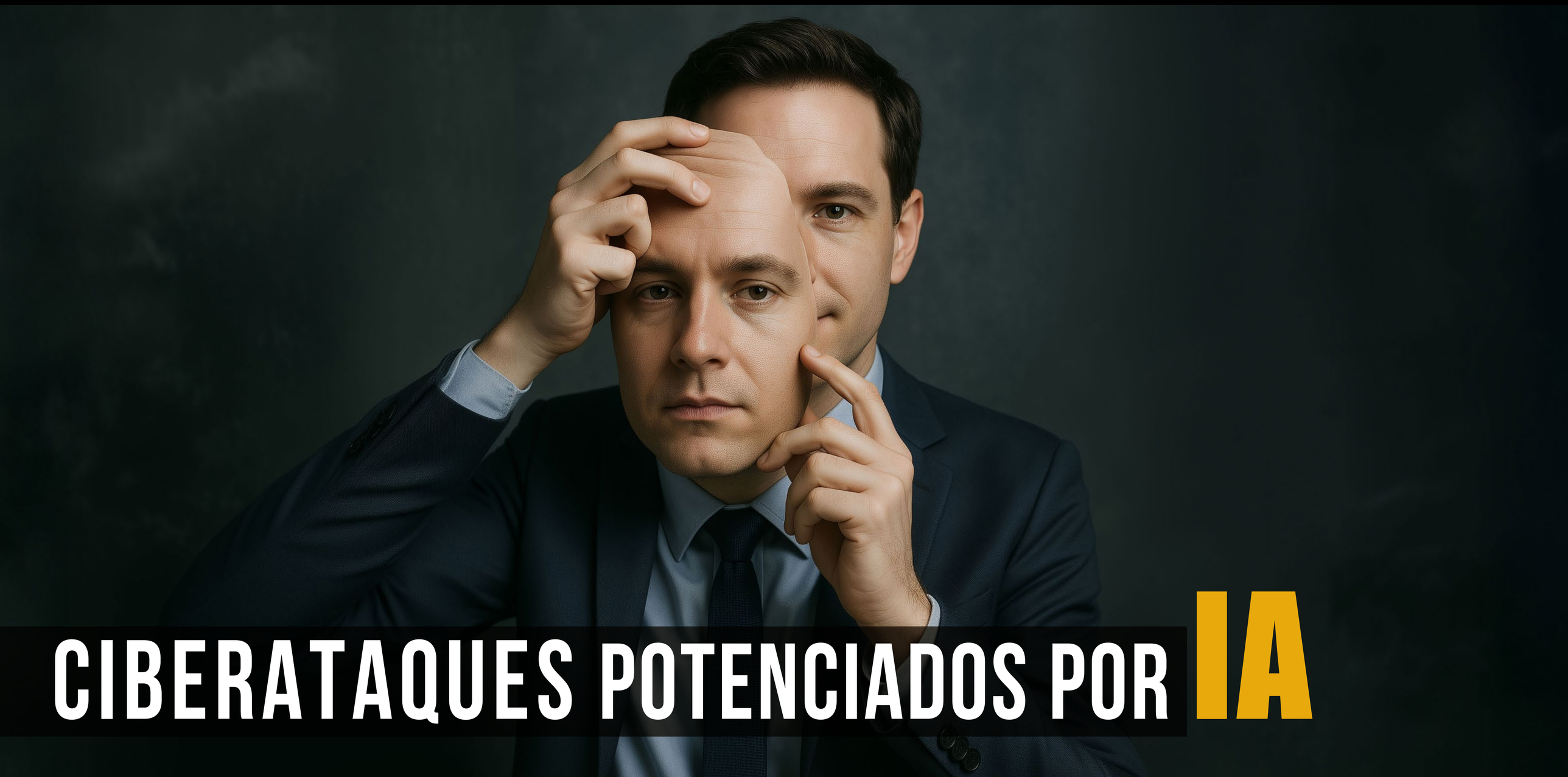
IT Insight SECURITY

#26 OUTUBRO 2025



CIBERATAQUES POTENCIADOS POR IA

We live and breathe Security

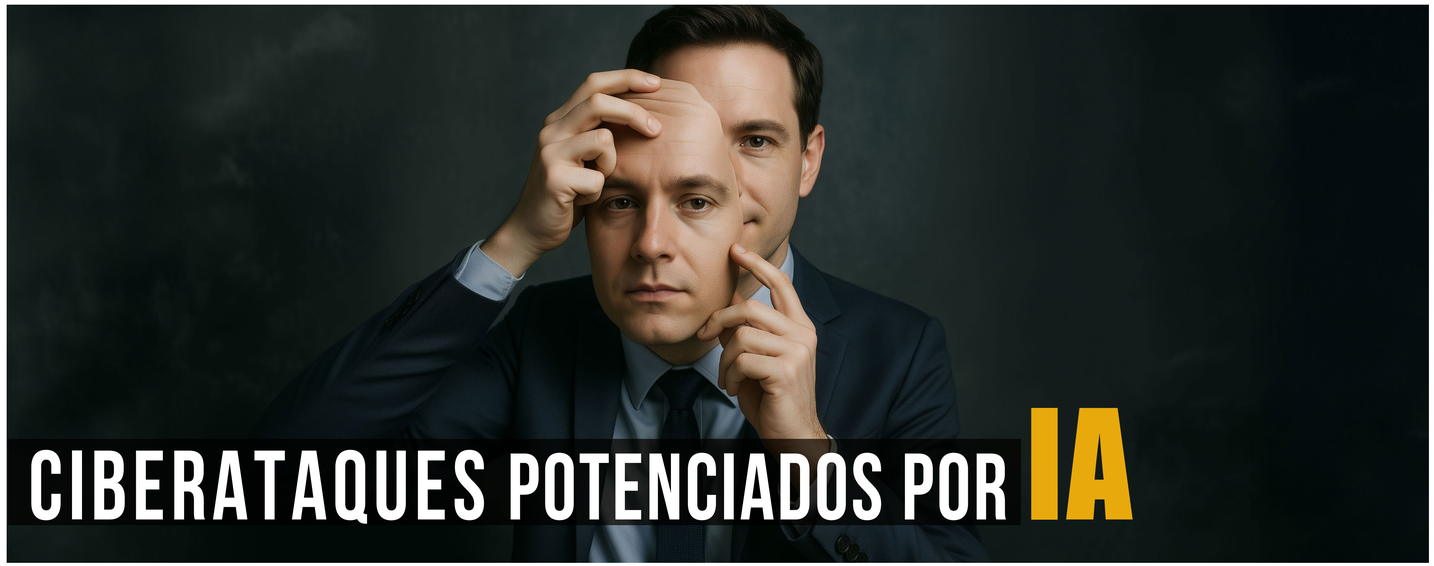
Soluções de proteção, monitorização e mitigação de riscos, incluindo a formação de colaboradores para uma postura de segurança mais eficaz.

Visite: claranet.com/pt/security

claranet | Make modern happen®

BROWSE

COVER



CHAT

▶ CARLOS SANTOS SILVA, BANCO CTT



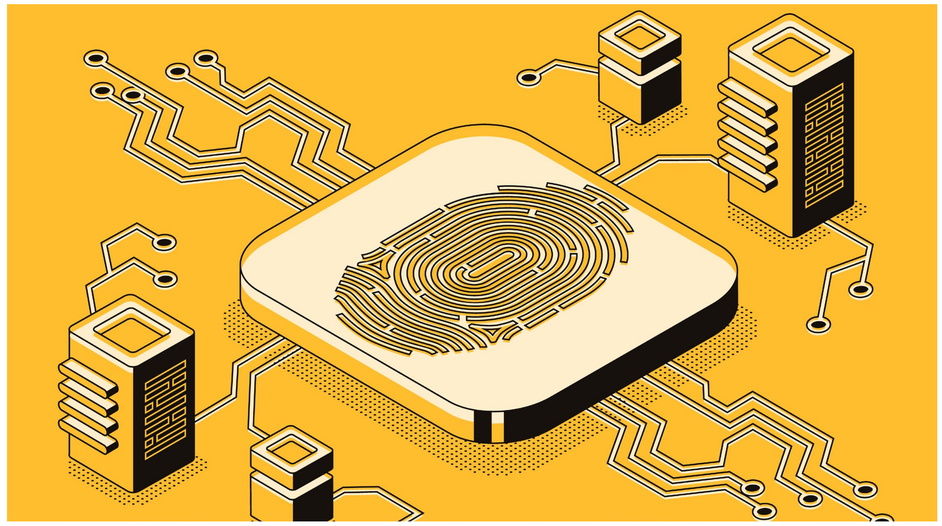
EXPERT

▼ NUNO GOES, CIIWA



BRAVE NEW WORLD

▼ DIGITAL FORENSICS AND INCIDENT RESPONSE



BLUE TEAM

▼ LAYER8



RISK

▼ NIS2 EM PORTUGAL



CYBER protecht

Antecipamos. Atuamos. Protegemos.

Com o Cyber Protecht combinamos plataformas com inteligência artificial, processos e equipas certificadas e altamente qualificadas.
Analisamos e mitigamos ciberataques em tempo real, e monitorizamos continuamente os seus sistemas, ajudando a prevenir incidentes e garantindo uma resposta imediata 24 horas por dia.
Uma solução chave-na-mão, sustentada na qualidade e experiência MEO Empresas.



MEO empresas

contacte o seu gestor

meoempresas.pt

S.LABS

balwurk cyber security
claranet®
CSO chief security officers
DIVULTEC
IP Telecom
MEO empresas
PROLOGIN PRODUTOS E SERVIÇOS
redShift
SECURNET ALWAYS ONLINE | ALWAYS SECURE
VARONIS
VisionWare since 2005

S.LABS

O S.Lab ou Security Labs é um espaço de criação e partilha dentro da IT Security, onde exploramos e desenvolvemos ideias em colaboração com os nossos parceiros. Aqui, transformamos conceitos em conteúdos relevantes e envolventes, seja através de artigos, vídeos, webinars, podcasts ou conferências. O nosso objetivo é dar forma a ideias que não cabem nos formatos tradicionais, criando novas formas de comunicar e inovar.

Security Supply Chain

em Conformidade com a SRI2 (NIS2)

Proteja o *Software* contra potenciais ameaças em todas as fases do seu ciclo de vida.

➔ Realizamos uma análise completa da Composição do ***Software (SCA)*** para identificar as componentes de código aberto e as suas potenciais vulnerabilidades.

➔ Geramos o SBOM ***(Software Bill of Materials)***, oferecendo transparência e rastreabilidade de cada elemento do software

➔ A nossa abordagem estende-se à análise da **cadeia de fornecimento de software,** identificando e mitigando os riscos associados a componentes de terceiros.

mail@balwurk.com

balwurk cyber security

POR FIM

RUI DAMIÃO



A aprovação da transposição da NIS2 em Portugal pela Assembleia da República representa um marco crítico que chegou com 11 meses de atraso relativamente ao prazo europeu de outubro de 2024.

O novo regime jurídico de cibersegurança introduz alterações que transcendem a simples conformidade regulamentar, redefinindo fundamentalmente o panorama de responsabilidades em cibersegurança.

A responsabilização pessoal dos órgãos de gestão constitui uma das mudanças mais disruptivas. Ao contrário do regime anterior, onde a responsabilidade se diluía nos departamentos técnicos, a NIS2 coloca os gestores de topo na linha da frente da cibersegurança organizacional. Esta responsabilização não é meramente simbólica; os gestores podem enfrentar suspensões temporárias de funções, declarações públicas de responsabilidade por incidentes e, em casos de negligência grave, sanções administrativas previstas na lei, sem prejuízo de eventuais consequências penais decorrentes de outros diplomas legais. Para os responsáveis de cibersegurança, isto representa tanto uma oportunidade quanto um desafio: o acesso direto ao *board* tornou-se inevitável, mas com ele vem a pressão de demonstrar valor tangível e resultados mensuráveis.

O reforço das competências do Centro Nacional de Cibersegurança como autoridade supervisora, aliado à integração com outros regulamentos como RGPD e Diretiva CER, cria um ecossistema regulamentar mais coeso, mas também mais complexo. Esta convergência regulamentar exige uma abordagem holística à conformidade, onde os silos organizacionais se tornam contraproducentes.

Para as organizações que têm esperado pela clareza legislativa, o momento da decisão chegou. A NIS2 não é apenas mais uma obrigação regulamentar: é a formalização de uma realidade onde a cibersegurança se tornou indissociável da estratégia empresarial. Para quem gere a cibersegurança, representa a oportunidade de elevar a cibersegurança ao nível estratégico que sempre mereceu. ◀

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



SHAI-HULUD:

UM WORM DE SUPPLY CHAIN COM POSSÍVEL GÉNESE EM AI

HENRIQUE CARREIRO

O npm (Node Package Manager), gerido pela npm, inc, uma subsidiária do GitHub é o maior gestor de bibliotecas JavaScript do mundo e constitui, desde há anos, uma infraestrutura central para o desenvolvimento de software. Em vez de escreverem cada componente de raiz, os programadores recorrem a blocos de código JavaScript — *packages* — partilhados por outros *developers*. Esta lógica de reutilização permite velocidade e inovação, mas também cria dependências invisíveis: cada aplicação moderna assenta em centenas ou milhares de *packages* publicados por desconhecidos, confiando que estão íntegros, que não escondem armadilhas e que não se transformam em vetores de ataque. O npm não é apenas um repositório; é a engrenagem que liga uma parte crítica do software atual.

Foi precisamente esta posição central que tornou tão grave o episódio registado em setembro de 2025, quando pelo menos 187 *packages* foram comprometidos por um worm

auto-replicante batizado de Shai-Hulud. Ao contrário de malware tradicional que tenta ocultar-se, este código rouba tokens e outras credenciais e expõe-nas publicamente, criando de forma automática repositórios GitHub com o nome da criatura retirada de *Dune*. Não é apenas um ataque silencioso: é um gesto que prefere anunciar-se, exibir os despojos e deixar um rasto visível em cada movimento.

O FUNCIONAMENTO INTERNO

O mecanismo do Shai-Hulud é ao mesmo tempo simples e devastador. Sempre que um *package* infetado é instalado, o worm procura no ambiente local tokens de autenticação npm. Se encontra um válido, modifica até vinte *packages* controlados por esse token, injeta neles o seu código e publica imediatamente novas versões contaminadas no repositório. Não há *command and control server*, não há centro a desligar: cada *developer* comprometido torna-se veículo da propagação. A estratégia replica a lógica biológica de um vírus, mas aplicada ao tecido da cadeia de fornecimento do software.

Para ampliar o alcance, o malware integra o TruffleHog, uma ferramenta concebida para auditorias de segurança que aqui serve para procurar API keys, chaves SSH, tokens de GitHub e credenciais de cloud AWS, Azure e Google Cloud.

Segundo a análise da Palo Alto, o worm não se limita às variáveis de ambiente: percorre ficheiros de configuração e tira partido de GitHub Actions para automatizar tanto a extração como a exposição das credenciais encontradas. O resultado é um ataque que não compromete apenas bibliotecas de código, mas também infraestruturas inteiras ligadas a *pipelines* de CI/CD e serviços de cloud em produção.

SINAIS PRECURSORES

Este não foi o primeiro aviso. Poucas semanas antes, uma campanha de phishing dirigida a *developers* do npm introduzira falsos pedidos de atualização de MFA, que resultaram na publicação de malware em dezenas de *packages* com o objetivo de desviar pagamentos em criptomoedas. Em agosto, o nx toolkit, com milhões de *downloads* semanais, tinha sido adulterado para recolher credenciais e expô-las em repositórios GitHub públicos. Mas nesse caso não havia capacidade de auto-propagação. O Shai-Hulud vai mais longe: cada credencial roubada torna-se "combustível" para comprometer novos *packages*, desencadeando um efeito dominó que pode multiplicar-se sem controlo.

Em *Dune*, os vermes de areia deslocam-se debaixo da superfície até que uma vibração os chama à superfície. A metáfora não é forçada: a instalação banal de um *package* é a vibração que faz emergir o verme. O que parecia ter-

"CREDENCIAIS EXPOSTAS PODEM PERMITIR ACESSO A BUCKETS DE CLOUD, INSTALAÇÃO DE RANSOMWARE, MINERAÇÃO DE CRIPTOMOEDAS OU ATÉ DESTRUIÇÃO DELIBERADA DE AMBIENTES DE PRODUÇÃO"

reno estável revela-se um deserto instável, onde a confiança assenta em areia movediça. Cada comando de instalação pode tornar-se o passo em falso que reativa o ciclo.

IMPACTO IMEDIATO

Entre os afetados esteve a CrowdStrike, que viu cerca de 25 *packages* temporariamente comprometidos. A empresa reagiu depressa, retirando-os do repositório, rodando chaves e garantindo que os produtos principais não estavam em risco. Ainda assim, o episódio expôs fragilidades profundas. Plataformas como a StepSecurity confirmaram que o worm explorava *workflows* do GitHub para publicar repositórios de forma automática. O ataque mostrou que a cadeia de fornecimento não é apenas vulnerável: é por natureza fértil em pontos de entrada, porque cada token válido concede um poder quase ilimitado de publicação.

As potenciais consequências vão muito além da adulteração de bibliotecas. Credenciais expostas podem permitir acesso a *buckets* de cloud, instalação de ransomware, mineração de criptomoedas em larga escala ou até destruição deliberada de ambientes de produção. O Shai-Hulud não se limita a explorar o código; ameaça diretamente as infraestruturas que suportam serviços críticos.

O PROBLEMA ESTRUTURAL

Investigadores como Nicholas Weaver, da Universidade de Berkeley, descrevem este episódio como “um ataque à cadeia de fornecimento que executa outro ataque à cadeia de fornecimento”. O aparente paradoxo ilustra a fragilidade do modelo: um sistema que privilegia velocidade e automação sobre escrutínio humano, em que um único token pode publicar dezenas de *packages* sem qualquer barreira adicional. Enquanto a publicação em npm não exigir validação manual reforçada por mecanismos de autenticação antifraude, ataques deste género continuarão a repetir-se. A recomendação é clara: reduzir o alcance dos tokens, alterá-los frequentemente, aplicar MFA resistente a phishing e auditar cada dependência instalada.

DETALHES ADICIONAIS PERTURBADORES

A Palo Alto identificou ainda um elemento curioso: com confiança moderada, considera que partes do bash script malicioso podem ter sido geradas por um modelo de linguagem (LLM), dedução baseada no estilo dos comentários e no uso insólito de emojis no código. Isto sugere que a automação não está apenas no modo como o worm se replica, mas também na forma como foi escrito, antecipando uma tendência em que atacantes recorrem a ferramentas de IA para acelerar a produção de variantes, multiplicando o número de mutações possíveis e reduzindo custos.

Além disso, o relatório da Palo Alto (Unit 42) publicou hashes de ficheiros infetados, identificadores de repositórios e indicadores de compromisso, permitindo que equipas de segurança detetem instâncias do ataque. Também forneceu orientações práticas: mudar de imediato todas as credenciais (NPM tokens, chaves SSH, GitHub PATs e API keys), auditar ficheiros, em busca de versões maliciosas, rever *workflows* do GitHub em busca de automatismos inesperados, e reforçar políticas de obrigatoriedade de MFA em todas as contas críticas.

> O CÓDIGO PODE PERMANECER LATENTE, PRONTO A REINICIAR O CICLO ASSIM QUE UM DEVELOPER INSTALE INADVERTIDAMENTE UM PACKAGE COMPROMETIDO OU REUTILIZE UM TOKEN EXPOSTO

DORMÊNCIA NÃO É ERRADICAÇÃO

O endereço usado para exfiltração foi, entretanto, suspenso e o ritmo de propagação parece ter abrandado. Mas dormência não significa erradicação. O código pode permanecer latente, pronto a reiniciar o ciclo assim que um *developer* instale inadvertidamente um *package* comprometido ou reutilize um token exposto. Mais do que a astúcia de um atacante, este episódio revela a vulnerabilidade estrutural de uma infraestrutura onde confiança e automação se sobrepõem a controlo humano.

Tal como no deserto de Arrakis, nunca se sabe que vibração fará emergir novamente o verme. O que parecia firme é apenas superfície, e o Shai-Hulud recorda-nos que, na cadeia de fornecimento digital, o risco não está em incidentes pontuais, mas na própria lógica que permite multiplicá-los. ◀

DIVULTEC

Ao seu lado, nos desafios mais exigentes.

divultec.pt

Porto | Rua Escultor Barata Feyo 136, Paranhos • **Lisboa** | Av. Tomás Ribeiro 45, 3º, Carnaxide • info@divultec.pt | 220 162 410

PROGRAMA DA IT SECURITY CONFERENCE ESTÁ FECHADO



No próximo dia 9 de outubro todos os caminhos vão dar ao Clube – Monsanto Secret Spot, em Lisboa. O Dr. Ron Ross, ex-Fellow do NIST, é o convidado principal da quarta edição do evento.

O programa da IT Security Conference 2024 está oficialmente fechado. A quarta edição da conferência da revista IT Security realiza-se no próximo dia 9 de outubro, n'O Clube – Monsanto Secret Spot, em Lisboa.

Com a agenda fechada, destaque para a participação do Dr. Ron Ross como um dos *keynotes* principais do evento. Antes, e na abertura da conferência, recebemos o coordenador do Centro Nacional de Cibersegurança, Lino Santos.

