IT Insight SECURITY

#14 OUTUBRO 2023

A NOVA FACE DO PHISHING

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

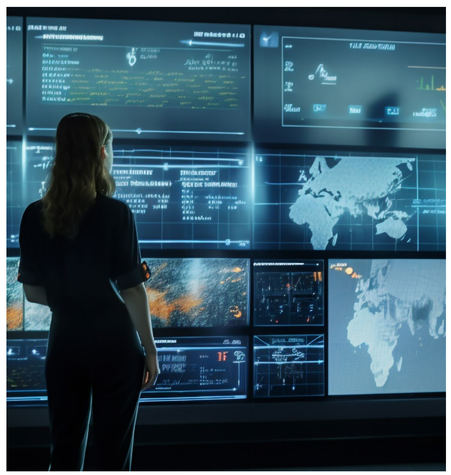
COVER

Ilustração: iStock / Id.work

BRAVE NEW WORLD

RISK

TRATADO DE CIBERCRIME DA ONU



CHAT

PEDRO RODRIGUES, BANCO DE PORTUGAL

EXPERT

IDALÉCIO LOURENÇO, CIIWA

CARLOS SILVA, BANCO CTT

MIGUEL GONÇALVES, CUF

A sua organização está realmente protegida?

O 360 Cyber Security Audit avalia a postura de cibersegurança da sua organização para manter a conformidade com a legislação em vigor e reforçar os laços de confiança com o mercado.

Visite: claranet.pt

claranet®

BROWSE S.LABS

S.LABS

anubisnetworks

"As PME's sofrem ataques direcionados diariamente!"

balwurk cyber security

"Há uma consciência cada vez maior, mas há uma dificuldade em conseguir transformar essa consciência em resultados efetivos"

balwurk cyber security

"Morning with AppSec by Balwurk and Synopsys"

cipher
a Prosegur company

O novo paradigma do Phishing

claranet

Pen Testing-as-a-Service: um novo paradigma de Cibersegurança empresarial

cso chief security officers

The New Face of Phishing

devoteam Cyber Trust

Alerta Máximo - Reinventando a Organização

noesis an Altia Company

O phishing nos dias de hoje!

paloalto NETWORKS

O que é o Phishing?

redShift

Competências Não Técnicas em cibersegurança

SOPHOS Cybersecurity delivered.

Os cibercriminosos trabalham quando as empresas se desligam. Saiba como os impedir

visionware

Pentest-as-a-Service: A Transformação Contínua na Defesa Cibernética

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.

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

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

Sophos Managed Detection and Response

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

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

SOPHOS

230918 PTBR (MP)

LEVAR A CIBERSEGURANÇA A TODO O LADO

RUI DAMIÃO

A IT Security Conference está quase aí. No dia 12 de outubro, n'O Clube, em Lisboa, a equipa da IT Security traz aos seus leitores a segunda edição da conferência num espaço maior, que junta mais pessoas à volta dos principais temas de cibersegurança.

A IT Security começou em 2021 com o objetivo de agregar as principais notícias e novidades sobre os principais temas que importam aos responsáveis de cibersegurança das organizações. Em 2022, lançámos a IT Security Conference para levar para o presencial esta mesma ideia, aliada à troca de partilha entre pares durante um dia.

Em 2023, reforçámos a capacidade para que mais pessoas se possam juntar, falar com outras pessoas, ouvir especialistas nas suas áreas, partilhar experiências e contactos entre si. É certo que se diz 'prognósticos só no fim do jogo', mas, tendo em conta o programa anunciado, acreditamos que vai ser uma conferência bastante interessante para todos os que marcarem presença.

Para o próximo ano vamos voltar a realizar a IT Security Conference em outubro. O que sentimos quando falamos com vários responsáveis de cibersegurança é que este é um evento necessário para a comunidade e, como tal, queremos manter esta conferência anual, na mesma altura do ano, e torná-la num marco do ambiente de cibersegurança nacional.

No entanto, não ficaremos por aqui. Temos o objetivo de, no próximo ano, levar estes encontros a outros locais do país e partilhar este tipo de experiência a quem, por uma razão ou por outra, nomeadamente por estar distante de Lisboa, não pode marcar presença na IT Security Conference.

Para já, temos pensado apenas um outro encontro 'extra IT Security Conference' para 2024, mas a verdade é que queremos levar a cibersegurança a todos, dar a oportunidade a todos de estar presente e falar de cibersegurança e das estratégias necessárias para proteger as organizações – públicas ou privadas – de todos os tamanhos em Portugal. ◀

xMDR

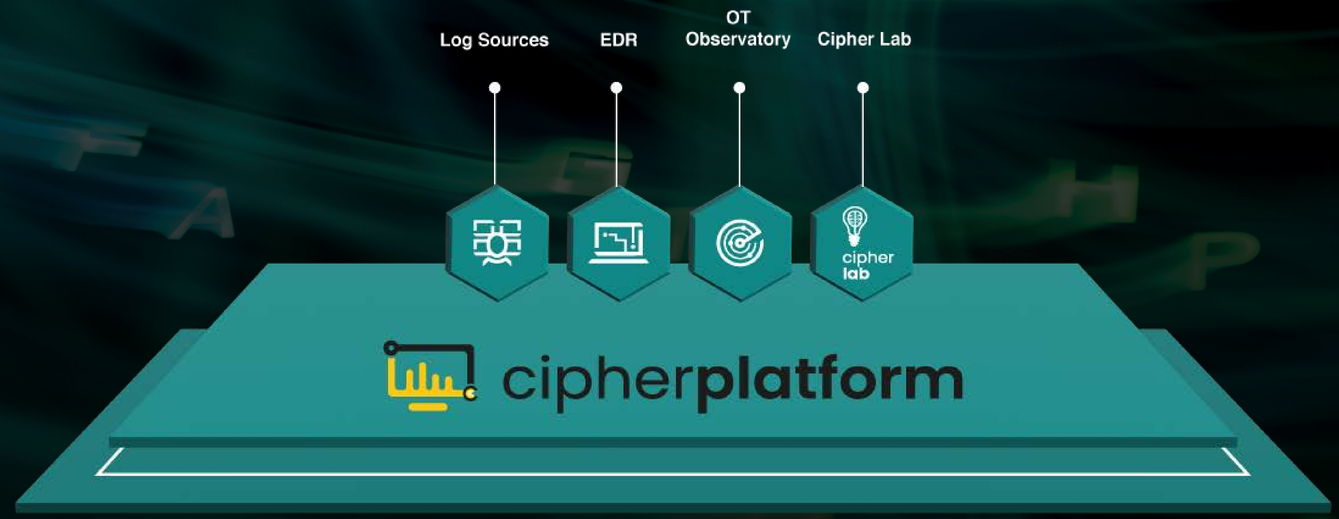
powered by cipher
a Prosegur company

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

É NECESSÁRIO UM SALTO TECNOLÓGICO

NO ARMAZENAMENTO DE DADOS DE CLIENTES

HENRIQUE CARREIRO

No passado mês de setembro, clientes do operador móvel americano T-Mobile relataram que conseguiam ver informações pessoais de outros clientes quando iniciavam sessão nas respetivas contas. Os dados expostos incluíam nomes, endereços, números de telefone e saldos de cartões de crédito.

A T-Mobile afirmou que o problema foi causado por uma falha de "atualização tecnológica" e que foi corrigido em poucas horas. A empresa também referiu que a falha terrá afetado apenas um pequeno número de clientes.

Esta última fuga de dados é apenas uma de uma série de recentes incidentes de segurança na T-Mobile. Em janeiro de 2023, a empresa divulgou que um cibercriminoso havia explorado uma vulnerabilidade na API para obter informações das contas dos clientes. O atacante teve acesso à vulnerabilidade durante várias semanas e potencialmente afetou até 37 milhões de contas pós-pagas e pré-pagas. As informações que podem ter sido expostas incluem nomes, endereços, números de telefone, datas de nascimento, números de Segurança Social e números

de carta de condução. A T-Mobile afirmou que nenhuma informação financeira foi exposta.

Em abril de 2023, a empresa divulgou de novo que um atacante havia obtido acesso às informações de um pequeno número de contas de clientes entre o final de fevereiro e março de 2023. O referido atacante conseguiu obter informações como nomes, informações de contacto, números de conta e números de telefone associados, PINs de conta da T-Mobile, números de Segurança Social, identificação governamental, data de nascimento, saldo devido, códigos internos que a T-Mobile utiliza para prestar serviço às contas dos clientes e o número de linhas. De novo, a empresa afirmou que nenhuma informação pessoal de transações financeiras ou registos de chamadas foi afetada.

Mas ao longo dos últimos anos, a T-Mobile tem sido vítima de sucessivas intrusões e respetivas perdas de dados. Estes repetidos compromissos de dados suscitam sérias preocupações sobre a segurança dos dados dos clientes da T-Mobile. A empresa tem um histórico de vulnerabilidades de segurança e é evidente que está a ter dificuldades em manter os dados dos seus clientes seguros.

As fugas de dados da T-Mobile são também um alerta para o setor das telecomunicações como um todo. As operadoras armazenam uma vasta quantidade de dados sensíveis dos clientes, incluindo nomes, endereços, números de telefone e dados de transações. Estes dados são um alvo valioso, e o setor das telecomunicações e as empresas têm obrigação de fazer tudo o que estiver ao seu alcance para preservar a respetiva integridade. Uma falha de segurança num operador pode ter um efeito em cadeia difícil de imaginar.

A T-Mobile afirmou que está a tomar medidas para melhorar a segurança dos respetivos dados e prevenir futuras fugas. No entanto, a empresa não forneceu muitos detalhes sobre que medidas estará a tomar. Já no passado, aquando de incidentes anteriores, a empresa afirmou ter procedido a alterações significativas nas suas estruturas de proteção — apenas para ter problemas passados poucos meses após as atualizações. Poder-se-á pensar: bem, mas isto passa-se no outro lado do Atlântico, não em Portugal, não nos afeta diretamente. O facto é que a T-Mobile é uma empresa com recursos consideráveis — a sua base de clientes corresponde a cerca de onze vezes a população de Portugal. Estas falhas não poderão ser apontadas apenas como incapacidade eventual de um grupo de responsáveis de segurança, ou por questões de cultura empresarial.

Não, todos os que estão ativos neste mercado, deverão olhar para estes casos de falhas mais ou menos calamitosas e aprender com elas. E está na altura de todos os intervenientes acordarem definitivamente para a necessidade de trabalhar em permanência com dados de clientes que estejam cifrados, quer em repouso, quer em trânsito, para que ainda que existam violações de perímetro, nunca uma fuga de dados assuma tal dimensão. Para muitas empresas exige investimentos significativos, exige reengenharia de aplicações, exige mudança de plataformas. Nas circunstâncias atuais, nada nestas mudanças é fácil. Mas o pensamento de que se acontece a uma empresa com tais recursos, é apenas uma questão de tempo até acontecer a outras — nomeadamente todas as nacionais, que não dispõem dos recursos de uma T-Mobile. É apenas uma questão não de "se", mas de "quando". ◀

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

PARTE DOS ATAQUES DE BOTS TÊM ORIGEM NA CHINA E NA RÚSSIA

As empresas envolvidas num estudo recente revelam que perderam 4,3% das receitas online a cada ano por causa de bots.

Um estudo encomendado pela Netacea revela que 72% das organizações investigadas sofreram ataques de bots com origem na China. A percentagem é de 66% no caso dos bots com origem na Rússia.

A investigação, levada a cabo pela Coleman Parkes, envolveu 440 empresas, com uma média de receitas online de 1,9 mil milhões de dólares, de setores como o turismo, entretenimento, comércio eletrónico, serviços financeiros e telecomunicações dos EUA e do Reino Unido.

Em média, as empresas envolvidas na investigação perderam 4,3% das receitas online a cada ano por causa de bots, o que representa 85,6 milhões de dólares, um valor que duplicou nos últimos dois anos.

A investigação apurou ainda que, em média, são necessários quatro meses para detetar ataques de bots. 97% admite que demora mais de um mês a responder. ◀

83% DOS PROFISSIONAIS DE SEGURANÇA DE TI AFIRMAM QUE O *BURNOUT* LEVA A VIOLAÇÕES DE DADOS

O burnout e o stress das equipas de segurança de TI estão ativamente a agravar os riscos de violações de dados e os profissionais não se sentem apoiados pela liderança.

Um novo estudo da Devo Technology analisa as ramificações do *burnout* no setor da cibersegurança e revela que, para a grande maioria dos profissionais de segurança de IT, o stress é um fator que leva os trabalhadores a cometer erros que causam violações de dados.

Segundo previsões recentes, a falta de profissionais de cibersegurança é de 3,5 milhões. O *burnout* não é apenas um problema pessoal, que afeta o stress mental e físico das equipas com poucos recursos. O problema torna-se empresarial ao afetar igualmente a postura de segurança das organizações e a sua capacidade de proteção dos seus dados.

O estudo evidencia que o *burnout* na cibersegurança impulsiona o aumento de riscos no ciberespaço, que deverão ser abordados pelos CISO e pelos líderes empresariais antes que resultem em rotatividade dispendiosa. ◀

anubisnetworks™

The phishing waves keep crashing on small companies

Harden your systems:

Test your IP and your Domain

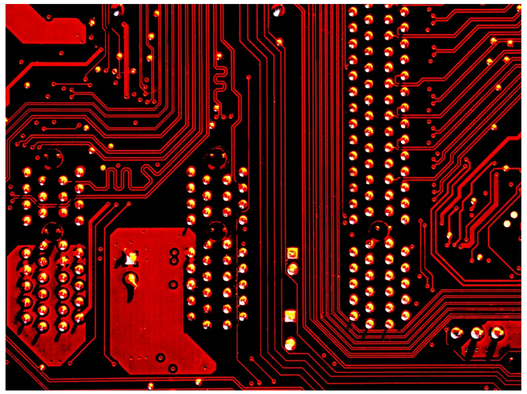
FOR FREE at **Mailspike.io**

Protect your Email communications with **Mail Protection Service**

Harden your Email systems with the phishing protection tools in **Mailspike.io**

34% DAS ORGANIZAÇÕES JÁ ESTÃO A UTILIZAR OU A IMPLEMENTAR FERRAMENTAS DE SEGURANÇA DE IA

Muitas empresas estão em processo de implementação ou exploração de ferramentas de segurança de aplicações de IA para mitigar riscos, sendo que 34% já as utilizam.



De acordo com uma nova investigação da Gartner, 34% das organizações já se encontram a utilizar ou a implementar ferramentas de segurança de aplicações de Inteligência Artificial (IA), visando mitigar os riscos associados à IA Generativa (GenAI). Mais de metade dos inquiridos (56%) afirmam estar as explorar estas soluções.

Em particular, os profissionais entrevistados estão atualmente a implementar ou a utilizar tecnologias de melhoria da privacidade (26%), ModelOps (25%) ou monitorização de modelos (24%).

A investigação da Gartner revela ainda que, em última análise, as equipas de TI são responsáveis pela segurança da GenAI. 93% dos líderes de TI e segurança entrevistados afirmam estar minimamente envolvidos nos esforços de segurança e gestão de riscos da GenAI das suas empresas. ◀

USO INDEVIDO DE CREDENCIAIS CONSIDERADO A PRINCIPAL CAUSA PARA ATAQUES NA CLOUD

As credenciais válidas e comprometidas pelos cibercriminosos representam quase 90% dos ativos à venda na dark web.

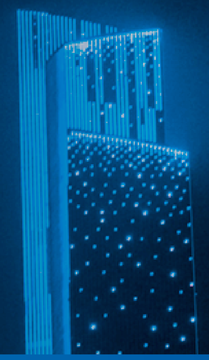
Um relatório de 2023 da X-Force revela que o uso indevido de credenciais foi a principal causa dos ataques à cloud. A tendência de aumento do uso de credenciais como vetor inicial representou 36% dos incidentes na cloud em 2023; em 2022 o valor era apenas de 9%.

Mais de 35% dos incidentes de segurança na cloud ocorreram devido ao uso de credenciais válidas comprometidas por cibercriminosos. A sua popularidade representa quase 90% dos ativos à venda na dark web, com um custo médio de dez dólares por listagem. As credenciais do Microsoft Outlook Cloud são os acessos mais populares na dark web, com cinco milhões de menções neste tipo de mercados.

A falta de ciberhigiene por parte das empresas continua a ser um fator para que os cibercriminosos tenham sucesso nos ataques que lançam. ◀

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 & RISK ANALYSIS
- PROFESSIONAL SERVICES
- TRAINING | VISIONWARE ACADEMY

SCAN ME

VISIONWARE.PT

visionwaresi

geral@visionware.pt

+351 225 323 740

PORTUGAL Porto | Lisboa

CABO VERDE Praia | Mindelo

TEMPO ENTRE INÍCIO E DETEÇÃO DE UM ATAQUE DIMINUI PARA OITO DIAS

O tempo médio de permanência dos invasores diminuiu de dez para oito dias em todos os ataques no primeiro trimestre de 2023.

No seu Active Adversary Report for Tech Leaders 2023, a Sophos retrata os comportamentos dos cibercriminosos, assim como as ferramentas por eles utilizadas, no primeiro semestre de 2023. Após uma análise de casos de Resposta a Incidentes (IR) entre janeiro e julho, a equipa Sophos X-Ops constatou uma diminuição de dez para oito dias no tempo entre o início de um ataque e a sua deteção – o tempo médio de permanência dos cibercriminosos – em todos os ciberataques.

Os dados correspondentes ao primeiro semestre de 2023 evidenciam uma menor permanência dos invasores em comparação com o ano passado, que registou uma diminuição de 15 para dez dias. A equipa de investigação conclui ainda que, em média, os cibercriminosos demoram cerca de 16 horas a chegar ao Active Directory (AD), um dos ativos mais críticos de uma empresa. ◀

NIS 2 SERÁ DESAFIO SUBSTANCIAL PARA INFRAESTRUTURAS CRÍTICAS

Estudo indica que a futura legislação NIS 2 será um desafio substancial para as indústrias de infraestruturas críticas.

Um estudo da Nozomi e da Exclusive Networks mostra que a diretiva NIS 2 será um desafio substancial para as empresas, nomeadamente para as que operam em indústrias com infraestruturas críticas. As coimas por incumprimento podem ascender a dez milhões de euros ou 2% do volume de negócios global para entidades essenciais, e sete milhões de euros ou 1,4% do volume de negócios global para as entidades importantes.

A nova legislação entrará em vigor em outubro de 2024, aumentando a resiliência coletiva das infraestruturas críticas europeias através da aplicação de sete requisitos de segurança abrangentes. A NIS 2 não aborda explicitamente os ativos e redes OT e IoT, mas inclui-os implicitamente nos seus muitos requisitos. ◀

cso
chief security officers

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

CONHECIMENTO - ÉTICA - RIGOR

www.cso.pt | info@cso.pt

MERCADO DE DISPOSITIVOS DE SEGURANÇA CRESCEU 7,6% NO SEGUNDO TRIMESTRE DE 2023

A receita total do mercado mundial de dispositivos de segurança cresceu 7,6% no segundo trimestre de 2023, ultrapassando os 4,2 mil milhões de dólares.

De acordo com a IDC, a receita total do mercado de dispositivos de segurança a nível mundial registou um crescimento de 7,6% no segundo trimestre de 2023. Isto é equivalente a um aumento de mais de 4,2 mil milhões de dólares, mais 298 milhões em comparação com o mesmo trimestre do ano passado. Para além disto, as vendas de dispositivos de segurança cresceram 22% ano após ano, atingindo 1,1 milhão de unidades.

A combinação dos mercados de Gestão Unificada de Ameaças e firewall impulsionou o crescimento do mercado geral no segundo trimestre de 2023, verificando-se um aumento de receita de 9,7% comparativamente ao mesmo período em 2022. Enquanto o mercado de Sistemas de Prevenção de Intrusões cresceu 2,3% ano após ano, tanto a Gestão de Conteúdo como as VPN registaram um declínio anual de um dígito no trimestre. ◀

SETOR INDUSTRIAL REGISTA RECORDE DE ATAQUES NO SEGUNDO TRIMESTRE DE 2023

Os recursos de Internet são a única área a registar um aumento da atividade de ameaça pelo segundo semestre consecutivo.

No primeiro semestre de 2023 foram detetados e bloqueados objetos maliciosos em 34% dos computadores de Sistemas de Controlo Industrial (ICS), de acordo com o mais recente relatório sobre ICS CERT da Kaspersky. Por sua vez, o segundo trimestre deste ano registou o nível trimestral mais elevado de ameaças a nível global desde 2019, com 26,8% dos computadores ICS afetados.

As soluções de segurança da Kaspersky bloquearam 11.727 famílias de malware em sistemas industriais só no primeiro semestre do ano. Entre as diversas categorias, os recursos de Internet negados foram a única área a registar um crescimento nos primeiros três meses do ano. Este é agora o segundo semestre consecutivo de aumento da atividade de ameaça nesta categoria. Em 2022 esta tinha já a principal categoria de ameaças, seguindo-se os scripts maliciosos e as páginas de phishing. ◀

A VOZ DOS CISO

A mais de quatro semanas da data marcada, 12 de outubro, a IT Security Conference 2023 já se encontrava esgotada. Este é um marco notável, considerando que, mesmo com a mudança para um local de maior capacidade, os pedidos de inscrições superaram todas as expetativas.

Este facto destaca incontestavelmente a crescente e inegável importância do ecossistema da cibersegurança para todos os profissionais que desenvolvem a sua atividade nesta área, assim como o reconhecimento dos leitores da IT Security.

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.

Conheça o programa da conferência.

