao próprio setor onde atuam.

O crime cibernético tem sido aquele que mais tem aumentado desde o início da pandemia, tanto ao nível do volume de ataques registados como de denúncias, reforçando que estas situações continuam sem conseguirem ser travadas pelas entidades competentes e, nelas, estão incluídas não só as autoridades que investigam este tipo de ataques, como as próprias empresas que continuam a não dar o devido valor ou investimento a esta área de atuação.

A aposta terá de ser sempre pela via da crescente literacia (em cibersegurança) de todos os cidadãos, independentemente da sua função/cargo, visto que, qualquer um de nós poderá ser vítima de um ataque malicioso ou fraudulento. O fator humano continua a ser um dos grandes responsáveis pela consumação

BRUNO CASTRO, VISIONWARE

das ameaças e estas tanto podem vir de fora, como dentro da própria organização.

O ciberespaço não pode ser visto como antigamente; hoje, é um campo (e batalha) de interesses, mas, além disso, é também um campo de guerra. Por isso, é tempo de agir e proteger-nos a nós próprios – às nossas sociedades e costumes –, às nossas empresas e às nossas nações, dos perigos eminentes da cibercriminalidade e do ciberterrorismo. Temos de passar a assimilar que, com a evangelização da convivência no mundo cibernético, também as ameaças cibernéticas vieram para ficar e nada será como antes.◀

34 ANOS DE VIDA PROFISSIONAL, SEMPRE LIGADA AO MUNDO DO IT. INICIOU-SE COM O SAUDOSO ZX SPECTRUM, NOS ANOS 80, ONDE O INTERESSE FOI MUITO MAIS DO QUE JOGOS. A VIDA PROFISSIONAL FICOU LIGADA AO COBOL, COM PASSAGEM POR VÁRIAS EMPRESAS. DESDE HÁ 6 ANOS A TRABALHAR NO SETOR FINANCEIRO, PRIMEIRO COMO CIO E AGORA COMO CISO.

A CIBERSEGURANÇA EM PORTUGAL

POR SÉRGIO MARTINHO, CISO, LUSITANIA SEGUROS

FOI RECENTEMENTE (23JUN23) PUBLICADO A EDIÇÃO DE 2023 (4ª)DO RELATÓRIO RISCOS & CONFLITOS DO OBSERVATÓRIO DE CIBERSEGURANÇA DO CNCS, ESTE DOCUMENTO ANALISA OS PRINCIPAIS DADOS RELATIVOS ÀS CIBERAMEAÇAS DE 2022 E APONTA TENDÊNCIAS PARA 2023 E 2024.

PRINCIPAIS DESTAQUES:

• Os incidentes de cibersegurança e cibercrimes em Portugal continuaram a aumentar em 2022, com um crescimento significativo de incidentes com elevado potencial disruptivo.

• As ciberameaças mais comuns em 2022 foi o ransomware, cibersabotagem/indisponibilidade, o phishing/smishing/vishing, a burla online, outras formas de engenharia social e o comprometimento de contas/tentativas de login.

• As vítimas de incidentes de cibersegurança mais relevantes em Portugal durante 2022 foram os setores da Banca (sobretudo clientes) da Educação e Ciência, Tecnologia e Ensino Superior, dos Transportes, da Saúde, bem como da Comunicação Social. No âmbito dos subsetores da Administração Pública, destaca-se, comparativamente, a Administração Pública Local como alvo com maior número de incidências.

• A perceção de risco aumentou em 2022 e 2023.

• As principais tendências nacionais são a crescente profissionalização do cibercrime, a incerteza resultante da guerra na Ucrânia e algumas ciberameaças específicas, tais como o ransomware, o DDoS, o malware de furto de credenciais e os smishing/vishing/spoofing oportunistas relativamente ao uso massificado do telemóvel.

• Como cenário persistente, mantêm-se as ameaças típicas do contexto geopolítico e estratégico atual, devido ao prolongamento da guerra na Ucrânia, o que provoca o acentuar de antagonismos que encontram formas de polarização em ações de atores estatais e hacktivistas que pretendem ganhos informacionais ou propagandísticos para o seu lado do conflito. Enquanto a guerra na Ucrânia não terminar, prevê-se que este cenário se mantenha e possa mesmo agudizar-se.

AS VÍTIMAS DE INCIDENTES DE CIBERSEGURANÇA MAIS RELEVANTES EM PORTUGAL DURANTE 2022 FORAM OS SETORES DA BANCA (SOBRETUDO CLIENTES) DA EDUCAÇÃO E CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR, DOS TRANSPORTES, DA SAÚDE, BEM COMO DA COMUNICAÇÃO SOCIAL. NO ÂMBITO DOS SUBSETORES DA ADMINISTRAÇÃO PÚBLICA, DESTACA-SE, COMPARATIVAMENTE, A ADMINISTRAÇÃO PÚBLICA LOCAL COMO ALVO COM MAIOR NÚMERO DE INCIDÊNCIAS.

• Ainda numa fase emergente, e com resultado incerto quanto à transformação que efetivamente poderá trazer, devem considerar-se as ameaças que têm vindo a surgir em resultado da disponibilização de plataformas de Inteligência Artificial para o público em geral e o seu potencial de utilização para o desenvolvimento de ferramentas úteis na realização de ações maliciosas no ciberespaço. Esta

disponibilização tem-se mostrado apta a apresentar soluções técnicas para a efetividade de ciberataques, mas também para a criação de campanhas de desinformação.

PORQUE COMEÇO A REFERIR ESTE DOCUMENTO EM ESPECÍFICO?