Ao longo do dia serão vários os *keynotes* a passar pelo auditório principal da IT Security Conference, com destaque para as apresentações de Jorge Vicente, Diretor Segurança da Informação do Lidl Portugal, David Marques, Head of Cibersecurity do Grupo Nabeiro e Sérgio Trindade, CIO, CDO e CISO das Águas do Tejo Atlântico – Águas de Portugal.

Como habitual, a IT Security Conference 2025 conta com quatro mesas-redondas, dedicadas aos temas que marcam o atual panorama da cibersegurança: Jorge Fernandes, da CMVM, Rui Alves, da Vieira de Almeida, Miguel Gonçalves, da CUF e David Grave, da Claranet Portugal; Paulo Martins, do SL Benfica, Miguel Gonçalves, da Vinci Energies, Luís Amorim, da Medialivre e Rui Antunes, da Cisco; José Cabrera, da Makro Portugal, Luís Morais, da Galp, Orlindo Santos, da Glintt e Bruno Castro, da VisionWare; Ivo Rosa, da EDP, Carlos Silva, do Banco CTT, Luís Duarte, da Agência Portuguesa do Ambiente e António Correia, da WatchGuard.

O encerramento no auditório principal ficará a cargo do Major-General João Vieira Borges.

No palco das Technical Tracks, a IT Security Conference vai contar com uma sessão especial de abertura, a cargo do Contra-Almirante António Gameiro Marques, ex-diretor-geral do Gabinete Nacional de Segurança. A sessão da tarde abre com o keynote de Scott Nichols, especialista em ameaças de Estados-nação.

IP Telecom

Housing
IPT Cloud

CloudSolutions
Housing
Hosting

Nato Secret

EU Secret

Rede Nacional CSIRT

gaia-x

LIGAMOS NEGÓCIOS

Telecomunicações | Data Center | Cloud Computing



www.iptelecom.pt

comercial@iptelecom.pt

PORTUGAL REGISTA AUMENTO DE INCIDENTES E CONSOLIDAÇÃO DE CIBERAMEAÇAS

O mais recente relatório do Centro Nacional de Cibersegurança revela um crescimento significativo dos incidentes em 2024 e projeta um 2025 marcado pela exploração de vulnerabilidades.



O Centro Nacional de Cibersegurança (CNCS) publicou a sexta edição do relatório Cibersegurança em Portugal – Riscos & Conflitos, que traça um retrato inquietante da evolução do ciberespaço nacional em 2024 e das ameaças que marcam 2025. Os dados revelam um aumento expressivo no número de incidentes, a sofisticação crescente dos cibercriminosos e a consolidação da Inteligência Artificial (IA) como uma tecnologia crítica tanto para a defesa como para o ataque.

"Em 2024, o número de incidentes de cibersegurança aumentou significativamente", pode ler-se no documento, com o CERT.PT a registar um total de 11.163 casos. Este valor inclui dados de fontes automatizadas, mas mesmo excluindo esses registos, o número de incidentes ascendeu a 2.758 – um aumento de 36% face a 2023. O CNCS destaca que se trata de um regresso à tendência de crescimento acelerado observada ao longo da última década.

Os incidentes mais relevantes no ano passado estiveram ligados a código malicioso, em particular ransomware e infostealers, frequentemente acompanhados por fugas massivas de credenciais. Entre os casos destacados figura um ataque de ransomware contra uma entidade da administração pública central, cujo impacto se estendeu a todo o país, bem como as falhas globais resultantes de uma atualização crítica de software de EDR, que deixaram entidades públicas e privadas indisponíveis.

As campanhas de phishing e smishing mantiveram-se como a ameaça mais frequente, o que confirma a perceção da comunidade de cibersegurança: 92% dos profissionais inquiridos em 2024 consideraram que o risco de incidentes aumentou, e 90% acreditam que vai continuar a crescer em 2025. A engenharia social e as burlas online surgem também entre os métodos mais usados para comprometer vítimas.

SECURNET

ALWAYS ONLINE | ALWAYS SECURE

MAIS DO QUE UMA MARCA, UM PARCEIRO DE CONFIANÇA.

☆☆ **HPE 'FY24**	Parceiro do Ano - HPE GreenLake Parceiro do Ano - HPE Aruba Networking
☆ **Veeam Software**	The best COM partner of the year 2024, Portugal
☆☆ **IT Channel Award2025**	Parceiro Cybersecurity Parceiro do Ano

A TECNOLOGIA EVOLUI. E NÓS TAMBÉM.

PORTO +351 224 673 094
LISBOA +351 213 622 204

CISA ALERTA PARA EXPLORAÇÃO ATIVA DE VULNERABILIDADES CRÍTICAS NO IVANTI EPMM

Através das falhas identificadas, os atacantes obtiveram acesso a servidores, executaram scripts maliciosos, fizeram reconhecimento de rede e roubaram credenciais LDAP.

A CISA publicou informações técnicas sobre malware utilizado em ataques que exploraram duas falhas críticas no Ivanti Endpoint Manager Mobile (EPMM), identificadas como *CVE-2025-4427* (desvio de autenticação) e *CVE-2025-4428* (execução remota de código). As vulnerabilidades, descobertas em bibliotecas de código aberto integradas no EPMM, podem ser encadeadas para permitir RCE não autenticado.

A CISA recomenda a atualização imediata para versões corrigidas do Ivanti EPMM (11.12.0.5, 12.3.0.2, 12.4.0.2, 12.5.0.1 ou superiores), a aplicação de restrições e medidas adicionais de monitorização em sistemas de gestão de dispositivos móveis e a adoção de boas práticas de segurança para mitigar riscos de exploração futura. ◀

NOVA BOTNET UTILIZA ROUTERS E FALHAS DE DNS PARA CAMPANHAS GLOBAIS DE SPAM

Uma campanha botnet aproveita configurações incorretas de DNS e milhares de routers comprometidos para enviar emails maliciosos em escala global, o que dificulta a deteção por filtros tradicionais.



Investigadores da Infoblox detetaram uma campanha botnet que combina dispositivos de rede sequestrados e falhas de DNS para impulsionar operações massivas de spam. Mais de 13 mil routers MikroTik comprometidos funcionam como proxies SOCKS4, permitindo que emails maliciosos passem despercebidos por filtros tradicionais e cheguem às caixas de entrada empresariais.

A campanha começou com o envio de emails que pareciam faturas de transporte legítimas e cada um continha um arquivo ZIP com um script JavaScript malicioso. Quando executado, este script inicia um loader em PowerShell que se conecta a um servidor de comando e controlo (C2) com histórico de ligações a agentes de ameaças russos.

A botnet não explora uma vulnerabilidade específica, mas sim configurações padrão ou mal protegidas dos routers MikroTik. ◀

20 anos

VisionWare

since 2005

A **missão da VisionWare** é contribuir para o Sucesso das organizações, aumentando a sua cultura e maturidade em Segurança da Informação.

+100
colaboradores

+200
clientes ativos

5000
projetos desenvolvidos

Os nossos serviços

- Cyber Defense Operations
- Privacy & Legal
- Cybersecurity
- Professional Services
- Ethics & Compliance
- Strategic Intelligence & Risk Analysis
- Forensic Investigations
- VisionWare Academy

Challenging an Unsafe World

Porto | Lisboa | Praia | Mindelo

geral@visionware.pt

+351 225 323 740

SCAN ME

visionware.pt

FALHA CRÍTICA EM DISPOSITIVOS ANDROID EXPLORADA EM ATAQUES ZERO DAY

A Samsung lançou uma atualização para mitigar uma vulnerabilidade grave que estava a ser explorada em ataques direcionados a utilizadores de dispositivos Android.



A Samsung corrigiu uma vulnerabilidade de execução remota de código, identificada como *CVE-2025-21043*, que estava a ser ativamente explorada em ataques de zero day contra dispositivos Android da marca. A vulnerabilidade foi descoberta pela Meta e pelo WhatsApp e afetava dispositivos com Android 13 ou posterior. De acordo com a Samsung, o problema afetava a biblioteca de análise de imagens, desenvolvida pela Quramsoft, utilizada em vários serviços de mensagens. A falha estava associada a uma vulnerabilidade de gravação fora dos limites, permitindo que os atacantes executassem código malicioso remotamente em dispositivos vulneráveis. A Samsung confirmou a existência de um *exploit* ativo para a falha, mas não detalhou se os ataques estavam a afetar apenas utilizadores do WhatsApp em dispositivos Android da marca.

FALTA DE TALENTO EM CIBERSEGURANÇA LEVA EMPRESAS DA EMEA A RECORRER A SOLUÇÕES DE RISCO

Estudo da Insight Enterprises revela que 64% das empresas recorrem a soluções temporárias para colmatar escassez de competências em cibersegurança nas empresas da região EMEA.



Uma crise crescente de competências em cibersegurança está a obrigar 64% das organizações da Europa, Médio Oriente e África (EMEA) a recorrer a atalhos arriscados e soluções temporárias para responder às exigências de segurança. A conclusão é de um estudo recente da Insight Enterprises.

No Reino Unido, o cenário é ainda mais grave: 67% das empresas reportam falta de competências, com mais de metade (56%) a classificar o impacto como "grave" ou "significativo".

Apenas 24% dos decisores de IT da região EMEA afirmam ter competências internas suficientes para acompanhar a evolução das ameaças. Como consequência, 57% das empresas admitem atrasos em iniciativas críticas e dificuldades em cumprir requisitos de conformidade.



09 OUT 2025 | LISBOA

A VOZ DOS CISO

A quarta edição da IT Security Conference 2025 já tem data marcada para **09 de outubro, em Lisboa**, onde os temas mais relevantes sobre o ecossistema da cibersegurança voltam a estar em debate e análise pelos mais proeminentes especialistas da área.

MARQUE A DATA NA SUA AGENDA.

PARCEIROS:

Diamond

paloalto NETWORKS + inspiring solutions

Platinum

ACS Agile Cybersecurity Solutions · CHECK POINT · claranet · elred · FORTINET · HPE · pwc · SOPHOS

Golden

FUJIFILM · hp · Ingecom IGNITION An Exclusive Networks Company · LOGICALIS Architects of Change · ManageEngine · redShift · tenable · SECURNET ALWAYS ONLINE | ALWAYS SECURE · VARONIS

Silver

ART RESILIA · balwurk cyber security · cisco · devoteam Cyber Trust · DIVULTEC · IDW YOUR BUSINESS · OUR CHALLENGE · kaspersky · oramix EXPERT SERVICES · TD SYNNEX · VisionWare since 2005 · V-Valley

Bronze

WatchGuard · anubisnetworks · CROSSJOIN · eset Cybersecurity Progress. Protected. · factis® · PingIdentity

Institutional Partners

CNCS Centro Nacional de Cibersegurança PORTUGAL · CIWA

GRUPO DE RANSOMWARE AKIRA EXPLORA FALHAS EM FIREWALLS

O grupo de ransomware explora falhas em dispositivos SonicWall SSL VPN através de credenciais comprometidas, alerta a Rapid7.



O grupo de ransomware Akira continua a atacar dispositivos SonicWall SSL VPN, recorrendo a contas previamente comprometidas, segundo um alerta da Rapid7.

Em agosto, a SonicWall revelou que a atividade maliciosa explorava a vulnerabilidade *CVE-2024-40766*, detetada na versão 9.3 das firewalls. O problema estava relacionado com a migração de utilizadores locais em que as palavras-passe não eram redefinidas.

Apesar da disponibilização de um *patch* de segurança, a Rapid7 sublinha que muitos clientes não concluíram todas as etapas de remediação, incluindo a redefinição obrigatória de todas as palavras-passe locais — um passo crítico que terá sido ignorado em alguns casos.

Segundo os investigadores, esta situação permitiu ao Akira aceder a redes sem recorrer a exploits, apenas reutilizando credenciais comprometidas. ◀

KIT DE PHISHING SALTY2FA CONTORNA MFA E DESAFIA DEFESAS TRADICIONAIS

Uma investigação revelou um novo kit de phishing altamente sofisticado, capaz de imitar portais de empresas e de contornar mecanismos de autenticação multifator.



O Centro de Cibersegurança da Ontinue descobriu uma campanha de phishing que utiliza o kit Salty2FA, caracterizado por uma elevada sofisticação técnica e pela capacidade de contornar mecanismos de segurança avançados.

A campanha tem início com um email fraudulento que redireciona a vítima para uma página falsa de partilha de documentos, alojada numa plataforma legítima. De acordo com o relatório, esta infraestrutura, criada no início de setembro de 2025, explora contas de teste gratuita da plataforma.

Ao abrir o link, o utilizador é conduzido através de uma cadeia de ataque em várias fases. Entre os mecanismos usados encontra-se o captcha Cloudflare Turnstile, um recurso que foi concebido para bloquear bots, mas que neste caso atua como filtro contra ferramentas de análise automatizadas. ◀



Business Continuity

IT Insight talks

Garantir a Continuidade do Negócio na Era Digital

23 de outubro| Quinta-feira | 10h

A IT Insight convida-o a participar na mesa-redonda Business Continuity, no dia 23 de outubro de 2025, no Fórum Tecnológico Lispolis, em Lisboa. Neste evento, vamos explorar as estratégias, tecnologias e boas práticas que permitem às organizações assegurar a continuidade das operações e reforçar a resiliência digital, com especial enfoque na implementação da diretiva NIS2 e no seu impacto para empresas e entidades públicas. Junte-se a especialistas do setor e descubra como garantir a proteção e a estabilidade do seu negócio num mundo cada vez mais exigente.

Fórum Tecnológico Lispolis | A partir das 9h30 | Participação **presencial** e **online**
Escolha a sua forma de participar:

QUERO ESTAR PRESENTE **QUERO ASSISTIR POR ZOOM**

Com o apoio de: LISPOLIS Pólo Tecnológico de Lisboa · COMMVAULT · IP Telecom · veeam · VisionWare since 2005

“PROLOGIN: SEGURANÇA DIGITAL COM ASSINATURA PORTUGUESA”

OUTUBRO É O MÊS EUROPEU DA CIBERSEGURANÇA — MAS PROTEGER A SUA EMPRESA DEVE SER UMA PRIORIDADE O ANO INTEIRO.

Fundada em 2011, a PROLogin é uma empresa portuguesa especializada na comercialização, implementação e desenvolvimento de soluções informáticas para empresas de todos os setores como comércio, telecomunicações, banca, seguros e indústria.

Com uma equipa experiente, motivada e em constante formação, destacamo-nos pela proximidade com os clientes e pela capacidade de integrar soluções robustas, escaláveis e ajustadas às reais necessidades de cada negócio.

Desde o início, adotámos a inovação, a integridade e a excelência como pilares da nossa atuação — valores que se refletem na confiança dos nossos clientes e na solidez das nossas parcerias.

Mas num mundo cada vez mais digital, a tecnologia só é eficaz quando está protegida. É por isso que, desde cedo, fizemos da cibersegurança uma prioridade, integrando no nosso portfólio soluções Líderes como a Sophos, e mais recente-



VICTOR ANDRADE – CEO – PROLOGIN

"A CIBERSEGURANÇA NÃO DEVE SER VISTA COMO UM CUSTO, MAS COMO UM INVESTIMENTO ESTRATÉGICO. O IMPACTO DE UM ATAQUE ULTRAPASSA A PERDA DE DADOS: IMPLICA INTERRUPÇÕES OPERACIONAIS, POTENCIAIS SANÇÕES LEGAIS E, MUITAS VEZES, UMA QUEBRA DE CONFIANÇA DIFÍCIL DE RECUPERAR".

mente, a Fortinet, para garantir níveis de proteção superiores, tanto na segurança endpoint como na gestão de acessos (NAC).

E é neste contexto que celebramos o Mês Europeu da Cibersegurança, uma iniciativa da ENISA e da Comissão Europeia que visa alertar para os riscos do mundo digital. Para nós, este mês é mais do que uma campanha: é uma oportunidade para reforçar o nosso compromisso com a educação continua, a prevenção inteligente e a resiliência digital das empresas portuguesas.

Vivemos num cenário de constante evolução tecnológica, e também de ameaça constante. 0 trabalho remoto e híbrido, o uso crescente da cloud e a multiplicação de dispositivos conectados aumentam drasticamente a superfície de ataque das organizações. 0s cibercriminosos sabem disso e estão cada vez mais organizados, rápidos e sofisticados.

Em particular, a engenharia social tornou-se um dos maiores riscos atuais. Ao invés de atacar diretamente sistemas, estes métodos exploram o elo mais fraco: o comportamento humano. Técnicas como phishing, smishing, vishing e impersonation estão mais dificeis de detetar, e bastam alguns segundos para comprometer redes inteiras, dados sensíveis ou até a reputação de uma marca.

Na PROLogin, acreditamos que a cibersegurança deve assentar em três pilares fundamentais:

1. Tecnologia robusta, com soluções adaptadas à realidade de cada empresa;

2. Processos bem definidos, com políticas claras de acesso, backup e resposta a incidentes;

3. Pessoas preparadas, através de formações regulares e sensibilização continua.

Durante este mês de outubro, (e ao longo de todo o ano), apoiamos os nossos clientes com auditorias, testes de vulnerabilidades, consultorias de risco e planos de melhoria continua. A nossa missão é simples: garantir que as empresas têm não só ferramentas, mas também estratégia para enfrentar os desafios da era digital.

A cibersegurança não deve ser vista como um custo, mas como um investimento estratégico. 0 impacto de um ataque ultrapassa a perda de dados: implica interrupções operacionais, potenciais sanções legais (como o incumprimento do RGPD) e, muitas vezes, uma quebra de confiança difícil de recuperar.

A cibersegurança não vive de alarmismos, mas de ação continua.

Com a PROLogin, informação certa, tecnologia robusta e apoio especializado, a sua empresa estará sempre um passo à frente! ◀

PROLOGIN
PRODUTOS E SERVIÇOS

Mordeu o isco?

A PROLogin protege a sua empresa contra as armadilhas digitais. Somos especialistas em IT e cibersegurança, com soluções completas para manter os seus dados e sistemas a salvo.

A cibersegurança não vive de alarmismos, mas de ação contínua
Visite prologin.pt e fale connosco.

www.prologin.pt
(+351) 214 261 699
(Chamada para a rede fixa nacional)
@prologin_pt

redShift

por Diogo Carou,
Head of Security Operations, Redshift Global

RED.BOX: A PLATAFORMA QUE TORNA A CIBERSEGURANÇA VISÍVEL

VIVEMOS NUMA ÉPOCA EM QUE OS CIBERATAQUES DEIXARAM DE SER SIMPLES INCIDENTES ISOLADOS, CADA VEZ MAIS SOFISTICADOS, MUITOS DELES SÃO ORIGINADOS E POTENCIADOS COM RECURSO A INTELIGÊNCIA ARTIFICIAL.

O seu efeito é imediato: ataques mais rápidos, mais credíveis e mais difíceis de detetar e prevenir. No entanto, mesmo perante esta realidade, muitas organizações continuam a confiar em serviços de SOC/ MDR que funcionam como verdadeiras "caixas negras", onde os seus clientes pouco ou nada sabem sobre o serviço que lhes está a ser prestado, tendo apenas visibilidade sobre alertas quando um determinado ataque já se poderá encontrar em curso, e, posteriormente, sobre os respetivos relatórios mensais, no momento da sua apresentação.

Este é um problema crítico. Um serviço de SOC/ MDR não deve apenas detetar e responder a incidentes de segurança. Deve também fornecer aos clientes visibilidade clara e em tempo real sobre o trabalho que está a ser realizado, traduzindo dados técnicos complexos em informação objetiva que permita avaliar riscos e potenciar processos de tomada de decisão. A confiança só existe quando há transparência e a ausência de métricas claras torna o investimento neste tipo de serviços algo difícil de justificar.

É precisamente aqui que a abordagem da Redshift, através da sua plataforma RED.Box, se distingue.



DIOGO CAROU, HEAD OF SECURITY OPERATIONS, REDSHIFT GLOBAL



Ao contrário de um modelo opaco, a plataforma RED.Box foi concebida para trazer luz a todo este processo, fornecendo dashboards intuitivos que permitem acompanhar em tempo real não apenas os alertas e incidentes de segurança que vão sendo detetados, mas também o desempenho do próprio serviço de SOC/MDR. Os clientes deixam de depender de relatórios mensais que chegam, por vezes, tarde, passando a ter acesso imediato a indicadores como o tempo médio de deteção, confirmação e resposta, os vetores de ataque mais comuns, a evolução da postura de risco, assim como a forma como os alertas e casos são geridos pelas equipas operacionais, no decorrer das diferentes fases de um incidente.

Para as equipas técnicas, esta informação detalhada permite acompanhar a eficácia da operação, correlacionar eventos e detetar eventuais padrões que de outra forma passariam despercebidos. Já para os executivos, a plataforma RED.Box traduz estes indicadores em impacto de negócio: quantas ameaças críticas foram bloqueadas, qual o tempo de inatividade que foi evitado e qual o retorno real do investimento no serviço. Esta ponte entre o mundo técnico e o estratégico é, a meu ver, o verdadeiro diferenciador que o mercado exige há anos e que a Redshift conseguiu materializar com esta plataforma.