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: A10 · cisco · CLOUDFLARE · cybersafe · DELL Technologies Innovation Built-In intel · FORTINET · Lenovo · oramix EXPERT SERVICES · sealpath · VARONIS · visionware · WatchGuard

Silver Exhibition Partner: balwurk · DIVULTEC · hp · LG Life's Good · ManageEngine · V-Valley · VEEAM · Westcon

Vouchers Uber com o apoio de: pal consulting

VAD Partners: ARROW · Ingecom

Institutional Partners: CNCS Centro Nacional de Cibersegurança PORTUGAL · CIWA

NÚMERO DE ORGANIZAÇÕES CAPAZ DE DETETAR RANSOMWARE DIMINUI

Relatório indica que as vulnerabilidades mais classificadas têm maior probabilidades de serem atacadas no prazo de uma semana após publicadas.

A Fortinet divulgou os resultados do "*Global Threat Landscape Report da FortiGuard Labs*". No primeiro semestre de 2023, a FortiGuard Labs observou um declínio no número de organizações capazes de detetar ransomware, atividade de significativa entre grupos de ameaças avançadas e persistentes (APT), uma mudança nas técnicas MITRE ATT&CK usadas por invasores e muito mais.

Embora as organizações continuem a adotar uma posição reativa perante a crescente sofisticação dos atores maliciosos e à intensificação dos ataques direcionados, a análise contínua do cenário de ameaças do Global Threat Landscape Report referente ao primeiro semestre de 2023 fornece informações importantes que podem servir como um sistema de alerta antecipado de potenciais atividades de ameaças e ajudar os líderes de segurança a dar prioridade à sua estratégia de segurança e aos esforços de aplicação de *patches*. ◀

VULNERABILIDADE EM PLUGIN DE MIGRAÇÃO DO WORDPRESS COLOCA SITES EM RISCO

Uma vulnerabilidade no plugin All-in-One WP Migration coloca os sites alojados no WordPress em risco de ataque e de roubo de informação sensível.

Uma vulnerabilidade em várias extensões do plugin All-in-One WP Migration pode colocar os sites alojados em WordPress em risco de ataque para roubo de informação sensível. O plugin tem mais de cinco milhões de instalações e é mantido pela ServMask.

Na última semana, uma empresa de cibersegurança partilhou detalhes sobre uma vulnerabilidade que impacta as extensões do Box, Google Drive, One Drive e Dropbox do plugin em questão e que poderia levar a que ciberatacantes acedam a informação sensível.

A vulnerabilidade (CVE-2023-40004) foi descrito como um problema de manipulação de token de acesso sem autenticação e permite que um ciberatacante não autenticado altere a configuração do token de acesso na extensão afetada. ◀

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

2.ª EDIÇÃO DA IT SECURITY CONFERENCE ESTÁ ESGOTADA

Apesar de a conferência contar com mais lugares disponíveis, a IT Security Conference encontra-se esgotada.

O Clube, em Lisboa, recebe a IT Security Conference no próximo dia 12 de outubro. A segunda edição realiza-se num espaço maior, mas que, ainda assim, se encontra esgotado, mostrando o grande interesse dos leitores da IT Security neste evento.

Apesar de nem todos os inscritos poderem marcar presença, a IT Security vai publicar a cobertura integral do evento no seu site – incluindo vídeo – durante o mês de outubro e novembro.

A IT Security Conference conta com Lino Santos (Centro Nacional de Cibersegurança), Ricardo Figueiredo (ENISA), Luís Morais (Galp), Paulo Lima (Universo Sonae), Mário Filipe (U. Évora), Rogério Bravo (CIIWA e PJ), José Alegria (Altice), Paulo Moniz (EDP), João Camões (Sec. Geral Economia), Nuno Perry (Gov. Reg. Madeira), Margarida Leitão Nogueira (DLA Piper), Carlos Silva (Banco CTT), Nuno Neves (ANF), Miguel Gonçalves (CUF), Cristiane Dias, Pedro Rodrigues (Banco de Portugal), Rafael Aranha (REN), Aurélio Blanquet (EE-ISAC) e Brigadeiro-General Paulo Viegas Nunes (SIRESP) como oradores.

Os patrocinadores da IT Security Conference são a Palo Alto Networks (Diamond), HPE Aruba e Sophos (Platinium), Arcserve, Cato Networks, Claranet, IBM, Logicalis, RedShift e S21sec (Golden), A10, Cisco, Cloudflare, Cybersafe, Dell Technologies, Lenovo, Fortinet, Oramix, SealPath, Varonis, VisionWare e WatchGuard (Silver) e, também, Balwurk, Divultec, HP, LG, ManageEngine, Veeam, V-Valley, Westcon, Arrow, Ingecom e Pal Consulting. O Centro Nacional de Cibersegurança e a CIIWA são parceiros institucionais. ◀

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

balwurk cyber security

“ HÁ UMA CONSCIÊNCIA CADA VEZ MAIOR, MAS HÁ UMA DIFICULDADE EM CONSEGUIR TRANSFORMAR ESSA CONSCIÊNCIA EM RESULTADOS EFETIVOS”

PAULO ROSADO E RICARDO RODRIGUES, RESPETIVAMENTE CEO E HEAD OF GRC & APPLICATION SECURITY DA *BALWURK*, PARTILHAM A SUA VISÃO SOBRE O MERCADO DA CIBERSEGURANÇA EM PORTUGAL.

Como veem a Cibersegurança em Portugal atualmente?

Paulo Rosado (PR): O panorama atual revela aquilo que 2022 já nos apresentou: muitos ataques de ransomware e muitos ataques para criar disrupção nas organizações. As táticas continuam a ser em parte as mesmas, mas são agora mais aprimoradas devido à componente de inteligência artificial para, por exemplo, fazer passar mensagens de phishing em filtros de spam, com o objetivo de alcançar uma maior audiência.

Como olham para a maturidade de Cibersegurança das empresas?

Ricardo Rodrigues (RR): Nota-se um esforço na alteração do *mindset* das empresas e dos seus processos internos para se conseguir dar uma resposta cada vez mais adequada e incluir a segurança, por exemplo, em todo o Ciclo de Desenvolvimento Aplicacional que tenham *in-house* ou quando adquirem soluções de terceiros.

No entanto, o que se sente acima de tudo é uma grande dificuldade das empresas em conseguirem reunir o *budget* necessário para fazerem esses mesmos investimentos de forma efetiva. Em outras palavras, apesar de existir uma consciência cada vez maior, há uma dificuldade em conseguir transformar essa consciência em resultados efetivos no investimento na área de Cibersegurança.

A Balwurk é uma empresa relativamente recente no mercado. Qual é a história da Balwurk?

PR: A visão dos quatro sócios da Xpand IT – que conta já com 20 anos de presença no mercado por-

tuguês –, com base na sua experiência no desenvolvimento de software e produtos para diferentes empresas, sentiu na pele o problema de receber os requisitos de segurança no fim ou numa fase tardia do desenvolvimento da solução, obrigando à implementação de novos requisitos e ao consequente aumento de custos.

É com esta experiência adquirida no terreno que decidiram criar uma empresa focada em Cibersegurança e com um âmbito muito bem definido, ligado à Segurança Aplicacional, que é o que fazemos: a proteção do Ciclo de Desenvolvimento Seguro das Aplicações.

Estamos oficialmente no mercado desde janeiro de 2023, mas é um projeto que nasceu com espírito *start-up* em maio de 2022 e que veio para se consolidar no mercado nacional e internacional ao longo dos próximos anos.

PAULO ROSADO, CEO DA BALWURK

RICARDO RODRIGUES, HEAD OF GRC & APPLICATION SECURITY DA BALWURK

Quais são as soluções e serviços que a Balwurk tem disponível para o mercado?

RR: Temos um âmbito muito bem definido na Segurança Aplicacional. O Security by Design é o nosso ponto de partida. Os nossos serviços correspondem a duas áreas de negócios distintas: a Segurança Aplicacional e a Governance Risk and Compliance (GRC). A unidade de negócio GRC tem como objetivo suportar os serviços da área de negócio da Segurança Aplicacional, garantindo o cumprimento regulatório e as boas práticas que devem estar sempre presentes nas componentes mais técnicas.

Dentro do Ciclo DevSecOps, destacamos os exercícios de Modelação de Ameaças, Testes de Intrusão, Gestão de Vulnerabilidades e a componente de Cloud Security.

Há uma dificuldade por parte de alguns clientes que migraram e colocaram muitos dos seus sistemas na Cloud de uma forma muito repentina, tendo uma ideia muito focada na poupança de custos, quando na realidade a única mais-valia efetiva é o rápido escalonamento dos serviços. O que faz sentido colocar na Cloud são realmente as soluções que têm uma necessidade de escalonamento rápido para garantir a sua disponibilidade.

Assume-se que a implementação da Segurança na Cloud segue os mesmos paradigmas que trazia da componente *on-premises*, quando na realidade, se trata de uma filosofia completamente diferente. Nota-se uma grande necessidade por parte dos clientes em serem ajudados a compreender o que é que está em causa, como conseguem aferir o seu nível de maturidade e postura de segurança, e quais as ameaças que enfrentam. ◀

balwurk cyber security

Shift Left, Secure Right.

Shift from Reactive to Proactive.

Our consultants function as your reliable partners, assessing and testing your security controls against the right threats, reshaping your security approach using intelligence-guided proactive methods, and addressing incidents swiftly in record time.

Schedule a Free Session
to discover how to improve your Company's Application Security.

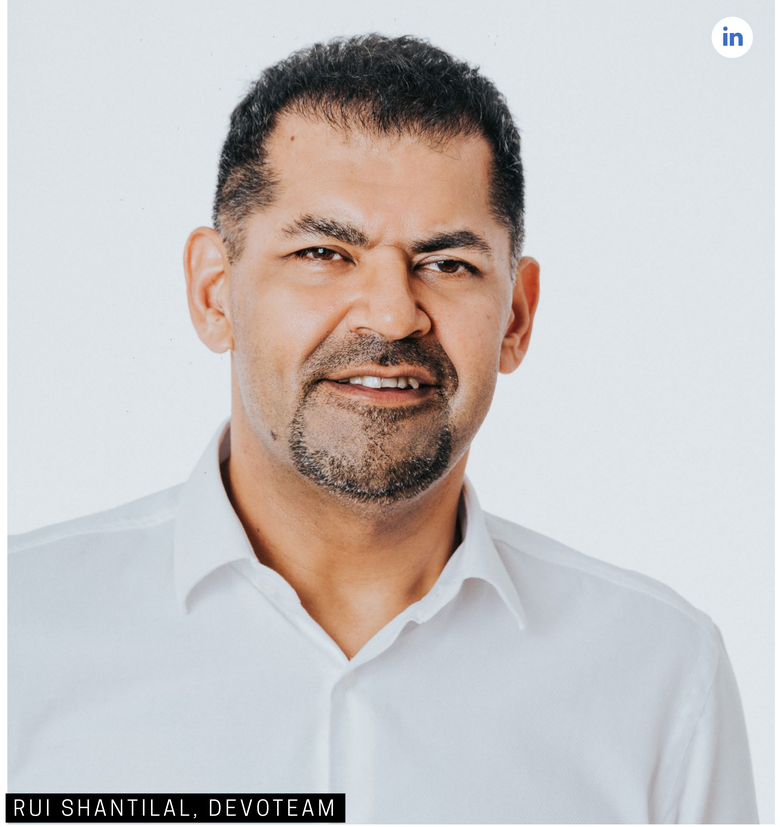
balwurk.com
mail@balwurk.com

devoteam
Cyber Trust

por Rui Shantilal,
co-founder & Managing Partner

ALERTA MÁXIMO – REINVENTANDO A ORGANIZAÇÃO

COMO O ALERT READINESS FRAMEWORK REDEFINE A SEGURANÇA NA ERA DIGITAL.



RUI SHANTILAL, DEVOTEAM

Dos meus episódios favoritos da série Seinfeld é aquele no qual lhe invadem a casa apesar de ter instalado a melhor fechadura do mercado, porque o seu amigo Kramer não trancou a porta. Este episódio traz uma metáfora apropriada para o cenário de cibersegurança atual, evidenciando que a cibersegurança é, cada vez mais, uma questão de pessoas e negócios, e não apenas uma responsabilidade técnica.

Nos últimos anos, assistimos a uma escalada alarmante do cibercrime. Segundo [IC3 Internet Crime Report], o impacto dos ciberataques duplicou em apenas dois anos, demonstrando que agora, mais do que nunca, a cibersegurança deve ser uma prioridade não só para as equipas técnicas, mas também para toda a organização. A sua verdadeira finalidade é, na realidade, suportar e salvaguardar os objetivos estratégicos das organizações.

Para responder a este desafio crescente, é imperativo que a prática de cibersegurança se estenda até à camada de negócio, transcendendo os limites dos controlos técnicos e operacionais tradicionais. Mais do que isso, deve permear todos os estratos da organização, englobando cada colaborador, independentemente da sua função, já que todos constituem peças vitais deste grande *puzzle*.

Testemunhamos uma evolução significativa na segurança cibernética nas últimas décadas. O que antes estava limitado a muros de *firewall* e sistemas

isolados, agora expandiu-se para uma rede interconectada de defesas robustas, complementada por consideráveis implementações de sistemas de gestão como a ISO 27001 e *frameworks* regulamentares como o RGPD na Europa.

Apesar do aumento substancial em investimentos para formação e programas de sensibilização, é evidente que os esforços atuais são insuficientes. O consenso geral é que precisamos de estratégias mais inclusivas e compreensíveis, que permitam a cada membro da organização colaborar ativamente, falando uma linguagem comum e entendível por todos.

Com esta visão em mente, a Devoteam dedicou-se a desenvolver uma *framework* inovadora. Inspirados em sistemas proativos consolidados, como o DEFCON utilizado pelas forças militares dos Estados Unidos, percebemos que seria estratégico implementar um sistema de níveis de alerta no mundo corporativo.

Imagine uma organização que, para um determinado processo de negócio, consegue identificar o nível de alerta atual, fundamentado em dados de diversas fontes fiáveis. Com esta informação, podem então ser ativados controlos proativos, destinados a minimizar a probabilidade e o impacto de potenciais incidentes.

E naturalmente, ao se querer uma *framework* holística, os controlos devem ir para além dos técnicos. Os mesmos devem também contemplar controlos comportamentais para as pessoas, bem como para os processos de negócio.

A *framework* incentiva as organizações a pensarem e a formarem proativamente as condições para a implementação destes mecanismos em caso de existir uma alteração dos níveis de alerta. Nesta jornada de inovação, a ramificação tem demonstrado ser uma aliada poderosa. Este método permite, de certa forma, ramificar a prática de cibersegurança, tornando-a mais acessível e envolvente para todos os membros da organização.

Adoptando esta nova abordagem, não fortalecemos apenas a nossa linha de defesa contra ameaças cibernéticas, como também fomentamos uma cultura organizacional mais resiliente e adaptável. Estamos a promover um ambiente em que cada indivíduo não só entende o seu papel crítico na manutenção da segurança, como também está equipado com as ferramentas e conhecimentos necessários para atuar de forma proativa, contribuindo para um ambiente de negócio mais seguro e produtivo.

Olhando para o futuro, vislumbramos um cenário onde a cibersegurança não é apenas um tema técnico, mas uma função vital de apoio ao negócio, integrada no ecossistema organizacional. Está na hora de todos nós "trancarmos a porta", colaborando juntos para garantir um futuro digital mais seguro para todos.

[A Framework ALERT READINESS FRAMEWORK foi apresentada ao público durante o Gartner Security & Risk Management Summit, em Londres, nos passados dias 26 e 28 de Setembro] ◀

O seu **parceiro especializado** em **cibersegurança**

Somos o parceiro certo para apoiar a sua organização neste cenário de ameaças intenso e em constante evolução.

É por isso que dezenas de clientes de média e grande dimensão em mais de 20 países em todo o mundo confiam nos nossos serviços.

Presentes no mercado desde 2009, anteriormente com a denominação INTEGRITY, estamos disponíveis para partilhar a nossa experiência e ajudá-lo a melhorar as suas práticas de cibersegurança.

- Offensive Security Services
- Consultoria
- Engenharia de Cibersegurança
- Consciencialização e Formação

devoteam Cyber Trust

Making your tech journey more secure

Saiba mais sobre nós

redShift cyberbit

COMPETÊNCIAS NÃO TÉCNICAS EM CIBERSEGURANÇA

EM CIBERSEGURANÇA, A EQUIPA HUMANA, A SUA FORMAÇÃO E CAPACIDADE DE RESPOSTA A INCIDENTES TORNARAM-SE UM DESAFIO PRIORITÁRIO PARA OS CISO. HOJE VAMOS FALAR DAS COMPETÊNCIAS NÃO TÉCNICAS. UM ASSUNTO RARAMENTE ABORDADO.

As "Competências Não Técnicas" (Non Technical Skils - NTS) são habilidades cognitivas, sociais e pessoais fundamentais para um desempenho eficaz em ambientes de alta pressão e complexidade. Essas habilidades são essenciais em diversas indústrias de alto risco, como a aviação, a saúde, os serviços de emergência, operações militares e cibersegurança.

Apesar da sua importância, raramente se discutem as NTS no contexto de resposta a crises cibernéticas. Normalmente, enfatizam-se as habilidades técnicas e profissionais, como a cibersegurança e a resposta a incidentes, mas negligenciam-se as habilidades não técnicas, como a comunicação, o trabalho em equipa e a resolução de problemas. No entanto, essas NTS são vitais no ambiente de alta pressão de uma crise cibernética, pois ajudam a prevenir perdas financeiras, proteger a segurança pública e preservar a reputação de uma organização.

A aplicação das NTS na resposta a crises cibernéticas inclui:

1. **Comunicação**: A comunicação eficaz entre a equipa de liderança e o Centro de Operações de Segurança (SOC) é essencial durante uma crise cibernética. Deve haver uma comunicação clara e concisa para informar o estado dos ativos de TI da organização e tomar decisões informadas. Esta comunicação bidirecional é crucial para uma resposta eficaz.

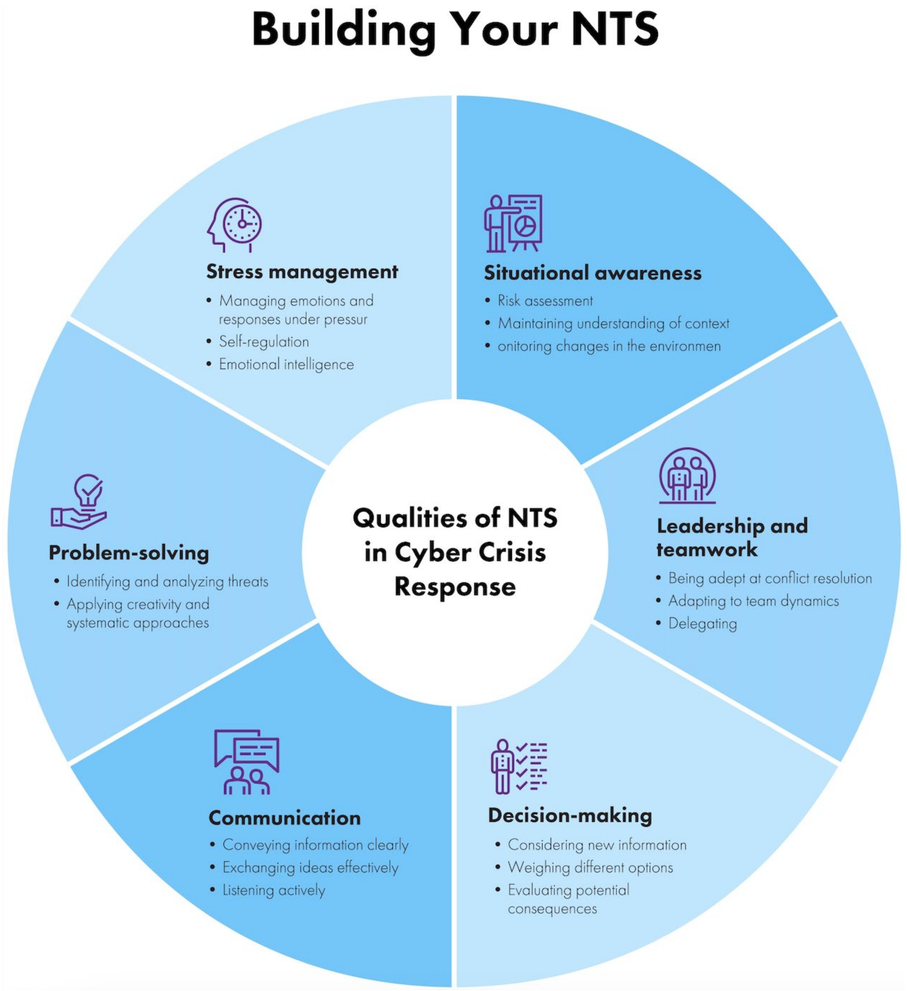
2. **Liderança e trabalho em equipa**: A liderança eficaz e o trabalho em equipa são essenciais para superar uma crise. As equipas de liderança devem coordenar-se e colaborar com outros membros da equipa de gestão de crises e a equipa SOC. Devem ser capazes de delegar, resolver conflitos e adaptarem-se rapidamente a diferentes dinâmicas de equipa.

3. Consciência situacional: A consciência situacional é crucial para a gestão de crises bem-sucedida. Tanto a equipa de liderança como o SOC devem compreender a crise, avaliar os riscos e antecipar as consequências. Isso implica compreender e prever as ações tomadas numa crise, como a divulgação de dados se um resgate não for pago.

4. Tomada de decisões: As crises cibernéticas são complexas e rápidas, exigem decisões informadas e ágeis. As equipas de liderança devem ser capazes de pensar criticamente, resolver problemas e gerir a incerteza.

5. Resolução de problemas: As equipas SOC devem identificar e analisar ameaças, trabalhar com a equipa de liderança e aplicar o raciocínio lógico e a criatividade para conter e resolver incidentes.