Porque considero que temos muita coisa bem feita no nosso país, falta é haver uma notoriedade mais abrangente do que de bem se faz, pois como sabemos no que concerne à problemática da segurança no ciberespaço é algo que está em crescente relevância na vida das pessoas, como um todo, há muito que deixou de ser um tema apenas de preocupação das empresas, em especial para as grandes empresas, aquelas que terão de se preocupar em especial com regulamentos e frameworks, como o é o caso do decreto-lei 65/2021, ISSO 27001, NIS2, DORA, Norma 6/2022-R, obviamente apenas para referir uns quantos de muitos.

AS GRANDES EMPRESAS:

Para estas, a cibersegurança é hoje um tema comum na mesa da administração, comum pois este tema deixou de ser uma coisa de índole técnica para algo que está intimamente relacionado com o negócio, já não há dúvida que quem não considera com a devida atenção a cibersegurança simplesmente pode estar a colocar em jogo existência da sua organização. Porque estamos numa sociedade cada vez mais interligada e muito dependente de poucos players, tipicamente grandes organizações, que fornecem serviços essenciais no mundo digital, já se percebeu o perigoso que é o efeito dominó, quando falha uma grande, muitas outras vão por arrasto. Estas grandes empresas devem continuar a investir em qualificação, avaliação comparativa, formação em gestão de crise e protocolos de forma a conseguirem melhorar a sua capacidade de identificar e prevenir ciberameaças, tanto que a resiliência passou a estar no topo das preocupações destas organizações.

ONDE ACHO QUE PODERÍAMOS MELHORAR AQUI?

Haver uma maior centralização de orientações normas, regulamentos e leis, pois por vezes, o que noto é um atropelo entre orientações e cumprimento com determinados requisitos mais de índole processual que leva a que se invista tempo e recursos para preparar informação por vezes redundante.

Um maior espírito de comunidade dos especialistas em cibersegurança, onde a partilha de boas práticas e das outras que não sendo tão boas, serão de importância o seu conhecimento mais alargado. Sendo isto possível, será dúvida algo de valor acrescentado quer para a comunidade, quer para a sociedade em geral.

Os líderes a pensar mais profundamente sobre cibersegurança e ouvir mais atentamente os especialistas nesta matéria , os especialistas incrementarem a sua capacidade de empatia de forma que o diálogo flua a fim de garantir a resiliência corpo-

PORQUE ESTAMOS NUMA SOCIEDADE CADA VEZ MAIS INTERLIGADA E MUITO DEPENDENTE DE POUCOS PLAYERS QUE FORNECEM SERVIÇOS ESSENCIAIS NO MUNDO DIGITAL, TIPICAMENTE GRANDES ORGANIZAÇÕES, JÁ SE PERCEBEU O PERIGOSO QUE É O EFEITO DOMINÓ

rativa. Infelizmente os líderes cibernéticos ainda lutam para articular claramente o risco que as questões cibernéticas representam para suas organizações numa linguagem que seus colegas de negócios compreendam plenamente e possam agir. Como resultado, chegar a um acordo sobre a melhor forma de lidar com o risco cibernético continua sendo um desafio para os líderes organizacionais.

A transformação digital continua na moda, tanto que muitas organizações estão com grandes projetos de transformação digital. Adicionar tecnologia emergente à TI legada aumenta a complexidade dos ambientes digitais das organizações e, portanto, seu risco de segurança cibernética. É relevante que os decisores tenham preocupação acrescida para equilibrar o valor da nova tecnologia com o potencial de aumento do risco cibernético nas suas organizações.

Creio que faça sentido haver mudanças na estrutura organizacional que incorporem discussões de risco cibernético em toda a empresa e assim promover uma comunicação mais fluida e uma gestão eficaz de riscos cibernéticos.

O recrutamento e retenção de talentos especializados em cibersegurança continua a ser um desafio fundamental para a gestão da ciber resiliência. Creio necessária uma solução mais ampla para aumentar a oferta de profissionais nesta especialidade é expandir e promover esforços de inclusão e diversidade. Além disso, entender o amplo espectro de habilidades necessárias hoje pode ajudar as organizações a expandir a contratação. Estão já em curso várias iniciativas promissoras, mas não creio que seja suficiente. É preciso tempo, reflexão e investimento para tornar os programas de desenvolvimento de competências cibernéticas escaláveis.

E AS EMPRESAS QUE REPRESENTAM 99,9% DO NOSSO TECIDO EMPRESARIAL?

Os números mais recentes do INE, PORDATA indicam que em Portugal 99,9% (1.357.657) são PME (que incluem micro, pequenas e médias empresas) e apenas 0,1% (1.378) que são consideradas grandes empresas (>=250 pessoas ao serviço).

Estas organizações não tem nem de perto nem de longe capacidade de investimento em tecnologia e recursos, por isso, é necessária uma abordagem

diferente mas necessariamente inclusiva pois os ciberataques estão mais assertivos, o efeito dominó nestas organizações tende a ser tão ou mais nefasto que nas grandes organizações, por isso, é tempo de, em vez de se estar a inventar a roda, é tempo de se tirar partido do que de muito bom se está a fazer qui. Julgo que deve haver uma maior publicitação do CNCS, em especial o que fazem a nível da sensibilização e treino para comportamentos e atitudes mais seguros; produção e disseminação de alertas, orientações e boas práticas par ao uso seguro da tecnologia por parte de todos, assim como recomendações técnicas e produção de normativos e referenciais para as organizações e não esquecer que através do seu serviço CERT.PT realiza efetiva coordenação da resposta a incidentes que afetem o ciberespaço de interesse nacional.