Neste contexto, é igualmente importante sublinhar o papel das atividades forenses. A investigação forense digital permite compreender não apenas que um determinado incidente ocorreu, mas também como tal aconteceu, qual a sua origem e até

ESTE É O FUTURO INEVITÁVEL DA CIBERSEGURANÇA: SERVIÇOS ASSISTIDOS E ENRIQUECIDOS POR IA QUE PERMITEM APOIAR E CAPACITAR AS EQUIPAS OPERACIONAIS NOS PROCESSOS DE PREVENÇÃO, DETEÇÃO, RESPOSTA E MITIGAÇÃO PERANTE AS DIFERENTES AMEAÇAS EMERGENTES

que ponto determinados sistemas e dados foram efetivamente comprometidos. É esta análise apro-fundada que fornece as respostas certas para reforçar mecanismos de defesa, apoiar processos legais ou regulatórios e retirar lições práticas de cada ataque. Neste contexto, a plataforma RED.Box permite a centralização e consolidação de todas as evidências recolhidas, a correlação de indicadores com toda a base de conhecimento de alertas e incidentes anteriores presentes na plataforma e a disponibilização aos clientes de uma visão clara, sustentada e transparente sobre todo o ciclo de vida do incidente - desde a fase de deteção até a erradicação do mesmo.

A utilização de Inteligência Artificial na RED.Box não serve apenas para acelerar o processo de análise e resposta a incidentes, mas também para automatizar fluxos de contenção e tornar a informação mais relevante e contextualizada para a realidade dos clientes. Num cenário em que os atacantes já exploram IA para aumentar a sua eficácia, é imperativo que quem está responsável pelas linhas de defesa utilize as mesmas armas, mas com um foco adicional: a transparência. Mostrar em tempo real o valor que está a ser entregue é, hoje, tão importante quanto a própria capacidade de resposta.

Se muitos serviços SOC/MDR continuam a ser avaliados de forma subjetiva, baseados apenas na promessa da "monitorização contínua" a Redshift, com a plataforma RED.Box, apresenta um modelo objetivo e mensurável. Não se trata de um serviço invisível, mas de uma operação clara, acompanhada por indicadores técnicos e executivos que colocam os clientes no centro do processo e lhes permitem perceber, em cada momento, de que forma é que estão a ser protegidos.

Este é o futuro inevitável da cibersegurança: serviços assistidos e enriquecidos por IA que permitem apoiar e capacitar as equipas operacionais nos processos de prevenção, deteção, resposta e mitigação perante as diferentes ameaças emergentes. Prestadores de serviços que continuem a operar como uma caixa negra, sem visibilidade e sem transparência, arrisca-se a perder relevância num mercado cada vez mais exigente.

No fim, o que diferencia verdadeiramente um serviço de cibersegurança não é apenas a capacidade de detetar e responder, mas a forma como consegue demonstrar o seu valor de forma transparente. E, neste campo, a plataforma RED.Box mostra que o futuro já chegou. ◀

RED Box

A plataforma para *fortalecer as suas operações de segurança*

Centralize as suas operações de cibersegurança num só lugar

Automatize a deteção, triagem e mitigação de incidentes de cibersegurança

Verifique a postura e a exposição da sua organização em matéria de cibersegurança

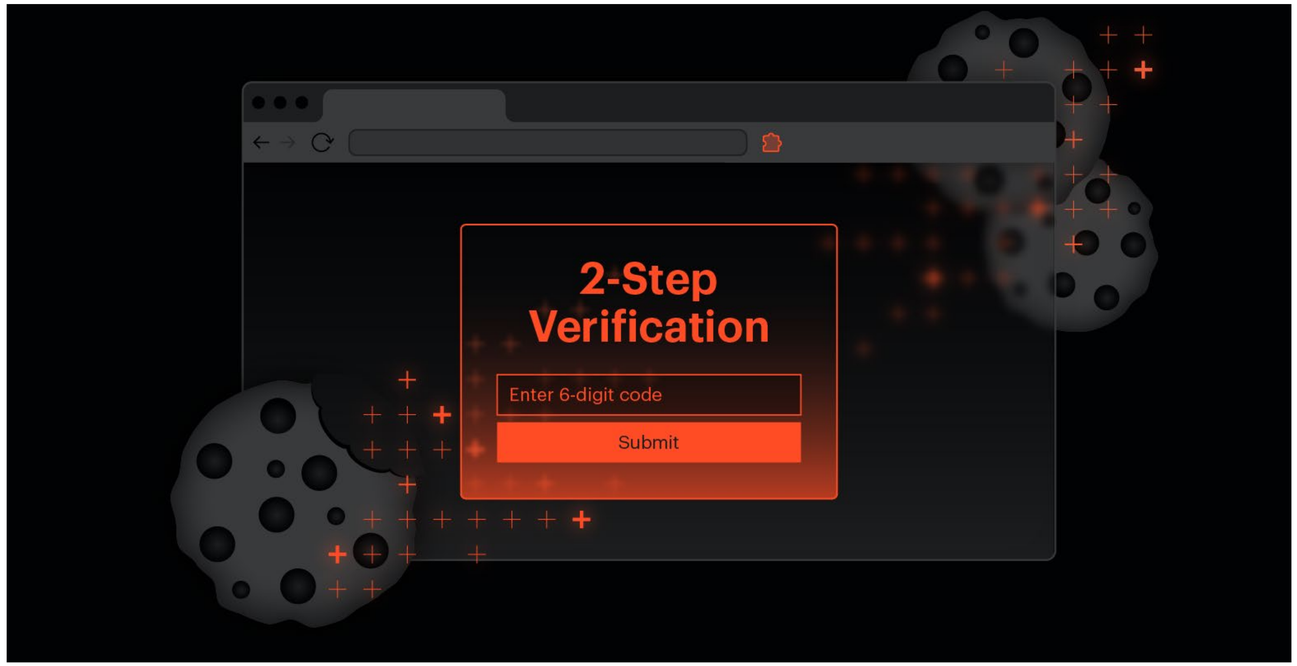
Saiba mais em:
redshift.global

+351 217 230 635
sales@redshift.global

redShift

COOKIE-BITE: QUANDO UM SIMPLES COOKIE ABRE AS PORTAS A ATAQUES AVANÇADOS

DURANTE ANOS, A AUTENTICAÇÃO MULTIFATOR (MFA) FOI ACLAMADA COMO A BARREIRA INTRANSPONÍVEL CONTRA O ACESSO NÃO AUTORIZADO.



No entanto, uma investigação da Varonis revela uma nova e preocupante técnica, o "Cookie-Bite", que desafia essa confiança. Ao explorar o furto de cookies de sessão, atacantes conseguem contornar a MFA e manter acesso persistente a aplicações na cloud críticas como Microsoft 365, Outlook ou Teams, sem a necessidade de credenciais adicionais. Este artigo explora o funcionamento do Cookie-Bite, o seu impacto devastador e as estratégias de mitigação essenciais para as organizações.

COMO FUNCIONA O COOKIE-BITE: A APROPRIAÇÃO DA IDENTIDADE DIGITAL

O Cookie-Bite baseia-se no furto de cookies, pequenos fragmentos de dados que validam a autenticação de um utilizador. Uma vez na posse

destes cookies, os atacantes podem realizar o sequestro de sessão, assumindo a identidade do utilizador legítimo e tornando-se praticamente indetetáveis pelos mecanismos de autenticação tradicionais.

Os investigadores da Varonis identificaram várias táticas para comprometer estes cookies:

• **Infostealers**: Malware especializado no roubo de informações que exfiltra automaticamente credenciais e cookies de sessão, frequentemente comercializados em mercados clandestinos.

• ***Adversary-in-the-Middle*** (AiTM): Campanhas de phishing com proxy reverso que capturam em tempo real senhas, tokens MFA e cookies, simulando sites legítimos.

• ***Extensões Maliciosas para o Browser***: Disfarçadas de utilitários legítimos, estas extensões obtêm permissões excessivas, acedendo a dados sensíveis, incluindo cookies de sessão.

• **Extração de Memória e Desencriptação de Cookies Locais**: Técnicas avançadas que permitem aceder a cookies armazenados na memória ou em bases de dados encriptadas no dispositivo da vítima.

IMPACTO PARA AS ORGANIZAÇÕES: A INVISIBILIDADE DO PERIGO

O maior perigo do Cookie-Bite reside na sua invisibilidade. Para os sistemas de autenticação, a sessão comprometida parece perfeitamente legítima. Isto significa que, mesmo com a MFA ativa, os atacantes podem:

• **Aceder a aplicações na cloud críticas**: (Microsoft 365, SharePoint, Teams, Outlook), operando dentro do ambiente da organização sem levantar suspeitas.

• **Executar elevação de privilégios e movimentos laterais**: Explorando as permissões do utilizador comprometido para aceder a outros sistemas e recursos.

• **Manter acesso persistente**: sem desencadear alertas imediatos, permitindo que as atividades maliciosas se prolonguem por longos períodos.

Na prática, um atacante com acesso a emails e plataformas de colaboração pode manipular comunicações internas, lançar campanhas de phishing altamente direcionadas ou exfiltrar informações críticas sem ser detetado. Esta capacidade de permanecer oculto representa uma ameaça significativa à integridade dos dados e à segurança operacional.

PORQUE A MFA JÁ NÃO CHEGA: O PARADIGMA DA SEGURANÇA PÓS-AUTENTICAÇÃO

A MFA continua a ser um componente essencial de uma estratégia de segurança robusta, mas a investigação da Varonis demonstra que não é suficiente por si só. O problema não reside na autenticação inicial, mas sim no que acontece após o login.

Se um atacante obtiver um cookie válido, esse "passe" digital permite-lhe circular livremente dentro do ambiente da cloud, contornando os controlos tradicionais. Por isso, a questão central já não é apenas autenticar, mas investir proativamente em segurança pós-autenticação.

MITIGAÇÃO: UEBA E DEFESA EM CAMADAS – A ESTRATÉGIA ABRANGENTE

A investigação da Varonis sublinha a importância de uma abordagem de defesa em camadas, que combine prevenção robusta com deteção contínua e adaptativa.

Entre as medidas essenciais destacam-se:

• **Implementação de User and Entity Behavior Analytics** (UEBA): Esta tecnologia cria perfis de comportamento normais para utilizadores e entidades, identificando padrões anómalos como acessos fora de horas, downloads atípicos de grandes volumes de dados ou logins a partir de localizações geográficas suspeitas.

• **Políticas de Rotação de Sessões e Invalidação Rápida de Cookies Comprometidos**: A implementação de sessões de curta duração e mecanismos que permitam invalidar cookies de forma expedita em caso de suspeita.

• **Monitorização de Endpoints**: Para deteção proativa de infostealers e extensões maliciosas que possam comprometer a segurança dos dispositivos.

• **Formação Contínua dos Utilizadores**: Essencial para reduzir o impacto de campanhas de phishing AiTM, educando os colaboradores sobre os riscos e como identificar tentativas de engano.

A plataforma da Varonis integra estas capacidades, oferecendo visibilidade abrangente sobre dados sensíveis, monitorização de sessões e deteção comportamental avançada. Desta forma, as equipas de segurança conseguem identificar acessos suspeitos em tempo útil e prevenir que um simples cookie se transforme num ataque persistente e devastador.

CONCLUSÃO

O Cookie-Bite demonstra de forma clara como os atacantes continuam a inovar para explorar pontos cegos na segurança na cloud. Confiar apenas no MFA já não é suficiente: as organizações precisam de olhar para além do login e garantir mecanismos eficazes de deteção pós-autenticação.

Tal como mostra a investigação da Varonis, sem uma estratégia sólida de defesa em camadas, um simples cookie pode ser o bilhete de entrada para ataques persistentes e devastadores, com consequências severas para a confidencialidade, integridade e disponibilidade dos dados empresariais. A vigilância e a adaptação contínua são cruciais para proteger o ambiente digital em constante evolução.

O QUE FAZER A SEGUIR?

Descubra como pode continuar a sua jornada para reduzir o risco de dados na sua empresa:

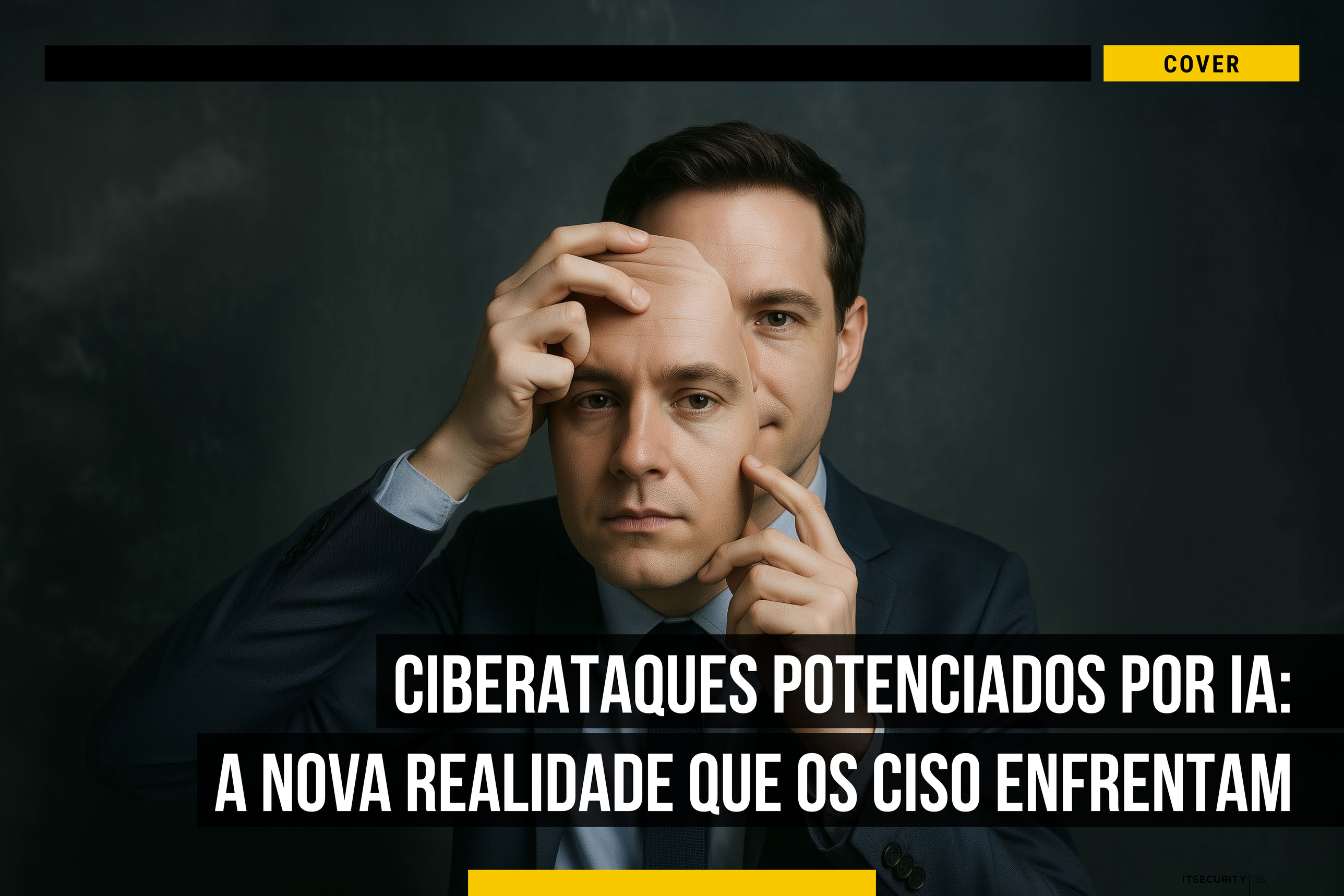
1. *Leia aqui o artigo completo*
2. *Agende uma demonstração connosco* para ver a Varonis em ação. Personalizaremos a sessão de acordo com as necessidades de segurança de dados da sua organização e responderemos a todas as suas perguntas. .
3. *Consulte um exemplo da nossa Avaliação de Risco de Dados* e descubra os riscos que podem estar latentes no seu ambiente. *A Avaliação de Risco de Dados da Varonis* é totalmente gratuita e oferece um caminho claro para a remediação automatizada.
4. Siga-nos no *LinkedIn*, *YouTube* e *X (Twitter)* para obter informações rápidas sobre tudo o que se refere à segurança de dados, incluindo DSPM, deteção de ameaças, segurança de IA e muito mais.

VARONIS

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

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

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



CIBERATAQUES POTENCIADOS POR IA: A NOVA REALIDADE QUE OS CISO ENFRENTAM



POR RUI DAMIÃO

A INTELIGÊNCIA ARTIFICIAL TRANSFORMOU-SE NA MAIS RECENTE FRONTEIRA DA CIBERSEGURANÇA, CRIANDO UMA REALIDADE PARADOXAL ONDE A MESMA TECNOLOGIA PROMETE REVOLUCIONAR A PRODUTIVIDADE EMPRESARIAL E SE TORNOU, TAMBÉM NA ARMA DE ELEIÇÃO DOS CIBERCRIMINOSOS. ESTA NOVA GERAÇÃO DE ATAQUES EXIGE UMA REAVALIAÇÃO FUNDAMENTAL DAS ESTRATÉGIAS DE CIBERSEGURANÇA ONDE A VELOCIDADE DE RESPOSTA E A SOFISTICAÇÃO DAS DEFESAS SE TORNARAM QUESTÕES DE SOBREVIVÊNCIA ORGANIZACIONAL.

O panorama de cibersegurança enfrentou uma transformação radical em 2025, com a Inteligência Artificial (IA) a emergir simultaneamente como ferramenta de defesa e arma ofensiva. O relatório "*Cost of Data Breach 2025*" da IBM revelou que 13% das organizações reportaram violações de modelos ou aplicações de IA, enquanto 16% das violações de dados envolveram atacantes que utilizaram inteligência artificial, mais frequentemente para phishing gerado por IA (37%) e ataques de *deepfake* (35%).

Estas estatísticas ganham maior relevância quando analisadas no contexto empresarial global. O "*Cybersecurity Readiness Index 2025*" da Cisco descobriu que quase nove em cada dez (86%) dos líderes empresariais com responsabilidade de cibersegurança reportaram pelo menos um incidente relacionado com IA nos últimos 12 meses, demonstrando que esta já não é uma ameaça futura, mas uma realidade presente.

A SOFISTICAÇÃO DOS ATAQUES

A Microsoft, por seu lado, observa uma evolução preocupante nas técnicas dos atacantes, tendo identificado a utilização de IA por atores de ameaça para reconhecimento, investigação de vulnerabilidades, tradução, técnicas de comando operacional refinadas por LLM, desenvolvimento de recursos, técnicas de scripting, evasão de deteção, engenharia social e ataques de força bruta.

A sofisticação destes ataques é particularmente evidente na personalização em escala. A IBM reportou que a IA generativa reduziu o tempo necessário



para escrever um email de phishing convincente de 16 horas para apenas cinco minutos, demonstrando como a tecnologia democratiza capacidade que antes eram exclusivas de grupos altamente especializados.

O CUSTO DE NÃO AGIR

O estudo "*Global Digital Trust Insights 2025*" da PwC revelou que apenas 2% das organizações implementaram ciber-resiliência em toda a organização, apesar de 77% das organizações esperarem que o seu orçamento de cibersegurança aumente no próximo ano.

Esta lacuna entre consciencialização e implementação é especialmente crítica num contexto que dois terços dos líderes de segurança notam que a IA generativa expandiu a superfície de ciberataque no último ano, à frente de outras tecnologias como cloud (66%) e produtos conectados (67%).

Os custos financeiros destas ameaças são substanciais: embora os custos globais médios das violações de dados tenham diminuído para 4,44 milhões de dólares em 2025, segundo o "*Cost of Data Breach 2025*" da IBM, 20% das organizações experienciaram violações ligadas ao uso não autorizado de inteligência artificial, adicionando uma média de 670 mil dólares aos custos de violação.

No entanto, de acordo com a IBM, 97% das organizações que sofreram violações relacionadas com inteligência artificial não tinham controlos de acesso à IA em vigor. Segundo a Cisco, apenas 48% das empresas acredita que os seus funcionários compreendem totalmente como é que os atores maliciosos estão a usar a IA para melhorar os seus ataques.

Para os CISO portugueses, estes dados representam mais do que apenas estatísticas: são um alerta de que a era dos ataques previsíveis acabou. No seu lugar emerge uma nova geração de ameaças que aprendem, adaptam-se e evoluem a uma velocidade sem precedentes, exigindo uma reavaliação fundamental das estratégias de cibersegurança organizacional.

A ESCALA E VELOCIDADE DOS NOVOS ATAQUES

A transformação mais significativa no panorama de cibersegurança não reside apenas na sofisticação dos ataques, mas na sua velocidade e escala sem precedentes. A IBM registou um aumento de 71% ano após ano em ataques que utilizam credenciais comprometidas, enquanto a IBM X-Force observou um aumento de 84% em emails de phishing que entregam infostealers numa base semanal.

Chester Wisniewski, Director, Global Field CISO da Sophos, contextualiza esta evolução e afirma que é na velocidade e escala que se "espera ver o maior avanço por parte dos agentes de ameaças que utilizam IA", especificando que "os ataques, em si mesmos, não deverão tornar-se muito mais sofisticados,





CHESTER WISNIEWSKI, DIRECTOR, GLOBAL FIELD CISO DA SOPHOS

"NA MAIORIA DOS CASOS, SIMPLESMENTE NÃO SABEMOS SE UM EMAIL DE PHISHING FOI ESCRITO POR UMA IA, NEM PODEMOS DIZER SE UM SCRIPT SHELL OFUSCADO FOI CRIADO MANUALMENTE OU GERADO POR IA"

mas sim mais frequentes e de maior qualidade", onde os "atacantes menos qualificados vão aumentar as suas capacidades enquanto os atacantes de nível médio vão encontrar mais vítimas e explorá-las mais rapidamente".