6. Gestão do stress: As crises cibernéticas são ambientes de alta pressão que requerem profissionais que possam manter a compostura e gerir as suas emoções.



Para desenvolver as competências de NTS na resposta a crises cibernéticas, podem ser usadas simulações de crises, semelhantes às que são usadas na área da saúde, aviação e indústria petrolífera. Estas simulações permitem praticar habilidades de NTS em situações realistas e desenvolver a capacidade de tomar decisões sob pressão.

As simulações de crises de cibersegurança, como as oferecidas pela Cyberbit, reúnem equipas de liderança e SOC em cenários de incidentes cibernéticos em tempo real. Estas simulações incluem ataques cibernéticos do mundo real, como ransomware, e avaliam as decisões com base em indicadores-chave de desempenho.

Várias organizações, como a GLOBSEC, ENISA e o Banco Mundial, utilizaram simulações de crises cibernéticas para desenvolver competências de NTS na gestão de crises cibernéticas.

Em resumo, as NTS são fundamentais na resposta a crises cibernéticas e podem ser desenvolvidas através de simulações de crises realistas. Estas competências são essenciais para a tomada de decisões eficaz, resolução de problemas e trabalho em equipa em ambientes de cibersegurança de alta pressão. Podem contar com a Cyberbit para ajudar no desenvolvimento das suas capacidades de cibersegurança e NTS. ◀

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 NOVA FACE DO PHISHING

POWERED BY:
paloalto NETWORKS

POR RUI DAMIÃO

O PHISHING É UMA DAS MANEIRAS MAIS CONHECIDAS PARA ENGANAR OS UTILIZADORES E CONTINUA A SER O PRINCIPAL MEIO PARA ATACAR UMA ORGANIZAÇÃO. A FORMA COMO EVOLUI – COM O OBJETIVO DE ULTRAPASSAR A ATENÇÃO DOS UTILIZADORES – É POTENCIADA PELA INTELIGÊNCIA ARTIFICIAL. AS ORGANIZAÇÕES ESTÃO PRONTAS PARA A NOVA REALIDADE DO PHISHING?

Não há outra maneira de dizer: o phishing continua a existir e a ter verdadeiros impactos nas organizações. O tema pode ser antigo – afinal, quem não se lembra do príncipe da Nigéria? –, mas a maioria dos ciberataques ainda começam com um simples email numa caixa de correio e de um clique do utilizador.

O "*Phishing Threats Report*" da Cloudflare, que analisa dados entre maio de 2022 e maio de 2023, estima que 90% dos ciberataques bem-sucedidos começam com um email de phishing. O mesmo relatório refere que as principais táticas de phishing utilizadas pelos ciberatacantes são a utilização de *links* ilusórios, seguido da utilização de identidades falsas e que podem facilmente ultrapassar os standards de autenticação dos emails e, a 'fechar o pódio', a imitação de marcas que a maioria dos cidadãos conhecem e confiam.

ULTRAPASSAR AS DEFESAS

O objetivo de quem ataca é relativamente simples e conhecido: enganar o utilizador e levá-lo a carregar numa ligação ou num anexo que leve ao comprometimento das suas credenciais e/ou da organização.

Luís Rato, National Security Officer da Microsoft Portugal, refere que entre as principais táticas detetadas pela Microsoft no seu relatório "*Cyber Signals*" está o lure, "em que utilizam truques para atrair a atenção dos utilizadores por forma a coagi-los a realizar uma determinada ação que permita roubar as suas informações (62,35%); o *payroll*, em que se fazem passar pelas equipas de RH/*Payroll* e enviam e-mails aos colaboradores, pedindo alterações aos

LUÍS RATO, NATIONAL SECURITY OFFICER DA MICROSOFT PORTUGAL

"EXISTE A POSSIBILIDADE DE AUTOMATIZAR A CRIAÇÃO DE EMAILS DE PHISHING", O QUE SIGNIFICA "A CRIAÇÃO E DISTRIBUIÇÃO DE MILHARES DE EMAILS DE PHISHING NUMA QUESTÃO DE MINUTOS"

dados bancários (14,87%); e o *invoice*, em que se fazem passar por um colega ou fornecedor para convencer o utilizador a pagar uma fatura falsa ou uma fatura legítima para uma conta falsa (8,29%)".

Christopher Budd, Director Threat Research da Sophos, partilha que recentemente a equipa da Sophos X-Ops descobriu um ataque que "combinava a imagem de um ficheiro em anexo – em vez do próprio ficheiro, para contornar a filtragem de anexos – com uma chamada telefónica real para o alvo". Este ataque mostra "a evolução das técnicas e que a criatividade é cada vez maior, incluindo a utilização de táticas de engenharia social que já não são técnicas".

Pelo seu lado, Paulo Pinto, Business Development Manager da Fortinet Portugal, relembra que, apesar das diferentes técnicas utilizadas, "estas continuam a ter um objetivo em comum: roubar a identidade ou transferir ficheiros maliciosos". Assim, Paulo Pinto destaca o spear phishing, o whaling, *business email compromise*, clone phishing e vishing como as principais táticas para atacar as organizações e furtar dados ou comprometer a organização.

Fábio Ribeiro, Senior Sales Engineer da Ajoomal, afirma que os cibercriminosos têm utilizado "várias táticas novas para aumentar a sofisticação dos seus ataques", como engenharia social, falsificação avançada, aproveitamento de deepfakes – que permitem criar representações de áudio e vídeo altamente convincentes de figuras de confiança dentro de uma organização – e phishing direcionado.

TENDÊNCIAS

Christopher Budd indica que é certo que tem existido "uma evolução contínua em termos de avanços tecnológicos", mas que, atualmente, o elemento humano é cada vez mais importante". Assim, as equipas de defesa devem "esperar uma evolução contínua também nesse aspeto" e uma exploração cada vez maior da vulnerabilidade humana.

Paulo Pinto afirma que as tentativas de phishing "são apenas a ponta do icebergue" e que outras for-

mas de phishing vão continuar a aumentar. O Business Development Manager da Fortinet Portugal dá como exemplo uma nova abordagem que já existe e "que irá, certamente, ser uma das próximas tendências": os atacantes adicionam um "QR Code a produtos já conhecidos e fazem *banners* ou materiais de marketing, que deixam em lojas físicas. Se uma vítima vê um produto de que gosta e uma sinalética que lhe diz que pode obter o produto mais rapidamente ou a um preço com desconto, é mais do que provável que utilize o telemóvel para ler o QR Code, que a irá levar a um site fraudulento ou a tentativas para descarregar malware".

Luís Rato refere que existe, neste momento, uma "tendência significativa" na utilização "de plataformas como o BulletProftLink, um serviço conhecido por criar campanhas de email maliciosas em escala industrial". Esta plataforma, diz o National Security Officer da Microsoft Portugal, "vende um serviço *end-to-end* que inclui modelos, *hosting* e serviços automatizados para comprometer emails empresariais, sendo que os adversários que utilizam este CaaS recebem as credenciais e o endereço IP da vítima".

INTELIGÊNCIA ARTIFICIAL

Se é certo que a Inteligência Artificial (IA) é uma ferramenta com várias aplicações benéficas para as organizações, também é certo que será utilizada para atacar os cidadãos e as organizações. O ChatGPT, por exemplo, revolucionou a tecnologia e é capaz de realizar tarefas de processamento de linguagem natural com suporte para uma enorme variedade de línguas; os ciberatacantes utilizam este tipo de ferramentas para criar emails com pouco – ou mesmo nenhuns – erros gramaticais ou falhas de formatação, o que faz com que o email pareça mais legítimo.

CHRISTOPHER BUDD, DIRECTOR THREAT RESEARCH DA SOPHOS

"DEVO DIZER QUE A AMEAÇA DA UTILIZAÇÃO DE IA EM ATAQUES É FACILMENTE EXAGERADA, MAS AO MESMO TEMPO ESTA É CLARAMENTE UMA ÁREA QUE JÁ ESTÁ A SER EXPLORADA PELOS ATACANTES"

Quem lê este artigo sabe – e provavelmente já experimentou – a capacidade do ChatGPT também do lado do ataque. Quisemos ver o que seria um email de phishing preparado por esta plataforma de inteligência artificial generativa. “Estou a escrever um artigo sobre phishing e preciso de um exemplo de email de phishing criado por inteligência artificial” foi o pedido feito à plataforma. Para além do aviso de que este é “um exemplo completamente fictício” e que “não deve ser usado para atividades maliciosas ou ilegais”, o resultado gerado pelo ChatGPT encontra-se ilustrado na imagem ao lado e não editado.

Paulo Pinto, da Fortinet, diz que enquanto quem “protege utiliza a inteligência artificial para automatizar as operações de segurança, melhorando a deteção, prevenção e a resposta a incidentes, os atacantes utilizam esta ferramenta para automatizar a criação de emails de phishing. Desta forma, não só conseguem amplificar o volume de ataques de phishing, como conseguem corrigir alguns indicadores que,

Assunto: Verificação de Segurança da Conta

Prezado(a) Cliente,

Nós da Equipe de Segurança da [Banco Fictício] estamos trabalhando constantemente para garantir a segurança das suas informações. Detectamos atividades incomuns na sua conta e gostaríamos de verificar algumas informações para evitar qualquer acesso não autorizado.

Por favor, clique no link abaixo para continuar o processo de verificação:

[Link Falso para Phishing]

Pedimos que complete este procedimento o mais rápido possível para evitar qualquer suspensão temporária da sua conta.

Lembre-se: [Banco Fictício] nunca solicitará informações confidenciais por e-mail ou através de links suspeitos. Certifique-se de verificar a autenticidade dos e-mails que receber.

Agradecemos pela sua cooperação.

Atenciosamente,
Equipe de Segurança
[Banco Fictício]

PAULO PINTO, BUSINESS DEVELOPMENT MANAGER DA FORTINET PORTUGAL

APESAR DAS DIFERENTES TÉCNICAS UTILIZADAS, "ESTAS CONTINUAM A TER UM OBJETIVO EM COMUM: ROUBAR A IDENTIDADE OU TRANSFERIR FICHEIROS MALICIOSOS".

anteriormente, associávamos facilmente como sendo um ataque de phishing, como é o caso da gramática, ortografia e formatação".

Luís Rato sublinha a possibilidade de automatizar a criação de emails de phishing, o que significa "a criação e distribuição de milhares de emails de phishing numa questão de minutos". Além do mais, "os próprios algoritmos de inteligência artificial também podem personalizar os ataques, tornando-os mais convincentes".

Christopher Budd menciona uma investigação recente da Sophos X-Ops onde foram descobertas "provas claras" de que os ciberatacantes utilizam "capacidades semelhantes às do ChatGPT" para atacar os seus alvos, trabalhando-os todos os dias durantes semanas ou meses antes de se conseguir que sejam vítimas de burlas. "Devo dizer que a ameaça da utilização de IA em ataques é facilmente exagerada, mas ao mesmo tempo esta é claramente uma área que já está a ser explorada pelos atacantes. O mais relevante neste momento é que estão a utilizar as capacidades da IA não para encontrar soluções tecnológicas para os seus ataques, mas sim para encontrar soluções centradas no ser humano. É razoável esperar que a IA seja utilizada de forma mais eficaz, e o mais rapidamente possível, no phishing", explica.

BOAS PRÁTICAS

Empregar boas práticas – e principalmente ensiná-las aos colaboradores – não elimina por completo o risco de um ataque contra uma organização ter sucesso, mas permite reduzir esse mesmo risco.

Fábio Ribeiro, da Ajoomal, refere que a formação dos colaboradores é uma necessidade, principalmente através da explicação de como reconhecer tentativas de phishing e a importância de verificar pedidos de informações sensíveis, assim como uma consciência de segurança através da promoção de uma cultura de segurança dentro da organização.

Aliada a essa formação, importa ter filtragem de email, autenticação multifator e segurança de endpoint.

Christopher Budd, da Sophos, sublinha, também, a importância de "educar os utilizadores para não abrirem anexos e não clicarem em *links*" que, diz, "continua a ser uma prática importante", em conjunto com a promoção interna de bons hábitos, "não utilizando *links* e anexos nos seus emails internos". O Director Threat Research afirma que, se este hábito for adotado, "os utilizadores podem adquirir o hábito de clicar neles, o que enfraquece a formação e a mensagem de segurança. Para além disso, dessa forma também é mais fácil para os utilizadores evitarem emails de phishing que se fazem passar por emails internos".

Paulo Pinto, da Fortinet, explica que "as equipas de segurança e os colaboradores de uma organização têm papéis importantes a desempenhar" quando "se trata de evitar ciberataques como o phishing". Apesar disso, "há muitas ações simples que as empresas podem tomar para melhorar a sua postura de segurança", como a ativação de filtros de spam, atualizar o software regularmente, implementar a autenticação multifator, ter um *backup* dos dados e bloquear sites que não sejam fiáveis".

Apesar da componente mais tecnológica, Paulo Pinto sublinha a necessidade de "implementar um programa de formação contínuo em toda a organização", que identifique "as principais áreas que apresentam os maiores riscos para o utilizador final" e, "inevitavelmente, para a empresa".

Luís Rato reforça a importância de também maximizar as definições de segurança que protegem a caixa de entrada de cada colaborador, nomeadamente através da ativação de notificações para remetentes não verificados, bloquear remetentes com identidades que não pode confirmar de forma independente e denunciar os seus e-mails como phishing ou spam nas aplicações de correio eletrónico, e tornar o correio eletrónico mais difícil de comprometer, ativando a autenticação multifator, por exemplo. No entanto, "a sensibilização é fundamental e meio caminho para se travar logo à partida qualquer tentativa maliciosa de extrair informação confidencial". ◀

FÁBIO RIBEIRO, SENIOR SALES ENGINEER DA AJOOMAL

▼

OS CIBERCRIMINOSOS TÊM UTILIZADO "VÁRIAS TÁTICAS NOVAS PARA AUMENTAR A SOFISTICAÇÃO DOS SEUS ATAQUES",

paloalto NETWORKS

O QUE É O PHISHING?

VAMOS COMEÇAR POR REVER DE UMA FORMA SIMPLES O CONCEITO DE UM ATAQUE DE *PHISHING*: É UMA FORMA DE *SOCIAL ENGINEERING* (TÁTICA UTILIZADA PARA CONSEGUIR MANIPULAR, INFLUENCIAR OU ENGANAR UMA POTENCIAL VÍTIMA) TRANSMITIDA ATRAVÉS DE UMA MENSAGEM DIRETA, GERALMENTE POR E-MAIL. DISFARÇADA DE UMA COMUNICAÇÃO LEGÍTIMA, A MENSAGEM FRAUDULENTA INDUZ O DESTINATÁRIO A RESPONDER, INCENTIVANDO-O A CLICAR NUM *LINK*, ABRIR UM ANEXO OU FORNECER DIRETAMENTE INFORMAÇÕES CONFIDENCIAIS. NOS DIAS DE HOJE, ESTE CONCEITO PARECE ESTAR PELO MENOS INCOMPLETO.

Os ataques de *Phishing* tornaram-se um dos métodos mais prevalentes e eficazes do cibercrime porque são capazes de contornar os métodos de deteção e são de baixo risco para os cibercriminosos, pois há poucas possibilidades de serem capturados ou de sofrerem uma retaliação. Uma mensagem de *Phishing* é simples de introduzir, facilitando o envio de grandes quantidades de mensagens numa única tentativa. Somando-se à facilidade de introdução está a disponibilidade de kits de *Phishing* de baixo custo que incluem software de desenvolvimento de sites, codificação, spam, software e conteúdo, que podem ser utilizados para criar sites e e-mails convincentes.

O PAPEL DAS REDES SOCIAIS NA PROLIFERAÇÃO DOS ATAQUES DE PHISHING

Com o aumento significativo de utilizadores e dispositivos que acedem a aplicações online e a massificação das redes sociais, o conceito de *Phishing* tem de considerar uma maior quantidade e diversidade de canais através dos quais é possível alcançar potenciais vítimas. Do ponto de vista da cibersegurança, estamos perante não só um aumento do número de potenciais vítimas, mas também de um aumento exponencial da superfície de ataque.

Os ataques de *Phishing* agora são perpetrados através das redes sociais também. Os cibercriminosos atraem as potenciais vítimas para websites de falsificação de identidade, incorporando URLs de *Phishing*

em *posts* ou comentários. Os cibercriminosos têm como alvo as redes sociais como o Facebook, o LinkedIn, o Twitter (X), o Instagram, entre outos, inundando os utilizadores destas redes socias com milhares de *Phishing* ou URLs maliciosos. Os cibercriminosos também utilizam SMS, Skype, Messenger ou outros serviços de mensagens como canais de ataque de *Phishing*. Estes novos vetores de ataque demonstram que os cibercriminosos se adaptaram à crescente mobilidade da sociedade e à diversidade atual de plataformas de mensagens.

EVOLUÇÃO DOS ATAQUES DE *PHISHING*

O principal objetivo de um ataque de *Phishing* continua a ser o de roubar as credenciais e/ou informações confidenciais ou induzir uma pessoa a enviar dinheiro. O que mudou, foi não só o número de ferramentas ao dispor de um cibercriminoso para encontrar as suas vítimas, a diversificação da motivação e também as técnicas utilizadas para perpetrarem estes ataques. A Inteligência Artificial e as técnicas de Machine Learning assumem um papel-chave na condução deste tipo de ataques.

Os cibercriminosos evoluíram significativamente ao longo dos anos. Eles são capazes de produzir mensagens e anexos fraudulentos que podem convencer qualquer pessoa, e até mesmo os profissionais de cibersegurança mais experientes acham difícil detetá-los.

Atualmente e de forma muito acessível e rápida, o modo como um cibercriminoso pode "aprender" os hábitos, os contactos e até o estado de espirito de uma potencial vítima, tornou muito mais fácil manipulá-la de forma a perpetrar um ataque bem-sucedido e que pode ser devastador, quer para as organizações quer para pessoas.

Desde sempre, os ciberataques trabalham arduamente para fazer com que as mensagens de *Phishing* pareçam legítimas e convincentes. Vamos imaginar agora que um cibercriminoso já sabe quais os gatilhos emocionais, como urgência ou curiosidade, para obter uma resposta imediata. E que consegue compreendê-los, aprender com eles e automatizar estes ataques. Estamos a falar de um cenário de máquinas vs. humanos, numa luta desigual.

COMO ENFRENTAR A NOVA REALIDADE DESTES ATAQUES?

As técnicas de ataque evoluíram e as técnicas de defesa têm de evoluir também. Devemos considerar não só a educação das pessoas, mas também uma forma capaz de minimizar os ataques de *Phishing* bem-sucedidos com uma plataforma de segurança abrangente focada em pessoas, processos e tecnologia.

Ações de formação e consciencialização sobre segurança podem ajudar as pessoas a procurar sinais de um ataque antes que ele aconteça. Ao prevenir ataques de *Phishing* desde o início, as empresas podem evitar uma quantidade significativa de danos aos seus colaboradores e à organização.

Investir numa solução de deteção de *Phishing* é fundamental. Colocar máquinas a combater máquinas é uma inevitabilidade. O papel da Inteligência Artificial e das técnicas de Machine Learning, no ataque e na defesa, são uma realidade. ◀

anubisnetworks™

“AS PME’S SOFREM ATAQUES DIRECIONADOS DIARIAMENTE!”

PARA ESTA EDIÇÃO, SOBRE *PHISHING*, É INDISPENSÁVEL ENTREVISTAMOS O CEO DO ÚNICO VENDOR PORTUGUÊS DE CIBERSEGURANÇA DE EMAIL.

Já conhecemos a Anubis há uns anos, e continuam muito fortes no nosso mercado de segurança de email, apesar de maiores concorrentes estrangeiros. Qual é o segredo?

A Anubisnetworks está focada na segurança de email desde 2009! Acho que é a nossa objetividade relativamente aos nossos serviços que nos mantém saudáveis - conhecemos perfeitamente o nosso mercado e os nossos clientes, com quem estamos muito “ligados” no nosso suporte e na altura de criar novas funcionalidades. Tudo na nossa empresa gira à volta da segurança de email. Não temos centenas de recursos humanos, mas também não temos dezenas de produtos, pelo que somos mais ágeis e focados. E depois há a nossa capacitação técnica para lidar com as ameaças.

Capacitação técnica dos produtos?

E também humana - Os ataques às empresas portuguesas são parcialmente distintos dos ataques a qualquer outra geografia - por questões linguísticas, culturais e pela atualidade nacional e empresarial.

O *phishing* é tanto global como local?

Bom, o *phishing* é um ataque que visa enganar as vítimas para obter informações pessoais e financeiras. Tem uma componente de tecnologia - seja por *malware* e sites

maliciosos a que conduz, seja pela própria construção do email, que tem de passar várias barreiras tecnológicas e parecer legítimo, mas tem, acima de tudo, uma parte de engenharia social - a linguagem tem de estar correta, o abuso de uma organização tem de ser credível. E é neste aspeto que o conhecimento local ganha evidência: por exemplo, saber que os CTT publicitam serviços bancários ou que a EDP mudou recentemente a sua identidade corporativa, e por aí em diante. Isto tudo requer ajustes em Threat Intelligence e pessoas especializadas.

E como estão os ataques de *phishing* em Portugal?

Observámos uma subida acentuada coincidente com a pandemia e o teletrabalho. Períodos de 3 ou 4 vezes mais emails enviados e recebidos, e claro, muito mais ataques. Já reduziu, mas continua muito forte. Vemos muitas marcas nacionais a serem abusadas, e muito Business Email Compromise destinados aos executivos das empresas. Nos últimos 12 meses, quase 50% dos emails que vimos são fraudulentos, de *spam*, ou contendo *links*, código, ou software maliciosos. *Phishing* e *fraud* situam-se nos 26%.