Os fabricantes de tecnologias / serviços de segurança terem ofertas verdadeiramente inclusivas para este tipo de empresas.

É com agrado que vejo uma start-up nacional, que está a mostrar que o paradigma tem de mudar, pois a sua convicção é que a única forma de providenciar um serviço eficaz e acessível, sobretudo às PME, passa por combinar inteligência artificial e humana numa relação simbiótica na identificação das vulnerabilidades e resolvê-las proactivamente.

JULGO QUE DEVE HAVER UMA MAIOR PUBLICITAÇÃO DO CNCS, EM ESPECIAL O QUE FAZEM A NÍVEL DA SENSIBILIZAÇÃO E TREINO PARA COMPORTAMENTOS E ATITUDES MAIS SEGUROS; PRODUÇÃO E DISSEMINAÇÃO DE ALERTAS, ORIENTAÇÕES E BOAS PRÁTICAS PARA O USO SEGURO DA TECNOLOGIA POR PARTE DE TODOS, ASSIM COMO RECOMENDAÇÕES TÉCNICAS E PRODUÇÃO DE NORMATIVOS E REFERENCIAIS PARA AS ORGANIZAÇÕES

Não duvido que temos de incentivar a criação de mais empresas com este foco, por isso é preciso criar condições para que isso aconteça, nomeadamente com uma maior ligação à academia, que provavelmente deve ter conteúdos programáticos com maior assertividade para este tipo de realidade.

PORQUE O TEMA DA CIBERSEGURANÇA NÃO SE PODE LIMITAR A PORTUGAL...

Foi uma agradável surpresa que reparo que a Presidência Espanhola do Conselho da União Europeia (de 01JUL a 31DEZ23) debaixo do pilar "Reindustrializar a EU e assegurar a sua autonomia estratégica aberta" coloca a inteligência artificial e a cibersegurança com grande relevância. É na minha opinião um excelente ponto para dar a tão necessária relevância europeia nestes domínios, o que irá atrair/criar empresas e empregos para solo europeu e reduzir as nossas dependências estrangeiras.

É MESTRE EM SEGURANÇA INFORMÁTICA PELA FCUL E TEM UM MBA PELO LISBONMBA. PASSOU POR DUAS CONSULTORAS INTERNACIONAIS, NA ÁREA DE SISTEMAS DE INFORMAÇÃO E RISCO. É DESDE 2016 CISO NA FARMINVESTE, HOLDING DA ANF, COM A RESPONSABILIDADE TRANSVERSAL DOS TEMAS DE CIBERSEGURANÇA

ESTADO DA NAÇÃO NA CIBERSEGURANÇA

POR NUNO NEVES,
CHIEF SECURITY OFFICER, ASSOCIAÇÃO NACIONAL DAS FARMÁCIAS

O TEMA DA CIBERSEGURANÇA CONTINUA A TER UM IMPACTO SIGNIFICATIVO NA VIDA EM SOCIEDADE, MESMO QUE NEM SEMPRE TENHA ESSE DESTAQUE A TODOS OS NÍVEIS.

De acordo com a 4.ª edição do Relatório de Riscos & Conflitos, referente a 2022, o número de incidentes continuou a aumentar em 2022, com um aumento na sofisticação de alguns incidentes. Notou-se também o aumento de crimes registados pelas autoridades relativamente à Lei do Cibercrime, o que indicia, felizmente, que as empresas começam a participar mais às autoridades este tipo de incidentes.

Ainda de acordo com o mesmo relatório, as ameaças mais relevantes foram o ransomware, a cibersabotagem, o phishing ou o comprometimento de contas.

Em 2022, todos acompanhámos alguns exemplos muito visíveis destes ataques, desde o ataque diruptivo ao grupo Impresa, Vodafone e Laboratórios Germano de Sousa entre Janeiro e Fevereiro, até à intrusão na Segurança Social em Novembro, alguns dos quais ainda não totalmente recuperados.

NA COMPONENTE EMPRESARIAL, AQUILO QUE SE NOTA MUITAS VEZES É QUE O MEDIATISMO DESTES CASOS LEVA A UMA NOTORIEDADE MOMENTÂNEA, EM QUE AS EQUIPAS DE GESTÃO LEVANTAM INTERNAMENTE O TEMA, QUESTIONAM AS EQUIPAS TÉCNICAS, PERGUNTAM SE ESTÃO OU NÃO SALVAGUARDADAS, PEDEM PLANOS DE AÇÃO, ORÇAMENTOS E CALENDÁRIOS E DEPOIS, COM O ESBATIMENTO MEDIÁTICO E COM OS CUSTOS ENVOLVIDOS, OPTAM POR DEIXAR PASSAR A OPORTUNIDADE E CONFIAR NA SORTE QUE ESTE TIPO DE ATAQUES SÓ ACONTECE AOS OUTROS.

Este Relatório refere ainda que as vítimas de incidentes de Cibersegurança mais relevantes foram os setores da Banca, sobretudo os seus clientes.

Todas estas informações nos mostram que a cibercriminalidade veio para ficar e que cada vez mais tem maior predominância no dia-a-dia, quer nas empresas quer nos cidadãos. Para os cidadãos, conhecemos alguns esquemas de fraude que foram amplamente explorados, como o Olá Pai e Olá Mãe e para os quais houve, infelizmente, muitas vítimas. Algumas dessas vítimas até conheciam já o esquema e só se lembraram de confirmar com os filhos depois de serem burlados. Isto mostra a cada vez maior necessidade de formação em cyber higiene para toda a população, algo que as gerações mais novas já fazem quase sem pensar. Apesar do meritório esforço que o Centro Nacional de Ciber Segurança tem feito no sentido de sensibilizar e formar os cidadãos, é necessário o reforço desse trabalho para que a sociedade se torne mais resiliente.