Bruno Castro, Fundador e CEO da VisionWare, afirma que "quantificar exatamente a diferença em velocidade ou escala entre ataques tradicionais e ataques potenciados por IA é difícil porque os operadores misturam várias técnicas". No entanto, diz, "o que antes estava ao alcance de grupos altamente especializados passa agora a ser acessível a atores com menos recursos, pois a IA reduz o conhecimento técnico necessário para executar ataques sofisticados".

Esta democratização é corroborada por dados da Cisco, que apontam que 52% das organizações reportam que os funcionários não compreendem totalmente como os atores maliciosos estão a usar IA, enquanto apenas 49% dos inquiridos acreditam que os funcionários compreendem totalmente as ameaças de cibersegurança relacionadas com IA.

AUTOMAÇÃO E PERSONALIZAÇÃO EM ESCALA

A diferença fundamental reside na capacidade de automação inteligente. Bruno Castro explica que se observa "um aumento expressivo da personalização de phishing, crescimento rápido de casos de *voice cloning* usados em fraudes e automação de tarefas que antes exigiam intervenção humana".

O "*Digital Defense Report 2024*" da Microsoft observou um aumento de 2,75 vezes ano após ano em ataques de ransomware, demonstrando como os



atacantes estão a combinar inteligência artificial com táticas tradicionais para aumentar a eficácia.

Wisniewski refere que, "na maioria dos casos, simplesmente não sabemos se um email de phishing foi escrito por uma IA, nem podemos dizer se um script Shell ofuscado foi criado manualmente ou gerado por IA". No entanto, destaca um padrão revelador: "o aumento do volume de ataques com pequenas variações no tema, algo que antes poderia ser difícil para os humanos sem contarem com automação sofisticada".

A Cisco revelou que 71% dos líderes acreditam que um incidente de cibersegurança terá lugar e vai afetar a organização dentro dos próximos 12 a 24 meses, o que reflete a urgência das ameaças. Bruno Castro resume a situação atual: "a IA reduz o custo por alvo, permitindo atingir milhares de vítimas com conteúdo adaptado, ou seja, mais velocidade e escala operacional". Esta transformação leva a que os CISO enfrentam não apenas ameaças mais sofisticadas, mas também mais frequentes e economicamente viáveis para os atacantes, alterando completamento o cálculo de risco-benefício no panorama de cibersegurança.

O ESPETRO ATUAL DAS AMEAÇAS

A diversidade de ataques potenciados por inteligência artificial expandiu dramaticamente, abrangendo desde técnicas tradicionais aprimoradas até vetores de ataque completamente novos. Chester Wisniewski refere que "os dois tipos mais prolíficos, e confirmados como gerados por IA, são os emails de phishing e as campanhas de mensagens fraudulentas (SMS, WhatsApp, etc.). A principal razão pela qual podemos confirmar que são gerados por IA é que atacantes ficaram sem dinheiro para fazer melhor, e então mensagens cheias de erros geradas por LLM passaram a aparecer nas tentativas de fraude".

Bruno Castro oferece uma catalogação mais abrangente e indica que os ataques "que se têm observado com maior frequência são principalmente phishing altamente personalizado", como spear phishing e vishing com scripts criados por IA, "clonagem de voz para fraudes telefónicas, *deepfake* vídeo/áudio para chantagem ou manipulação pública, malware com componentes adaptativos (malware que ajusta a sua assinatura ou comportamento segundo o host), automação de BEC e negociação de resgates com chatbots".

Esta evolução representa uma mudança fundamental no panorama de ameaças onde os atacantes já não dependem exclusivamente de uma técnica, mas combinam múltiplos vetores potenciados por IA para maximizar o sucesso. Desde emails de phishing gerados em minutos até malware que se adapta autonomamente aos sistemas que infeta, a IA democratizou capacidades avançados e criou um ecossistema de ameaças onde a velocidade, personalização e automação convergem para desafiar as defesas tradicionais.



A DIFICULDADE TÉCNICA DE IDENTIFICAÇÃO

Um dos aspetos mais preocupantes dos ataques potenciados por IA é a sua capacidade de mimificar comportamentos legítimos, tornando a deteção extremamente complexa. Chester Wisniewski, da Sophos, diz, diretamente, que "é muito difícil, se não impossível, na maioria dos casos" distinguir tecnicamente entre um ataque tradicional automatizado e um verdadeiramente potenciado por inteligência artificial. "A menos que existam artefactos específicos deixados pelo LLM do qual estão a abusar, não há nenhuma forma óbvia de determinar isto", explica.

Bruno Castro, da VisionWare, oferece uma abordagem mais estruturada para a identificação. "Tecnicamente, um CISO pode distinguir (ou, pelo menos, suspeitar) entre um ataque tradicional automatizado e um verdadeiramente "*AI-powered*" observando características como: (1) grau de personalização sem precedentes nas mensagens (contexto recente, referências pessoais que não vêm de *leaks* públicos comuns), (2) texto/linguagem que se adapta o tom ao interlocutor em tempo real, (3) voz ou vídeo sintetizados de alta qualidade e sincronizados e (4) interação conversacional com variações muito ligeiras e sistemáticas entre mensagens que revelam alguns padrões", afirma.



BRUNO CASTRO, FUNDADOR E CEO DA VISIONWARE

O Fundador & CEO da VisionWare detalha, também, os indicadores que diz serem mais fiáveis para deteção: "anomalias de conteúdo, por exemplo, em linguagem que não corresponde ao histórico do remetente, e metadados inconsistentes. Anomalias em áudio como pausas não naturais e palavras mal

"UM DOS PONTOS DESTACADOS NO MAIS RECENTE RELATÓRIO DE RISCOS E CONFLITOS DO CNCS É QUE A IA GENERATIVA ESTÁ A EMERGIR COMO VEÍCULO FACILITADOR DE ATAQUES: SIMPLIFICA CAMPANHAS DE PHISHING ALTAMENTE DIRECIONADAS, COM A CRIAÇÃO DE DEEPFAKES UTILIZADOS EM FRAUDES EMPRESARIAIS E A AUTOMAÇÃO DA IDENTIFICAÇÃO DE VULNERABILIDADES"





pronunciadas, e anomalias em vídeo detetáveis através de artefactos subtis, inconsistência de iluminação, incongruência de movimentos", entre outros.

Bruno Castro enfatiza que a deteção eficaz requer uma combinação de técnicas. "A um nível mais técnico, é essencial combinar análise forense de conteúdo, *ML-detectors* de *deepfake* e enriquecimento de *indicators of compromise*, que aumentam a fiabilidade de deteção".

A realidade, contudo, permanece desafiante: enquanto as ferramentas de deteção evoluem, os atacantes também refinam as suas técnicas. Como diz Wisniewski, da Sophos, a distinção entre ataques tradicionais e potenciados por IA muitas vezes só se torna aparente após análise forense detalhada, quando os danos já podem estar consumados. Isto coloca os CISO numa posição reativa, enfatizando a importância de estratégias de defesa em profundidade que assumam a presença de conteúdo gerado por IA no panorama de ameaças.

O PANORAMA PORTUGUÊS

Em Portugal, os padrões de ataque seguem tendências específica que refletem tanto a estrutura económica nacional, como as vulnerabilidades setoriais, Bruno Castro identifica os alvos preferenciais: "financeiro, saúde e administração pública e/ou infraestruturas críticas", em linha com o panorama europeu.

A preocupação, reforça Bruno Castro, é reconhecida ao mais alto nível e "um dos pontos destacados no mais recente relatório de Riscos e Conflitos do CNCS é que a IA generativa está a emergir como veículo facilitador de ataques: simplifica campanhas de phishing altamente direcionadas, com a criação de *deepfakes* utilizados em fraudes empresariais e a automação da identificação de vulnerabilidades".

Em Portugal, os *gaps* mais críticos "abrangem tanto a deteção de conteúdos sintéticos, como *deepfake*s de voz e vídeo, como a resposta a campanhas de phishing avançadas e em larga escala", explica Bruno Castro, acrescentando que "muitas empresas não dispõem de ferramentas capazes de identificar manipulações multimédia credíveis nem de soluções de filtragem preparadas para mensagens altamente personalizadas, criadas em vários idiomas e adaptadas



ao contexto da vítima". Ao mesmo tempo, "os processos de verificação de identidade também continuam frágeis, sobretudo em fluxos financeiros ou de comunicação executiva, onde pedidos falsificados podem ser aceites sem autenticação robusta ou validações alternativas".

O Fundador & CEO da VisionWare observa que são poucas as organizações portuguesas que têm políticas específicas para enfrentar conteúdo gerado por inteligência artificial. "Os dados públicos são limitados e não existe um levantamento nacional público e atualizado que diga quantas organizações têm políticas específicas para *deepfakes*/IA. Ainda assim, e uma vez que as ameaças *deepfake* têm ganho cada vez uma maior expressão em Portugal, diria que a grande maioria ainda não tem protocolos formais para *deepfakes*, principalmente, claro, as empresas de menor dimensão".

Bruno Castro refere, ainda, a questão da preparação humana. "Em muitos casos, a formação de colaboradores ainda está orientada para sinais tradicionais de fraude e não para conteúdos criados por IA e poucas organizações têm políticas o exercícios de red teaming específicos para estas ameaças", afirma.

ABORDAGEM PRAGMÁTICA PARA OS CISO

Face às limitações orçamentais que caracterizam muitas organizações portuguesas, a questão central não é implementar todas as soluções disponíveis, mas priorizar investimentos que ofereçam o maior retorno em termos de segurança. Chester Wisniewski partilha que, hoje, "a IA é utilizada principalmente para aumentar a eficácia da engenharia social. O passo mais importante que um CISO pode dar é rever os seus processos de verificação humana quando realmente importa e implementar uma autenticação multifator eficaz e resistente a phishing".

Já Bruno Castro defende que, "independente serem ameaças potenciadas por IA", um CISO com um orçamento limitado deve "apostar numa fórmula que funciona à data de hoje para a maioria das organizações: implementar um modelo formal de governação de segurança com o envolvimento obrigatório do *top management* que permita avaliar, detetar e corrigir continuamente as principais vulnerabilidades dentro de casa – técnicas ou procedimentais".

Para Wisniewski, da Sophos, há três áreas críticas que requerem atenção imediata: "os processos de suporte técnico para verificar a identidade do utilizador antes de este poder redefinir credenciais de acesso; os processos de verificação para que as transferências bancárias e outras transações financeiras tenham autenticação mútua; e a atualização das formações de sensibilização de segurança, para que vão além da procura por erros gramaticais e ortográficos ou *links* suspeitos". Estas técnicas básicas, acrescenta, "já não são eficazes num mundo de conteúdos gerados por LLM que se tornam cada vez mais inteligentes".

A NOVA REALIDADE DA CIBERSEGURANÇA

Os ciberataques potenciados por inteligência artificial deixaram de ser uma ameaça futura para



se tornarem uma realidade presente e premente para as organizações de todo o mundo, onde se inclui, naturalmente, Portugal. Como demonstrado pelos dados da IBM, da Microsoft, da Cisco e da PwC, estamos perante uma transformação fundamental no panorama de ameaças: 13% das organizações já reportaram violações de modelos ou aplicações de IA, enquanto 86% dos líderes empresariais experienciaram pelo menos um incidente relacionado com IA nos últimos 12 meses.

Chester Wisniewski resume a evolução: "os ataques, em si mesmos, não deverão tornar-se muito mais sofisticados, mas sim mais frequentes e de maior qualidade". Bruno Castro complementa e observa que "o que antes estava ao alcance de grupos altamente especializados passa, agora, a ser acessível a atores com menos recursos, pois a IA reduz o conhecimento técnico necessário para executar ataques sofisticados".

Os dados revelam uma janela crítica de oportunidade. Apenas 2% das organizações implementaram resiliência cibernética em toda a organização, apesar de 77% esperarem aumentar os orçamentos de cibersegurança. Esta discrepância entre consciencialização e ação efetiva representa simultaneamente o problema e a solução.

A magnitude desta transformação exige colaboração entre setores, partilha de inteligência de ameaças e uma abordagem coordenada a nível nacional. Com 67% dos líderes a observarem que a IA generativa expandiu a superfície de ataque, a resposta não pode ser individual.



A era dos ataques previsíveis terminou e, no seu lugar, emerge uma nova realidade onde a inteligência artificial democratizou capacidades avançadas de ataque, mas também oferece ferramentas poderosas para a defesa. O sucesso dos CISO portugueses vai depender da sua capacidade de navegar esta dualidade, transformando uma ameaça existencial numa oportunidade de fortalecimento organizacional através de estratégias inteligentes, investimentos direcionados e uma governação de segurança verdadeiramente integrada no ADN empresarial. ◀

balwurk cyber security

AFERIR O RISCO NA ADOÇÃO DA IA

A IA GENERATIVA, COMO POR EXEMPLO UM LARGE LANGUAGE MODEL (LLM), É UMA FERRAMENTA QUE CONQUISTOU O SEU LUGAR NO DIA-A-DIA DAS ORGANIZAÇÕES E DAS PESSOAS NO GERAL.

Se devidamente utilizada, o aumento da produtividade é um fator diferenciador e que tem marcado um novo patamar de competitividade entre organizações. No entanto, como qualquer outra inovação tecnológica, a sua adoção comporta Riscos. O problema surge quando a própria organização se sujeita à adoção de uma nova tecnologia, sem de facto conhecer o de Risco que enfrenta e terá de tratar.

O verdadeiro desafio não está na tecnologia, mas sim nos processos e pessoas e na forma como está a ser adotada dentro das organizações, frequentemente através do uso pelos colaboradores a título pessoal e através de dispositivos não geridos, criando uma superfície de ataque difícil de mapear.



A ILUSÃO DA PRODUTIVIDADE SEM RISCOS

Imaginemos o seguinte cenário, um colaborador pressionado por prazos, começa a recorrer ao ChatGPT para criar relatórios em poucos minutos. Entusiasmado,

começa a copiar informações confidenciais, dados de clientes e estratégias de negócio diretamente para o chat. Nunca lhe ocorreu que está a partilhar segredos comerciais com um sistema externo sem qualquer controlo organizacional.

Como qualquer outro **LLM**, as vulnerabilidades definidas no OWASP TOP 10 LLM, demonstram que um dos maiores Riscos da sua utilização recai na fuga de informação e acesso não autorizado à infraestrutura. Por exemplo, explorando a vulnerabilidade de ***Prompt Injection***, um email aparentemente inócuo pode conter instruções ocultas que, quando processadas por um assistente de **Inteligência Artificial** (**IA**), levam à divulgação de informações sensíveis ou execução de ações não autorizadas.

AS VULNERABILIDADES QUE NINGUÉM VÊ

A fuga de informação sensível pode decorrer de forma insuspeita e silenciosa, e não decorre devido a uma falha técnica ou acesso não autorizado a um sistema por um agente malicioso. Decorre tão simplesmente quanto um colaborador pedir a um assistente de **IA** para otimizar ou criar um componente de uma aplicação e este partilhar, para o efeito, parte do código da solução que está a desenvolver, ou copiar e colar a solução sugerida pelo **LLM** no repositório final dessa aplicação. Este ato pode facilmente levar à fuga de credenciais ou código proprietário bem como levar à injeção de código malicioso. Adicionalmente, controlar o uso destas ferramentas não é uma tarefa simples, sobretudo quando podem ser integradas em processos críticos da organização sem que esta se aperceba. Tal pode resultar do desconhecimento sobre a forma como determinados serviços contratados intercetam a infraestrutura de uma organização, ou do facto de, mesmo não sendo adotadas formalmente, os colaboradores poderem recorrer às suas versões pessoais das ferramentas em ativos da empresa ou em dispositivos próprios, como computadores ou smartphones.

A URGÊNCIA NA CAPACIDADE DE AFERIR O RISCO

A capacidade de aferir e classificar o risco torna-se absolutamente crítica, pois não podemos simplesmente proibir o uso de ferramentas baseadas em **IA**, sendo necessária uma abordagem sistemática para classificar e gerir estes Riscos proactivamente.

E é por isso que a Balwurk desenvolveu uma *framework* que visa solucionar esta preocupação: "***Multidimensional AI Classification and Risk Matrix***". Esta solução está disponível publicamente e adequa-se a qualquer organização e, em última instância, permite aos decisores tomar uma decisão sustentada por uma análise de risco na adoção e utilização de uma dada solução **IA** incluindo produtos de mercado, ou aplicações desenvolvidas internamente. Com a realização desta análise de Risco, a organização estará mais bem preparada para adotar os controlos de segurança necessários para a mitigação do risco, bem como adaptar a sua política de Uso Aceitável alargada à **IA**.

A questão não é se a organização deve ou não adotar uma solução **IA**, pois na conjuntura atual a organização, quer queira quer não, já a adotou ou tem de a adotar. **A verdadeira questão é se consegue identificar e gerir o Risco dessa adoção antes que seja tarde demais**.

claranet®

por David Grave,
Security Director, Claranet Portugal

AI-POWERED CYBERATTACKS:

QUANDO A NOSSA MELHOR DEFESA É TAMBÉM A ARMA DO INIMIGO

VIVEMOS NUM MERCADO SATURADO POR UMA PROMESSA DA INTELIGÊNCIA ARTIFICIAL (IA) COMO A SOLUÇÃO DEFINITIVA PARA A CIBERSEGURANÇA. TODOS OS DIAS SOMOS BOMBARDEADOS COM "NEXT-GEN AI", "MACHINE LEARNING" E PLATAFORMAS AUTÓNOMAS QUE PROMETEM ERRADICAR AMEAÇAS MESMO ANTES DE ESTAS SE MATERIALIZAREM. A VERDADE É QUE, ENQUANTO VENDEMOS A IA COMO A NOSSA SALVAÇÃO, OS ATACANTES JÁ TÊM À DISPOSIÇÃO A ARMA MAIS SOFISTICADA QUE ALGUMA VEZ TIVERAM.

Este é o paradoxo da era em que vivemos: a mesma *IA* que utilizamos para detetar anomalias é usada por threat actors para criar deepfakes perfeitos para fraude de CEO. Os mesmos modelos de linguagem que ajudam a analisar logs são usados para gerar e-mails de phishing com uma gramática e contexto impecáveis, tornando a deteção humana praticamente impossível.

E, ao contrário do que acontece nas nossas organizações, estes atacantes não enfrentam constrangimentos de compliance ou aprovações de comités. Enquanto debatemos ROI e procurement, eles já estão para lá da implementação.

Os dados são inequívocos. Nos últimos 18 meses, observámos um aumento de 340% em ataques de phishing assistidos por *IA*, segundo relatórios da nossa própria Threat Intelligence. Estes não são os emails mal escritos com erros de gramática que costumávamos receber. São mensagens personalizadas, contextualmente relevantes, que imitam



DAVID GRAVE, SECURITY DIRECTOR, CLARANET PORTUGAL

"O OBJETIVO DO **SOAR** NÃO É SUBSTITUIR O ANALISTA DE SEGURANÇA; É LIBERTÁ-LO. É AUTOMATIZAR 80% DAS TAREFAS REPETITIVAS PARA QUE OS ESPECIALISTAS POSSAM CONCENTRAR-SE NOS 20% QUE EXIGEM INTUIÇÃO, CONTEXTO DE NEGÓCIO E DECISÃO ESTRATÉGICA."

perfeitamente o tom e estilo de comunicação das organizações-alvo.

SOAR: AUTOMAÇÃO E A FALSA SENSAÇÃO DE SEGURANÇA

O *Security Orchestration, Automation and Response (SOAR)* representa uma das aplicações mais promissoras da IA em *Cibersegurança*. No entanto, não devemos ver esta solução como mágica; devemos encará-la como um amplificador de capacidade. O objetivo do SOAR não é substituir o analista de *Segurança*; é libertá-lo. É automatizar 80% das tarefas repetitivas – triagem de alertas, enriquecimento de dados, contenção inicial de ameaças – para que os especialistas possam concentrar-se nos 20% que exigem intuição, contexto de negócio e decisão estratégica.

A *IA* amplifica capacidades existentes, não cria capacidades. Se não tem visibilidade adequada da sua rede, processos de resposta testados, ou equipas devidamente formadas, implementar *IA* apenas multiplica a confusão. A organização torna-se, ironicamente, mais vulnerável e dependente, confiando cegamente numa "caixa preta", enquanto os seus fundamentos de *Cibersegurança* não são testados nem evoluem e, em alguns caos, nem sequer existem.

O FATOR HUMANO: O ELO MAIS IGNORADO DA EQUAÇÃO DA IA

Um sistema de *IA* mal configurado gera um ruído de falsos positivos que dessensibiliza a equipa. Os alertas críticos acabam por ser ignorados no meio de um oceano de irrelevâncias.

A *IA* pode identificar um padrão; não pode compreender o impacto de um sistema crítico para o negócio estar offline por duas horas durante o pico de produção. Pode detetar uma anomalia de dados; não pode negociar com um diretor de produção a decisão de insular um segmento da rede, para investigação. A *IA* não substitui a competência humana; exige-a. Paradoxalmente, quanto mais sofisticada a tecnologia, mais especializada precisa de ser a equipa que a opera.