Em número e tipos de ataques, somos similares a outras geografias europeias, mas uma parte dos ataques é muito dirigida ao idioma português e às empresas nacionais mais conhecidas. As PME's sofrem ataques direcionados diariamente, ou seja, fraudes com conteúdo específico a essas organizações e pessoas.

Porquê mais ataques às PME's? Porque são muitas?

É possível, mas diríamos que a componente técnica dos ataques explora sempre as tecnologias mais comuns e mais vulneráveis. Devem existir uns milhares de atacantes a explorar diariamente as tecnologias utilizadas por 90% das empresas, como o Exchange, o Gmail, o Microsoft Word, e por aí. As empresas maiores utilizam essas tecnologias mas sobrepõem outros recursos tecnológicos, para além da capacitação de pessoal mais abrangente.

Temos um problema de qualificação de pessoal nas empresas para lidar com estas ameaças?

As empresas devem ter os especialistas possíveis, mas sabemos que haverão limitações, pelo que devem também alavancar-se nos seus parceiros tecnológicos, sejam operadores ou sejam MSPs, da mesma maneira que o fazem noutras exigências do negócio. E apostar nos processos e na formação adequada a todos os funcionários, que são a última barreira de defesa e muitas vezes é o seu desleixo ou desconhecimento que despoleta um ataque bem sucedido.

Do ponto de vista tecnológico, já mencionou a necessidade de ter sistemas complementares. O que mais limita os ataques de *phishing* de email?

A parte técnica dos ataques, seja evadir um SPF, ou infiltrar um link malicioso num anexo, é prevenida com tecnologias dedicadas. Claro, um gateway de segurança de email - de preferência fora do perímetro -, mas também várias outras ferramentas que ajudem a determinar o comportamento do utilizador - Muitos ataques surgem por contas comprometidas, e por utilizadores que acedem a sistemas ou websites que deveriam ter levantado suspeitas anteriores.

A Inteligência Artificial tem piorado o problema do *phishing*?

As ferramentas de AI em conjunto com as bases de dados de utilizadores que foram comprometidas, dão uma vantagem aos *phishers* - que conseguem criar mensagens individualizadas de *phishing*, e com informação muito pertinente e dirigida às vítimas. Portanto, sim. Mais *phishing* e bem mais perigoso é algo que devemos começar a sentir.

cipher
a Prosegur company

por Roberto Gilperez,
Red Team Manager na Cipher,
a Prosegur company

O NOVO PARADIGMA DO PHISHING

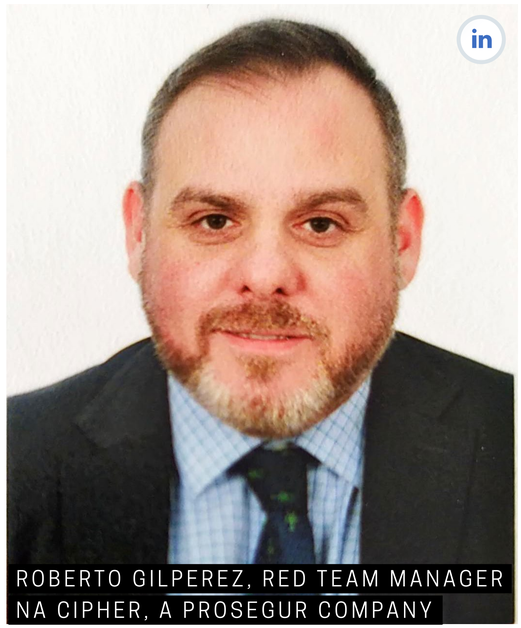
NOS ÚLTIMOS ANOS, TEMOS ESTADO DEDICADOS A COMBATER O CRESCENTE PROBLEMA DO PHISHING, QUE SE TORNOU UM DOS MÉTODOS PREFERIDOS DOS CIBERCRIMINOSOS PARA INFILTRAR ORGANIZAÇÕES. NESTE ARTIGO, IREMOS EXPLORAR ALGUMAS DAS NOVAS TÉCNICAS UTILIZADAS NO PHISHING, INCLUINDO EXEMPLOS RECENTES QUE DEMONSTRAM A SOFISTICAÇÃO DESSES ATAQUES.

PHISHING E *SMISHING*: UMA COMBINAÇÃO PERIGOSA

Uma das tendências mais preocupantes no mundo do *phishing* é a combinação de campanhas de *phishing* com smishing. O *smishing*, ou *phishing* através de mensagens de texto, tornou-se cada vez mais comum. Os cibercriminosos enviam mensagens de texto falsas que parecem vir de bancos, empresas de entrega ou serviços de mensagens, solicitando informações confidenciais ou tentando convencer as vítimas a clicar em links maliciosos. Esta técnica capitaliza na familiaridade das pessoas com mensagens de texto e na sua tendência a confiar nelas.

O USO DE INTELIGÊNCIA ARTIFICIAL (IA) NO *PHISHING*

Na Cipher, observamos que os cibercriminosos adotaram a inteligência artificial para as suas campanhas de *phishing*. Eles usam IA para criar imitações quase perfeitas de comunicações legítimas, tornando cada vez mais difícil para as pessoas diferenciar o que é real do que não é. Por exemplo, os *e-mails* e mensagens de *phishing* gerados por IA podem imitar o estilo de escrita e as assinaturas de e-mail de empresas legítimas, aumentando a eficácia desses ataques.


ROBERTO GILPEREZ, RED TEAM MANAGER NA CIPHER, A PROSEGUR COMPANY

EXEMPLOS ILUSTRATIVOS DE NOVAS TÉCNICAS DE *PHISHING*

1. **Filmes populares como isco**:

Um exemplo revelador desta evolução é o uso de filmes populares como isco para ataques de *phishing*. Os cibercriminosos criam *websites* maliciosos que oferecem *streaming* gratuito de filmes antes do seu lançamento oficial. Para aceder a esta "oferta especial", os utilizadores são solicitados a pagar uma taxa simbólica, geralmente um euro, para se registarem no serviço de *streaming* falso. Este tipo de ataque capitaliza na excitação e interesse gerado por um filme popular para roubar dinheiro e dados pessoais das vítimas.

2. **Ofertas enganosas com vários temas**:

Outro exemplo que observamos demonstra a diversidade de temas usados em ataques de *phishing*. Neste caso, os cibercriminosos criaram websites maliciosos que oferecem promoções especiais em artigos relacionados com o lançamento de um filme popular nos cinemas. Aproveitando o interesse dos utilizadores da internet neste brinquedo icónico, os atacantes promoveram ofertas irresistíveis. No entanto, por trás dessas ofertas estava a intenção de roubar dinheiro e dados pessoais de utilizadores desprevenidos.

COMO PROTEGER-SE CONTRA NOVAS TÉCNICAS DE *PHISHING*

Compreendemos a importância de proteger-se contra novas técnicas de *phishing*. Por isso, recomendamos:

- Manter-se informado sobre as últimas tendências e técnicas de *phishing*.
- Ser cético em relação a ofertas que parecem ser boas demais para ser verdade.
- Verificar a autenticidade de mensagens e *links* antes de tomar qualquer ação.
- Utilizar soluções avançadas de segurança, como filtragem de e-mails e sistemas de deteção de ameaças.
- Educar os funcionários sobre como reconhecer e denunciar possíveis ataques de *phishing*.

Em conclusão, na Cipher, estamos empenhados em combater o novo rosto do *phishing* e preservar a segurança das organizações na era digital. É essencial manter-se vigilante e tomar medidas proativas para evitar cair nas armadilhas criadas pelos cibercriminosos. ◀

por Álvaro Godinho,
Security Consultant, CSO

THE NEW FACE OF PHISHING

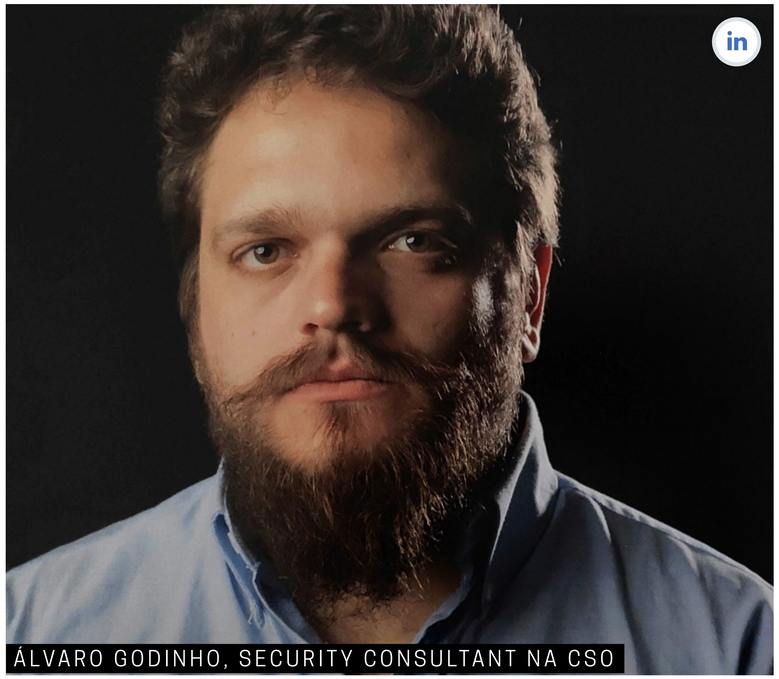
NO PANORAMA ATUAL DE CONSTANTE EVOLUÇÃO DO CIBERCRIME E APESAR DE JÁ FAZER PARTE DO NOSSO MUNDO HÁ BASTANTE TEMPO, O PHISHING TRANSCENDEU AS SUAS ORIGENS COMO SIMPLES EMAILS DE SPAM E EMERGE COMO UMA AMEAÇA ALTAMENTE SOFISTICADA.

O *phishing* pode ser uma das formas mais antigas de cibercrime, mas está longe de ser obsoleto. Esta nova face do *phishing* é adaptativa, tecnologicamente experiente e enraizada na psicologia do comportamento humano, seguem algumas das táticas usadas pelos *phishers*.

Spear *phishing*: Em vez de lançarem uma rede alargada, os *phishers* direcionam os ataques para utilizadores ou grupos privilegiados, recolhendo informações detalhadas sobre os alvos para criar emails convincentes que são difíceis de distinguir da comunicação legítima.

Business Email Compromise: Os *phishers* fazem-se passar por indivíduos da organização (ou parceiros desta), pedindo aos funcionários que efetuem transferências monetárias ou que transmitam informações sensíveis. Estes ataques podem ser devastadores para uma organização e para a sua reputação, e envolvem táticas sofisticadas de engenharia social, investigação extensiva aos alvos e até ataques à infraestrutura de email corporativo.

Smishing: Combina o SMS e *phishing*. Este método aproveita o instantâneo e confiança associados às SMS, para induzir os utilizadores a efetuar pagamentos ou obter informações pessoais e financeiras.


ÁLVARO GODINHO, SECURITY CONSULTANT NA CSO

Brand Impersonation: Os *phishers* estão cada vez mais a visar marcas e serviços populares, criando réplicas convincentes dos seus *websites* e aplicações. As vítimas introduzem inadvertidamente as suas credenciais nestes sites falsos, fornecendo informações valiosas.

Social Engineering: Estes ataques utilizam a manipulação psicológica para explorar a confiança e a curiosidade humanas. Os atacantes criam mensagens que induzem medo, urgência ou excitação para levar a ações rápidas, como clicar numa ligação ou revelar dados sensíveis. Esta tática também aparece associada ao *phishing* por voz (*vishing*).

Zero-Day Exploits: Algumas campanhas de *phishing* aproveitam agora vulnerabilidades de Zero-Day em software e hardware, tornando-as ainda mais difíceis de detetar.

A evolução do fenómeno *phishing* tem um enorme impacto nos indivíduos e nas organizações. Os ataques resultam em várias consequências e impactos, incluindo perdas financeiras, roubo de identidade, violações de dados, infeções por *malware*, contas comprometidas e perda de confiança. Além disso, há consequências legais, como multas por violações de regulamentos de proteção de dados. Lidar com as consequências do *phishing* consome tempo e recursos significativos. Além disso, um ataque de *phishing* bem-sucedido pode levar a ataques mais avançados e graves. Portanto, é essencial que tanto indivíduos quanto organizações tomem medidas para se protegerem contra o *phishing* e minimizarem seus impactos.

À medida que os ataques de *phishing* se tornam mais sofisticados, é crucial que os indivíduos e as organizações se tornem proactivos para se defenderem, adicionado algumas camadas de proteção implementando MFA, utilizando soluções de *email filtering* em conjunção com técnicas de *sandbox* de forma a detonar ficheiros e ligações maliciosas, que possam detetar e colocar em quarentena email de *phishing* antes deste chegar aos destinatários, utilizando também soluções robustas nos *endpoints* para que possam identificar e bloquear software malicioso, mantendo o software e hardware atualizado para minimizar as vulnerabilidades que possam ser exploradas e criando planos de resposta para minimizar incidentes no caso de ataques bem sucedidos.

Reconhecendo a ameaça contínua que o *phishing* representa, muitas organizações investem na educação e formação dos funcionários para aumentar a consciencialização e reduzir o risco de serem vítimas de tais ataques. Atualmente existem soluções para lançar simulações de *phishing* e promover formação interna nessa temática, com a possibilidade de obter resultados segmentados e assim focar a sensibilização às equipas mais vulneráveis e mais críticas. Apesar das empresas sensibilizarem os seus colaboradores para o perigo do *phishing*, mesmo os indivíduos bem informados podem ser vítimas destes ataques, o que realça a necessidade de uma educação e vigilância contínuas em matéria de cibersegurança.

Numa era digital em que as informações pessoais e sensíveis estão constantemente em risco, os indivíduos e as organizações devem manter-se proativos na defesa contra ataques de *phishing*. A utilização de uma combinação de medidas robustas de cibersegurança, formação atualizada e uma dose saudável de ceticismo quando se depara com mensagens ou *e-mails* não solicitados pode contribuir muito para atenuar os riscos colocados por esta ameaça em evolução. O *phishing* pode ter vindo para ficar, mas com a sensibilização e as precauções corretas, o seu impacto pode ser significativamente reduzido. ◀

noesis
an Altia Company

por Miguel Azevedo,
Senior IT Specialist na Noesis

O PHISHING NOS DIAS DE HOJE!

COM A ENTRADA DA INTELEGÊNCIA ARTIFICIAL EM JOGO, OS ATAQUES DE *PHISHING* EVOLUIRAM DE FORMA CONSIDERÁVEL EM TRÊS VERTENTES, NA "CONSTRUÇÃO DO PERFIL" DE QUEM VAI SER ALVO DE ATAQUE, NOS CONTEÚDOS, *LINKS* E ANEXOS ENVIADOS E NA PERSISTÊNCIA ATÉ O UTILIZADOR "CEDER".

"Construção do perfil do alvo" – Nos dias de hoje, há a tendência dos utilizadores exporem nas redes sociais (facebook, whatsapp, linkedin, etc) informação das funções e responsabilidades que tem na organização, tarefas que fazem, aplicações ou serviços que utilizam, por vezes informação sensível, e expondo, por vezes, a forma como a organização funciona e o papel que o utilizador tem na organização.

Conteúdos, *links* e anexos – Com o recurso a IA os conteúdos enviados são cada vez mais orientados para a função/responsabilidade que o utilizador tem na organização. Deixaram de ter erros ortográficos/formatação e o próprio conteúdo do e-mail leva os utilizadores a considerar que é fidedigno. O mesmo acontece com os *links* e anexos que são semelhantes aos habitualmente recebidos fidedignamente. Por exemplo no caso dos anexos o ficheiro word e pdf é exatamente igual, mas ao abrir o ficheiro sem o utilizador perceber pode ser executado código malicioso (ex. *remote code execution*/macros).

Persistência – Com o recurso aos chatbots (por vezes os conteúdos podem não ser os mais sofisticados), há uma tentativa contínua para o mesmo alvo até o utilizador ter a "tentação" de clicar em algum link malicioso ou disponibilizar informação sensível.

Quais as estratégias a seguir para responder a este tipo de ataques?

Focando-nos nas iniciativas que podem reduzir de forma significativa o risco, para ataques através de


MIGUEL AZEVEDO, NOESIS

phishing, recomenda-se a **criação da ciber cultura na organização**, sessões de sensibilização e formação, campanhas de *phishing* e avaliação das mesma e tecnologia que permita responder à evolução que este tipo de ataques tem tido.

Criação de ciber cultura na organização – Para que a estratégia de ciber segurança seja eficaz é essencial que a mensagem que se passa aos utilizadores/colaboradores seja simples e clara (ex. através de *newsletters*, *papers*, redes sociais ou outros canais de comunicações que existam na organização) e que os utilizadores percebam o risco e impacto que determinados tipos comportamentos podem representar para a organização.

Sensibilização e formação dos colaboradores – Sendo este tipo de ataque focado no utilizador é essencial que as organizações tenham sessões de sensibilização e formação com alguma regularidade, e que as mesmas se adaptem à evolução e sofisticação que este tipo de ataques tem sofrido.

A nível individual ou para organizações que não tenham programadas sessões de formação e sensibilização nos temas de cibersegurança recomendo o curso **Cidadão Ciberseguro** disponibilizado pelo Centro Nacional de Cibersegurança na plataforma Nau (*https://www.nau.edu.pt/pt/curso/cidadao-ciberseguro/*).

Campanhas de phishing – Com a evolução e sofisticação (ex. IA e chatbots) que há atualmente nos ataques de *phishing* (é recomendável também ter em consideração os ataques *smishing* e *vishing* e ter iniciativas semelhantes) é essencial que sejam feitas campanhas de *phishing* com bastante regularidade e que o modelo utilizado nas campanhas acompanhe a evolução que este tipo de ataques tem tido. Neste momento o conteúdo dos e-mails de *phishing* já são orientados para a função que o utilizador tem na organização e os *links* e anexos recebidos são semelhantes aos fidedignos.

Das campanhas de *phishing* que a Noesis suporta em cliente, a percentagem de utilizadores que ainda é "ludibriado", anda na faixa dos 10% a 30%, incluindo utilizadores com nível de literacia tecnológico elevado.

Tecnologia - A par da sensibilização e formação dos colaboradores é essencial que a estratégia de cibersegurança que a organização tem implementada ou prevê implementar responda de forma eficaz a este tipo de ataque. Desta forma é importante que a própria solução de e-mail já tenha a capacidade de identificar e bloquear e-mails de *phishing* com base em comportamentos (se é ou não habitual a troca de e-mails com este *sender*), na origem (*sender*), no conteúdo (*links*) e em anexos. Da experiência do dia a dia da Noesis, como complemento, a "filtragem" feita pela solução de e-mail, recomenda-se o uso de soluções assentes em Intelegência Artificial/Machine Learning que tem a capacidade de identificar automaticamente novos padrões de ataque e tem por base a informação já recolhida e avaliar alterações de padrões/comportamentos. A filtragem (identificação e bloqueio) adicional que este tipo de soluções efetua é considerável, reduzindo desta forma os emails com conteúdo malicioso que possam chegar aos utilizadores.

A estratégia de cibersegurança também já deve considerar medidas de mitigação para responder de forma eficaz e automática, se possível caso as credênciais ou o dispositivo do utilizador fiquem comprometidos (ex. forçar o bloqueio da conta ou isolar o dispositivo), tendo as soluções de **Endpoint Detection & Response** (**EDR**) ou **Extended Detection and Response** (**XDR**) um papel importante. ◀

SOPHOS
Cybersecurity delivered.

OS CIBERCRIMINOSOS TRABALHAM QUANDO AS EMPRESAS SE DESLIGAM. SAIBA COMO OS IMPEDIR

UMA VEZ QUE 90% DOS ATAQUES DE *RANSOMWARE* OCORRE FORA DO HORÁRIO NORMAL DE EXPEDIENTE, O SERVIÇO DE DETEÇÃO E RESPOSTA GERIDAS (MDR) 24/7 DA SOPHOS É AGORA UMA PARTE ESSENCIAL DE UM *STOCK* DE SEGURANÇA EFICAZ.

O novo relatório *Active Adversary 2023* para líderes de tecnologia da Sophos X-Ops destaca como a evolução dos comportamentos dos adversários está a acelerar a necessidade de detetar e responder a ameaças 24/7.

Com base na análise de casos de resposta a incidentes resolvidos pela Sophos no primeiro semestre de 2023, o relatório ilustra como os cibercriminosos de *ransomware* estão a dificultar a resposta atempada dos defensores aos seus ataques.

A JANELA PARA RESPOSTA A AMEAÇAS É CADA VEZ MAIS PEQUENA

Uma das principais conclusões do relatório é que o tempo disponível para responder a um ataque de *ransomware* foi reduzido para quase metade *vs* o início do ano. O tempo médio de permanência em ataques de *ransomware* caiu de nove dias em 2022 para apenas cinco dias neste primeiro semestre. Os adversários estão a acelerar a execução dos seus ataques, e os

defensores têm menos tempo para os detetar e interromper antes que os ficheiros sejam encriptados.

A análise da Sophos X-Ops a todos os tipos de ataques revelou que os atacantes demoraram, em média, menos de 1 dia - aproximadamente 16h – a chegar ao Active Directory (AD), um dos ativos mais críticos das empresas. O AD é frequentemente o sistema mais poderoso e privilegiado da rede, proporcionando um amplo acesso a sistemas, aplicações, recursos e dados que os atacantes podem explorar.

OS ATACANTES TRABALHAM QUANDO NÃO O FAZEMOS

O relatório também revelou que os cibercriminosos de *ransomware* lançam os seus ataques em alturas em que é menos provável que os defensores se apercebam deles. De facto, 90% deles ocorre agora fora do horário normal de expediente (dias úteis das 8h-18h). Os ataques também aumentam no final da semana, com quase metade (43%) à sexta ou ao sábado. Se não monitorizar o seu ambiente a todo o momento, incluindo à noite e aos fins-de-semana, está a correr um sério risco.