Na componente empresarial, aquilo que se nota muitas vezes é que o mediatismo destes casos leva a uma notoriedade momentânea, em que as equipas de gestão levantam internamente o tema, questionam as equipas técnicas (algumas vezes nem têm equipas de segurança da informação e portanto direcionam para as equipas tecnológicas), perguntam se estão ou não salvaguardadas, pedem planos de ação, orçamentos e calendários e depois, com o esbatimento mediático e com os custos envolvidos, optam por deixar passar a oportunidade e confiar na sorte que este tipo de ataques só acontece aos outros.

Esta postura é mais difícil de mudar. Apesar dos esforços feitos, quer no plano nacional, quer no plano europeu, com a criação de legislação específica para a Cibersegurança (Diretiva NIS, Lei de Segurança do Ciberespaço, Diretiva NIS2, etc.) que tenta responsabilizar as entidades a criarem mecanismos de segurança concretos, continua a ser difícil obter essa segurança transversal, particularmente num país como o nosso, em que muitas das empresas são de reduzida dimensão, e têm dificuldade em justificar os custos envolvidos, apesar de fornecerem serviços para empresas maiores. As empresas maiores, por seu lado, apesar de já terem investido na segurança e terem implementado internamente toda a capacidade,

dependem para alguns serviços desses fornecedores de pequena dimensão e, apesar de pedirem o preenchimento de formulários e declarações de segurança, sabem que muitas vezes não passam de declarações de intenções. No extremo oposto, os fornecedores internacionais de grande dimensão não dão grande margem de manobra aos clientes para definirem requisitos específicos de segurança e conformidade, sendo necessário a adaptação do lado do cliente.

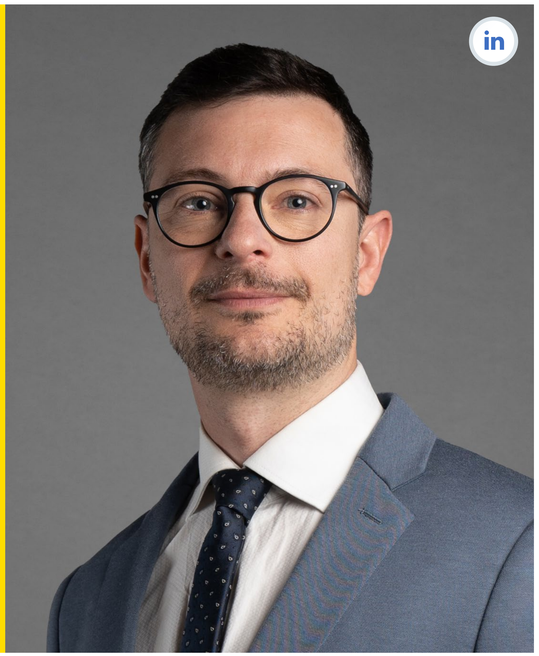
A agudizar este problema temos também uma escassez de profissionais qualificados na área da ciber segurança que limitam muito a capacidade das empresas de melhorarem neste aspeto.

O Centro Nacional de Ciber Segurança tem vindo a promover cursos, desde o ensino online até à C-Academy que tenta, em conjunto com instituições de ensino superior, disponibilizar formação avançada em Cibersegurança e o setor privado tem tentado colmatar estas lacunas para as pequenas e médias empresas, fornecendo várias componentes de segurança "as a Service" para que seja possível às empresas terem o serviço sem terem o custo inicial de montar toda uma estrutura.

COM A INCORPORAÇÃO DA TECNOLOGIA, A ÁREA TECNOLÓGICA FOI GANHANDO IMPORTÂNCIA, PASSANDO A RESPONDER DIRETAMENTE À GESTÃO EXECUTIVA E, MAIS TARDE, PASSANDO A INTEGRAR A PRÓPRIA GESTÃO EXECUTIVA.

Dada a crescente criticidade que a segurança da informação tem no destino das empresas, na capacidade de operarem e na definição estratégica das mesmas, torna-se cada vez mais necessário que o tema da Cibersegurança passe a ser encarado nas escolas de gestão como um pilar fundamental na condução dos destinos de uma qualquer organização, qualquer que seja o seu setor de atividade. Inversamente, é necessário também que os profissionais de Cibersegurança tenham consciência que o seu envolvimento nas empresas deve alinhar com a gestão e participar na estratégia da própria organização.

Estamos a vivenciar com a segurança da informação o fenómeno que ocorreu com a tecnologia no final do século passado. A tecnologia era vista como uma área de custos, liderada por tecnólogos e que estava muitas vezes numa segunda ou terceira linha, com reporte ao responsável financeiro. O que interessava nesse formato era controlar os custos que essas áreas representavam. Com a incorporação da tecnologia, a área tecnológica foi ganhando importância, passando a responder diretamente à gestão executiva e, mais tarde, passando a integrar a própria gestão executiva. Passámos do "informático" para o "Diretor de Informática" para o "Chief Information Officer" ou "Chief Technology Officer". Na segurança da informação vamos ter de seguir a mesma evolução, a um ritmo, como em tudo atualmente, mais acelerado ainda. Vamos deixar de ter o "técnico que trata da segurança" para o "Diretor de Segurança da Informação" para o "Chief Information Security Officer". De notar que, apesar do nome ser atualmente utilizado, na prática, há poucos CISO nos órgão de gestão, funcionando como diretores ou assessores. ◀



CONSULTOR SÉNIOR
DA ÁREA DE TMT DA
CCA LAW FIRM

POR DR. EDUARDO MAGRANI,
CONSULTOR SÉNIOR DA ÁREA DE TMT DA CCA LAW FIRM

CIBERSEGURANÇA EM PORTUGAL: TENDÊNCIAS E *COMPLIANCE*

SE O CIBERCRIME FOSSE UM ESTADO SERIA A TERCEIRA MAIOR ECONOMIA DO MUNDO, DEPOIS DOS ESTADOS UNIDOS E CHINA, COM UM PIB DE US$ 10 TRILHÕES" AFIRMOU O PRIMEIRO-MINISTRO DA ALBÂNIA, CONSIDERANDO A POTENCIAL FATURAÇÃO DO CIBERCRIME EM 2025.