O DESAFIO PARA OS LÍDERES

A *IA* transformou definitivamente o panorama da *Cibersegurança*, mas não de forma linear. Cada avanço defensivo é rapidamente espelhado do lado ofensivo. A diferença da correta adoção destas ferramentas continuará a ser a qualidade da implementação, a competência das equipas e a maturidade dos processos.

Os seus problemas de falta de recursos humanos, processos mal definidos ou uma cultura de segurança inexistente não vão ser resolvidos pela *IA*. A *IA* é um amplificador. Vai amplificar uma boa estratégia, processos robustos e uma equipa competente. Mas também vai amplificar o caos, a ineficiência e a confusão de uma organização impreparada. ◀

DIVULTEC

por Luís Correia,
Business Developer Manager,
Divultec

INTELIGÊNCIA ARTIFICIAL: AVANÇOS NA CIBERSEGURANÇA E NOVOS RISCOS DIGITAIS

A INTELIGÊNCIA ARTIFICIAL (IA) TROUXE AVANÇOS EXTRAORDINÁRIOS PARA A CIBERSEGURANÇA, MAS TAMBÉM ABRIU CAMINHO A NOVAS FORMAS DE ATAQUE DIGITAL, ELEVANDO O RISCO DE CIBERAMEAÇAS POTENCIADAS POR IA.

Por isso, torna-se essencial criar estratégias que tanto empresas como cidadãos possam adotar, de forma a estarmos todos melhor preparados para esta nova realidade.

Durante anos, celebrámos a IA como motor de inovação. Contudo, ela tornou-se uma faca de dois gumes. Se, por um lado, fortalece a proteção de redes e sistemas — através da deteção precoce de padrões anómalos, da resposta automatizada a incidentes ou da análise em tempo real de grandes volumes de dados —, por outro, multiplica a capacidade ofensiva dos cibercriminosos, permitindo ataques mais rápidos, personalizados e difíceis de detetar.

A diferença em relação às técnicas tradicionais está na escala e sofisticação que a IA proporciona: o phishing rudimentar, antes fácil de identificar por erros ortográficos ou inconsistências, evoluiu para mensagens sem qualquer "defeito", adaptadas ao perfil da vítima e capazes de enganar até utilizadores experientes. Em paralelo, deepfakes de voz e vídeo estão a ser usados para imitar executivos com preci-



LUÍS CORREIA, BUSINESS DEVELOPER MANAGER, DIVULTEC

são quase perfeita, originando fraudes milionárias em ataques do tipo Business Email Compromise (BEC).

O problema, no entanto, não se limita à engenharia social. Já existem formas de malware inteligente, com capacidade de se infiltrar em sistemas, aprender com o ambiente, ajustar o comportamento e permanecer "invisíveis" às diversas camadas de defesa. Plataformas como WormGPT ou FraudGPT permitem a qualquer pessoa, mesmo sem conhecimentos técnicos, criar campanhas de ataque bastante sofisticadas.

O impacto ultrapassa a dimensão tecnológica: é também psicológico, social e empresarial. A confiança — pilar essencial das relações digitais, profissionais e até institucionais — está a ser posta em causa. Quando já não conseguimos distinguir entre o que é humano ou artificial, legítimo ou manipulado, enfrentamos uma verdadeira mudança de paradigma. Além disso, os ataques com IA devem ser vistos como risco estratégico, com impacto direto na continuidade do negócio, na reputação da marca e na relação com clientes e parceiros. A gestão deste risco precisa de ser integrada nos sistemas de gestão corporativos, e tratada ao nível da gestão de topo (e não apenas na equipa de IT).

COMO REAGIR PERANTE ESTA NOVA ERA?

Não existem respostas simples, mas há caminhos claros que devem ser considerados pelas organizações:

1. **Literacia Digital e Sensibilização Contínua**

– O fator humano continua a ser a superfície de ataque mais explorada. É fundamental investir em programas de awareness contínuos com simulações realistas de phishing, ajustadas ao contexto organizacional e pessoal. Esses exercícios devem incluir cenários com deepfakes de voz e vídeo, reforçando o pensamento baseado em risco: desconfiar de mensagens urgentes, com carga emocional ou pressão de tempo.

2. **Zero Trust Architecture (ZTA)**

– O paradigma atual exige abandonar a confiança implícita. O princípio de "never trust, always verify" deve ser aplicado em todos os níveis: cada acesso precisa de autenticação forte, validação contínua e apenas ao estritamente necessário (least privilege).

3. **Verificação Multicanal de Transações e Ordens Críticas**

– Processos financeiros e operacionais críticos devem seguir a two-man rule: nenhuma deci-

são sensível deve depender de uma única pessoa. Além disso, a validação deve ser feita através de canais de comunicação independentes (por exemplo, confirmar um pedido via chamada telefónica quando este chega por e-mail).

4. Tecnologia Defensiva Baseada em IA

– Tal como os atacantes recorrem à IA, os defensores devem explorar ferramentas de deteção de anomalias potenciadas por IA. Plataformas capazes de correlacionar eventos de múltiplas origens (endpoint, rede, cloud) e enriquecidas com Threat Intelligence — incluindo dados da DarkWeb — permitem identificar padrões suspeitos e antecipar comportamentos anómalos.

5. Proteção contra Manipulação de Modelos de IA

– Organizações que já utilizam IA nos seus processos internos enfrentam riscos específicos, como o data poisoning. É imperativo validar os conjuntos de treino, proteger pipelines de dados e monitorizar continuamente as API, para detetar manipulação de modelos.

6. Modelo de Governação e Regulação Interna

– Os modelos de governo do uso da IA deve assentar em políticas claras que definam onde e como os modelos podem ser aplicados. Este alinhamento deve ainda considerar o enquadramento regulatório internacional — como a diretiva NIS2, o AI Act Europeu, ou normas emergentes como a ISO/IEC 42001 — que definem requisitos de segurança, transparência e responsabilidade. Auditorias periódicas a algoritmos, datasets e processos de decisão são essenciais para garantir conformidade e reforçar a confiança.

7. Resposta e Recuperação

– A prevenção é crítica, mas a capacidade de reação é vital. Os Planos de Resposta a Incidentes devem contemplar cenários específicos de ataques baseados em IA: campanhas massivas de phishing automatizado, uso de deepfakes para manipulação de decisões ou adulteração de dados em sistemas críticos.

Os **AI-Powered Cyberattacks** já não pertencem ao domínio da ficção científica: são uma realidade presente e em rápida evolução. Sendo a IA uma tecnologia neutra, que tanto pode fortalecer a "defesa" como ampliar a capacidade de "ataque", cabe-nos a nós equilibrar a balança. O desafio para governos, empresas, e cidadãos é claro: usar a mesma inteligência artificial que alimenta as ameaças para reforçar a proteção, construir resiliência e garantir a confiança no ecossistema digital. ◀

IP Telecom

por Ana Gouveia,
Diretora de Sistemas de Gestão e Cibersegurança
da IP Telecom

IA: O ALIADO E O INIMIGO DA CIBERSEGURANÇA

A INTELIGÊNCIA ARTIFICIAL (IA) DEIXOU DE SER PROMESSA PARA SE TORNAR UMA FORÇA TRANSFORMADORA NA CIBERSEGURANÇA. O PARADOXO É CLARO: A MESMA TECNOLOGIA QUE PROTEGE SISTEMAS É USADA POR CIBERCRIMINOSOS PARA CRIAR ATAQUES SOFISTICADOS, ADAPTÁVEIS E DIFÍCEIS DE DETETAR.

A questão já não é "se" devemos usar IA na defesa, mas "como" aplicá-la de forma estratégica e responsável.

DO RISCO AO INVESTIMENTO

O ponto de partida é simples: só é possível investir bem quando se conhecem os riscos. Identificar vulnerabilidades, mapear ameaças e priorizar ativos críticos é essencial para aplicar a IA onde gera maior valor. Não basta adotar tecnologia avançada, é preciso usá-la com propósito.

A proteção eficaz nasce do equilíbrio entre processos claros, pessoas capacitadas e tecnologia adequada. A IA acrescenta valor integrada num ecossistema robusto, isolada é apenas mais uma peça do arsenal.

DÉFICE DE COMPETÊNCIAS

Um dos riscos mais críticos é o défice global de competências em cibersegurança. Sem equipas preparadas, mesmo as melhores soluções tecnológicas tornam-se ineficazes. A formação contínua, especialmente no uso de IA para defesa, é tão vital quanto firewalls ou sistemas de deteção avançada. Se os atacantes já exploram IA, não investir em tecnologia e capacitação é "correr atrás do prejuízo".



ANA GOUVEIA, DIRETORA DE SISTEMAS DE GESTÃO E CIBERSEGURANÇA DA IP TELECOM

IMPACTO DOS ATAQUES

As consequências de ataques potenciados por IA podem ser devastadoras. Em infraestruturas críticas, há risco de interrupção de serviços essenciais, manipulação de dados sensíveis e até ameaças físicas à população. No sector corporativo, podem traduzir-se em perdas financeiras, danos reputacionais e fuga de propriedade intelectual.

ESTRATÉGIAS DE DEFESA

As defesas precisam ser tão inteligentes quanto os atacantes, combinando deteção comportamental, análise preditiva e resposta automatizada.

Práticas como segmentação de redes, redundância de sistemas e simulações de ataques aumentam a resiliência organizacional, enquanto a colaboração entre setores público e privado acelera a partilha de inteligência e a resposta coordenada a ameaças emergentes.

Adaptar-se rapidamente deixou de ser uma vantagem competitiva para se tornar uma exigência estratégica. As organizações que resistem a incorporar IA tornam-se vulneráveis a ataques automatizados e em constante evolução.

Estratégias como Zero Trust, baseadas em “nunca confiar, verificar sempre”, reduzem a superfície de ataque e dificultam o movimento lateral dos invasores.

Ainda assim, permanece uma questão crítica: estarão as práticas atuais preparadas para enfrentar algoritmos que aprendem e exploram vulnerabilidades em tempo real? A rapidez com que a IA evolui pode ultrapassar os métodos tradicionais de defesa, exigindo não apenas novas ferramentas, mas uma filosofia de defesa mais dinâmica, colaborativa e orientada para cenários futuros, até os que ainda não conseguimos imaginar.

RISCOS DA IA

Apesar das vantagens, a IA traz diversos riscos que não podem ser ignorados. Entre estes, destaca-se o viés algorítmico, que ocorre quando modelos são treinados com dados incompletos ou tendenciosos, levando a decisões incorretas, desde classificar falsamente um comportamento legítimo até falhar na deteção de um ataque real,

Outro risco relevante é a dependência excessiva da IA. As organizações que delegam demasiadas funções críticas a sistemas automatizados podem perder a capacidade de resposta manual e de análise crítica. Se a IA falhar ou for manipulada, a ausência de competências humanas preparadas para intervir pode aumentar os danos do ataque.

O FUTURO DA SEGURANÇA

A era dos cibertaques potenciados por IA já é realidade. A questão não é mais “se” vai acontecer, mas “quando” e “como” cada organização vai responder.

Unir inteligência artificial e humana é o único caminho para manter as portas digitais seguras num mundo onde as máquinas já aprenderam a atacar e não vão desaprender.

O futuro da segurança não será construído apenas por máquinas, mas pela colaboração, adaptação e, sobretudo, pelo fator humano.

empresas

CIBERATAQUES COM IA: A PRÓXIMA GRANDE AMEAÇA ÀS EMPRESAS

A INTELIGÊNCIA ARTIFICIAL (IA) É MOTOR DE INOVAÇÃO, MAS TAMBÉM UMA ARMA PARA ATACANTES. OS AI-POWERED CYBERATTACKS ELEVAM O RISCO E DESAFIAM A RESILIÊNCIA DAS EMPRESAS.

A IA tornou-se um dos pilares centrais da transformação digital. Da produtividade à previsão de negócio, passando pela automação, a sua adoção é vista como motor de competitividade e inovação. Mas, como em todas as grandes revoluções tecnológicas, existe um lado sombrio: os atacantes também perceberam rapidamente o potencial da IA ao serviço do cibercrime. Hoje, assistimos ao surgimento de uma nova geração de ataques — os chamados *AI-powered cyberattacks* — que elevam o nível de sofisticação e representam um desafio sem precedentes para profissionais de cibersegurança.



Para as **empresas**, a questão deixou de ser apenas tecnológica: a cibersegurança é hoje indissociável da continuidade e sobrevivência das organizações.

A BOA NOTÍCIA É QUE A IA TAMBÉM ESTÁ A SER USADA NA DEFESA. AS SOLUÇÕES DE CIBERSEGURANÇA MAIS AVANÇADAS RECORREM A MODELOS INTELIGENTES PARA APOIAR A AVALIAÇÃO DE RISCO, MONITORIZAR COMPORTAMENTOS, DETETAR E RESPONDER DE FORMA AUTOMÁTICA E MAIS ATEMPADA.

A INTELIGÊNCIA ARTIFICIAL AO SERVIÇO DO CIBERCRIME

Os ataques potenciados por IA distinguem-se pela sua capacidade de serem mais rápidos, adaptativos, dissimulados e difíceis de detetar. Algoritmos avançados permitem criar campanhas de **emails fraudulentos** altamente personalizadas, reduzindo a eficácia das defesas tradicionais.

Outra vertente é o **malware evasivo**: software malicioso que se adapta ao ambiente de IT das empresas para escapar a antivírus e a **soluções de segurança**.

A proliferação de **deepfakes** é também um vetor em crescimento. Ao combinar engenharia social com conteúdos falsificados, mas aparentando elevada credibilidade, os **hackers** conseguem manipular vítimas para partilhar credenciais ou autorizar transferências financeiras, por exemplo.

Além disso, a IA permite automatizar a exploração de vulnerabilidades e o mapeamento de **sistemas de informação** de uma qualquer empresa, ampliando a superfície de ataque e reduzindo a margem de reação.

IMPACTOS NAS ORGANIZAÇÕES

Para as empresas, a ameaça não é apenas tecnológica — é também estratégica e reputacional. Um ataque pode provocar **danos financeiros** diretos, danos na imagem/marca das empresas, sujeitar a pagamento de **coimas no âmbito da NIS2** e até levar à **responsabilização pessoal de executivos**, além de abalar a confiança de clientes e parceiros.

Não se trata apenas de grandes organizações. Embora setores como a **banca, saúde, telecomunicações, energia, transportes, distribuição de água e administração pública** estejam especialmente expostos pela criticidade dos serviços que prestam e pelo valor dos dados que gerem, todas as organizações enfrentam riscos relevantes. O tema da **proteção de dados** e da **segurança da informação** está, por isso, no centro do debate.

Imagine-se um hospital confrontado com ransomware potenciado por IA, capaz de contornar backups e atingir de forma dirigida **dispositivos** médicos. A



falta de **proteção** adequada à sofisticação do ataque traduz-se em risco financeiro, operacional e humano.

Outro fator relevante é a velocidade com que estes ataques evoluem. Um modelo de IA pode aprender com cada tentativa falhada e ajustar-se automaticamente, tornando-se progressivamente mais eficaz.

A RESPOSTA DEFENSIVA: IA CONTRA IA

A boa notícia é que a IA também está a ser usada na defesa. As **soluções de cibersegurança** mais avançadas recorrem a modelos inteligentes para apoiar a **avaliação de risco**, monitorizar comportamentos, detetar e responder de forma automática e mais atempada.

Ferramentas de **deteção comportamental** e **análise preditiva** permitem identificar padrões suspeitos mesmo quando não existem assinaturas conhecidas, reduzindo a exposição a novas **ciberameaças**. Em paralelo, a **automação de resposta** oferece às equipas a possibilidade de isolar máquinas e redes comprometidas ou bloquear rapidamente comunicações suspeitas.

Mas tecnologia não chega: a **gestão de risco** continua a ser determinante. Conhecer os ativos críticos e os dados fulcrais a preservar, avaliar vulnerabilidades e aplicar controlos adequados periódicos, são passos inadiáveis.

GOVERNAÇÃO E RESILIÊNCIA

Na União Europeia, a **ENISA** e o recente **AI Act** têm definido diretrizes específicas para segurança em sistemas de IA, ajudando as organizações a gerir riscos. Paralelamente, discute-se a necessidade de enquadramentos normativos ainda mais robustos para acompanhar a rápida evolução tecnológica.

Para os **CISO** (Chief Information Security Officer), a governação da IA é uma prioridade dupla: proteger os sistemas internos das empresas e, em paralelo, garantir que os próprios modelos utilizados não se tornam vulnerabilidades.

Neste cenário, a **segurança cibernética** ativa e a resiliência organizacional passam a ser palavras-chave, exigindo a combinação de **soluções de segurança** com processos claros, equipas treinadas e uma cultura de cibersegurança disseminada a todos os níveis em cada empresa.

SENSIBILIZAÇÃO: UM PILAR ESSENCIAL

Mesmo os ataques mais sofisticados acabam quase sempre por explorar a vulnerabilidade humana. A IA amplifica o poder da engenharia social, implicando o reforço da necessidade de programas de sensibilização mais eficazes e continuados no tempo.

Colaboradores capazes de identificar **emails fraudulentos**, desconfiar de chamadas inesperadas de vishing, validar e reconfirmar pedidos de transações financeiras, confirmar identidades por canais alternativos, ou reportar comportamentos anómalos continuam a ser a primeira linha de defesa.

CONCLUSÃO

Os AI-powered cyberattacks não são uma previsão futurista — são uma realidade. A sofisticação e a velocidade que a IA traz ao **cibercrime** obrigam as organizações a repensar estratégias, investir em **soluções de cibersegurança** e cultivar uma cultura de **segurança da informação**.

3 EXEMPLOS DE ATAQUES POTENCIADOS POR IA

1. **Phishing automatizado** – geração de milhares de **emails fraudulentos** personalizados, adaptados ao perfil de cada vítima.

2. **Deepfakes para fraude financeira** – uso de áudio e vídeo falsificados para convencer executivos ou equipas financeiras a autorizar transferências.

3. **Malware adaptativo** – código malicioso que analisa o ambiente em tempo real e altera o seu comportamento para escapar às normais ferramentas de **cibersegurança**.

O **Mês Europeu da Cibersegurança**, em outubro, sublinha a urgência de agir. Porque se a IA está a transformar a dinâmica dos **negócios**, também está a redefinir as ameaças no **ciberespaço**. Só uma abordagem proativa, equilibrando inovação com proteção abrangente, permitirá às empresas enfrentar este novo paradigma com confiança.

Neste cenário, contar com parceiros especializados é cada vez mais determinante. O **MEO Empresas** tem vindo a investir de forma consistente em plataformas, competências técnicas e serviços avançados de cibersegurança combinados com IA, disponibilizando soluções ajustadas à dimensão e ao setor de cada organização. Ao apoiar as empresas na proteção de redes, sistemas e dados críticos, contribui não apenas para a redução do risco, mas também para o reforço da resiliência digital, fator essencial para sustentar a competitividade num ambiente de ameaças em constante evolução. ◀

VisionWare since 2005

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

CIBERATAQUES & IA: A DUPLA QUE DESAFIA EMPRESAS E DEMOCRACIAS

A UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL (IA) EM CIBERATAQUES ESTÁ A TRANSFORMAR O PANORAMA DA SEGURANÇA DIGITAL EM TODO O CIBERESPAÇO, IMPLICANDO TANTO O SETOR EMPRESARIAL COMO O CONTEXTO GEOPOLÍTICO.

Os chamados "AI powered cyberattacks", ciberataques potenciados por IA, distinguem-se pela capacidade de operar com maior velocidade, escala e sofisticação, tirando partido da automatização e da personalização. Hoje, um grupo cibercrimoso, até com pouco conhecimento, através do potencial de evolução disponibilizado por IA, consegue criar ciberataques com bastante sofisticação e complexidade, por exemplo, através de campanhas de phishing multilingues, adaptadas ao perfil de cada vítima, praticamente indistinguíveis da comunicação legítima. É uma realidade no panorama atual do cibercrime. A IA veio dar força, conhecimento e escalabilidade à comunidade cibercriminosa ao permitir desenvolver mais ciberataques, com a agravante de maior taxa de sucesso.

No setor empresarial, já se verificaram inúmeros casos em que deepfakes de voz e vídeo foram utilizados para simular executivos em reuniões virtuais, induzindo colaboradores a autorizar transferências milionárias. Estes ataques exploram não só vulnerabilidades técnicas, mas também a vulnerabilidade humana e a resiliência dos processos internos,



BRUNO CASTRO, VISIONWARE

SE OS CIBERATAQUES JÁ SÃO UMA AMEAÇA POR SI SÓ, QUANDO POTENCIADOS PELA IA REPRESENTAM NÃO APENAS UMA EVOLUÇÃO TÉCNICA, MAS TAMBÉM UMA MUDANÇA ESTRUTURAL EM TODO O ESPECTRO DE CIBERAMEAÇAS CONTEMPORÂNEAS.

demonstrando como a IA potencia esquemas de fraude e engenharia social com grande facilidade e com enorme taxa de sucesso. A capacidade de replicar a identidade de líderes organizacionais com grande realismo coloca em causa modelos tradicionais de verificação e exige novas medidas de controlo e validação.