OBTENHA COBERTURA 24/7 ULTRA RÁPIDA COM O SOPHOS MDR

Proporcionar cobertura por especialistas 24/7 é, assim, um desafio para a maioria das organizações. No entanto, é importante perceber esta lacuna operacional, que os adversários exploram ativamente.

O ***serviço Sophos MDR*** fornece monitorização e resposta a ameaças 24/7, através de uma equipa de mais de 500 especialistas espalhados por sete Centros de Operações de Segurança (SOCs). Sempre que os adversários tentam lançar o seu ataque, a nossa equipa está lá para o detetar e parar – e somos rápidos. Com um tempo médio de resolução de apenas 38min, pode ficar descansado sabendo que a sua organização está sempre protegida, mesmo que a janela de resposta diminua.

O **Sophos MDR** funciona como uma extensão da sua equipa, complementando-a da forma que melhor lhe convier – desde um serviço SOC completo e chave na mão até à cobertura de noites e fins de semana.

Também trabalhamos com as suas ferramentas de segurança existentes para o ajudar a tirar mais valor dos seus investimentos atuais, sem o desperdício de custos de uma abordagem de substituição. Quer utilize ferramentas Sophos, Microsoft ou de qualquer outro fornecedor para proteger o seu ambiente, podemos aumentar as suas defesas mesmo contra os ataques mais avançados.

Com o Sophos MDR tem está protegido pelo serviço de MDR mais fiável do mundo. Protegemos mais organizações do que qualquer outro fornecedor e somos os mais bem classificados pelos clientes e analistas.

Se quiser saber mais sobre as mais recentes abordagens dos atacantes, não procure mais: consulte o **Sophos X-Ops Active Adversary Report 2023 for Business Leaders**. Concebido para ajudar os gestores de tecnologia a tomar melhores decisões sobre como utilizar os seus recursos limitados, está repleto de informações sobre ameaças e material para garantir que pode apoiar a estratégia corporativa, ao mesmo tempo que promove uma melhor proteção em toda a sua organização. ◀

OS TESTES DE PENETRAÇÃO – OU PEN TESTING – SÃO IMPORTANTES PARA QUE AS ORGANIZAÇÕES DESCUBRAM AS SUAS VULNERABILIDADES ANTES QUE ALGUÉM COM INTENÇÕES CRIMINOSAS O FAÇA PELAS EQUIPAS DE SEGURANÇA

Imagem rawpixel / Freepik

POR RUI DAMIÃO

ATACAR ANTES DE SER ATACADO

Com o advento da transformação digital, a exposição aumentou. A larga maioria das organizações – se não mesmo todas – têm algum tipo de serviço virado para a Internet, o que faz com que esteja sujeito a um ciberataque.

Os testes de penetração – ou pen testing – permitem identificar as vulnerabilidades mais críticas e avaliar a segurança dos sistemas e aplicações. No entanto, com a escassez de recursos humanos, realizar estes testes não é necessariamente fácil. Para isso, várias empresas fornecem estes testes como um serviço às organizações.

METODOLOGIAS

Luís Martins, Diretor Geral da Cipher em Portugal, explica que nos testes de penetração são "utilizadas várias metodologias e técnicas nos testes de intrusão que dependem essencialmente dos objetivos que as organizações que contratam estes serviços pretendem atingir, mas servem essencialmente para avaliar a segurança de sistemas, redes e aplicações", como "testes Black Box, White Box, Gray Box, Vulnerabilidade, Fuzzing, Autenticação e Autorização, Injeção de SQL, XSS e CSRF, Análise de Tráfego de Rede, Engenharia Social, Análise de Código, DoS", entre outros.

Bruno Castro, Fundador e CEO da VisionWare, explica que no caso da VisionWare são aplicados modelos de avaliação de segurança assentes nestes testes "que visem o contexto aplicacional ou tecnológico a avaliar". Este tipo de ações, refere, são baseados "nas principais normas e *checklists* do setor", mas que não aplicam "cegamente uma tecnologia só porque se trata de uma referência", sendo ajustado ao contexto.

LUÍS MARTINS, CIPHER EM PORTUGAL

Luís Catarino, Offensive Security Manager da S21sec, afirma que "este tipo de exercício é tradicionalmente conduzido como um projeto com datas rigorosas de início e de fim da execução, seguido de uma entrega de relatório e apresentação dos resultados, contando ainda opcionalmente com uma segunda bateria de testes após correção ou mitigação das vulnerabilidades por parte da organização, no sentido de verificar se estas foram abordadas de acordo com as melhores práticas". Recentemente,

> SÃO "UTILIZADAS VÁRIAS METODOLOGIAS E TÉCNICAS NOS TESTES DE INTRUSÃO QUE DEPENDEM ESSENCIALMENTE DOS OBJETIVOS QUE AS ORGANIZAÇÕES QUE CONTRATAM ESTES SERVIÇOS PRETENDEM ATINGIR, MAS SERVEM ESSENCIALMENTE PARA AVALIAR A SEGURANÇA DE SISTEMAS, REDES E APLICAÇÕES"
>
> LUÍS MARTINS, DIRETOR GERAL DA CIPHER EM PORTUGAL


BRUNO CASTRO, VISIONWARE

"têm vindo a ser desenvolvidas abordagens de testes de intrusão continuados, testes estes que permitem um acompanhamento constante com atualizações periódicas para lidar com novas vulnerabilidades emergentes e garantir uma segurança robusta a longo prazo".

David Grave, Security Director da Claranet Portugal, indica que são utilizadas várias metodologias e técnicas para identificar vulnerabilidades e avaliar a segurança de sistemas e redes. As principais metodologias incluem OWASP Top Tem – focada em identificar as dez vulnerabilidades mais críticas em aplicações web –, *Penetration Testing Execution Standard* – que oferece um guia abrangente para a execução de testes de penetração em várias fases – e NIST SP 800-115 – que fornece diretrizes detalhadas para testes de penetração em sistemas de informação. As técnicas, que dependem do âmbito e do ambiente alvo, "incluem *scan* de portas, análise de vulnerabilidades, exploração, engenharia social e testes de intrusão, entre outras".

AMBIENTES COMPLEXOS

Nenhuma empresa é igual e cada uma tem o seu próprio ambiente. Estes ambientes podem ser mais ou menos complexos, mais ou menos personalizados e é importante que o fornecedor dos serviços de pen testing faça um trabalho ético e com sucesso.

Bruno Castro refere que "é fundamental ter conhecimento especializado nas vertentes de programação, *networking* e infraestrutura de segurança ativa. Atualmente, e face à evolução para serviços cloud, é também importante saber auditar em pla-

> "É FUNDAMENTAL TER CONHECIMENTO ESPECIALIZADO NAS VERTENTES DE PROGRAMAÇÃO, NETWORKING E INFRAESTRUTURA DE SEGURANÇA ATIVA. ATUALMENTE, E FACE À EVOLUÇÃO PARA SERVIÇOS CLOUD, É TAMBÉM IMPORTANTE SABER AUDITAR EM PLATAFORMAS AS-A-SERVICE EM AMBIENTE CLOUD".
>
> BRUNO CASTRO, FUNDADOR E CEO DA VISIONWARE

taformas as-a-Service em ambiente cloud". Ao mesmo tempo, "e face à evolução e inovação do mundo digital, é também crítico que estejam constantemente atualizados com os mais recentes desenvolvimentos em tecnologia e estar cientes das novas técnicas e métodos de intrusão. Criatividade, curiosidade, persistência e fortes habilidades de se ajustar a novos ambientes digitais são também ativos valiosos para qualquer pessoa que trabalhe na área de segurança informática".


LUÍS CATARINO, S21SEC

ESTE TIPO DE EXERCÍCIO É TRADICIONALMENTE CONDUZIDO COMO UM PROJETO COM DATAS RIGOROSAS DE INÍCIO E DE FIM DA EXECUÇÃO, SEGUIDO DE UMA ENTREGA DE RELATÓRIO E APRESENTAÇÃO DOS RESULTADOS, CONTANDO AINDA OPCIONALMENTE COM UMA SEGUNDA BATERIA DE TESTES APÓS CORREÇÃO OU MITIGAÇÃO DAS VULNERABILIDADES POR PARTE DA ORGANIZAÇÃO, NO SENTIDO DE VERIFICAR SE ESTAS FORAM ABORDADAS DE ACORDO COM AS MELHORES PRÁTICAS

LUÍS CATARINO, OFFENSIVE SECURITY MANAGER DA S21SEC

Luís Catarino explica que ao lidar com ambientes complexos ou personalizados é necessária uma "abordagem mais cuidadosa e estratégica", percebendo "o ambiente em questão". Este enquadramento permite "criar um plano de testes adaptado, capaz de abordar eficazmente as particularidades do ambiente. É também importante colaborar com as equipas que desenvolvem e mantêm o mesmo, pois estas poderão fornecer-nos informações relevantes para a identificação de componentes que poderão ser mais propensos a vulnerabilidades".

Sublinhando que cada ambiente é único, David Grave indica que é necessária uma "abordagem adaptada e contínua" e é "crucial fazer uma análise de risco inicial, detalhada, do ambiente antes do teste, para identificar particularidades e garantir que as técnicas e cenários de teste são adequados".

Luís Martins relembra que "a cibersegurança é um campo em constante evolução" e que os testes de intrusão "devem ser realizados de forma ética e cuidadosa para garantir a proteção dos sistemas e dados da organização". Para o sucesso de um teste de intrusão é necessário "ter-se um bom entendi-

mento do ambiente, executar a recolha de informações, fazer a personalização de abordagens, perceber se é possível fazer testes de integração e testes de aplicações sempre em estrita colaboração com a equipa de segurança interna. Só depois executar os testes de intrusão controlados para evitar qualquer impacto negativo na operação normal".

APOIAR A IMPLEMENTAÇÃO DAS RECOMENDAÇÕES

Feito o teste de penetração e percebendo quais são as vulnerabilidades mais críticas para a organização, é necessário implementar as remediações necessárias para que o seu ambiente fique mais seguro.

Luís Catarino, da S21sec, afirma que "é essencial fornecer ao cliente um relatório detalhado, mas também compreensível, das vulnerabilidades identificadas e recomendações correspondentes. A partir daí, a assistência na elaboração de um plano de ação focado e pragmático para abordar as vulnerabilidades torna-se um próximo passo lógico, onde

> "UM AUMENTO NA CONSCIENCIALIZAÇÃO SOBRE CIBERSEGURANÇA NAS ORGANIZAÇÕES PORTUGUESAS", O QUE "TEM LEVADO MUITAS DELAS A INVESTIR EM TESTES DE PENETRAÇÃO COMO PARTE DAS SUAS ESTRATÉGIAS DE REFORÇO DA POSTURA DE SEGURANÇA".
>
> DAVID GRAVE, SECURITY DIRECTOR DA CLARANET PORTUGAL


DAVID GRAVE, CLARANET PORTUGAL

se priorizam as ações com base no nível de risco de cada uma".

David Grave sublinha o "apoio contínuo" após o teste, a identificação das vulnerabilidades e da classificação do risco associado. "Esta abordagem contínua permite acompanhar a implementação das recomendações ao longo do tempo, garantindo que as vulnerabilidades são corrigidas de forma consistente e que a postura de segurança é fortalecida", diz.

Para Luís Martins, da Cipher, a "chave" para uma "abordagem bem-sucedida na implementação das recomendações é a colaboração próxima com o cliente, a priorização adequada das correções e a atenção contínua à cibersegurança", até porque, relembra, "a segurança é um processo contínuo e dinâmico e a organização deve estar preparada para se adaptar às ameaças em constante evolução".

Bruno Castro refere que, a seguir a um teste de penetração, "e assente numa visão estritamente pragmática, criamos uma matriz operacional, onde cruzamos as vulnerabilidades detetadas, a sua criticidade para a organização, o seu potencial de impacto, e por fim, o esforço financeiro ou humano para as resolver. Daí, e com o envolvimento direto da gestão de topo, decidimos a estratégia de segurança no que respeita aos próximos seis meses". O Fundador e CEO da VisionWare ressalva, ainda, que é preciso "conhecer as nossas fragilidades, e baseado na nossa capacidade, desenvolver as melhores estratégias para minimizar a probabilidade de sucesso de um potencial ataque".

AUMENTAR A POSTURA DE CIBERSEGURANÇA DAS ORGANIZAÇÕES PORTUGUESAS

David Grave, da Claranet, observa "um aumento na consciencialização sobre cibersegurança nas organizações portuguesas", o que "tem levado muitas delas a investir em testes de penetração como parte das suas estratégias de reforço da postura de segurança".

Luís Martins indica que, em Portugal, "assim como em muitos outros países", as organizações "estão cada vez mais conscientes da importância da cibersegurança e estão a investir em medidas para melhorar a sua postura. Os testes de intrusão são uma das ferramentas essenciais que as organizações utilizam para avaliar e fortalecer a sua cibersegurança".

Admitindo que "a cibersegurança e as políticas de segurança da informação continuam a ser subestimadas em Portugal", Bruno Castro indica que "nunca tivemos tantas solicitações de ajuda para responder e investigar as situações, muitas vezes de desastre, oriundos de ciberataques bem-sucedidos como agora". Tem ainda registado "um número avultado de solicitações de empresas, as quais começam a preocupar-se com a questão da segurança da informação e da cibersegurança, incluindo o interesse na implementação e gestão de um SOC ou no cuidado em incluir a realização de auditorias de cibersegurança".

Luís Catarino verifica que as organizações portuguesas – sejam elas privadas ou públicas – "têm vindo a mostrar-se mais proativas nas suas medidas de proteção". O Offensive Security Manager da S21sec explica que "esta tendência se deve a múltiplos fatores, tais como a crescente conscientização sobre a importância da cibersegurança, o crescente número de incidentes de segurança reportados, e também a legislação e regulamentos europeus" que tem "vindo a incentivar as organizações a tomarem este tipo de medidas. Entre outras medidas, este aumento de proatividade verifica-se também na crescente realização de testes de penetração. Conduzidos de forma isolada, ou como parte de um diagnóstico mais alargado ao estado da organização, estes testes têm vindo a mostrar-se uma iniciativa valiosa para iden-

tificar e resolver vulnerabilidades, de forma a prevenir potenciais incidentes de segurança".

MANTER A POSTURA DE SEGURANÇA

Luís Martins recomenda as organizações a "manter uma postura de segurança sólida, o que requer um esforço contínuo e a participação de toda a organização. É importante lembrar que a cibersegurança é dinâmica, e as ameaças estão em constante evolução. Portanto, a vigilância e a adaptação contínuas são essenciais para proteger a organização contra as ameaças".

Bruno Castro, da VisionWare, explica que, "logo após um processo de auditoria de cibersegurança, obrigatoriamente, todo o *mindset* da organização, nomeadamente da sua gestão de topo, se modifica para sempre. Passam a ter conhecimento de causa de quais são as suas fragilidades, e na realidade, passam a ser solidários entre todos na gestão de risco daí em diante. O tempo da 'bem-dita ignorância' fica para trás, e daqui em diante, terão que trabalhar no sentido de minimizar o risco de cibersegurança face ao que passam a ter noção, e na eventualidade de virem mais tarde a serem vítimas de um ciberataque, também terão de estar todos conscientes e responsabilizados das decisões que tomaram baseados nos resultados da última auditoria de cibersegurança".

Luís Catarino refere que, após um teste de penetração, é "importante agir no sentido de remediar as vulnerabilidades identificadas durante o teste, priorizando as de maior risco". Existindo uma monitorização ativa dos sistemas e aplicações, os testes de intrusão "podem permitir identificar potenciais lacunas neste processo, ou dar visibilidade sobre sistemas que, devido aos riscos existentes, poderão requerer uma maior atenção. Simulações de ataque periódicas podem também ser úteis para manter a equipa alerta e preparada para dar resposta a incidentes de segurança de forma coordenada e eficaz".

David Grave reforça a importância de adotar uma abordagem contínua à cibersegurança, que descreve como "crucial", uma vez que "permite identificar e corrigir vulnerabilidades de forma proativa, garantindo uma postura de segurança robusta ao longo do tempo". ◀

claranet®

por Ricardo Silva,
Business Developer na Claranet

PEN TESTING-AS-A-SERVICE:
UM NOVO PARADIGMA DE CIBERSEGURANÇA EMPRESARIAL

DE UMA FREQUÊNCIA MUITO ESPAÇADA NO TEMPO A UMA LÓGICA CONTÍNUA DE PROTEÇÃO, OS TESTES DE PENETRAÇÃO TORNARAM-SE ESSENCIAIS PARA COMBATER A NATUREZA CADA VEZ MAIS FLUIDA DOS ATAQUES.

Num ambiente empresarial em constante mutação, as ameaças cibernéticas tornaram-se mais sofisticadas e insidiosas. Os cibercriminosos, "patrocinados" por interesses internacionais diversos e atores maliciosos, aproveitam-se de qualquer vulnerabilidade para ganhos financeiros e para comprometer a integridade das operações empresariais. Os líderes empresariais estão agora conscientes de que a cibersegurança não é um destino, mas sim uma jornada contínua.

Os testes de penetração, ou *Pen Tests*, emergiram como uma ferramenta vital para identificar e mitigar vulnerabilidades em cibersegurança antes que sejam exploradas por atacantes maliciosos.

Tradicionalmente, os testes de penetração eram realizados anualmente ou em intervalos regulares, por equipas internas ou empresas de cibersegurança contratadas. Mas não era raro algumas organizações improvisarem testes com soluções mais ou menos oficiosas, que acabavam por comprometer ainda mais a segurança dos respetivos sistemas de TI.

A natureza fluida das ameaças e o aumento dos ataques às empresas e aos respetivos colaboradores acabou por demonstrar que a frequência desta abordagem era insuficiente para proteger ativos críticos.


RICARDO SILVA, CLARANET

NOVO MODELO, PROTEÇÃO REFORÇADA

O Pen Testing-as-a-Service, ou PTaaS, representa uma mudança de paradigma. Consiste em testes de penetração contínuos e a pedido, realizados por especialistas em cibersegurança altamente qualificados. E as vantagens deste modelo justificam bem a sua adoção:

Resposta em Tempo Real: as organizações podem identificar e abordar imediatamente novas vulnerabilidades, a qualquer momento;

Redução de Riscos: ao identificar vulnerabilidades antes dos cibercriminosos, é possível reduzir significativamente os riscos associados a violações de dados e interrupções de negócios;

Economias de Custos: o modelo de PTaaS elimina a necessidade de equipas internas, bem como investimentos em hardware e software.

UMA QUESTÃO DE CONFIANÇA

Para enriquecer a identificação de todas as necessidades de proteção, as organizações podem ainda optar por uma avaliação de maturidade dos seus processos e procedimentos associados à cibersegurança.

Os serviços específicos de auditoria – à imagem do *360 Cyber Security Audit*, da **Claranet** – permitem criar uma imagem completa da eficácia dos procedimentos de segurança implementados numa organização, confirmando se correspondem ao esperado.

Quanto mais holística esta abordagem numa organização, mais eficaz será a identificação das áreas de risco e vulnerabilidades, bem como as recomendações para melhorar a sua postura de segurança. Para gerar informações estratégicas que ajudem a melhorar a eficiência operacional e tomar decisões fundamentadas de proteção, os processos de auditoria são um excelente ponto de partida para uma abordagem mais profunda e eficiente. Como é o caso dos testes de penetração.

Para implementar eficazmente o PTaaS, as organizações devem considerar quatro passos essenciais:

1. Seleção de um Fornecedor PTaaS: escolher um *provider* confiável e com experiência em cibersegurança é crucial, tal como avaliar o histórico, especializações e métodos de teste do fornecedor;

2. Âmbito de Teste Claro: definir claramente o âmbito dos testes, incluindo sistemas, aplicações e infraestruturas a serem testados;

3. Integração com SIEM e SOAR: integrar os resultados dos testes de penetração com sistemas de informações de segurança empresarial (SIEM) e respostas automatizadas a incidentes de segurança (SOAR), para uma ação imediata;

4. Formação e Sensibilização: garantir que as equipas internas compreendem os objetivos e os resultados dos testes de penetração, de forma a promover uma cultura de cibersegurança.

Assim, a implementação eficaz do PTaaS requer uma *parceria estratégica com fornecedores experientes*, que possuam capacidade e *know-how* para interpretar os resultados dos testes de penetração efetuados e aplicar as melhores soluções nas operações de cibersegurança.

Para diretores de TI, CISOs, CIOs, CEOs e responsáveis de cibersegurança, adotar o PTaaS é um passo crucial na construção de uma empresa resiliente à cibercriminalidade em constante evolução, capaz de enfrentar os desafios com confiança e determinação. ◀

visionware

por Milton Araújo,
Cybersecurity Consultant, VisionWare

PENTEST-AS-A-SERVICE:
A TRANSFORMAÇÃO CONTÍNUA NA DEFESA CIBERNÉTICA

A CIBERSEGURANÇA, NUM MUNDO CADA VEZ MAIS INTERLIGADO, É UMA NECESSIDADE INCONTORNÁVEL. AS ORGANIZAÇÕES, SEJAM ELAS PEQUENAS *STARTUPS* OU GRANDES MULTINACIONAIS, ENCONTRAM-SE NO CORAÇÃO DE UM AMBIENTE DIGITAL EM ACELERADA MUDANÇA, CHEIO DE RISCOS E POTENCIAIS AMEAÇAS. NESTE CENÁRIO, A QUESTÃO NÃO É SE A ORGANIZAÇÃO SERÁ ALVO DE UM ATAQUE, MAS QUANDO.