A verdade é que atualmente a indústria do cibercrime representa uma das mais lucrativas áreas tecnológicas e cresce à medida que organizações criminosas evoluem e profissionalizam o desenvolvimento e distribuição de atividades maliciosas, como ransomware, phishing, roubo de credenciais, entre outros ataques[1].

Com números e impactos significativos, uma das principais preocupações e prioridades da União Europeia (EU) nos últimos anos é justamente a cibersegurança, com um reflexo claro na elaboração de novas estratégias e regulações que têm vindo

a ser aprovadas e discutidas de modo a garantir uma Europa mais segura, mais conectada e mais digital.

A primeira lei da UE sobre cibersegurança, a Diretiva NIS de 2016, ajudou a alcançar um nível comum de segurança de rede e sistemas de informação em todos os Estados-membros. De forma complementar, a Lei de Cibersegurança da UE, em vigor desde 2019, muniu a Europa de uma estrutura de certificação de cibersegurança de produtos, serviços e processos e reforçou o mandato da Agência para a Cibersegurança na UE (ENISA).

Nunca, no entanto, o âmbito de aplicação destas regras foi tão abrangente como o da Diretiva NIS 2 (Diretiva 2022/2555), em vigor desde 2023. Este novo documento revoga a Diretiva NIS (Diretiva 2016/1148/EC) e melhora a gestão de riscos de segurança digital ao introduzir obrigações de relatórios em setores específicos. O seu objetivo principal é a aplicação de medidas que garantam um alto nível de cibersegurança comum em toda a União Europeia[2]. Existe hoje, portanto, uma concertação geral sobre a necessidade de uma aplicação eficaz e medidas efetivas de Cibersegurança em cada um dos países.

Em Portugal, especificamente, o Governo tem vindo a adotar medidas de cibersegurança contra essas ameaças, possuindo, desde 2015, uma estratégia nacional voltada para o cibercrime. Quatro anos mais tarde, em 2019, este sistema foi revisto e alterado, dando origem à atual Estratégia Nacional para a Segurança do Ciberespaço.

Conforme informação do Governo português[3], o cumprimento e aplicação desta estratégia tem como objetivo tornar Portugal um país mais seguro, através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade. Deste modo, o Centro Nacional de Cibersegurança está também encarregue de coordenar a elaboração, o acompanhamento da implementação e a revi-

COM NÚMEROS E IMPACTOS SIGNIFICATIVOS, UMA DAS PRINCIPAIS PREOCUPAÇÕES E PRIORIDADES DA UNIÃO EUROPEIA (EU) NOS ÚLTIMOS ANOS É JUSTAMENTE A CIBERSEGURANÇA, COM UM REFLEXO CLARO NA ELABORAÇÃO DE NOVAS ESTRATÉGIAS E REGULAÇÕES QUE TÊM VINDO A SER APROVADAS E DISCUTIDAS DE MODO A GARANTIR UMA EUROPA MAIS SEGURA, MAIS CONECTADA E MAIS DIGITAL.

são do Plano de Ação da Estratégia Nacional para a Segurança do Ciberespaço, em cooperação com todas as entidades responsáveis pela segurança do ciberespaço nacional.

Quanto aos números de incidentes de cibersegurança em Portugal, os episódios recentes demonstram que, mais do que nunca, a segurança digital deve ser vista como um tópico essencial e central, já que é notório o crescimento significativo de crimes tipificados na Lei do Cibercrime (crimes informáticos) e de incidentes com elevado potencial disruptivo, registados pelas autoridades policiais. O número de incidentes registados pelo CERT.PT aumentou 14%, passando de 1781 em , para 2023 em 2022. De entre esses incidentes, ocorreram diversos ciberataques de grande impacto nas infraestruturas e serviços em Portugal[4], sendo os setores mais afetados os da Banca (sobretudo através de phishing aos clientes), a Educação e Ciência, Tecnologia e Ensino Superior, os Transportes e a Saúde.

QUANTO AOS NÚMEROS DE INCIDENTES DE CIBERSEGURANÇA EM PORTUGAL, OS EPISÓDIOS RECENTES DEMONSTRAM QUE, MAIS DO QUE NUNCA, A SEGURANÇA DIGITAL DEVE SER VISTA COMO UM TÓPICO ESSENCIAL E CENTRAL, JÁ QUE É NOTÓRIO O CRESCIMENTO SIGNIFICATIVO DE CRIMES TIPIFICADOS NA LEI DO CIBERCRIME (CRIMES INFORMÁTICOS) E DE INCIDENTES COM ELEVADO POTENCIAL DISRUPTIVO, REGISTADOS PELAS AUTORIDADES POLICIAIS

Conforme informações do CNCS, verificou-se nos últimos meses um aumento na sofisticação e impacto de alguns incidentes. As ciberameaças a afetar o ciberespaço de modo mais contundente foram o ransomware, a cibersabotagem/indisponibilidade, o phishing/smishing/vishing, a burla online, além de incidentes de negação de serviços distribuída (DDoS) e outros ataques.