No plano geopolítico, a IA tem vindo a ser usada para campanhas de desinformação em larga escala, dirigidas contra estados ou blocos regionais inteiros. Exemplos incluem operações atribuídas à China, que recorrem a redes de contas falsas e conteúdos criados por IA para influenciar perceções políticas em Taiwan, ou campanhas ligadas à Rússia durante a guerra na Ucrânia, com uso de bots e vídeos manipulados para fragilizar a confiança pública e semear divisão social. Um dos desenvolvimentos mais preocupantes é o uso da IA para microtargeting em processos eleitorais: campanhas de desinformação são desenhadas à medida de perfis individuais ou de grupos específicos e exploraram dados pessoais para difundir mensagens polarizadoras altamente eficazes. Este tipo de ataque, invisível para o público em geral, tem o potencial de influenciar diretamente a opinião e o voto em contextos democráticos, com a agravante, de ser realizado em larga escala e de forma acelerada.

Perante este cenário, as organizações enfrentam um desafio duplo: proteger-se de fraudes financeiras sofisticadas e preparar-se para contextos de desinformação ou manipulação que podem afetar toda a supply chain, mercados e até a confiança nas instituições democráticas. A resposta passa por reforçar mecanismos de autenticação, integrar Threat Intelligence específica sobre técnicas assistidas por IA nos Security Operations Center (SOC), adotar soluções de monitorização que analisem padrões comportamentais e investir na literacia digital dos colaboradores e cidadãos.

Se os ciberataques já são uma ameaça por si só, quando potenciados pela IA representam não apenas uma evolução técnica, mas também uma mudança estrutural em todo o espectro de ciberameaças contemporâneas. Ao mesmo tempo que disponibilizam novas oportunidades para a defesa, colocam nas mãos da comunidade cibercriminosa – sejam agentes criminosos, sejam estados – ferramentas muito poderosas capazes de manipular, enganar e influenciar numa escala sem precedentes. A preparação contra esta nova geração de ataques é, por isso, um imperativo tanto empresarial como estratégico, especialmente, em contextos geopolíticos, onde a confiança pública e a soberania digital é um dos ativos mais valiosos da nossa sociedade. ◀

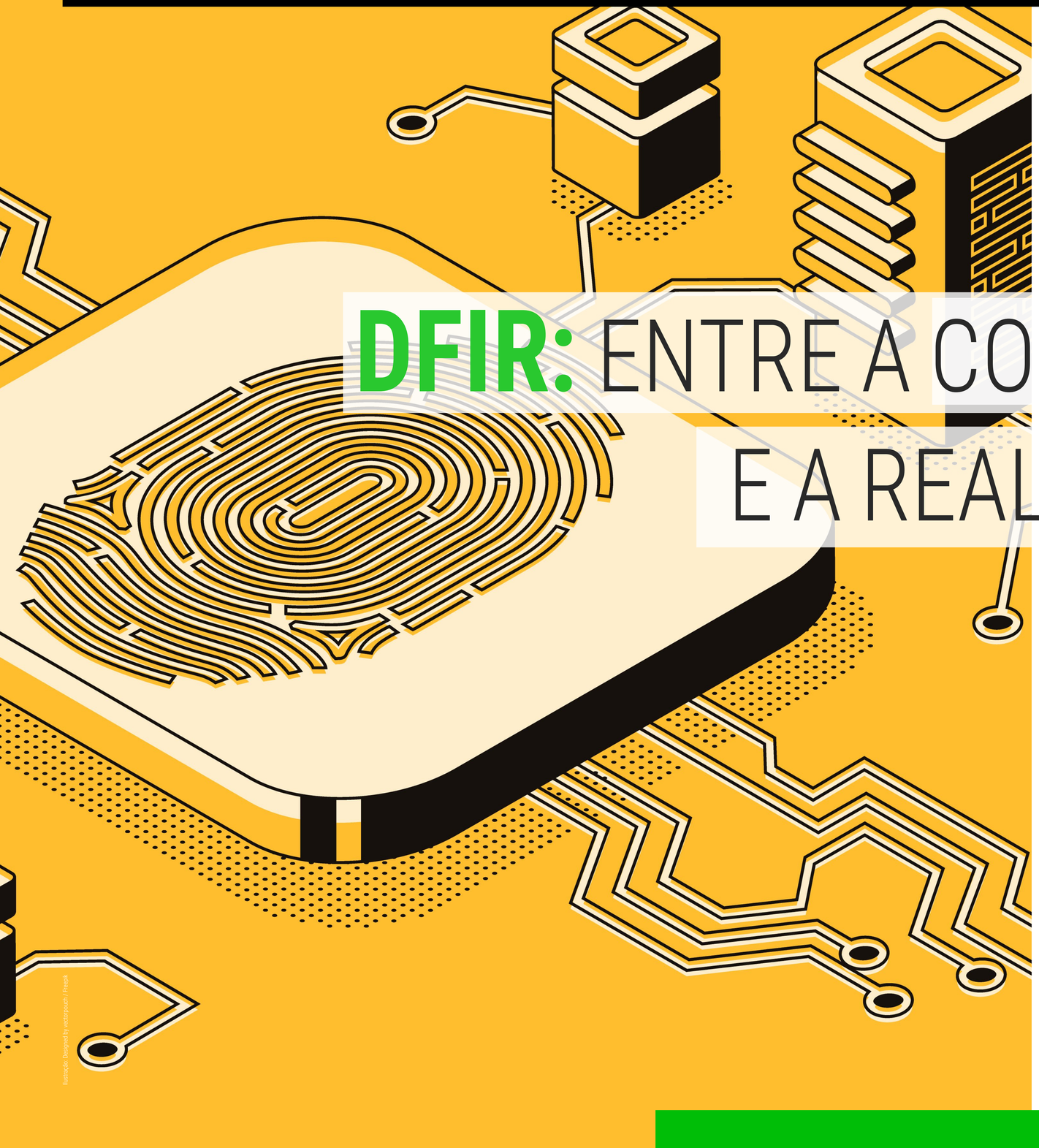


Ilustração: Designed by vectorpouch / Freepik

POR RUI DAMIÃO

DFIR: ENTRE A COMPETÊNCIA TÉCNICA E A REALIDADE OPERACIONAL

EM POUCO TEMPO, UM CIBERCRIMINOSO PODE TER ACESSO TOTAL AOS SISTEMAS CRÍTICOS DE UMA ORGANIZAÇÃO E A DIFERENÇA ENTRE RECUPERAR RAPIDAMENTE OU COLAPSAR POR COMPLETO DEPENDE DE UMA CAPACIDADE QUE MUITAS EMPRESAS PORTUGUESAS AINDA TRATAM COMO SECUNDÁRIO: O DIGITAL FORENSICS AND INCIDENT RESPONSE.



Quando um ataque de ransomware cifra uma rede inteira em menos de uma hora, a diferença entre sobreviver e colapsar está na capacidade de resposta imediata. O Digital Forensics and Incident Response (DFIR) deixou de ser uma especialidade técnica para se tornar numa competência crítica de sobrevivência empresarial.

Portugal encontra-se numa "posição curiosa" no panorama europeu de DFIR, como explica David Grave, Security Director da Claranet Portugal, porque o país é "tecnicamente competente, mas operacionalmente reativo". Esta observação resume a realidade nacional: enquanto as instituições financeiras e grandes operadoras de telecomunicações já possuem capacidades sólidas, um segmento significativo de PME e entidades públicas mantém níveis reduzidos de maturidade.

Pedro Soares, Diretor Nacional de Segurança da Microsoft Portugal, contextualiza: "Portugal encontra-se num nível intermédio de maturidade em DFIR no contexto europeu. As empresas nacionais têm vindo a reforçar as suas capacidades de resposta a incidentes, mas ainda não atingem o grau de especialização de países como o Reino Unido ou os nórdicos". A verdade é que a maioria das organizações nacionais só investe em DFIR depois do primeiro ataque significativo, tratando estas capacidades como o serviço de limpeza que se chama após o desastre.

AMEAÇAS EM EVOLUÇÃO

A velocidade dos ataques modernos transformou radicalmente o panorama do DFIR. Segundo Pedro Soares, "o ransomware tornou-se mais rápido e destrutivo, de acordo com investigações da Microsoft, que mostram redes inteiras cifradas em menos de 45 minutos após a intrusão inicial". Esta aceleração não é acidental; os atacantes desenham deliberadamente ataques para superar os tempos de resposta tradicionais.

"Os atacantes estão deliberadamente a desenhar ataques cada vez mais rápidos, sofisticados e furtivos", explica David Grave. "Utilizam técnicas de *living-off-the-land* e exploram ferramentas legítimas do sistema, o que torna a distinção entre atividade maliciosa e administrativa um pesadelo". Esta evolução leva a que as equipas forenses já não procurem apenas malware óbvio, mas sim comportamentos anómalos em ferramentas que deveriam ser legítimas.

A complexidade aumentou exponencialmente com os ataques *cloud-native*. Como refere Christiam Carrillo, Cyber Threats Management Offering Leader da IBM SPG, "estamos a observar um aumento significativo em comprometimentos na cloud e violações na cadeia de abastecimento, que podem ter impactos em cascata em todo o ecossistema". Estes ataques exploram credenciais, API e ambientes cloud distribuídos, tornando a recolha e análise de evidências substancialmente mais complexa.

A Inteligência Artificial (IA) emergiu como uma nova arma para os cibercriminosos. Tiago Sousa, Team Leader da Equipa de Cyber Defense Operations da VisionWare, observa que "a utilização cada vez mais evidente de inteligência artificial por parte dos atacantes, seja para automatizar ataques de larga escala, criar código malicioso adaptativo ou criar campanhas de phishing altamente personalizadas e credíveis". O resultado são investigações forenses que exigem correlação e validação muito mais sofisticadas do que no passado.

OS ERROS CRÍTICOS DAS ORGANIZAÇÕES PORTUGUESAS

O primeiro erro que as organizações portuguesas cometem é sistematicamente ignorado: confundir documentação com preparação. "O erro mais comum que observamos nas organizações portuguesas é a existência de planos de resposta que permanecem apenas no papel, sem nunca serem testados em exercícios práticos", alerta Olga Carvalho, Senior Cybersecurity Consultant da Noesis. Pedro


TIAGO SOUSA, VISIONWARE

Soares, da Microsoft, é mais direto: "o erro mais frequente é a ausência de um plano formal e testado de resposta a incidentes. Muitas organizações não desenvolvem um *playbook* claro nem realizam exercícios regulares, o que as deixa vulneráveis quando enfrentam um ataque real".

O segundo erro são os silos departamentais que se transformam em barreiras fatais durante crises. "O maior obstáculo não é técnico, é político. São os silos", constata David Grave, que acrescenta que "a equipa de IT, a de segurança, o departamento jurídi-

"A UTILIZAÇÃO CADA VEZ MAIS EVIDENTE DE INTELIGÊNCIA ARTIFICIAL POR PARTE DOS ATACANTES, SEJA PARA AUTOMATIZAR ATAQUES DE LARGA ESCALA, CRIAR CÓDIGO MALICIOSO ADAPTATIVO OU CRIAR CAMPANHAS DE PHISHING ALTAMENTE PERSONALIZADAS E CREDÍVEIS"


DAVID GRAVE, CLARANET PORTUGAL

co, os recursos humanos e a gestão de topo raramente falam a mesma língua ou têm os mesmos objetivos durante uma crise". Christiam Carrillo reforça que "um dos obstáculos mais comuns é a falta de definição clara de funções, responsabilidades e caminhos de escalabilidade dentro dos programas de resposta a incidentes".

O terceiro erro é técnico, mas com um impacto potencialmente devastador: os *gaps* críticos de visibilidade. Para David Grave, "muitas organizações têm uma obsessão com perímetros: investem fortunas em firewalls, mas não sabem o que se passa dentro da própria rede". Pedro Soares identifica problemas específicos, como "cobertura incompleta de ferramentas de deteção. Ainda há organizações sem soluções modernas de EDR ou XDR em todos os dispositivos, ou sem um SIEM integrado, o que cria zonas de invisibilidade".

Particularmente preocupante é a deficiência em *cloud forensics*. Olga Carvalho aponta "visibilidade limitada em ambientes cloud e SaaS" como um problema para as organizações nacionais. "Em muitos casos, não existem logs de API, identidade ou telemetria de plataforma suficientes para suportar uma investigação eficaz", diz. Esta lacuna torna-se crítica quando se considera que a maioria dos ataques modernos explora precisamente estes ambientes.

AUTOMAÇÃO OU HUMANO?

A automação no DFIR não é uma opção; é uma necessidade de sobrevivência. David Grave, da Claranet Portugal, reforça que "se a automação sem *expertise* humana é perigosa, a *expertise* humana sem

> "A EQUIPA DE IT, A DE SEGURANÇA, O DEPARTAMENTO JURÍDICO, OS RECURSOS HUMANOS E A GESTÃO DE TOPO RARAMENTE FALAM A MESMA LÍNGUA OU TÊM OS MESMOS OBJETIVOS DURANTE UMA CRISE"

automação é inviável". Esta dualidade define o futuro das investigações forenses.

O consenso entre especialista é claro onde a automação é superior. Christiam Carrillo explica que a "automação desempenha um papel crítico nas investigações forense modernas. Permite velocidade e escala ao recolher evidências, correlacionar alertas e lidar com tarefas repetitivas ou sensíveis ao tempo". Pedro Soares, da Microsoft, reforça que se deve "utilizar a automação para tarefas repetitivas e técnicas, libertando os analistas para se focarem em decisões mais complexas e estratégicas".

Contudo, a intervenção humana mantém-se insubstituível nas decisões críticas. "A experiência dos analistas é determinante para interpretar o contexto, identificar padrões novos, definir prioridades e coordenar equipas", afirma Pedro Soares. Olga Carvalho, da Noesis, especifica que as "decisões estratégias e complexas continuam a depender do fator humano. Atividades como engenharia reversa de malware, correlação de evidências, validação de

"O ERRO MAIS FREQUENTE É A AUSÊNCIA DE UM PLANO FORMAL E TESTADO DE RESPOSTA A INCIDENTES. MUITAS ORGANIZAÇÕES NÃO DESENVOLVEM UM PLAYBOOK CLARO NEM REALIZAM EXERCÍCIOS REGULARES, O QUE AS DEIXA VULNERÁVEIS QUANDO ENFRENTAM UM ATAQUE REAL"


OLGA CARVALHO, NOESIS

hipóteses de ataque ou comunicação com clientes, reguladores e autoridades não podem ser totalmente automatizadas".

A IA está a revolucionar este equilíbrio. Pedro Soares antecipa que as soluções "já ajudam os analistas a sintetizar grandes volumes de dados e a sugerir ações. É expectável que, dentro de três a cinco anos, assistentes baseados em IA estejam amplamente integrados nos centros de operações de segurança".

O modelo híbrido entre humano e máquina emerge como a solução ideal: automatizar a triagem,

recolha e análise inicial, reservando para especialistas humanos as interpretações complexas e decisões estratégicas que definem o sucesso ou o fracasso da resposta a incidentes.

O QUE OS RESPONSÁVEIS DE CIBERSEGURANÇA DEVEM FAZER

A pressão regulatória está a acelerar e as organizações não têm tempo a perder. Pedro Soares refere que "normas como a DORA e a NIS2 vão impor requisitos mais exigentes em matéria de resiliência e reporte de incidentes. É fundamental que os CISO antecipem estas obrigações, implementando processos compatíveis com os prazos legais de notificação".


PEDRO SOARES, MICROSOFT PORTUGAL

"NORMAS COMO A DORA E A NIS2 VÃO IMPOR REQUISITOS MAIS EXIGENTES EM MATÉRIA DE RESILIÊNCIA E REPORTE DE INCIDENTES. É FUNDAMENTAL QUE OS CISO ANTECIPEM ESTAS OBRIGAÇÕES, IMPLEMENTANDO PROCESSOS COMPATÍVEIS COM OS PRAZOS LEGAIS DE NOTIFICAÇÃO"

David Grave vai mais longe e defende que o "DFIR deixou de ser uma especialidade técnica para se tornar numa competência crítica de sobrevivência empresarial". Esta transformação exige ação imediata em três frentes prioritárias.

A primeira é a centralização e retenção adequada de logs. Olga Carvalho especifica que "superar estes *gaps* passa por investir em centralização de logs (SIEM/EDR/XDR), políticas de retenção adequadas e integração nativa com API de cloud, garantindo que as evidências ficam preservadas e acessíveis para suportar investigações completas e defensáveis".

O segundo ponto é o teste regular e rigoroso de capacidades. Pedro Soares alerta que "exercícios de simulação e simulações em ambientes controlados são essenciais para validar os planos de ação, identificar pontos fracos e garantir que as equipas conseguem agir com precisão sob pressão".


CHRISTIAM CARRILLO, IBM SPG

"DESENVOLVER PLANOS DE AÇÃO PARA INCIDENTES QUE ENVOLVAM SISTEMAS DE IA, VALIDAR COMO OS PROCESSOS SE VÃO ADAPTAR E CONSIDERAR A RESILIÊNCIA DA IA COMO PARTE DA ESTRATÉGIA MAIS AMPLA DA CIBERSEGURANÇA"

A terceira e última frente é a preparação para o futuro próximo da IA. "A integração de inteligência artificial e machine learning em ferramentas forenses será inevitável", antecipa Tiago Sousa, da VisionWare. "Os CISO devem começar já a preparar as suas organizações para esta evolução, ao investir em formação especializada e tecnologias adaptadas a ambientes híbridos".

Christiam Carrillo, da IBM, resume a preparação necessária para os responsáveis de cibersegurança: "desenvolver planos de ação para incidentes que envolvam sistemas de IA, validar como os processos se vão adaptar e considerar a resiliência da IA como parte da estratégia mais ampla da cibersegurança".

RESPOSTA CONTÍNUA

A mensagem dos especialistas é unânime e urgente: o tempo das meias-medidas no DFIR acabou. David Grave partilha uma realidade incontornável: "o DFIR vai deixar de ser 'resposta a incidentes' para se tornar 'resposta contínua', ou seja, não apenas como uma resposta reativa. A análise forense será proativa, integrada em atividades regulares de *threat hunting*".

Esta transformação não é uma possibilidade distante e já está a acontecer. As organizações que continuam a tratar o DFIR como um 'mal necessário' pós-incidente arriscam-se a ficar vulneráveis quando a próxima crise chegar, descobrindo que os seus processos reativos são insuficientes face à velocidade e sofisticação dos ataques modernos.

Para os responsáveis de cibersegurança a escolha é simples, mas não é fácil: evoluir para capacidades de DFIR proativas e integradas, ou aceitar que a próxima crise pode ser a última. A maturidade de Portugal no contexto europeu representa simultaneamente uma oportunidade e um aviso. Temos a competência técnica para dar o salto, mas é preciso ter vontade operacional para o fazer antes de ser tarde demais.

por Rafael Rosseto,
Network Security Engineer, CSO

DIGITAL FORENSIC AND INCIDENT RESPONSE:

A RELEVÂNCIA NA SEGURANÇA DE REDES

A CRESCENTE DEPENDÊNCIA DE SISTEMAS DIGITAIS TRANSFORMOU AS REDES CORPORATIVAS NUM DOS PRINCIPAIS ALVOS DOS CIBERCRIMINOSOS.

Fugas de dados, ataques de ransomware e intrusões silenciosas deixaram de ser exceções para se tornarem riscos diários. Neste contexto, as práticas de Digital Forensic e Incident Response afirmam-se como peças essenciais, não apenas para a recuperação de incidentes, mas também para a preservação da integridade e da segurança de toda a infraestrutura de rede.

O PAPEL DA FORENSE DIGITAL EM AMBIENTES DE REDE

A Forense Digital vai muito além da simples recolha de evidências após um ataque. Em redes modernas, distribuídas e com elevado volume de tráfego, a análise forense precisa de identificar padrões anómalos e preservar informação crítica sem comprometer a operação. Registos de firewall, autenticações e fluxos de tráfego tornam-se fontes valiosas para rastrear a origem de uma intrusão e reconstruir a cronologia de um ataque.

Outro ponto fundamental é a manutenção da cadeia de custódia dos dados, que garante a validade das evidências em caso de necessidade de utilização em processos legais, evitando qualquer contestação à sua autenticidade.

RESPOSTA A INCIDENTES: DA DETEÇÃO À CONTENÇÃO

A fase de Incident Response inicia-se logo após a identificação de um comportamento suspeito. Em redes empresariais, o tempo é um fator crítico: quanto mais rápida for a



RAFAEL ROSSETO, NETWORK SECURITY ENGINEER, CSO

contenção, menores são os impactos. Entre as medidas mais comuns destacam-se:

- Isolamento dos dispositivos comprometidos, para impedir a movimentação lateral do atacante.
- Análise de pacotes em tempo real, que permite identificar comandos de controlo remoto ou exfiltração de dados sensíveis.
- Aplicação de patches emergenciais em serviços vulneráveis.

Um plano eficaz de resposta a incidentes não se limita à resolução técnica. Deve igualmente contemplar a comunicação interna, a eventual notificação de clientes ou parceiros e o registo detalhado de todas as ações realizadas, permitindo um processo de aprendizagem contínuo.