Os testes de penetração, frequentemente referidos como *pentests*, têm-se afirmado como uma ferramenta essencial. Através da simulação de ataques em ambientes controlados, as empresas podem descortinar as suas vulnerabilidades e atuar para as corrigir. Contudo, a realização eficaz destes testes exige uma especialização que nem todas as organizações têm internamente.

É neste contexto que se destaca a solução do "**Pentest-as-a-Service**" (**PaaS**). Este modelo, cada vez mais adotado, propõe uma abordagem contínua e especializada à cibersegurança. Em vez de um único teste anual ou semestral, o PaaS proporciona uma monitorização constante, adaptando-se às mutações do panorama digital.

Mas por que razão é o PaaS tão pertinente? Primeiramente, pela sua natureza adaptativa. Num mundo onde as ameaças cibernéticas se transformam diariamente, a defesa necessita de ser igualmente dinâmica. O PaaS, ao garantir testes recorrentes e atualizados, assegura que as defesas de uma organização estão sempre na vanguarda face às potenciais ameaças.

Do ponto de vista económico, o modelo também é vantajoso. Falhas de segurança podem traduzir-se em custos exorbitantes para as organizações, não apenas monetariamente, mas também em danos reputacionais à sua imagem que podem ser irrecuperáveis. Ao investir num serviço proativo e contínuo, as organizações posicionam-se numa lógica de prevenção e não apenas de reacção.


MILTON ARAÚJO, VISIONWARE

Em suma, o **Pentest-as-a-Service** simboliza mais do que uma evolução na cibersegurança; representa uma revolução na forma como as organizações se resguardam num mundo digital. Priorizando a prevenção, adaptabilidade e especialização, o PaaS emerge como um parceiro crucial para todas as empresas que ambicionam prosperar no século XXI.

Fotografias: Rui Santos Jorge

RUI DAMIÃO

"PODEMOS TER A MELHOR TECNOLOGIA, MAS SE NÃO TIVERMOS BOAS EQUIPAS PARA AS GERIR NÃO VÃO VALER DE MUITO"

PEDRO RODRIGUES

CISO DO BANCO DE PORTUGAL

PEDRO RODRIGUES, CISO DO BANCO DE PORTUGAL, PARTILHA AQUELES QUE CONSIDERA COMO PONTOS PRINCIPAIS NA DEFESA DA ORGANIZAÇÃO E DA SUA VISÃO SOBRE O ATUAL AMBIENTE DE CIBERSEGURANÇA QUE AS ORGANIZAÇÕES – SEJAM OU NÃO CRÍTICAS – VIVEM.

Como olha para o ambiente de cibersegurança atual?

Cada vez mais é um tema preponderante, central. Deixou de ser algo que acontecia muito espaçado no tempo, passou a ser algo que é uma realidade do dia a dia e ganhou uma evidência cada vez maior com o aumento da dependência dos sistemas de informação e da exposição externa que as empresas têm, que, na maioria das empresas, vai muito para além de uma mera presença; parte do negócio começa a assentar no digital e temos empresas completamente nativas digitais em que qualquer disrupção significa uma paragem total da empresa. Mesmo naquelas que achamos que estão um bocado mais protegidas na componente industrial, o que vemos na prática – com notícias de ciberataques a empresas mais industriais – é que entram no lado do OT, das operações do dia a dia das empresas, paralisando-as completamente.

Dito isto, esta maior visibilidade também ajuda a que as empresas tenham uma preocupação maior e se preocupem em proteger os seus ativos digitais como protegem os seus ativos físicos. Quero acreditar que há aqui um evoluir desta posição que, infelizmente na maior parte dos casos, ainda vem com um atraso e os cibercriminosos ainda têm uma vantagem sobre os defensores na maior parte dos casos.

Aquilo que são as empresas operadoras de infraestruturas críticas ou outras empresas que, pela sua natureza, têm os seus sistemas mais fechados, mais controlados, mais protegidos e têm esta preocupação há mais tempo, normalmente apresentam uma resiliência mais elevada. Vemos uma tendência para generalização do que são os métodos de ataque, o que torna mais fácil e frequentes esse tipo de incidentes de cibersegurança e torna-se cada vez mais fácil e barato atacar as empresas. É algo que sinto que ainda está numa trajetória ascendente e esperamos que com este *awareness* seja cada vez mais difícil aos atacantes conseguirem atingir os seus objetivos.

Quais são as principais ciberameaças que tem visto a crescer nos últimos tempos?

Com a pressão tecnológica de as empresas não quererem ficar para trás na utilização da tecnologia – às vezes porque lhes abre perspetivas de negócio, outras porque não querem ficar para trás em relação à concorrência –, o ciclo para desenvolver e implementar aplicações e plataformas tecnológicas é mais

curto. Sendo mais curto – por essa pressão de *time to market* – significa, muitas vezes, que não estão tão sólidos e testados antes de irem para produção.

Isto também afeta os próprios fabricantes que têm a necessidade de introduzir novas funcionalidades nos seus produtos, não lhe dando, se calhar, o tempo necessário para um teste mais sólido. Isto resulta em mais vulnerabilidades e fragilidades em produção que podem ser exploradas pelos atacantes.

Por outro lado – que sempre aconteceu e continua a verificar-se –, é a exploração do fator humano, daquilo que é a engenharia social, as fragilidades do ponto de vista dos utilizadores que podem abrir as portas das organizações dos atacantes na maior parte das vezes sem darem conta de que o estão a fazer.

Sente que a cibersegurança já é um tema de toda a organização e não apenas uma preocupação do IT?

Da realidade que conheço e nas grandes organizações é algo que já é transversal. Existe uma preocupação e um conhecimento do tema – claro que o conhecimento mais especializado está com o IT e com as áreas de negócio que lidam mais de perto com as aplicações –, mas sinto que é um tema que é do conhecimento geral da organização.

Agora, o que é o entendimento da cibersegurança e a segurança da informação ainda não está disseminado, às vezes nem dentro do IT; ainda há muita visão da cibersegurança como a proteção de perímetro e é preciso fazer a transição para aquilo que é incorporar os princípios de segurança de informação e cibersegurança na génese da arquitetura de negócio e de arquitetura de sistemas da organização. É preciso pensar em cibersegurança e segurança de informação nos processos de negócio, não apenas na parte do IT.

Esse salto depende muito das áreas de negócio e das pessoas que as lideram. Há áreas que incorporam perfeitamente esses princípios, outras que ainda têm uma visão mais tecnológica da cibersegurança. Isto é transversal às organizações que eu conheço.

Acredito – daquilo que vou sabendo através de amigos e colegas de trabalho – que isso nem sempre é verdade. Pode parecer paradoxal, mas nas empresas mais pequenas existe um isolamento maior das funções de cada unidade e uma menor visão do todo e de complementaridade entre as funções e as áreas.

AQUILO QUE SÃO AS EMPRESAS OPERADORAS DE INFRAESTRUTURAS CRÍTICAS OU OUTRAS EMPRESAS QUE, PELA SUA NATUREZA, TÊM OS SEUS SISTEMAS MAIS FECHADOS, MAIS CONTROLADOS, MAIS PROTEGIDOS E TÊM ESTA PREOCUPAÇÃO HÁ MAIS TEMPO, NORMALMENTE APRESENTAM UMA RESILIÊNCIA MAIS ELEVADA

Principalmente desde o ano passado que têm sido introduzidas várias regulamentações e diretrizes a nível europeu que impactam a cibersegurança das organizações. Considera que é um passo necessário para obrigar as empresas a investir em cibersegurança ou, por outro lado, estas regulamentações estão a impactar as empresas que, à partida, já apostavam em cibersegurança?

Acho que isto é uma tendência de alargamento deste tipo de normativos. Começamos focados naquilo que são as infraestruturas críticas e, como fazemos em qualquer trabalho, primeiro foca-se naquilo que é mais crítico e é prioritário. Na minha opinião, tanto a legislação como esse tipo de regulamentações está a seguir esse princípio, e bem.

Quero acreditar que estes tipos de regras vão ser cada vez mais transversais. O RGPD é um exemplo disso; não é específico nem para as infraestruturas críticas nem para um determinado setor, é transversal. Acredito que as regras que foram introduzidas pelo NIS 2 e pelo DORA vão ser cada vez mais alargadas a todas as organizações.

Obviamente que, seguindo este fluxo de ir primeiro ao que é mais crítico, aí estamos a ir às empresas que têm maior consciência para o tema. Mais do que obrigá-las a implementar os controlos – que muitas já estavam a fazer – é importante sistematizar e uniformizar aquilo que é necessário implementar, até para ajudar as empresas a priorizar os seus investimentos em cibersegurança. Se sabem que têm de cumprir determinado regulamento, não há dúvida de que a empresa A vai apostar de uma certa forma e a empresa B também. Temos algo que é uniforme e permite priorizar aquilo que, a nível internacional, é considerado como mais relevante, que mais pessoas já pensaram sobre isto e que dá como pontapé de saída os tópicos que vão ser preponderantes na

proteção das organizações. Se não tivéssemos este tipo de guia, o que ia acontecer era que cada organização ia apostar naquilo que lhe parecia mais importante.

Às vezes há mais destaques em termos de notícias em coisas que a probabilidade de acontecer é baixa, mas que quando acontece tem um impacto muito elevado. Se calhar não é aí que devemos investir primeiro; deve ser naquilo que tem uma maior probabilidade de ocorrência, combinado com o impacto desse incidente.

Sente que as organizações que não são abrangidas por estas regulamentações devem olhar para as mesmas e melhorar as suas proteções?

Sem dúvida. Partindo dos *frameworks* – como é o caso do NIS, que é dos *frameworks* mais conhecidos para estruturar as organizações e a postura de cibersegurança –, aquilo que é a regulação e a legislação, mesmo que não seja aplicável a uma organização, devem o quanto antes para essa legislação e regulamentação se tiverem essa capacidade para antecipar aquilo que inevitavelmente vai chegar até eles. Se conseguirem ir fazendo esse caminho e antecipando essas medidas, quando lhes bater à porta já vão estar mais bem preparados.

Um tema com que os responsáveis de cibersegurança se deparam é a falta de investimento em recursos. Qual é a dica que deixa a quem está nessa situação e precisa de um investimento para fazer uma proteção adequada da sua infraestrutura?

Separaria o problema dos recursos na capacidade de investimento, nos orçamentos, e naquilo que é a capacidade de equipas e de recursos humanos. Apesar de haver uma relação entre elas – claro que uma empresa que tem grandes capacidades de investimento também pode recrutar e conseguir os melhores recursos humanos –, mas, mesmo assim, existe uma diferença significativa porque mesmo empresas com uma capacidade de CapEx podem não conseguir recrutar

QUERO ACREDITAR QUE ESTES TIPOS DE REGRAS VÃO SER CADA VEZ MAIS TRANSVERSAIS. O RGPD É UM EXEMPLO DISSO; NÃO É ESPECÍFICO NEM PARA AS INFRAESTRUTURAS CRÍTICAS NEM PARA UM DETERMINADO SETOR, É TRANSVERSAL. ACREDITO QUE AS REGRAS QUE FORAM INTRODUZIDAS PELO NIS 2 E PELO DORA VÃO SER CADA VEZ MAIS ALARGADAS A TODAS AS ORGANIZAÇÕES.

ou alargar as suas equipas por limitações de *head count*, por diretrizes numa multinacional com rácios que é preciso cumprir.

Mesmo havendo essa capacidade de investimento em hardware ou software, pode não haver essa capacidade de investimento nas equipas. Isso é um problema grande porque podemos ter a melhor tecnologia, a tecnologia mais moderna, as melhores plataformas, mas, se não tivermos boas pessoas e boas equipas para as gerir e as tornar operacionais, não vão valer de muito.

O Banco de Portugal tem conhecimento técnico, uma estrutura sólida e uma aposta forte nesta área que nos permite acompanhar aquilo que são as principais preocupações e tendências de mercado. No entanto, a cibersegurança é um mercado obviamente competitivo e, nos últimos anos, com a abertura daquilo que é o trabalho remoto, houve um impacto muito grande na abertura do mercado e na capacidade que as pessoas especializadas têm para empresas estrangeiras que têm uma capacidade de investimento e de pagar que as organizações portuguesas dificilmente conseguem acompanhar.

O tema do recrutamento é algo que é muito importante para nós e para as organizações em geral e existem diversas abordagens para lidar com isso. Podemos procurar e atrair talento através dos projetos que fazemos, através da divulgação de como encaramos o tema da cibersegurança, mas a parceria com as universidades e a capacidade de abrir programas de estágio interessantes que abrem as portas das organizações para os jovens, que lhes dão uma oportunidade de entrada no mercado de trabalho numa empresa sólida, que lhes permite adquirir conhecimento e evoluir, acho que é um atrativo muito grande. Essas pessoas trazem uma visão diferente e um valor acrescentado para as organizações que é enorme.

Combinando isso com o conhecimento de quem já está há muito tempo na organização e conhece muito bem os sistemas, existe algo – que tenho sempre procurado na liderança de equipa – que é esta diversidade que vai muito para além daquilo que

normalmente é referido quando falamos de diversidade nas equipas e tenho dado muita preponderância a esta capacidade de misturar experiência com juventude, o desafio com aquilo que é a preocupação com a estabilidade. Acho que é nesse equilíbrio que as empresas podem desenvolver os seus sistemas, não descurando a necessidade de investir na parte tecnológica.

Um dos temas de 2023 é a inteligência artificial. Como é que a inteligência artificial está a impactar a cibersegurança, tanto do lado de quem defende como de quem ataca?

Esse é um tema que me interessa bastante e ao qual tenho dedicado algum tempo a acompanhá-lo. É interessante perceber como é que as tecnologias se desenvolvem e como é que elas são vistas pelo grande público. Às vezes temos o desenvolvimento de algumas tecnologias que têm uma grande visibilidade mediática que, para o utilizador final, a pessoa que tem os seus *gadgets* e usa a título pessoal, tem um impacto muito grande, mas depois, na realidade das organizações, nem sempre são assim tão relevantes. Acredito que a inteligência artificial não é um desses casos. A inteligência artificial vai ter – e já está a ter – um impacto muito grande quer na vida pessoal quer na profissional das pessoas.

Para a cibersegurança, existe sempre – como em qualquer outra área em que isso acontece – uma preocupação inicial, que é como é que isto vai alterar o que temos neste momento e a maneira como pensamos a cibersegurança; o que é que vamos ter de mudar para nos adaptarmos ao advento da inteligência artificial. Ao mesmo tempo – e para mim é esse o grande ponto de viragem – é quando encaramos não apenas a ameaça, mas também como oportunidade daquilo que podemos acrescentar ao nosso lado defensivo, de proteção, como é que a inteligência artificial nos vai ajudar a detetar e a responder mais rapidamente aos eventos e incidentes de cibersegurança.

O facto de estarmos organizados com uma equipa que está mais focada na defesa e outra mais focada na pesquisa de vulnerabilidades e na maneira como os atacantes estão a desenvolver as suas tecnologias, há uma troca de experiên-

cias muito relevantes que a inteligência artificial vai servir quer a uns, quer a outros. Esta utilização crescente da inteligência artificial generativa vai permitir às unidades de negócio darem uma resposta mais rápida, a preocupação com a satisfação do cliente, com a resposta ao cliente, mas, nas equipas de retaguarda e de proteção da organização em termos de cibersegurança, também vai fazer o mesmo efeito para aquilo que são os nossos clientes internos, que são as áreas de negócio e a organização. Vai-nos ajudar a compreender melhor, a reagir mais rápido e com maior eficiência àquilo que são os nossos desafios e com aquilo com que nos deparamos.

Assumo que o Banco de Portugal já esteja a utilizar inteligência artificial nos seus temas de cibersegurança?

É algo que procuramos incorporar em parceria com os nossos parceiros e fabricantes que já estão a apostar nessas tecnologias e a desenvolver internamente, também, mecanismos e plataformas de inteligência artificial viradas quer para o negócio, quer para aquilo que é a componente interna do banco.

> QUEM ESTÁ A TRABALHAR NUMA INFRAESTRUTURA CRÍTICA – SEJA EM CIBERSEGURANÇA OU NOUTRA – TEM PERFEITA NOÇÃO QUE AQUILO QUE FAZ CONTRIBUI PARA UM PROPÓSITO MAIOR DO QUE A ORGANIZAÇÃO, CONTRIBUI PARA A SOCIEDADE E, COMO TAL, TEM UMA RESPONSABILIDADE DE GARANTIR A CONTINUIDADE DA SUA OPERAÇÃO, DO NEGÓCIO, NAQUILO QUE É O SEU DIA A DIA COM A RELEVÂNCIA QUE ISSO TEM PARA A SOCIEDADE

O Banco de Portugal não está a deixar passar a onda sem a acompanhar; está a apostar fortemente nesta área.

O Banco de Portugal é uma infraestrutura crítica para o país. Quais são as especificidades de proteger esta infraestrutura crítica em concreto?

As infraestruturas críticas que estão regulamentadas e legisladas como tal, foram e são identificadas de uma forma contínua pela relevância que têm para a sociedade. Quem está a trabalhar numa infraestrutura crítica – seja em cibersegurança ou noutra – tem perfeita noção que aquilo que faz contribui para um propósito maior do que a organização, contribui para a sociedade e, como tal, tem uma responsabilidade de garantir a continuidade da sua operação, do negócio, naquilo que é o seu dia a dia com a relevância que isso tem para a sociedade.

Isso coloca um peso e uma responsabilidade adicional em quem está do lado das infraestruturas críticas, também recompensado com este sentimento de propósito e utilidade pública. Aquilo que sinto, trabalhando em infraestrutura crítica – e é algo que

me acompanhou ao longo da minha carreira – é essa motivação adicional para cada vez que estamos a fazer um projeto, cada vez que encontramos um desafio que achamos que é relevante e pode ter um impacto grande para o nosso negócio e para a nossa organização, se calhar temos uma motivação extra ao perceber que vale a pena lutar por defender a cibersegurança, aquilo que é a nossa visão de resiliência da organização porque não estamos apenas a desenvolver um esforço para proteger a organização; estamos a fazê-lo para a sociedade como um todo, quer a nível local, nacional e até internacional, no caso do Banco de Portugal, no sistema europeu de bancos centrais, ou noutras infraestruturas críticas que têm outras ligações, como o setor da energia, das águas ou dos portos. Todas essas infraestruturas críticas têm um papel que vai além das fronteiras do nosso país.

Há algum ciberataque contra o Banco de Portugal que possa partilhar detalhes?

No Banco de Portugal mantemos a nossa monitorização e a nossa vigilância contínua, lidando com aquilo que são as ameaças comuns a qualquer organização, os grupos criminosos que procuram explorar alguma nova vulnerabilidade ou uma fragilidade no fator humano com as inúmeras tentativas de phishing que ocorrem diariamente. Felizmente, com uma combinação de tecnologia e *awareness* das nossas pessoas, tem sido possível controlar isso.

Nenhuma organização em Portugal, quando há um ciberataque relevante, consegue escondê-lo. A ausência de notícias de ciberataques relevantes ao Banco de Portugal já transmite essa resposta. De qualquer forma, isso não significa que possamos de alguma forma desleixar-nos ou baixar a guarda. Sabemos que é uma organização com uma grande visibilidade, quer a nível da sua operação, quer mediático, e temos de continuar sempre muito atentos para evitar algum ataque de maior expressão.

Quais são os conselhos que deixa a outros responsáveis de cibersegurança para melhorar as suas proteções?

Aquilo que diria a outros responsáveis de cibersegurança é o mesmo que aplico e digo a mim próprio. O primeiro ponto essencial é cuidar das nossas equipas. Uma equipa de cibersegurança, focada em segurança de informação, que trabalhe bem e em conjunto, que tenha o tal misto de experiência com vontade de inovar e desafiar, é a base de tudo. Nenhum responsável de segurança de informação consegue fazer o que quer que seja sem ter uma boa equipa em quem possa confiar e que faça um bom trabalho.

O segundo ponto é a comunicação e o *awareness*, em primeiro lugar interno. Levar os conceitos e as preocupações de cibersegurança numa linguagem que o negócio consiga entender, que o próprio IT consiga entender e levar essa preocupação ao longo da cadeia hierárquica que tiver, seja diretamente a um conselho de administração, seja a um diretor de IT ou de risco, qualquer que seja a cadeia de *report* do responsável de segurança de informação. Levar essa mensagem, levar uma visão, um pensamento e uma estratégia que consiga, depois, ganhar o suporte de quem toma as decisões a nível de prioridade de projetos e de orçamento.

Estando estes dois passos conseguidos, diria que grande parte do caminho está feito. A partir daí, é garantir que existe um foco naquilo que são os projetos processuais e de gestão de risco, mas também nos projetos tecnológicos, garantindo o equilíbrio entre os dois pontos e tentando manter o foco naquilo que é

essencial e relevante para a organização, às vezes sacrificando um pouco aquilo que são as tendências de mercado ou as modas porque nem tudo aquilo que é a última tendência de mercado é adequado para a nossa organização. Temos de perceber o que faz sentido trazer para dentro da organização de acordo com a maturidade que temos, os recursos que temos e o conhecimento que temos dentro da organização. ◀

Agradecimento:

Hotel AlmaLusa Baixa/Chiado pela cedência do espaço para a entrevista

balwurk cyber security

COBERTURA DE EVENTO

MORNING WITH APPSEC BY BALWURK AND SYNOPSYS

BALWURK E *SYNOPSYS* ANUNCIAM PARCERIA ESTRATÉGICA DIFERENCIADORA NO CENÁRIO DA SEGURANÇA APLICACIONAL EM PORTUGAL.

No dia 21 de setembro de 2023, o EPIC Sana Lisboa foi palco de um evento relevante para o setor de Cibersegurança em Portugal. Sob o título "Morning with AppSec by ***Balwurk*** and ***Synopsys***", esta iniciativa reforçou a parceria estratégica entre a ***Balwurk*** e a ***Synopsys***, líder global no campo da Segurança Aplicacional (AppSec).