Muitos dos casos de phishing, smishing e vishing e burla online estão ligados a técnicas de manipulação de indivíduos, o que reflete uma falta de cultura na prevenção destes crimes. Incidentes de comprometimento de contas e tentativa de login, são muitas vezes resultado de palavras-passe comprometidas e de extrações de dados pessoais que poderiam, por vezes, ser contornadas com a implementação de duplo fator de autenticação, entre outras medidas técnicas e organizativas.

As organizações devem, por isso, estar atentas e dispostas a investir nesta área uma vez que precisam de proteger os seus ativos de negócio críticos, gerar confiança e evitar danos financeiros e de reputação,

bem como garantir a conformidade com os regulamentos existentes.

Por esta razão os números de investimento em cibersegurança cresceram 10,7% em Portugal, fixando-se, este ano, nos 300 milhões de euros, demostrando representar uma prioridade para as empresas e organizações, dado o crescente risco e sofisticação dos ataques informáticos.

Uma boa estratégia de cibersegurança deve começar com um mapeamento adequado das regulações existentes como forma de compliance e um programa de gestão de dados e conscientização apropriado para cada negócio. O desenho de um programa de segurança da informação deve atender fundamentalmente a três pilares: Governação, tecnologia e cultura.

O pilar da Governação está ligado às estruturas de liderança e responsabilidade estabelecidas para garantir que as políticas, contratos e práticas de segurança da informação sejam implementadas e corretamente geridas. Já o pilar da tecnologia refere-se ao conjunto de ferramentas e sistemas utilizados para proteger a informação. Por último, o pilar cultural remete-se ao conjunto de valores, crenças e comportamentos que promovem a segurança da informação. Estes pilares desdobram-se em diferentes ações como a identificação e prevenção de riscos, a deteção de incidentes, a resposta e recuperação de ativos, entre outros.

Atualmente, revela-se fundamental para as organizações terem esta governação adequada, com bons indicadores de risco, capacidade de defesa adequada a ataques e gestão de crises, envolvendo as principais áreas da empresa, através de objetivos e estruturas claras, e bem implementadas, de modo a garantir que possuem capacidade para reagir com competência e rapidez aos novos desafios de Cibersegurança, com o compromisso e a expertise adequados. ◀

[1] *https://comunicado.inovativos.com.br/mid_guia_de_seg*
[2] *https://eur-lex.europa.eu/eli/dir/2022/2555*
[3] *https://portugaldigital.gov.pt/acelerar-a-transicao-digital-em-portugal/conhecer-as-estrategias-para-a-transicao-digital/estrategia-nacional-de-seguranca-do-ciberespaco/*
[4] *https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs15m.pdf*

UMA BOA ESTRATÉGIA DE CIBERSEGURANÇA DEVE COMEÇAR COM UM MAPEAMENTO ADEQUADO DAS REGULAÇÕES EXISTENTES COMO FORMA DE COMPLIANCE E UM PROGRAMA DE GESTÃO DE DADOS E CONSCIENTIZAÇÃO APROPRIADO PARA CADA NEGÓCIO. O DESENHO DE UM PROGRAMA DE SEGURANÇA DA INFORMAÇÃO DEVE ATENDER FUNDAMENTALMENTE A TRÊS PILARES: GOVERNAÇÃO, TECNOLOGIA E CULTURA.

A IT SECURITY É MEDIA PARTNER DO C-DAYS 2023

C-DAYS 2023:
"É NECESSÁRIA MAIS CIBERSEGURANÇA NAS PME"

O C-DAYS, ORGANIZADO PELO CENTRO NACIONAL DE CIBERSEGURANÇA, VOLTOU AO PORTO – MAIS CONCRETAMENTE À ALFÂNDEGA DO PORTO –, DESTA VEZ COM O MOTE "MAIS CONFIANÇA"

POR RUI DAMIÃO

Depois de em 2022 se ter realizado no Centro de Congressos do Estoril, o C-Days voltou à região norte do país com o mote "Mais Confiança". O evento, organizado pelo Centro Nacional de Cibersegurança, teve a IT Security como Media Partner e realizou-se entre os dias 14 e 16 de junho na Alfândega do Porto.

Na sessão de abertura, Filipe Araújo, Vice-Presidente da Câmara Municipal do Porto, referiu que "é com muito gosto que o Porto recebe" o C-Days, até porque, "mais do que nunca", é importante olhar para os temas da cibersegurança e das inovações tecnológicas. "Todas as medidas de prevenção são necessárias para dar mais proteção aos cidadãos", diz. "É absolutamente crucial para todos a realização do C-Days".

A cidade do Porto tem "vindo a trabalhar a prevenção através de planos de contingência e de *disaster recovery*", mas também tem "dedicado especial atenção a fatores como a formação e a partilha de boas práticas".

Por um lado, explica Filipe Araújo, a Câmara Municipal do Porto procura que as equipas muni-

FILIPE ARAÚJO, CÂMARA MUNICIPAL DO PORTO

cipais, que inclui as empresas municipais, "estejam preparadas para lidar com os desafios e os riscos que a Internet e o trabalho online representam". Por outro, também atua junto dos munícipes que pretende envolver e capacitar a população para uma atualização cada vez mais informada e segura dos meios digitais, promovendo, ao mesmo tempo, a inclusão social.