INTEGRAÇÃO COM A SEGURANÇA PREVENTIVA

Isso não deve ser visto apenas como uma reação a incidentes, mas como parte integrante da política global de segurança de redes. A partir da análise de incidentes passados, as equipas podem ajustar regras de firewall, reforçar sistemas de deteção e prevenção de intrusões (IDS/IPS) e aplicar controlos de acesso mais granulares. Este ciclo de aprendizagem contribui para uma rede mais robusta e resistente a ataques futuros.

FERRAMENTAS DE APOIO À PROTEÇÃO E RESPOSTA

Para implementar uma estratégia eficaz, as organizações recorrem a diferentes tipos de ferramentas especializadas, entre as quais:

- **Sistemas de Gestão de Eventos e Informações de Segurança** (SIEM) – Usados para centralizar e correlacionar logs de toda a infraestrutura.
- **IDS/IPS** (Intrusion Detection/Prevention Systems) – Ajudam a identificar tráfego suspeito e bloquear ataques em tempo real.
- **Ferramentas de análise forense** – Voltadas para a investigação de dispositivos e recolha de evidências digitais.
- **Plataformas de resposta a incidentes** (SOAR) – Permitem automatizar fluxos de resposta e reduzir o tempo de contenção.
- **Firewalls de próxima geração** (NGFW) – Que combinam filtragem tradicional com funcionalidades avançadas, como inspeção profunda de pacotes (DPI) e controlo de aplicações.
- **Monitorização de rede e tráfego** – Indispensáveis para reconstruir a atividade de um ataque.
- **EDR/XDR** (Endpoint/Extended Detection & Response) – Que monitorizam endpoints e permitem agir rapidamente sobre máquinas comprometidas.

DESAFIOS ATUAIS

Dois aspetos sobressaem como desafios constantes:

1. **Criptografia do tráfego** – embora garanta privacidade, dificulta a inspeção de pacotes maliciosos.
2. **Ambientes híbridos e na nuvem** – a recolha e correlação de registos em múltiplas plataformas exige ferramentas mais sofisticadas e equipas com competências multidisciplinares.

CONCLUSÃO

O Digital Forensic e Incident Response deixou de ser uma prática opcional e passou a constituir um pilar estratégico na defesa das redes empresariais. Ao conjugar a investigação forense com uma resposta célere e estruturada, as organizações conseguem reduzir danos, proteger dados sensíveis e reforçar a sua resiliência perante ameaças cada vez mais sofisticadas. ◀

SECURNET
ALWAYS ONLINE | ALWAYS SECURE

por Miguel Barreiros,
Sales & Marketing Director da SECURNET

DIGITAL FORENSICS AND INCIDENT RESPONSE:
UMA JOGADA QUE NÃO ACABA NO GOLO

USO MUITAS VEZES ANALOGIAS COM O FUTEBOL PARA FALAR DE CIBERSEGURANÇA. UM BOM EXEMPLO ENCONTRA-SE QUANDO COMPARAMOS A CIBERSEGURANÇA DEFENSIVA COM GUARDA-REDES E OS CIBERCRIMINOSOS COM AVANÇADOS - AOS PRIMEIROS BASTARÁ UMA FALHA PARA SEREM CULPADOS NAS DERROTAS, AOS AVANÇADOS BASTA UM GOLO PARA SEREM OS HERÓIS NAS VITÓRIAS!

Existe ainda a perigosa ilusão de que basta investir em prevenção para estar protegido - firewalls e antivírus de última geração, autenticação forte e todo um manancial de defesas essenciais como se de um muro intransponível se tratasse. O problema é simples: **os atacantes só precisam de acertar uma vez, as organizações precisam de acertar sempre** e por "muito bom que seja o guarda-redes" ninguém tem uma taxa de sucesso de 100%, nem tão pouco existem barreiras intransponíveis. Acreditar na invulnerabilidade das organizações é acreditar na infalibilidade das pessoas, uma convicção que muda no dia em que são notícia pelos piores motivos.

É aqui que surge e que se impõe como fundamental o **Digital Forensics and Incident Response** (**DFIR**). Não como um "plano B" ou uma "remediação", como quase sempre é interpretado, mas como peça central da ciber-defesa moderna. Como alguém disse, o **DFIR** "*não é sobre apagar fogos, mas sim garantir que a próxima faísca não se transforma num novo incêndio*". Se não juntarmos resposta imediata (também fundamental no controlo de danos) com investigação profunda, cada ataque será apenas mais um na estatística, em vez de uma oportunidade para reforçar a resiliência. Retomada por ousadia a linguagem futebolística, o ciclo de uma jogada não acaba quando a bola transpõe a linha de golo...


MIGUEL BARREIROS, SALES & MARKETING DIRECTOR DA SECURNET

Há muito que se deixou de equacionar a ocorrência de um ciberincidente, mas tão somente "quando" e sobretudo "como" lhe vamos reagir. O verdadeiro diferenciador não está apenas em evitar ataques, porque algum dia não será possível, mas em responder com eficácia, em aprender com eles. O DFIR representa a maturidade da ciberdefesa:

• por um lado, a **(análise) forense digital**, na maior parte das vezes vista como uma tarefa apenas com interesse jurídico, pode e deve servir para compreender o rasto do atacante. Como entrou, que técnicas usou e que falhas explorou? Permite transformar desastres (a evitar) em importantes lições, enquanto coleta evidências para, numa Era de "regulamentos", serem apresentadas a que de direito e, principalmente, provarem a existência de medidas adequadas, algo tão crítico, em determinados contextos, quanto a própria contenção do ataque.

• Do outro, a **resposta a incidentes** - verdadeira linha da frente, tem uma urgência diferente - exige rapidez, método e disciplina para conter danos e devolver a organização à normalidade. Quando dados são encriptados e informação sensível começa a circular na Dark Web, ou a organização tem playbooks preparados, equipas treinadas e uma cultura de continuidade de negócio ou entra em pânico e aumenta ainda mais o caos.

Estas dimensões formam em conjunto um profícuo ciclo contínuo: **reagir**, **compreender** e **evoluir**. Contudo, os desafios são reais: a falta crónica de especialistas, a complexidade crescente e a pressão regulatória no mesmo sentido. Mas ignorá-los não os torna menos urgentes. DFIR mais que um custo, é um seguro contra catástrofes que não as evita, mas garante um futuro, quiçá mais fortalecido depois da sua ocorrência. Aceitando que os riscos não se eliminam, mas que cada incidente será uma oportunidade para os mitigar e minimizar.

Ainda assim, mesmo que a tecnologia seja fantástica (e pode ser), ainda que automatismos sejam fundamentais (e são), ainda que Inteligência Artificial já seja um must have (e é), o que terá de existir, para além disso? Diria que humanos que coordenem, decidam, recuperem o negócio e, de forma cada vez mais consistentemente necessária, comuniquem!

Lembre-se (AI dixit) que "tempo é impacto, evidência é valor e resiliência é estratégia".

É precisamente por isso que a SECURNET tem vindo a desenvolver o DFIR como um serviço especializado, capaz de responder em 24/7 e trazendo a inteligência prática de outros incidentes e investigações, beneficiando de automação, inteligência artificial e diversas fontes de inteligência de ameaças, com equipas fortes, bem preparadas e multidisciplinares, recorrendo sempre que necessário às variadas unidades internas de SOC + NOC (com suporte e operação) + Engenharia (de sistemas + de redes + de segurança) + GRC + Consulting, para suportar os nossos clientes. Contate-nos em *info@securnet.pt*, ou Tel +351 224 673 094* / +351 213 622 204*

PS: Para terminar como comecei, a análise forense digital é o VAR, a reconstituição dos incidentes será o vídeo do jogo, mais tarde visualizado e explicado à equipa para "perceber e melhorar" os erros cometidos, enquanto o planeamento e continuado treino na resposta a incidentes são o treino diário ao longo de toda a época, melhorando desempenho, evitando golos e se possível marcando-os! Por outro lado, correndo até o risco de abusar das analogias futebolísticas e dos próprios conceitos, a equipa SECURNET propõe-se ser (toda ou em parte) a equipa técnica moderna, formada por inúmeros especialistas (de treinadores setoriais a vídeo analistas, de médicos a fisiatras e fisioterapeutas, de psicólogos a secretários-técnicos, entre muitos outros). ◀

NUNO GOES, CYBERSECURITY ENGINEER, É ESPECIALISTA EM SEGURANÇA DE INFORMAÇÃO E CIBERSEGURANÇA COM UMA EXTENSA EXPERIÊNCIA NO SETOR. É MEMBRO DA DIREÇÃO DA CIIWA, ONDE COORDENA O GRUPO DE TRABALHO ESPECIALIZADO DA SEGURANÇA DE INFORMAÇÃO. NESTE DOMÍNIO, AS SUAS PRINCIPAIS ÁREAS DE INTERESSE SÃO A SEGURANÇA DA INFORMAÇÃO, EM PARTICULAR, A FORENSE E RESILIÊNCIA DIGITAL.



POR NUNO GOES, CYBERSECURITY ENGINEER

COMPUTAÇÃO FORENSE DIGITAL:

O PILAR ESSENCIAL DA MITIGAÇÃO MODERNA

A DIGITALIZAÇÃO DAS ORGANIZAÇÕES TROUXE BENEFÍCIOS INDISCUTÍVEIS, MAS TAMBÉM AUMENTOU EXPONENCIALMENTE OS RISCOS NO CIBERESPAÇO

Se anteriormente a preocupação principal se restringia à proteção física de documentos e infraestruturas, hoje a informação circula através de redes distribuídas, na nuvem e em dispositivos móveis de forma quase invisível. Neste cenário, a segurança da informação, a cibersegurança e a computação forense digital não podem ser vistas de forma isolada, mas como pilares complementares de uma estratégia coesa e integrada.

SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA: FUNDAMENTOS COMPLEMENTARES

A segurança da informação é orientada pelos princípios fundamentais da disponibilidade, integridade e confidencialidade, estruturando-se em normas amplamente reconhecidas como a ISO/IEC 27001 ou o NIST Cybersecurity Framework. Transcende a simples implementação de ferramentas tecnológicas, envolvendo governança organizacional, gestão rigorosa de riscos, políticas internas bem definidas e alinhamento estratégico com os objetivos empresariais.

A cibersegurança concentra-se especificamente na proteção ativa de ambientes digitais. Confronta diariamente ameaças que evoluem num ritmo acelerado: ransomware que paralisa serviços públicos e privados, ataques sofisticados às cadeias de fornecimento que comprometem fornecedores estratégicos, ou campanhas de espionagem conduzidas por grupos patrocinados por Estados. Este campo exige adaptação constante, monitorização contínua e uma mentalidade de defesa ativa baseada na inteligência de ameaças.

METODOLOGIAS E PROCESSOS RIGOROSOS

A computação forense digital cumpre um papel singular neste ecossistema de segurança. Diferentemente das práticas tradicionais de segurança, não se limita a impedir incidentes, atuando sistematicamente para compreender o que ocorreu, como ocorreu e qual o impacto real causado. Trata-se da aplicação de princípios científicos e metodologias rigorosas para identificar, preservar, analisar e apresentar indícios digitais em conformidade com requisitos legais e regulamentares específicos. O processo investigatório é orientado por protocolos que asseguram a autenticidade, confidencialidade e integridade dos indícios valorados como prova, desde a recolha inicial até à apresentação em relatórios técnicos, ou mesmo, perante tribunais. A cadeia de custódia, a documentação detalhada e o uso de ferramentas devidamente validadas constituem condições indispensáveis para garantir que a investigação seja confiável e juridicamente defensável. Qualquer quebra nessa cadeia pode invalidar provas em tribunal.

Metodologias de referência como o NIST SP 800-86 estruturam a investigação em quatro fases distintas: recolha de dados, exame, análise e elaboração de relatório. Na fase de recolha, os investigadores identificam e recolhem informações relevantes, respeitando rigorosamente a ordem de volatilidade. A fase de exame envolve o processamento desses dados, distinguindo o que possui valor probatório daquilo que é irrelevante para a investigação.

A fase de análise permite correlacionar eventos, reconstruir linhas temporais e identificar padrões comportamentais. No final do processo, a elaboração do relatório formaliza os achados, descreve as metodologias empregues e propõe recomendações fundamentadas.

Este processo é complementado pela norma ISO/IEC 27037, que fornece diretrizes específicas para identificação, aquisição e preservação de evidências digitais, estabelecendo ainda requisitos de competência e certificação para os profissionais envolvidos.

DESAFIOS TECNOLÓGICOS EMERGENTES

O avanço tecnológico trouxe novos desafios para a análise forense digital. A crescente adoção de serviços na nuvem dificulta a recolha de evidências, seja pela localização distribuída dos dados, seja pelas múltiplas jurisdições, legislações diversas e armazenamento em ambientes partilhados entre diferentes clientes.

A proliferação de dispositivos conectados através da Internet das Coisas amplia exponencialmente as potenciais fontes de prova, exigindo abordagens holísticas e capacidade técnica para lidar com formatos heterogéneos de dados. A cifragem cada vez mais robusta, embora proteja a privacidade dos utilizadores, cria barreiras adicionais para os investigadores forenses.

> "A PROLIFERAÇÃO DE DISPOSITIVOS CONECTADOS ATRAVÉS DA INTERNET DAS COISAS AMPLIA EXPONENCIALMENTE AS POTENCIAIS FONTES DE PROVA, EXIGINDO ABORDAGENS HOLÍSTICAS E CAPACIDADE TÉCNICA PARA LIDAR COM FORMATOS HETEROGÉNEOS DE DADOS"

Adicionalmente, volumes sem precedentes de dados gerados por sistemas modernos obriga ao recurso à automação, à aprendizagem automática e às técnicas de análise em tempo real, sob pena de tornar impraticável qualquer investigação manual tradicional. Soma-se a isso a pressão regulamentar de legislações como o RGPD, NIS2 ou a DORA, que estabelecem limites claros para recolha e tratamento de dados pessoais.

INTEGRAÇÃO NA RESPOSTA A INCIDENTES

As contribuições da forense digital para a resposta a incidentes são inegáveis. Integrada no ciclo de resposta descrito pelo NIST SP 800-61, oferece suporte direto em todas as fases operacionais: deteção de atividades suspeitas, contenção e erradicação completa de intrusões, recuperação baseada em compreensão precisa do alcance do ataque e aprendizagem pós-incidente através de relatórios detalhados.

A maturidade organizacional está intimamente ligada ao conceito de "prontidão forense", sugerindo preparação prévia através de políticas de registo e retenção de logs, ferramentas de recolha bem posicionadas, equipas treinadas e laboratórios capazes de processar rapidamente grandes volumes de informação. Esta abordagem não apenas reduz tempo e

custos de investigação, mas aumenta significativamente a capacidade de reação e mitigação organizacional.

PERSPETIVAS FUTURAS E EVOLUÇÃO TECNOLÓGICA

O futuro da computação forense aponta para uma automação ainda maior nas fases iniciais da investigação, permitindo que sistemas inteligentes executem a recolha e o exame preliminar de dados em larga escala. Isto liberta os especialistas para se concentrarem na análise interpretativa, que depende fundamentalmente de contexto, julgamento humano e criatividade investigativa.

"A INTELIGÊNCIA ARTIFICIAL E A ANÁLISE COMPORTAMENTAL DESPONTAM COMO ALIADOS PROMISSORES, CAPAZES DE REVELAR PADRÕES ANÓMALOS INVISÍVEIS ÀS ABORDAGENS CONVENCIONAIS. NO ENTANTO A IA ACELERA E PODERÁ GERAR DESAFIOS ÉTICOS, COMO VIÉS ALGORÍTMICO EM INVESTIGAÇÕES."

A inteligência artificial e a análise comportamental despontam como aliados promissores, capazes de revelar padrões anómalos invisíveis às abordagens convencionais. No entanto a IA acelera e poderá gerar desafios éticos, como viés algorítmico em investigações. Simultaneamente, permanece o desafio ético e legal de equilibrar a necessidade de segurança organizacional com a proteção rigorosa da privacidade e dos direitos individuais.

CONCLUSÕES

A computação forense digital deixou de ser um luxo reservado a investigações criminais de alto nível, tornando-se uma necessidade operacional para qualquer organização que dependa de informação digital - por outras palavras, a maioria das organizações contemporâneas. A sua integração estratégica com a segurança da informação e a cibersegurança constitui a base fundamental de uma postura verdadeiramente resiliente, proativa e adaptativa.

Mais do que simplesmente reagir a ataques no ciberespaço, trata-se de aprender sistematicamente com eles, fortalecer continuamente as defesas organizacionais e antecipar proativamente riscos futuros. Em ambiente digital, marcado pela incerteza crescente e hostilidade persistente, as organizações que investirem estrategicamente em capacidades forenses estarão mais bem preparadas para transformar uma crise em oportunidade genuína de evolução e de diferenciação competitiva no mercado. ◀



Fotografias: Rui Santos Jorge

RUI DAMIÃO

"É PRECISO OLHAR PARA AS ORGANIZAÇÕES E PERCEBER SE A SEGURANÇA ESTÁ NA MENTE DA MAIORIA DOS COLABORADORES"

CARLOS SILVA,

DIRETOR DE CIBERSEGURANÇA NO BANCO CTT

EM ENTREVISTA À IT SECURITY, CARLOS SILVA, DIRETOR DE CIBERSEGURANÇA NO BANCO CTT, ABORDA OS TEMAS DO ROSI, DOS NOVOS PERFIS EM CIBERSEGURANÇA E DE COMO É QUE AS ORGANIZAÇÕES SE PODEM AVALIAR OS CIBER-RISCOS JUNTO DOS SEUS FORNECEDORES E PARCEIROS.

Como vê o cenário de ciberameaças a evoluir atualmente contra a banca portuguesa de uma forma geral?

Quero deixar a nota que o que vou partilhar são opiniões minhas e nenhuma destas opiniões obriga o Banco CTT em relação ao que quer que seja. Tentarei ser o mais transparente possível sobre aquilo que puder partilhar.

É interessante estarmos a falar sobre isso agora porque recentemente a Associação Portuguesa de Bancos lançou uma campanha junto dos media por existirem cada vez mais situações de fraude na utilização de meios de pagamento, nomeadamente cartões e na forma de pagamento digital que todos usamos.

Atualmente, vemos a banca nacional – e o Banco CTT não deixa de estar dentro dessa indústria – a ser muito afetada por situações de envios de SMS com *links* para tentar dirigir as pessoas para sites de phishing, onde tentam imitar os sites de cada banco para que seja possível, depois, recolher as credenciais desses utilizadores e, na sequência e conseguindo entrar dentro dos canais digitais, conseguir usar alguma da informação que possa lá estar para se fazerem passar pelo próprio banco e, com isso, levá-los a dar informações importantes, nomeadamente códigos de transação para levar o cliente a ceder parte do seu saldo para o ator malicioso.

Estamos a ver cada vez mais situações de smishing, seguidas de ataques de vishing, em que o ator malicioso já tem claramente o conhecimento sobre o tipo de transações que o cliente já fez ou que faz, porventura o número de telefone e associar que aquele clique daquele *link* daquele SMS está associado com o email e com o telemóvel.

Existe alguma coisa que os bancos, de uma forma geral, possam fazer junto dos utilizadores ou é apenas uma questão de consciencialização?

O Banco CTT assume publicamente com os seus clientes de que, por exemplo, não enviamos *links* dentro de SMS. É importante que os clientes e quem recebe este tipo de comunicações – seja de banca ou de outro sistema – duvide sempre do que estão a receber. Depois, é preciso terem atenção – e isto é a parte complicada – ao sentido de urgência que estes pedidos trazem; normalmen-

te isto não acontece e os bancos e as outras instituições não enviam SMS para serem resolvidos naquele dia.

Tanto por SMS como por emails, a lógica tem de ser sempre a mesma. Na dúvida, nunca aceitar e desconfiar, não fazer nada. Quando estamos a falar de bancos, e na dúvida, deve-se telefonar para o banco e dizer que se recebeu determinado SMS ou email e perguntar se foram eles que enviaram.

Do ponto de vista do que é que a banca pode fazer, todos tentam ter a capacidade de identificar este tipo de situações antes de se tornarem massificadas, tentam identificar sites de phishing, tentam identificar a geração de certificados e de domínios que, de alguma maneira, imitam aquilo que é a imagem de cada instituição bancária, tentam ter a capacidade de, junto de entidades especializadas, fazer o *take-down* desses sites de forma preventiva para evitar ao máximo que existam este tipo de ataques tenham sucesso junto dos clientes.



De uma forma transversal a todo o tecido empresarial, como é que se justificam os orçamentos de cibersegurança perante o conselho de administração?

Tenho a sorte de trabalhar numa instituição financeira e reconheço que quem trabalha na área de segurança ou cibersegurança numa instituição financeira tem alguma capacidade de influenciar o conselho de administração e as comissões executivas, exatamente pelo facto de termos um regulador tão forte e tão ativo na prevenção deste tipo de situações. A existência deste regulador é muito importante para não só regularizar a indústria, mas também para a ajudar a se proteger contra este tipo de soluções. Não estou a dizer que as instituições financeiras só atuam porque o regulador os obriga, mas sim que o facto de existir esse regulador também torna mais fácil demonstrar aos nossos administradores e conselhos de administração a urgência de implementar um determinado controlo de segurança.