A colaboração entre a ***Balwurk*** e a ***Synopsys*** representa uma parceria no âmbito da Segurança Aplicacional em que ambas as empresas se comprometem a trazer as melhores soluções e serviços de AppSec, de acordo com as necessidades específicas de cada cliente.

A mensagem central do evento focou-se na importância de alinhar a estratégia de AppSec com os riscos e objetivos empresariais. A ***Balwurk*** e a ***Synopsys*** estão empenhadas em fornecer às empresas as ferramentas necessárias para ultrapassar os desafios de segurança de forma proativa, assegurando que as aplicações que suportam os processos de negócio, são resilientes e seguras.

É importante sublinhar que a ***Synopsys*** tem sido consistentemente reconhecida como líder no Quadrante Mágico da Gartner para Testes de Segurança Aplicacional nos últimos sete anos. A empresa destacou-se também muito recentemente no Forrester Wave com a sua solução de Análise de Composição de Software.

No palco, o evento contou a presença do Paulo Rosado, CEO da Balwurk; Ricardo Rodrigues Head of GRC and Application Security da Balwurk; Jesus Strauss, Channel Manager IBERIA / Channel Operation Manager EMEA da Synopsys, Ignacio Baylina, Regional Manager Iberia da Synopsys; e Emmanuel Gonzales, Senior Channel Engineer da Synopsys.

Na plateia, assistiram um grupo exclusivo de convidados de diversos setores da indústria, incluindo Banca, Energia, Saúde, Telecomunicações e Tecnologia da Informação. A sala cheia de participantes e a atividade de *networking* evidenciaram o sucesso deste evento, que serviu como o marco para a parceria entre a ***Balwurk*** e a ***Synopsys*** no mercado português.

Durante o evento, foram também debatidas as mudanças que se avizinham, já que a Europa prepara o novo regulamento Cyber Resilience Act (CRA), na sequência da estratégia Digital Europeia para melhorar a Segurança e a Resiliência do espaço digital europeu. A UE lançou uma nova proposta que responda às necessidades do mercado e proteja os consumidores introduzindo regras comuns de Cibersegurança para os fabricantes e vendedores de produtos digitais e de serviços conexos.

Este evento com o mote "***Shift Left, Secure Right***" representou o começo de uma colaboração promissora entre a ***Balwurk*** e a ***Synopsys***, em que ambas as empresas estão empenhadas em ajudar as organizações a descobrir e aplicar as vantagens da Orquestração no Desenvolvimento de Aplicações.

O evento proporcionou uma visão completa das soluções disponíveis para proteger o código contra ameaças e vulnerabilidades, garantindo a Confidencialidade, Integridade e Disponibilidade da Informação. A parceria entre a ***Balwurk*** e a ***Synopsys*** visa não só fortalecer a segurança das aplicações empresariais no presente, mas também preparar as empresas para os desafios regulamentares em constante evolução. ◀

ENGENHEIRO INFORMÁTICO FORMADO NO IST, COM MESTRADO EM SEGURANÇA DA INFORMAÇÃO PELA CMU E FCUL, TEM AINDA UM MBA PELO LISBONMBA, TRABALHA NA ÁREA DA SEGURANÇA DESDE 2002, COM UM PERCURSO TECNOLÓGICO NA PORTUGAL TELECOM E NA S21SEC. ESTEVE 4 ANOS E MEIO A LIDERAR PRÁTICAS DE CIBERSEGURANÇA EM DUAS CONSULTORAS E, DESDE FINAIS DE 2021, É O DIRETOR DE SEGURANÇA E PROTEÇÃO DE DADOS NO BANCO CTT

POR CARLOS SILVA, DIRETOR DE SEGURANÇA E PROTEÇÃO DE DADOS, BANCO CTT

INCIDENTES DE SEGURANÇA: UMA PREPARAÇÃO DIFERENTE

À s 4 da manhã o responsável pela equipa de Operações de IT liga ao seu diretor para lhe comunicar que algo se passa nos principais sistemas da organização, as contas de administração dos sistemas não estão a permitir que nenhum dos vários elementos da equipa de Operações consiga autenticar-se nos sistemas. E que, inclusive, alguns sistemas já nem sequer respondem pelo nome ou pelo IP previamente conhecido. "Liga, por favor, de imediato ao responsável pela equipa de operações de Segurança", pede o diretor de IT ao seu responsável de operações, sabendo que este iria de imediato também entrar em contato com o responsável máximo da segurança da organização. 30 minutos depois, e após vários novos alertas e chamadas, todos estes protagonistas já estavam reunidos nas instalações do IT da organização a acompanharem o desenrolar destes acontecimentos altamente suspeitos.

Às 4h50, a decisão que nenhum dos responsáveis reunidos (IT e Segurança) queria tomar teve de ser concretizada, ligar aos principais elementos da administração da organização para lhes comunicar que a mesma estava sob um ataque de malware, muito

provavelmente uma qualquer variante de ransomware, e que já não era possível fazer contenção dos danos. Novas, e mais gravosas, decisões teriam de ser tomadas e era necessário que a administração da organização estivesse desde já envolvida. Desde logo era necessário analisar as várias alternativas existentes para pedir ajuda especializada para situações tão críticas como a que se estava a atravessar.

Às 5h40 da manhã iniciaram-se os contatos com as duas empresas sugeridas pelo diretor de segurança que poderiam ajudar a organização na tentativa de mitigar, ou pelo menos minimizar, o impacto da situação. 20 minutos depois toda a administração já estava reunida na sala de crise em conjunto com os responsáveis anteriormente já reunidos, e vários contatos já estavam a ser realizados para convocar os vários elementos previstos no plano de resposta a incidentes da organização, como era o caso dos diretores de RH, de Marketing e Comunicação, assim como o de Legal. Às 6h30, já com todo o gabinete de crise presente, o ambiente era tenso e sentia-se algum desconforto na maioria dos presentes devido à sensação de incapacidade e descontrolo que quase todos apresentavam. O responsável de segurança aparentava ser o elemento mais em controlo e tentava gerir as sensibilidades dos restantes ao mesmo tempo que recebia as primeiras indicações de atuação por parte da empresa entretanto escolhida para apoiar a sua organização. Não desligar sistemas e tentar garantir que o menor número de colaboradores da organização tentassem fazer a sua autenticação ao início do dia, eram as primeiras indicações que os especialistas lhe estavam a aconselhar através da chamada telefónica. Uma hora e meio depois, 3 elementos da empresa especialista já estariam nas instalações da organização para os auxiliar e liderar os processos de análise, contenção e recuperação em conjunto com as equipas técnicas de IT e Segurança.

Em paralelo, várias questões eram colocadas aos elementos do Gabinete de Crise:

- Como comunicar com os colaboradores da organização, informando-os da situação, transmitindo a informação o mais verdadeira possível, mas ao mesmo tempo sem alarmar desnecessariamente esses mesmos colaboradores?

- Que tipo de comunicação deveria ser, desde já, passada aos elementos da Comunicação Social que, entretanto, já tinha sido alertada para a indisponibilidade de alguns serviços na Internet da organização e tentava obter as primeiras respostas por parte da organização?

- Que comunicação se deveria começar a preparar perante a autoridade de controlo para a proteção de dados pessoais? E se existia outro tipo de comunicação que se devia preparar para alguma outra entidade ou autoridade nacional, perante as quais a organização poderia estar obrigada?

• Que tipo de comunicação se deveria preparar para enviar aos parceiros e fornecedores da organização para que pudessem iniciar também algumas atividades de análise dos seus sistemas, os quais poderiam também ter sido contaminados pelo mesmo agente malicioso que estava a provocar o caos atual?

• Que comunicação se deveria colocar online, nos sistemas ainda disponíveis e que não tinham sido afetados, para alertar os clientes sobre o sucedido e solicitar a sua compreensão perante o sucedido?

"BE PREPARED"

O cenário que se acabou de descrever, de forma bastante simplificada, poderia acontecer a qualquer organização que tem o seu negócio, ou parte dele, dependente de sistemas informáticos e serviços online. Grande parte delas não está preparada para responder às questões que o Gabinete de Crise desta organização fictícia tinha perante ao início da manhã daquele fatídico dia. Mas, olhando a esta distância, creio que muitos dos que me leem pensam "obviamente que tenho a resposta para todas estas questões e saberia, num curto espaço de tempo, endereçá-las todas.". Contudo, e mais do que as nossas opiniões, e conhecimentos, pessoais devemos garantir que as nossas organizações estão preparadas para este tipo de eventos críticos e que, principalmente, os principais "atores" das nossas organizações sabem o seu papel e as suas responsabilidades.

Tudo deverá começar pela elaboração, ou adaptação, de um processo de gestão de incidentes específico para ataques via malware, mais concretamente por ransomware. A identificação (ou até contratação) prévia de uma, ou mais, empresa especialista deverá ser outra das fases de preparação para este tipo de eventos. Garantir que se perde o menor tempo possível para se tomar decisões que podem já estar previamente estudadas e previstas, é um dos primeiros passos para se reduzir ao máximo o impacto que estes eventos trazem às organizações. Contudo, muitas outras devem ser consideradas, tais como:

• Preparar os colaboradores para a forma de atuar perante estes eventos, tanto interna como perante elementos externos às organizações;

CONTUDO, E MAIS DO QUE AS NOSSAS OPINIÕES, E CONHECIMENTOS, PESSOAIS DEVEMOS GARANTIR QUE AS NOSSAS ORGANIZAÇÕES ESTÃO PREPARADAS PARA ESTE TIPO DE EVENTOS CRÍTICOS E QUE, PRINCIPALMENTE, OS PRINCIPAIS "ATORES" DAS NOSSAS ORGANIZAÇÕES SABEM O SEU PAPEL E AS SUAS RESPONSABILIDADES

ESTAR PREPARADO, E TREINADO, DEVERIA SER A PRINCIPAL PREOCUPAÇÃO DAS ORGANIZAÇÕES NO QUE DIZ RESPEITO À SUA RESPOSTA PERANTE EVENTOS DE SEGURANÇA. A TECNOLOGIA É CRÍTICA PARA A SEGURANÇA, MAS PREPARAR AS PESSOAS E TER PROCESSOS DEFINIDOS É O INÍCIO DE UMA RESPOSTA ATEMPADA E EFICAZ PERANTE ESTE TIPO DE EVENTOS

- Preparar templates de comunicação para reportar estes eventos à comunicação social;

- Conhecer todas as responsabilidades regulatórias e de report perante autoridades de controlo e de regulação;

- Ter uma lista atualizada com contatos das principais autoridades policiais, judiciárias e centros nacionais de segurança nas geografias onde as organizações operam;

- Garantir um inventário atualizado dos principais parceiros e fornecedores que tenham sistemas interligados ou que possam contaminar, ou ser contaminados, com malware;

- Garantir a capacidade de colocar online sistemas alternativos repondo os serviços indisponíveis ou, como alternativa mínima, disponibilizar um site com informação sobre a indisponibilidade dos serviços afetados;

- Ter sempre atualizada a lista de contatos internos de todos os elementos que deverão participar, ou contribuir, para o Gabinete de Crise.

Estar preparado, e treinado, deveria ser a principal preocupação das organizações no que diz respeito à sua resposta perante eventos de segurança. A tecnologia é crítica para a segurança, mas preparar as pessoas e ter processos definidos é o início de uma resposta atempada e eficaz perante este tipo de eventos.

COM MAIS DE 25 ANOS DE EXPERIÊNCIA NA ÁREA DE REDES E CIBERSEGURANÇA, TRAZ CONSIGO UM SÓLIDO CONHECIMENTO EM PLANEAMENTO, IMPLEMENTAÇÃO E GESTÃO DE INFRAESTRUTURAS DE TI. COM UMA CARREIRA INTERNACIONAL, OCUPA, ATUALMENTE, O CARGO DE CISO NA CUF, ONDE LIDERA ESTRATÉGIAS DE SEGURANÇA CIBERNÉTICA E CONTRIBUI PARA A PROTEÇÃO DAS OPERAÇÕES CRÍTICAS DA ORGANIZAÇÃO

POR MIGUEL GONÇALVES, CISO DA CUF

RETENÇÃO DE TALENTOS EM CIBERSEGURANÇA: VALORIZANDO AS NOVAS GERAÇÕES E O TELETRABALHO

A CIBERSEGURANÇA É UM CAMPO CRÍTICO NA ERA DIGITAL, ONDE A PROTEÇÃO DE DADOS E SISTEMAS CONTRA AMEAÇAS CIBERNÉTICAS É DE SUMA IMPORTÂNCIA.

No entanto, um desafio significativo que as organizações enfrentam é a retenção de talentos em cibersegurança. Além disso, as novas gerações de profissionais têm uma perspectiva diferente sobre o trabalho, valorizando o teletrabalho e a flexibilidade. Este artigo explora como as organizações podem abordar a retenção de talentos em cibersegurança, considerando as expectativas das novas gerações em relação ao teletrabalho.

A MUDANÇA NAS EXPECTATIVAS DE TRABALHO

As novas gerações, como a Geração Y (Millennials) e a Geração Z, têm uma visão distinta do trabalho. Elas valorizam a flexibilidade, o equilíbrio entre trabalho e vida pessoal e a possibilidade de trabalhar remotamente. Para reter talentos em cibersegurança, as organizações precisam considerar essas expectativas.

Essas gerações cresceram num ambiente digital e têm uma compreensão profunda da tecnologia. Além disso, a mentalidade das novas gerações é moldada por experiências anteriores, como a recessão econômica e a crescente dependência da tecnologia. Isso torna-as mais propensas a buscar empregos que ofereçam não apenas estabilidade financeira, mas também flexibilidade e um propósito significativo no trabalho.

TELETRABALHO EM CIBERSEGURANÇA

O teletrabalho em cibersegurança pode ser um desafio devido à natureza sensível das atividades desempenhadas. No entanto, as novas tecnologias permitem que muitas tarefas sejam realizadas remotamente, e as organizações podem adotar estratégias para aproveitar essas vantagens.

AS NOVAS GERAÇÕES, COMO A GERAÇÃO Y (MILLENNIALS) E A GERAÇÃO Z, TÊM UMA VISÃO DISTINTA DO TRABALHO. ELAS VALORIZAM A FLEXIBILIDADE, O EQUILÍBRIO ENTRE TRABALHO E VIDA PESSOAL E A POSSIBILIDADE DE TRABALHAR REMOTAMENTE.

1. Tecnologia Avançada e ZTNA (*Zero Trust Network Access*) **e PAM** (*Privileged Access Management*)

Investir em tecnologias de segurança avançadas, incluindo soluções como ZTNA (Zero Trust Network Access) e PAM (Privileged Access Management), que permitem monitorização e resposta a ameaças remotamente, é essencial. A implementação de soluções de segurança em nuvem e a automação de processos podem permitir que os profissionais de cibersegurança gerenciem redes e sistemas de qualquer local, mantendo ao mesmo tempo um alto nível de controle sobre o acesso privilegiado.

2. Flexibilidade

Oferecer horários de trabalho flexíveis e opções de teletrabalho parcial ou integral permite que os profissionais de cibersegurança atendam às suas necessidades pessoais e profissionais. Isso pode incluir horários de trabalho condizentes com fusos horários diferentes ou a possibilidade de trabalhar em casa quando necessário.

3. Equilíbrio Entre Trabalho e Vida Pessoal

Promover um equilíbrio saudável entre trabalho e vida pessoal é fundamental para atrair e reter profissionais de cibersegurança. Isso envolve a definição de expectativas realistas em relação às horas de trabalho e o incentivo a pausas regulares para evitar o *burnout*.

4. Comunicação Eficiente

Implementar ferramentas de comunicação eficazes é crucial para garantir a colaboração e a troca de informações entre equipas de segurança remotas. Videoconferências, mensagens instantâneas seguras e sistemas de gestão de projetos podem facilitar a comunicação e a coordenação de atividades.

PROMOVER UM EQUILÍBRIO SAUDÁVEL ENTRE TRABALHO E VIDA PESSOAL É FUNDAMENTAL PARA ATRAIR E RETER PROFISSIONAIS DE CIBERSEGURANÇA. ISSO ENVOLVE A DEFINIÇÃO DE EXPECTATIVAS REALISTAS EM RELAÇÃO ÀS HORAS DE TRABALHO E O INCENTIVO A PAUSAS REGULARES PARA EVITAR O BURNOUT.

ESTRATÉGIAS PARA A RETENÇÃO DE TALENTOS

Além de considerar o teletrabalho e a tecnologia avançada, as organizações podem adotar estratégias adicionais para reter talentos em cibersegurança:

1. Desenvolvimento de Carreira

Oferecer oportunidades de crescimento profissional, treinamento e desenvolvimento contínuo é fundamental. Os profissionais de cibersegurança

estão constantemente atualizando suas habilidades para acompanhar as ameaças em evolução, e as organizações que apoiam essa busca por conhecimento têm uma vantagem na retenção de talentos.

2. Reconhecimento e Valorização

Reconhecer e valorizar o trabalho dos profissionais de cibersegurança por meio de programas de recompensas e reconhecimento pode criar um ambiente de trabalho mais positivo e motivador.

3. Cultura de Diversidade e Inclusão

Promover uma cultura diversificada e inclusiva que atraia profissionais de diferentes origens e perspetivas pode enriquecer a equipa de cibersegurança e contribuir para a retenção de talentos.

4. Mentorias

Estabelecer programas de mentoria para facilitar a transferência de conhecimento entre gerações de profissionais pode criar um senso de pertencimento e propósito, especialmente quando profissionais mais experientes partilham as suas experiências com aqueles que estão começando suas carreiras em cibersegurança.

> AS ORGANIZAÇÕES QUE RECONHECEM AS EXPECTATIVAS DAS NOVAS GERAÇÕES EM RELAÇÃO AO TELETRABALHO, ADOTAM TECNOLOGIAS AVANÇADAS E ESTRATÉGIAS DE DESENVOLVIMENTO PROFISSIONAL, E PROMOVEM UMA CULTURA INCLUSIVA TERÃO UMA VANTAGEM NA ATRAÇÃO E RETENÇÃO DE PROFISSIONAIS TALENTOSOS

CONCLUSÃO

A retenção de talentos em cibersegurança é vital para manter a segurança de dados e sistemas na nossa sociedade digital. As organizações que reconhecem as expectativas das novas gerações em relação ao teletrabalho, adotam tecnologias avançadas e estratégias de desenvolvimento profissional, e promovem uma cultura inclusiva terão uma vantagem na atração e retenção de profissionais talentosos. À medida que as tecnologias evoluem e as gerações continuam a entrar no mercado de trabalho, a flexibilidade e a adaptação às mudanças nas expectativas serão cruciais para o sucesso na retenção de talentos em cibersegurança. Com essas estratégias em mente, as organizações podem fortalecer as suas equipas de cibersegurança e manter um alto nível de proteção contra ameaças cibernéticas em constante evolução. ◀

ANALISTA E CONSULTOR. MEMBRO DA DIREÇÃO DA CIIWA. PÓS-GRADUADO EM GOVERNANCE & STRATEGIC INTELLIGENCE E EM GESTÃO DE MARKETING

POR IDALÉCIO LOURENÇO, ANALISTA E CONSULTOR

A EMERGÊNCIA DA GESTÃO DO RISCO DE PARCEIROS:

AS OPORTUNIDADES E OS DESAFIOS

PARTILHA, COLABORAÇÃO E PARCERIAS SÃO CONCEITOS OPERACIONAIS/FORMAS DE TRABALHAR CADA VEZ MAIS NECESSÁRIOS E INEVITÁVEIS À ATIVIDADE DAS ORGANIZAÇÕES, QUER INTERNA, QUER EXTERNAMENTE, SEJAM PÚBLICAS E/OU NÃO PÚBLICAS, E EMPRESARIAIS E NÃO EMPRESARIAIS. NO MUNDO DO SÉCULO XXI, AS ORGANIZAÇÕES NÃO PODEM MAIS SOBREVIVER “ORGULHOSAMENTE SÓS”.

A "ocupação" estratégica à escala global pela liderança dos recursos tradicionais e emergentes pelas principais potências, a globalização da economia e a internacionalização, sobretudo das empresas, acompanhadas paralelamente, pelo desenvolvimento tecnológico, estão a transformar a gestão estratégica das organizações. Isto acontece num contexto associado aos novos teatros de operações, em particular o digital, que amplifica o alcance, acelera a velocidade, aproxima o mundo e os seus atores e potencia a dimensão das coisas, a que acrescem os efeitos, impactos e consequências

Deste quadro resulta que, para sobreviverem e serem mais competitivas, as organizações (sobretudo as empresas) têm de se concentrar nos seus vetores estratégicos ("*core business*") e "deixar" o menos estratégico/operacional para terceiros (fornecedores/parceiros). Uma outra dimensão decisiva reside na criticidade das atividades que estão a ser terceirizadas, resultando em relacionamentos e interdependências estratégicas entre diferentes parceiros – e não apenas tarefas acessórias sem impacto nas operações – em que o elo comum é suporte/dependências do digital.

Não obstante as organizações conseguirem manter, em geral, a reserva do controlo e da liderança estratégica do negócio, tem de se reconhecer que ao serem cruciais (sobretudo, em termos de operação) para os negócios, as parcerias também têm o potencial de os expor a novos riscos. Em termos estratégicos, teremos então novos Riscos Relacionais, em termos operacionais iremo-nos focar de seguida na emergência de novos riscos ao nível da cibersegurança.

DOS RISCOS ÀS OPORTUNIDADES

Com a maior "dependência" da digitalização dos processos, sobretudo, da gestão dos riscos de terceiros (TPRM), esta é uma realidade incontornável, logo uma fonte de preocupação/riscos para a liderança e para a gestão.

Os especialistas identificam uma tipologia com quatro riscos principais.