"TODAS AS MEDIDAS DE PREVENÇÃO SÃO NECESSÁRIAS PARA DAR MAIS PROTEÇÃO AOS CIDADÃOS"

FILIPE ARAÚJO, VICE-PRESIDENTE DA CÂMARA MUNICIPAL DO PORTO

MAIS CONFIANÇA

Também na sessão de abertura, Lino Santos, Coordenador do Centro Nacional de Cibersegurança, afirmou que "esta conferência tem sido, há nove anos, um ponto de encontro de diferentes comunidades de cibersegurança: administração central e do Estado; operadores de serviços essenciais; pequenas e médias empresas; administração local; academia; forças e serviços de segurança. Este é o local para discutir os temas de cibersegurança".

"O mote que escolhemos para este ano foi 'Mais Confiança'. Mais confiança nos produtos – e aqui estamos a falar de certificação de produtos –, mas também estamos a falar na ótica do consumidor do receio criado a atos de ciber-resiliência e que está em discussão no seio da União Europeia", explica Lino Santos.

"Mais confiança nos serviços – e, mais uma vez, a certificação de serviços – mas também no Regime Jurídico da Segurança do Ciberespaço que nos assegura uma elevada qualidade na evolução dos serviços essenciais para a sociedade. Mais confiança na cadeia de fornecimento e nas relações entre empresas e fornecedores, e aqui com foco muito particular

> "O MOTE QUE ESCOLHEMOS PARA ESTE ANO FOI 'MAIS CONFIANÇA'. MAIS CONFIANÇA NOS PRODUTOS – E AQUI ESTAMOS A FALAR DE CERTIFICAÇÃO DE PRODUTOS –, MAS TAMBÉM ESTAMOS A FALAR NA ÓTICA DO CONSUMIDOR DO RECEIO CRIADO A ATOS DE CIBER-RESILIÊNCIA E QUE ESTÁ EM DISCUSSÃO NO SEIO DA UNIÃO EUROPEIA",
>
> LINO SANTOS, COORDENADOR DO CENTRO NACIONAL DE CIBERSEGURANÇA

LINO SANTOS, CENTRO NACIONAL DE CIBERSEGURANÇA

nas pequenas e médias empresas que precisam de vender os seus serviços a grandes empresas, sejam nacionais ou estrangeiras. Mais cibersegurança é necessária nas pequenas e médias empresas para criar estas relações de confiança na cadeia de fornecimento", refere o Coordenador do CNCS.

Esta nona edição do C-Days é particularmente importante por duas razões, explica Lino Santos. A primeira é que acontece num momento de transição entre duas estratégias nacionais de segurança do ciberespaço. "A segunda estratégia que Portugal teve nesta área foi criada em 2019 e termina em 2023 e, neste momento, já estamos a trabalhar na elaboração da terceira versão desta estratégia".

Por outro lado, este C-Days também é particularmente importante porque estamos, novamente, num momento de transição entre duas diretivas europeias para a segurança da gestão da informação. "Em janeiro deste ano foi publicada uma nova diretiva" que todos os Estados-membros têm até 2023 para transpor para o seu próprio regime jurídico.

"Estes dois contextos fazem com que este C-Days seja um ponto fulcral para a discussão destes futuros instrumentos da segurança. Futuros instrumentos devem focar um conjunto de desafios presentes e desafios futuros", indica o Coordenador do Centro Nacional de Cibersegurança.

PEDRO MATOS, CONSULTOR DO CNCS

"VISÃO MAIS CLARA E TRANSPARENTE"

Pedro Matos, Consultor do CNCS, subiu a palco para falar de políticas públicas, mais concretamente para revisitar a Estratégia Nacional de Segurança do Ciberespaço. 2015 foi o ano em que foi publicada a primeira Estratégia Nacional de Ciberespaço. Em 2019 foi lançada a segunda estratégia, em vigor até 2023. "Neste momento, estamos num momento de revisão desse processo", refere Pedro Matos.

"ESTA NÃO É UMA ESTRATÉGIA DO CENTRO NACIONAL DE CIBERSEGURANÇA OU DO GOVERNO; É UMA ESTRATÉGIA NACIONAL E TODOS NÓS FAZEMOS PARTE DESSA ESTRATÉGIA, SEJA COMO INDIVÍDUOS – PORQUE TEMOS ESSA RESPONSABILIDADE – OU COMO ORGANIZAÇÃO. É UMA ESTRATÉGIA DE TODOS NÓS"

PEDRO MATOS, CONSULTOR DO CNCS

"Há um aspeto que é importante deixar claro: a nossa estratégia não é uma estratégia de cibersegurança; é uma Estratégia Nacional de Segurança do Ciberespaço", ressalva Pedro Matos. Assim, a Estratégia Nacional de Segurança do Ciberespaço compreende quatro 'cibers': a cibersegurança, o combate ao cibercrime, a ciber defesa e a ciber diplomacia.

Em 2019, início da atual Estratégia Nacional de Segurança do Ciberespaço, existiram 206 atividades executadas no plano de ação; em 2022, o número subiu para 832. "Cada uma destas atividades, foram lidas, reescritas e interpretadas pelo CNCS e pelas entidades que as estavam a implementar", diz Pedro Matos. Em termos de entidades envolvidas, em 2019 existiam 32 organismos envolvidos; em 2022, o número cresceu para 102.

O plano de ação da Estratégia Nacional de Segurança do Ciberespaço conta, com base em dados de 2022, com 102 organismos envolvidos, com uma

taxa de implementação de 82%, 1.046 atividades registadas (entre 2019 e 2022), 45% das atividades focadas na capacitação das organizações, 32% das atividades com foco nas pessoas – através da sensibilização, da formação e da educação – e, entre 2019 e 2022, 589.043 pessoas participaram em ações de formação e sensibilização.