Amplitude do Risco Potencial. Com a proliferação de dados eletrónicos e as violações de dados frequentemente a ocupar as manchetes dos meios de comuni-

NÃO OBSTANTE AS ORGANIZAÇÕES CONSEGUIREM MANTER, EM GERAL, A RESERVA DO CONTROLO E DA LIDERANÇA ESTRATÉGICA DO NEGÓCIO, TEM DE SE RECONHECER QUE AO SEREM CRUCIAIS (SOBRETUDO, EM TERMOS DE OPERAÇÃO) PARA OS NEGÓCIOS, AS PARCERIAS TAMBÉM TÊM O POTENCIAL DE OS EXPOR A NOVOS RISCOS.

O *ONBOARDING* DO FORNECEDOR/PARCEIROS, INTEGRAÇÃO DE FLUXOS DE INFORMAÇÃO E OPERAÇÃO SÃO OUTRAS ETAPAS QUE DEVERÃO SER ACOMPANHADAS POR CONTROLOS ADEQUADOS, ATÉ AO PRÓPRIO *OFFBOARDING* OU ATIVAÇÃO DA DENOMINADA *EXIT STRATEGY*.

cação social, o risco que mais chama a atenção são os incidentes de cibersegurança por via da integração com terceiros. O quadro é, contudo, mais amplo e complexo. Podemos e devemos incluir fatores como a evolução geopolítica, a emergência e consolidação do ESG (*Environment*, *Social* e *Governance*), a privacidade e segurança dos dados, ou as componentes financeira, reputacional, operacional e... a lista pode continuar. Assim, quanto maior for a interdependência digital, maior será o número de riscos potenciais que teremos de gerir.

Análise e relatórios internos. Os executivos e os Conselhos de Administração, conscientes da sensibilidade e importância estratégica do tema, estão a pedir relatórios e informações mais detalhadas sobre o risco de terceiros. A necessidade de proteger as cadeias de fornecimento integradas fazem destacar as interligações com terceiros como matéria relevante para o negócio e para a sua continuidade.

Aumento da globalização e da complexidade da terceirização. Muitas organizações estão a lutar para se manterem atualizadas com as mudanças resultantes das regulamentações e outras diretrizes (*compliance*). Ao mesmo tempo, os regulamentos e padrões relativos às relações económicas-comerciais com terceiros estão em constante evolução. Estamos perante um quadro cada vez mais vasto e complexo, no ambiente externo e interno. Em todo o caso, muitas organizações estão a conseguir encontrar um caminho entre o custo/investimento em programas TPRM e os restantes.

Como transformar a prática de TRPM em valor?

Com base na abordagem colaborativa, em primeiro lugar, deverá visualizar-se as várias etapas de uma parceira. Em cada uma das fases teremos de gerir o risco relacional, bem como os riscos de cibersegurança.

Na fase de planeamento, teremos as boas práticas de seleção de parceiros e de *due dilligence* estando em causa o *fit* relacional como também um conjunto de requisitos mínimos de cibersegurança e assessment do risco inicial do fornecedor. Nesta fase de planeamento estratégico e seleção, existem vários controlos que irão mitigar os riscos e maximizar os benefícios das parcerias estratégicas.

Na formalização dos contratos existem medidas técnicas e organizativas, a par da segurança jurídica,

que irão prevenir e apoiar a deteção de eventuais incidentes.

O *Onboarding* do fornecedor/parceiros, integração de fluxos de informação e operação são outras etapas que deverão ser acompanhadas por controlos adequados, até ao próprio *offboarding* ou ativação da denominada *exit strategy*.

A UTILIZAÇÃO DE IA NA TPRM

As TPRM podem ser um estudo de caso prático de como a IA Generativa pode fazer a diferença para o negócio e sua exposição a riscos potenciais, por exemplo na avaliação de risco em ações proativas. Estes podem ser treinados para analisar feeds de notícias para identificar potenciais temas de risco e publicações nas redes sociais - relacionadas com reclamações de clientes -, para identificar padrões comuns e para avaliar a probabilidade e o impacto potencial destas reclamações na reputação da empresa. Estes podem ser usados para orientar proativamente a implementação de controles de segurança para mitigar tais riscos.

APESAR DA TECNOLOGIA PERMITIR QUE OS HUMANOS EFETUEM UMA GESTÃO DOS RISCOS DE TERCEIROS DE FORMA MAIS INTELIGENTE E EFICIENTE, ESTA ÁREA SERÁ DECISIVA PARA A SUCESSO DAS ORGANIZAÇÕES E EXIGE FORMAÇÃO E COMPETÊNCIAS.

UM DESAFIO EMERGENTE EXIGE NOVAS COMPETÊNCIAS

Em conclusão, num cenário complexo como o atual, é mais importante do que nunca que os líderes reconheçam que, apesar da organização poder terceirizar processos de negócios, não pode terceirizar a responsabilidade. Apesar da tecnologia permitir que os humanos efetuem uma gestão dos riscos de terceiros de forma mais inteligente e eficiente, esta área será decisiva para a sucesso das organizações e exige formação e competências.

A CIIWA, em conjunto com parceiros, está empenhada em desenvolver ofertas de soluções inovadoras que acrescentem valor a toda a comunidade. O TPRM será/é um tema incontornável num mundo cada vez mais digital e interdependente, baseado em cadeias de valor, assentes em cadeias de abastecimento/fornecimento e em especialização. Estar preparado para este desafio é uma necessidade e um imperativo! ◀

Referências: CyberRisk Alliance Resource, MIT/BCG, OneTrust, Prevalent, Process Unity, Threat Intelligence.

CIBERCRIME E DIREITOS HUMANOS: OS PERIGOS DO TRATADO DA ONU

Imagem: vecstock / Freepik

POR RITA SOUSA E SILVA

O TRATADO DA ONU SOBRE CIBERCRIME VISA PROPORCIONAR A COOPERAÇÃO INTERNACIONAL NA INVESTIGAÇÃO DE CASOS CRIMINAIS E OBTENÇÃO DE PROVA DIGITAL. MAS ATÉ QUE PONTO É QUE A CONVENÇÃO DEIXARÁ CAIR OS DIREITOS HUMANOS E SE TORNARÁ NUM INSTRUMENTO DE VIGILÂNCIA ESTATAL?

Com a dimensão global do cibercrime, torna-se difícil investigar casos criminais no ciberespaço sem uma cooperação internacional que permita às autoridades aplicar a lei no estrangeiro. É neste contexto que nasceu a necessidade de criar uma convenção global sobre cibercrime, elaborada pela ONU e ratificada pelos 193 estados-membros. Com visões cada vez mais polarizadas, organizações e empresas receiam que o texto trará mais perigos do que benefícios.

Não é a primeira vez que é concebido um instrumento jurídico global contra o cibercrime. Em 2001, a Convenção de Budapeste, a primeira internacional sobre a matéria, foi assinada por 64 países, contando hoje com 68, e entrou em vigor em 2004.

Países como a China, a Rússia, a Índia e o Brasil recusaram juntar-se, muito devido à "exigência de respeito dos direitos humanos" estipulada no documento, refere Pedro Verdelho, diretor do Gabinete de Cibercrime da Procuradoria-Geral da República e representante de Portugal no Comité da Convenção de Budapeste.

Reconhecendo a importância da colaboração transnacional, a Rússia, com o apoio posterior da China, propôs a criação de uma nova convenção sobre o cibercrime na Assembleia Geral das Nações Unidas – uma resolução aprovada pela ONU em maio de 2021. O projeto de tratado deverá ser aprovado em Assembleia até setembro de 2024.

Os trabalhos do comité *ad hoc* são abertos à sociedade civil, contando com a participação de ONG, universidades e empresas, que puderam candidatar-se ao estatuto de *stakeholders* em 2021, para assistir e participar ativamente nas sessões. O Center for Cooperation in Cyberspace (CCC) é a única ONG portuguesa a participar na convenção.

Terminada a penúltima ronda de negociações no início de setembro, o consenso parece estar cada vez mais longínquo. "As visões são tão díspares que nós

corremos o sério risco, hoje, de vir a não ter convenção", revela Filipe Domingues, co-fundador do CCC. "*Acaba por ser um reflexo perfeito da fragmentação geopolítica a que estamos a assistir*".

As divergências entre os estados-membros, influenciadas em parte pelos seus modelos de governação, resumem-se a duas visões: por um lado, os países do Ocidente, que defendem a "introdução de cláusulas estritas de respeito pelos direitos fundamentais, expressando aqui fortes exigências", explica Pedro Verdelho; por outro, Rússia, Irão, Egipto, Cuba, Venezuela, e outros Estados, que "mostraram maior resistência e desejo de limitar várias destas disposições".

O QUE É O CIBERCRIME?

Dois anos e seis rondas de negociação passadas, a definição do próprio conceito de cibercrime e do âmbito do tratado continuam em cima da mesa. "A dificuldade não é aparente, é real", reconhece Daniel Reis, advogado da DLA Piper. "O que está em causa é criar a primeira definição legal sobre o cibercrime".

PEDRO VERDELHO, PROCURADORIA-GERAL DA REPÚBLICA

Ainda não está acordada a lista de ações criminalizadas, estando a ser discutido a inclusão de crimes *cyber enabled* (ciberpotenciados) ou exclusivamente de *cyber dependent* (ciberdependentes), constata Filipe Domingues.

A posição é consensual no Ocidente e entre países com visões semelhantes, como o Japão, a Austrália e a Nova Zelândia, considerando que o tratado da ONU deverá incidir apenas sobre os crimes *cyber dependent*, que remetem para "aqueles crimes que precisam de

> NA CONVENÇÃO DE 2001, PAÍSES COMO A CHINA, A RÚSSIA, A ÍNDIA E O BRASIL RECUSARAM JUNTAR-SE, MUITO DEVIDO À "EXIGÊNCIA DE RESPEITO DOS DIREITOS HUMANOS".
>
> PEDRO VERDELHO, DIRETOR DO GABINETE DE CIBERCRIME DA PROCURADORIA-GERAL DA REPÚBLICA


FILIPE DOMINGUES, CO-FUNDADOR DO CCC

uma rede de computadores ou de um computador para serem cometidos", explica o co-fundador do CCC.

Porém, para outros países, o âmbito da convenção deve abranger os *cyber enabled*, ou seja, "um conjunto de ilegalidades que não dependem de tecnologias informáticas para serem cometidos, mas que podem ser potenciados por essas tecnologias".

VISÕES EM CHOQUE

"Tanto do lado ocidental como do lado não ocidental têm surgido propostas que são simplesmente inaceitáveis para os dois lados", indica Filipe Domingues.

Estados como o Vietname querem remover totalmente a linguagem de direitos humanos, enquanto o Uruguai e a Austrália visam reforçá-la. A China e outros países, por sua vez, tentaram limitar as secções sobre os direitos humanos a países que ratificaram tratados separados, como o Pacto Internacional sobre Direitos Civis e Políticos (PIDCP).

> "AS VISÕES SÃO TÃO DÍSPARES QUE NÓS CORREMOS O SÉRIO RISCO, HOJE, DE VIR A NÃO TER CONVENÇÃO"
>
> FILIPE DOMINGUES, CO-FUNDADOR DO CCC

Em janeiro, durante as negociações em Viena, a delegação chinesa propôs uma redefinição do conceito de cibercrime para incluir a divulgação de *fake news* online, enquanto diplomatas do Paquistão e do Irão procuraram introduzir uma secção que estabeleceria os insultos religiosos como um cibercrime.

"A criminalização de comportamentos como as *fake news* ou insultos religiosos pode atentar gravemente contra a liberdade de expressão, limitando a liberdade de opinião, por exemplo, nas redes sociais", alerta Francisco Pimenta, advogado da CCA Law Firm.

Muitas destas propostas foram deixadas cair pelo grupo de trabalho ao longo das sessões, não reunindo um "consenso mínimo". Pedro Verdelho expõe que, no entanto, "algumas delegações, com destaque para a da Federação Russa, insistiram em propostas suas anteriores – mesmo sabendo que a maioria

> "O QUE ESTÁ EM CAUSA É CRIAR A PRIMEIRA DEFINIÇÃO LEGAL SOBRE O CIBERCRIME".
>
> DANIEL REIS,
> ADVOGADO DA DLA PIPER

dos Estados não as subscreve. Esta abordagem gerou uma atmosfera geral de inflexibilidade".

DIREITOS HUMANOS EM PERIGO

O projeto de tratado tem sido alvo de fortes críticas, particularmente pela parte de várias organizações de direitos humanos. Durante as negociações mais recentes, as preocupações cresceram de tal forma que várias ONG organizaram uma conferência de imprensa para discutir os perigos do texto, receando a expansão do poder de vigilância dos governos e o fornecimento de ferramentas de repressão às ditaduras.

Entre as várias disposições contestadas, o Artigo 23.º é referido frequentemente por trazer "consigo a possibilidade de aumentar a vigilância sobre os cidadãos de uma forma preocupante", identificando a "necessidade de assegurar a recolha de prova digital relacionada com qualquer tipo de crime, independentemente da sua gravidade ou do crime estar associado a um sistema informático", adverte Jorge Pinto, presidente da Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI).

Ademais, no seu estado atual, a convenção permite aos governos "o acesso em tempo real, de dados de tráfego e comunicações, sem necessidade de prévia autorização judicial", mesmo em investigações de "crimes que nem sequer assumem natureza informática pura" e "desde que para fins de recolha de prova de natureza informática/eletrónica", analisa

DANIEL REIS, ADVOGADO DA DLA PIPER

Francisco Pimenta. Para o advogado, isto "permite um exercício de poder de vigilância dos estados com um espectro tão alargado que quase resulta num autoritarismo informático".

Uma proposta controversa apresentada foi a realização de investigações criminais em total sigilo, sem notificar os alvos de vigilância que os seus dados estão a ser acedidos. Em contraste, na penúltima sessão de negociações, a Comissão Europeia "seguramente consciente do que estava


FRANCISCO PIMENTA, CCA LAW FIRM

a fazer, fez uma proposta tão radical na proteção dos dados pessoais, que, se fosse tornada lei, impediria qualquer investigação criminal", relata Filipe Domingues.

A proposta determinava que, cada vez que um país solicitasse um pedido de preservação de dados, "haveria uma *due diligence* para garantir que o pedido estava de acordo com toda a legislação em matéria de direitos humanos, de proteção da privacidade". Com o tempo que demoraria, "o período habitual de preservação dos dados expiraria e, quando estivesse terminada a *due diligence*, já não haveria dados para investigar", completa.

Para além disto, a falta de controlo na colaboração transfronteiriça entre governos poderá afetar a proteção de dados pessoais e a privacidade dos cidadãos em vários níveis, colocando em causa os padrões de proteção de dados existentes no mundo. "É bastante claro que o texto atual não tem salvaguardas suficientes para proteger os cidadãos de cada país contra uma utilização indevida dos seus dados pessoais", defende Jorge Pinto.

Para o presidente da AP2SI, o texto atual "abre a possibilidade de abuso por parte de Estados com poucos controlos ou verificações", como, por exemplo, "a recolha de informação sobre dissidentes ou ativistas políticos que estejam localizados noutros países".

INVESTIGAÇÃO E EMPRESAS TECNOLÓGICAS

A ameaça ao trabalho dos investigadores de cibersegurança e dos hackers éticos é outra preocupação sentida por várias organizações e empre-

> "A CRIMINALIZAÇÃO DE COMPORTAMENTOS COMO AS FAKE NEWS OU INSULTOS RELIGIOSOS PODE ATENTAR GRAVEMENTE CONTRA A LIBERDADE DE EXPRESSÃO, LIMITANDO A LIBERDADE DE OPINIÃO, POR EXEMPLO, NAS REDES SOCIAIS",
>
> FRANCISCO PIMENTA, ADVOGADO DA CCA LAW FIRM

sas, devido às restrições impostas na investigação de vulnerabilidades.

Está em vias de discussão "a necessidade de o recurso pelos governos às ferramentas de investigação resultantes da Convenção ser sempre precedido de autorização judicial prévia", esclarece Fernando Pimenta, sendo o pedido instruído "como uma descrição e fundamentação do razão da necessidade de acesso aos dados solicitados".

JORGE PINTO, AP2SI

A autorização legal em questão seria concedida mediante "um juízo de proporcionalidade entre a necessidade de intrusão nos direitos de privacidade dos indivíduos e a essencialidade para a investigação", acrescenta.

Ainda mais, Fernando Pimenta explica que as empresas tecnológicas poderiam ver a sua atividade a ser "livremente controlada nestes termos" e, devido à sua base informática, "bloqueada por parte das entidades inspetivas de cada um dos estados-membros" ou até estrangeiras, graças à "livre partilha de dados obtidos no âmbito destas investigações".

Para o advogado, isto poderá conduzir a um "estado de quase autoritarismo digital, com um controlo de informação e dados imediato, constante e livre de quaisquer ónus".

A Microsoft foi a primeira grande empresa de tecnologia a manifestar-se contra a convenção da ONU. No final de agosto, Amy Hogan-Burney, uma representante do departamento de política de cibersegurança da empresa, recorreu ao Linkedin para tecer duras críticas ao projeto de tratado, considerando-o demasiado amplo e aberto a interpretação.

> O ARTIGO 23.º É REFERIDO FREQUENTEMENTE POR TRAZER "CONSIGO A POSSIBILIDADE DE AUMENTAR A VIGILÂNCIA SOBRE OS CIDADÃOS DE UMA FORMA PREOCUPANTE", IDENTIFICANDO A "NECESSIDADE DE ASSEGURAR A RECOLHA DE PROVA DIGITAL RELACIONADA COM QUALQUER TIPO DE CRIME, INDEPENDENTEMENTE DA SUA GRAVIDADE OU DO CRIME ESTAR ASSOCIADO A UM SISTEMA INFORMÁTICO".
>
> JORGE PINTO, PRESIDENTE DA ASSOCIAÇÃO PORTUGUESA PARA A PROMOÇÃO DA SEGURANÇA DA INFORMAÇÃO (AP2SI).

Na sua publicação do Linkedin, Hogan-Burney afirma que "os hackers éticos que trabalham para identificar vulnerabilidades, simular ciberataques e testar as defesas do sistema precisam de ser protegidos" e muitas disposições "não incluem uma referência à 'intenção criminosa', o que garantiria que atividades como testes de penetração permanecessem legais".

FUTURO DA CONVENÇÃO É INCERTO

As profundas divisões entre os estados-membros aparentam não ser conciliáveis na matéria de direitos humanos e vigilância governamental. "Ainda existem divergências fortes, que terão inevitavelmente de ser debatidas e resolvidas", prevê Pedro Verdelho. "Seria preferível aprovar o projeto da futura Convenção por consenso. Mas, quanto a alguns aspetos, a votação parece inevitável, para evitar o colapso do processo. A votação conduzirá a dificuldades na aceitação e ratificação subsequente pelos Estados-Membros".

Filipe Domingues revela que o processo está "muito atrasado". Na sexta ronda de negociações, a presidente do comité acrescentou nove horas extra de reuniões. A sétima e última, que ocorrerá entre janeiro e fevereiro de 2024, deveria servir somente para "coroar ou matar o tratado". No entanto, adianta que "não vai ser assim, porque o texto está todo vermelho, cheio de *track changes*".

Face à dificuldade em chegar a consenso, a solução poderá passar pela criação de um tratado com condições mínimas: "as indicações que nós temos é de

que ainda não caiu totalmente a hipótese de ter uma convenção minimalista, baseada em denominadores comuns mínimos, à qual poderá ser mais tarde, seja daqui a dez anos, seja daqui a 20, acrescentado um protocolo adicional", revela o co-fundador do CCC.

O futuro da convenção da ONU sobre cibercrime não é certo e o seu sucesso poderá estar em risco. "Se nós, por um lado, estamos otimistas em relação à capacidade que os estados ocidentais têm de proteger os nossos direitos humanos e as nossas liberdades e garantias, não estamos tão otimistas em relação a um desfecho positivo deste tratado", confessa Filipe Domingues. "Continua a haver atores estatais e não estatais que não tem problema rigorosamente nenhum em deitar este processo abaixo, desde que isso impeça a agenda de estados como a Rússia e a China". ◀

OBRIGADO POR TER LIDO A

IT Insight SECURITY

Se ainda não é um leitor registado da IT Insight Security e para ter acesso a todo o nosso conteúdo registe os seus dados profissionais aqui

Conheça a política de privacidade da IT Insight Security aqui

IT Insight SECURITY

PUBLISHER: Jorge Bento
DIRETOR : Rui Damião - rui.damiao@medianext.pt
ANCHOR: Henrique Carreiro
REDAÇÃO: Margarida Bento, Marta Quaresma Ferreira, Rita Sousa e Silva
BUSINESS DEVELOPMENT:
Beatriz Salzedas - (+351) 910 788 082 - beatriz.salzedas@medianext.pt
João Calvão - (+351) 910 788 413 - joao.calvao@medianext.pt
MARKETING COMMUNICATIONS ASSISTANT:
Rita Rodrigues - (+351) 912 971 161 - rita.rodrigues@medianext.pt
ARTE E PAGINAÇÃO: Teresa Rodrigues
FOTOGRAFIA: Rui Santos Jorge
DESENVOLVIMENTO WEB: Global Pixel
COLABORARAM NESTE NÚMERO: Carlos Silva, Idalécio Lourenço, Miguel Gonçalves

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

CEO: Pedro Botelho

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

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

Consulte aqui o Estatuto Editorial

IT Insight Security é membro de:

ASSOCIAÇÃO PORTUGUESA DE IMPRENSA
acepi ASSOCIAÇÃO DO COMÉRCIO ELECTRÓNICO E PUBLICIDADE INTERACTIVA
CIWA COMPETITIVE INTELLIGENCE & INFORMATION WARFARE ASSOCIATION

Editado por:
media NEXT