Pedro Matos refere que esta estratégia traz várias oportunidades. Uma delas é refletir e discutir para identificar novas ideias, mas também para aproximar as pessoas e as organizações, para clarificar objetivos e promover alinhamentos, promover o compromisso, o envolvimento e a responsabilização e, também, para identificar, difundir e partilhar boas práticas e casos de sucesso. "Isto faz com que as pessoas se envolvam com as suas organizações e cria responsabilização", refere Pedro Matos.

"Vamos querer chegar ao momento da avaliação e querer desenhar uma visão mais clara e transparente sobre aquilo que é o estado da cibersegurança em Portugal", diz o Consultor do CNCS.

Um dos objetivos passa por ajudar num processo de tomada de decisão mais informada, desenvolver uma cultura nacional de cibersegurança, capacitar os cidadãos e as organizações e ajudar a tornar as políticas públicas mais eficazes e eficientes.

"Esta não é uma estratégia do Centro Nacional de Cibersegurança ou do governo; é uma estratégia nacional e todos nós fazemos parte dessa estratégia, seja como indivíduos – porque temos essa responsabilidade – ou como organização. É uma estratégia de todos nós", conclui Pedro Matos.

ANATOMIA E CIBERSEGURANÇA

Júlio César, Coordenador do Departamento de Operações do Centro Nacional de Cibersegurança

JÚLIO CÉSAR, CENTRO NACIONAL DE CIBERSEGURANÇA (CNCS), CERT.PT

(CNCS) e do CERT.pt, subiu ao palco do C-Days 2023 para falar das semelhanças entre a anatomia e os ciberataques.

As várias cyber kill chains desenvolvidas ao longo dos anos – como da Lockheed Martin, da FireEye ou da Mandiant – "estão certas". O Centro Nacional de Cibersegurança e o CERT.pt desenvolveram a

sua própria cyber killchain com cinco pontos: reconhecimento e primeiro acesso; criação de pontos de acesso alternativos, ou backdoors; escalar privilégios ou movimentação lateral; exfiltração ou o cumprimento de outros objetivos; e persistência.

O último ponto, diz, é um ponto importante; nenhum atacante desiste à primeira só por ter sido detetado e eventualmente ter visto os seus acessos negados. Na maioria das vezes, mantêm a sua intenção de continuar o ciberataque.

"Porque há ciberataques?", pergunta Júlio César. A resposta é uma combinação de três fatores: motivação; capacidade; e oportunidade. "E os ataques acontecem". Os setores com mais ataques registados pelo CERT.pt no primeiro trimestre do ano foi o setor bancário (75 ciberataques), seguido dos serviços de computação em cloud (62) e da educação, ciência, tecnologia e ensino superior (43).

> "O CERT.PT FUNCIONA COM UM ANFITEATRO DE ANATOMIA. O PACIENTE ESTÁ NO MEIO E NÓS ESTAMOS À VOLTA A TENTAR DESCOBRIR O QUE ACONTECEU. NA MAIOR PARTE DOS CASOS, CONSEGUIMOS DESCOBRIR"
>
> JÚLIO CÉSAR, COORDENADOR DO DEPARTAMENTO DE OPERAÇÕES DO CENTRO NACIONAL DE CIBERSEGURANÇA (CNCS) E DO CERT.PT

"A anatomia e a cibersegurança têm coisas parecidas", explica. Quer na anatomia, quer na cibersegurança, é preciso ter uma abordagem sistemática – com protocolos de atuação para a deteção, contenção, erradicação e recuperação –, é preciso ter capacidade de diagnóstico (no caso da cibersegurança para analisar logs, tráfego e análise comportamental), é preciso uma resposta rápida, analisar casos passados e aprender e adaptar-se continuamente.

O representante do CNCS e do CERT.pt especifica que o CERT.pt responde a incidentes de toda a economia. "O CERT.pt funciona com um anfiteatro de anatomia. O paciente está no meio e nós estamos à volta a tentar descobrir o que aconteceu. Na maior parte dos casos, conseguimos descobrir", refere Júlio César.

#13 AGOSTO 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

SEDE E REDAÇÃO: Largo da Lagoa, 7c, 2795-116 Linda-a-Velha, Portugal
TEL: (+351) 214 147 300 | **FAX**: (+351) 214 147 301

PUBLISHER: Jorge Bento
DIRETOR : Rui Damião - rui.damiao@medianext.pt
ANCHOR: Henrique Carreiro
REDAÇÃO: Margarida Bento, Maria Beatriz Fernandes, Marta Quaresma Ferreira
BUSINESS DEVELOPMENT:
Beatriz Salzedas - (+351) 910 788 082 - beatriz.salzedas@medianext.pt
João Calvão - (+351) 910 788 413 - joao.calvao@medianext.pt
MARKETING COMMUNICATIONS ASSISTANT:
Rita Rodrigues - (+351) 912 971 161 - rita.rodrigues@medianext.pt
ARTE E PAGINAÇÃO: Teresa Rodrigues
DESENVOLVIMENTO WEB: Global Pixel
COLABORARAM NESTE NÚMERO: Eduardo Magrani, Nuno Neves, Sérgio Martinho

A REVISTA DIGITAL INTERATIVA IT INSIGHT SECURITY É EDITADA POR:
MediaNext Professional Information Lda.

PERIODICIDADE: Bimestral

CEO: Pedro Botelho

REGISTO E.R.C
Entidade Reguladora para a Comunicação Social nº 127602

Consulte aqui o Estatuto Editorial

Editado por:
media NEXT