"PODEMOS FAZER QUASE UM SELF-ASSESSMENT, EM QUE PEDIMOS A ESSE FORNECEDOR PARA DIZER COMO É QUE ESTÁ, COMO É QUE IMPLEMENTA UM CONJUNTO DE CONTROLOS A UM DETERMINADO TIPO DE PREOCUPAÇÕES, COMO É QUE TRATA OS DADOS QUE PASSAMOS E QUE DAMOS DOS NOSSOS CLIENTES, COLABORADORES OU NEGÓCIO"

De um ponto de vista global, diria que o ideal é fazer uma análise de risco e, com essa análise de risco, demonstrar o nível e o número de ameaças que vamos conseguir reduzir ao fazer aquele investimento de segurança.

Cada vez mais não é só tecnologia, mas sim investir nas pessoas, na sua formação e dos colaboradores como um todo, garantir processos que estão atualizados e seguem as melhores práticas. Tentarmos que as organizações sigam uma *framework*, ou seja, mesmo que não seja tentar implementar uma ISO 27001 e ter uma certificação que, se calhar, pode ser *overwhelming* para a maioria das organizações, mas tentar seguir uma destas *frameworks* como orientação para justificar algum destes tipos de investimentos, sempre numa lógica de perceber qual o risco, os impactos que esses riscos podem ter na minha organização, para tentar mitigar primeiro.

Fazendo essa análise e seguindo esse caminho parece-me ser sempre o melhor, até porque os conselhos de administração estão habituados a trabalhar com risco. Usando essa mesma metodologia, mas aplicada à cibersegurança – e tenho tido essa experiência e daquilo que falo com outros responsáveis de segurança – é a melhor abordagem para justificar investimentos e aquilo que são as urgências de cada direção de cibersegurança vai ter dentro de cada organização.

Como última nota, devemos tentar evitar sempre criar medo; fazer algo porque existe um medo de que algo acontece não parece ser a melhor solução. Pode resultar uma ou duas vezes, mas depois vamos sempre nesse caminho e não há a noção de existir um perigo de facto iminente, o que acaba por ser contranatura e atuar contra nós próprios no futuro e não nos permitirá seguir um caminho que seja definido com a própria administração.

Como é que se pode medir o ROI de investimentos em segurança que, por natureza, previnem eventos que podem nunca acontecer?

Existe uma aproximação que é uma derivada do ROI, que é o ROSI – *Return On Security Investment* – que tem em linha de conta o custo do incidente



de segurança. Se tiver uma expectativa de quanto é que aquele incidente pode custar para a minha organização, mais facilmente consigo calcular esse ROSI. Ou seja, a forma como devemos atuar é olhar para o que é me pode trazer em termos de redução de impacto, de custo, por acontecer alguma situação menos interessante.

Outra abordagem é o que é que isso me pode dar a ganhar em termos de negócio, ou seja, a segurança também pode e deve ser utilizada como uma vantagem competitiva das organizações. Uma organização que consiga, com a implementação de um determinado controlo ou mecanismo, aumentar as suas vendas, pode também utilizar esse valor para mais facilmente calcular o retorno no investimento. Acho que essa seria a abordagem mais interessante porque é aquela mais palpável, a que se diz que, fazendo isto, vou ganhar '*x*' ao fim de um determinado tempo.

Felizmente estou numa casa onde isso ainda não aconteceu pelo menos a grande escala ou escala minimamente palpável, mas todos passaremos por um ataque de maior escala e maior impacto. Quem passa por este tipo de situações consegue muito mais facilmente perceber o que é que perdeu. Nessas situações é mais fácil mostrar e identificar os custos que a organização teve.

Como é que se podem avaliar os ciber-riscos de fornecedores críticos?

Esse é um dos temas mais críticos que as organizações têm. A NIS2 já traz esse tipo de abordagem e acho que é muito interessante a forma como está definido. A DORA, concretamente para o setor financeiro, é muito verboso, por assim dizer, nesta componente de garantir que conseguimos gerir os nossos fornecedores, nomeadamente críticos, perceber o que pode acontecer e tentar criar cenários o que pode acontecer à nossa organização na iminência de algo acon-

tecer a esses fornecedores. Essa é uma forma de garantir algum cumprimento desta regulamentação, de olhar para os mesmos e podermos fazer algum nível de avaliação.

Depois, há vários níveis que podemos implementar dessa avaliação. Pode ser uma avaliação quase *self-assessment*, em que pedimos a esse fornecedor para dizer como é que está, como é que implementa um conjunto de controlos a um determinado tipo de preocupações, como é que trata os dados que passamos e que damos dos nossos clientes, colaboradores ou negócio. Com esse *assessment* também podemos fazer algum *check* do próprio *assessment*. Sem entrarmos tecnicamente nas organizações, muitas vezes conseguimos – olhando para aquilo que são as respostas aos *assessments* – perceber se aquilo que vemos em termos de superfície de ataque externa faz *match* com aquilo que responderam.

Uma das soluções que podemos utilizar são aqueles mecanismos e soluções de *security rating* que fazem exatamente isso, onde elas próprias já estão a ver a superfície de ataque externo das organizações e dão esses *ratings*, inclusive informação para saber onde é que podem estar mais vulneráveis. Olhando para isso, podemos ver também se as respostas que nos deram batem certo com aquilo que também é visto externamente e de forma pública por essas organizações.

Entrando nos críticos, começa a fazer sentido que possa existir um *assessment* já não só baseado naquilo que são as respostas, mas também olhando para aquilo que são políticas, processos e procedimentos que essas organizações têm implementado. Pedirmos informação sobre testes de intrusão sobre análises de vulnerabilidades para podermos também ver qual é que é o espectro de proteção e de vulnerabilidade que podem ter nas suas infraestruturas.

Em última análise, o que acontece nomeadamente nos fornecedores mais críticos, é termos em contrato a capacidade de nós próprios podermos fazer testes de intrusão ou solicitar testes de intrusão a um prestador de serviços independente para fazer esses testes.

"DEVERÍAMOS TENTAR CRIAR CONDIÇÕES (...) PARA IDENTIFICAR O NÚMERO DE INCIDENTES, O TEMPO QUE DEMORARAM A RESPONDER A ESSES INCIDENTES, AS PESSOAS COM KNOW-HOW DENTRO DA ORGANIZAÇÃO QUE RESPONDEM AOS TEMAS DA CIBERSEGURANÇA, O PRÓPRIO INVESTIMENTO E O ORÇAMENTO QUE PODEM APLICAR"

Olhando para os relatórios percebemos qual é o estado da segurança desses parceiros, mas estamos sempre a olhar para fotografias, estamos sempre a olhar para hoje está assim e amanhã pode ter acontecido alguma coisa.



Que indicador se pode utilizar para medir a maturidade de cibersegurança das organizações?

Não é fácil criar ou ter um indicador. Podemos falar naquilo que vemos e que referi, das soluções das plataformas de *ratings* de segurança. Isso parece-me ser um indicador suficientemente razoável e já comummente aceite pela maioria das organizações que já olha de forma consciente e consistente para o tema da cibersegurança.

Deveríamos tentar criar condições, dentro da comunidade e dentro daquilo que é uma qualquer *best practice*, para identificar o número de incidentes, o tempo que demoraram a responder a esses incidentes, as pessoas com *know-how* dentro da organização que respondem aos temas da cibersegurança, o próprio investimento e o orçamento que podem aplicar. Acho que todo este número e todos estes valores poderiam ser usados para chegarmos a um conjunto de indicadores que nos levam a identificar a maturidade daquela organização perante a cibersegurança.

Obviamente que isto não é nada fácil porque nenhuma organização quer partilhar com os outros – sejam concorrentes ou com o resto – as suas fragilidades. Todos temos fragilidades e vulnerabilidades. Numa organização média ou grande, quem diz que não tem centenas de milhares de vulnerabilidades para gerir constantemente está a mentir porque é normalíssimo isso acontecer.

Priorizar, definir a criticidade dessas vulnerabilidades, os ativos onde elas existem, isso sim é o trabalho mais importante que temos de realizar e, dessa forma, conseguirmos muito mais facilmente irmos reduzindo as vulnerabilida-

des ou, pelo menos, ir eliminando aquelas que podem criar um problema para a organização.

Tipicamente, a banca tem uma série de regulamentações que impactam sua a atividade. Com a introdução de diretivas, como a DORA e a NIS2, quais são as dificuldades específicas da cibersegurança neste campo?

Muitas vezes tem a ver com o próprio entendimento interno que as várias áreas dentro de uma organização têm de ter. A segurança de informação não termina dentro da direção destes temas. A segurança de informação, tal como a proteção de dados, impacta todas as áreas dentro de uma organização.

Se toda a organização tiver essa consciência, será sempre mais fácil. Não é pela direção de cibersegurança implementar um conjunto de controlos, definir um conjunto de políticas e regras para a sua atuação que responde a 100% a este tipo de regulamentação, a este tipo de normas, a este tipo de políticas que nos são trazidas, vindas tanto do regulador como do legislador nacional e internacional.

Se tivermos esse nível de perceção em que a grande maioria das áreas serão impactadas, o que importa é ter claro de que não é porque eu – responsável de cibersegurança – me preocupei com a minha quinta, com o meu silo, que respondo diretamente a tudo aquilo que vem destas diretivas e destes regulamentos tem de ser um objetivo comum dentro da organização.

Acho que estamos a caminhar nesse sentido. Acho que a maioria das organizações e nomeadamente estas que são impactadas – seja pela DORA, nas instituições financeiras, seja na NIS2, em grande parte das médias e grandes empresas em Portugal – perceberem que pode haver um interlocutor comum, que pode haver uma voz que marca o ritmo, quase como se estivéssemos numa banda, mas depois tem de haver solistas e intérpretes em cada uma das direções que respondam também às necessidades que são identificadas, seja pelo regulamento, seja por quem está a liderar a implementação desses regulamentos.

> "OS PRINCIPAIS PERFIS QUE ESTAREMOS AGORA A OLHAR QUE ANTIGAMENTE NÃO OLHÁVAMOS TEM A VER MUITO COM A GESTÃO DE IDENTIDADES E GOVERNAR ESSAS MESMAS IDENTIDADES"

Abordando o tema do talento em cibersegurança, que perfis se procuram agora que há três ou cinco anos não se procuravam?

É um tema cada vez mais premente, embora exista aqui um bocado a expectativa – não necessariamente que seja a minha opinião muito forte, mas não



deixo também de ter alguma afinidade com a mesma – de que a inteligência artificial vem resolver alguns dos nossos problemas. Pessoalmente, não acho que vem resolver os nossos problemas de falta de *skills* e falta de pessoas; acho que vem acelerar algumas das tarefas que ainda são realizados por seres humanos para que seja mais fácil atuar e reagir a situações não expectáveis.

Diria que os principais perfis que estaremos agora a olhar que antigamente não olhávamos tem a ver muito com aquilo que é a preocupação das próprias organizações de cada vez mais gerir identidades e governar essas mesmas identidades dentro das organizações, sejam elas humanas ou não humanas.

Esta capacidade de trabalhar com plataformas de governo de identidades é cada vez mais premente no mercado. Há cada vez mais organizações a implementar este tipo de soluções. Há coisa de quatro ou cinco anos, nas organizações fora das instituições financeiras, de saúde e telecomunicações, não víamos tanto esta necessidade de definir corretamente os perfis, trabalhar com plataformas para identificar esses perfis e as permissões que cada perfil deve ter no acesso a quê e a que aplicações, é um dos perfis são requisitados.

Outro tem a ver com a inteligência artificial e a capacidade de construir boas *prompts*, e um bom *prompt* não pode ser apenas um *prompt builder* ou um *prompt engineer*, como agora se fala. No caso da segurança, têm de ser pessoas com experiência sobre o que é que é preciso perguntar, quais é que são os campos e qual é que é o tipo de informação e de eventos que quero, de facto, relacionar e pedir àquele meu motor, àquela minha inteligência artificial que, pegando naquela informação, me construa um caso de uso que me permita, depois, mais facilmente detetar alguma ofensa ou algum tipo de incidente contra a minha organização.

Diria que são o tipo de perfis que temos mais necessidade, até porque com o advento da inteligência artificial – não falo tanto da generativa, mas sim,

fundamentalmente, da preditiva, do machine learning – temos de cada vez mais caminhar para uma situação em que deixamos de ter tantos analistas de segurança e vamos passar a ter engenheiros de seguranças, pessoas que estão preocupadas com o detalhe e não com a maioria da informação que recebem, que estão preocupadas a identificar uma alteração num determinado comportamento e com essa alteração dizer que esta alteração de comportamento aqui pode significar algo diferente que está a acontecer na minha organização. A inteligência artificial é muito boa a identificar esses *outliers*; o que ainda não é boa é, pegando nesse *outlier*, o que é que vou fazer com ele, o que é que vou procurar para perceber se aquele *outlier* corresponde a um ataque, a uma má utilização de uma tecnologia ou a uma utilização normal que acontece esporadicamente dentro da organização, mas nunca tinha sido catalogada como sendo uma utilização normal.

Essa capacidade tem de ser muito ao nível deste tipo de perfis muito específicos, com muito conhecimento. Tenho algum receio que o facto de cada vez mais caminharmos para um mundo, entre aspas, onde não existem analistas de segurança, ou onde estes analistas foram sendo substituídos pelos mecanismos de inteligência artificial, nos possam dificultar o aparecimento de engenheiros de segurança que já tenham experiência e conhecimento suficiente para, ao depararem-se com uma situação menos normal, chegar a uma conclusão que pode ajudar uma organização a defender-se perante um ataque.

Que conselhos deixa a outros CISO ou diretores de cibersegurança das organizações?

Acho que há três ou quatro conselhos que podem e devem ser passados e era aqueles que eu, porventura, mais gostaria também de ir ouvindo e de ir recebendo, porque acho que têm muito a ver com o nosso trabalho do dia a dia.

É preciso olhar para dentro, olhar para nós, para as organizações, perceber se a cultura das organizações é uma cultura onde a segurança está no *top of mind* da maioria dos colaboradores. Isso é muito importante. Conseguirmos chegar a esse tipo de objetivo onde a esmagadora maioria dos colaboradores cumpre um conjunto de regras de higiene de segurança bastante básicas todos os dias vai limitar bastante o tipo de situações graves que podem ocorrer à organização, e isso é muito importante. Dentro deste conselho, olhar para aqueles que não o cumprem, ou seja, garantir que conseguimos identificar os comportamentos menos bons, que conseguimos perceber de que forma é que esses colaboradores podem e devem ser formados. Acho que é um ponto cada vez mais importante dentro das organizações, que é não olhar apenas para o *awareness* segurança como mais um *tick in the box* num conjunto de objetivos de formação que as organizações têm; é muito mais do que isso. Também é, mas não é só formação, é educação.

Outro ponto crítico é não achar que a tecnologia e a implementação de mais tecnologia, de mais controlos, resolve os meus problemas. Não faz sentido imple-

mentar a tecnologia e controlos se não tivermos capacidade de monitorizar, se não tivermos capacidade de, perante um alerta, perante uma situação menos normal, não ter a capacidade de ir perceber o que está a acontecer. Não é isso que me vai ajudar. Sim, posso comprar a tecnologia que me dá esses alertas e que ela própria também atua e tem algum nível de automação, mas temos de estar perfeitamente conscientes do que está a acontecer, quais é que são as consequências de não olharmos para aquela informação.

Como último ponto tem a ver com aquilo que falámos no início: tentar identificar os riscos, tentar perceber se aqueles riscos podem ter um impacto grande nas nossas organizações e, com base nesses riscos, justificar orçamentos, a aquisição de soluções, a contratação de serviços, a entrada de mais pessoas para a organização para ajudar a mitigar aqueles riscos.

"ACHO QUE EM PORTUGAL, SE CALHAR PORQUE VIVEMOS COM RECURSOS FINANCEIROS FINITOS, SOMOS BASTANTE BONS A GERIR ESTES TEMAS DAQUILO QUE, DE FACTO, PRECISAMOS PARA AS NOSSAS ORGANIZAÇÕES"

Acho que é cada vez mais importante tanto fazer este *Risk Based Approach* em tudo aquilo que fazemos, seja no nosso dia-a-dia, seja nos pedidos adicionais que fazemos aos conselhos de administração. Diria que é um dos melhores conselhos que posso dar.

Não devemos muitas vezes ir atrás – e é difícil às vezes – dos vendedores, dos fabricantes. Todos eles querem vender, todos nós temos clientes e queremos vender mais e queremos ter mais *revenue*, sem dúvida nenhuma, mas às vezes é preciso parar um bocado e perceber se faz sentido tomar o meu caminho, ou se faz sentido perceber que é preciso a tecnologia '*x*' para mitigar problemas que tenho na minha organização e escolher o *best of breed*. Acho que em Portugal, se calhar porque vivemos com recursos financeiros finitos, somos bastante bons a gerir estes temas daquilo que, de facto, precisamos para as nossas organizações.

ASSEMBLEIA DA REPÚBLICA APROVA NIS2 E ABRE CAMINHO A NOVOS DESAFIOS



POR INÊS GARCIA MARTINS

A ASSEMBLEIA DA REPÚBLICA APROVOU A PROPOSTA DE LEI QUE TRANSPÕE A DIRETIVA EUROPEIA NIS2, UM PASSO DECISIVO PARA REFORÇAR A CIBERSEGURANÇA EM PORTUGAL. NO ENTANTO, ESPECIALISTAS ALERTAM QUE A ADAPTAÇÃO DAS ORGANIZAÇÕES SERÁ COMPLEXA E VAI EXIGIR MUITO MAIS DO QUE CUMPRIR FORMALIDADES

A aprovação em plenário da proposta de lei que transpõe a Diretiva *Network and Information Security* (NIS2) marca o arranque de um novo capítulo na cibersegurança em Portugal, mas o consenso é que este é apenas o início de um caminho exigente para entidades públicas e privadas que terão de alinhar práticas, processos e infraestruturas às exigências europeias.

O diploma foi aprovado com os votos favoráveis de PSD (89), CDS-PP (2), PAN (1) e JPP (1), enquanto PS (58), Livre (6) e PCP (3) votaram contra, Chega (60) e Iniciativa Liberal (9) optaram pela abstenção, já o Bloco de Esquerda não esteve presente na votação. Com esta aprovação, Portugal recupera o atraso na transposição da diretiva, cujo prazo terminava a 17 de outubro de 2024, tendo sido incumprido devido a sucessivos bloqueios políticos, incluindo a dissolução do Parlamento e alterações de Governo.

Este atraso não é apenas formal, uma vez que a Comissão Europeia já tinha alertado que os Estados-Membros em incumprimento poderiam enfrentar processos de infração, com potenciais penalizações financeiras. Aliás, a 7 de maio deste ano, Bruxelas enviou um parecer fundamentado aos Estados-Membros que ainda não tinham comunicado a transposição integral da diretiva, incluindo Portugal, dando-lhes dois meses para avançar com o processo antes de a Comissão poder remeter os casos para o Tribunal de Justiça da União Europeia.

De acordo com o NIS2 Directive Transposition Tracker da European Cyber Security Organisation (ECSO), atualizado a 12 de setembro de 2025, 14 dos 27 Estados-Membros da União Europeia já transpuseram a diretiva NIS2 para o direito nacional. Entre estes estão Bélgica, Chipre, Croácia, Dinamarca, Eslovénia, Eslováquia, Finlândia, Grécia, Hungria, Itália, Letónia, Lituânia, Malta, Roménia. Os restantes 13 Estados-Membros, incluindo Portugal, Áustria, Alemanha, Bulgária, Chequia, Espanha, Estónia,

França, Irlanda, Luxemburgo, Países Baixos, Polónia e Suécia, ainda se encontram em fase de projeto de lei.

DA AUTORIZAÇÃO LEGISLATIVA À APLICAÇÃO

Daniel Reis, Sócio da DLA Piper, sublinha que esta aprovação é "apenas uma autorização legislativa e não a transposição em si". Na prática, o Parlamento deu luz verde ao Governo para avançar, mas ainda não está em causa a aplicação direta da diretiva. O Governo tem 180 dias para aprovar o decreto-lei que aplicará a NIS2. Só depois desse diploma ser publicado em Diário da República arranca um novo prazo: 120 dias até à sua entrada em vigor efetiva.


DANIEL REIS, DLA PIPER

"HÁ, SOBRETUDO, CLARIFICAÇÃO DO TEXTO, SENDO DE NOTAR A REDUÇÃO DO MONTANTE DAS COIMAS DAS CONTRAORDENAÇÕES MUITO GRAVES"

Logo de seguida, será disponibilizada uma plataforma eletrónica onde as entidades abrangidas devem proceder ao registo. Como explicou Martim Bouza Serrano, Sócio e Coordenador da área de prática de TMT (Tecnologia, Media & Telecomunicações) da CCA, "as entidades abrangidas devem, no prazo de 60 dias, fazer o seu registo e, em 24 meses, adotarem medidas para a adaptação às novas exigências estabelecidas".

No nosso país, a NIS2 ganha contornos próprios, com alterações que refletem a realidade das organizações portuguesas. Os advogados destacam que a maioria das diferenças introduzidas no país é de natureza técnica. "Há, sobretudo, clarificação do texto, sendo de notar a redução do montante das coimas das contraordenações muito graves", observa Daniel Reis, destacando que algumas alterações visam simplificar a interpretação e aplicação das regras.

Catarina Mascarenhas e Catarina Rodrigues Rocha, respetivamente Consultora e Advogada Estagiária da Abreu Advogados, lembram que a

NIS2 é uma diretiva de harmonização mínima, pelo que os Estados-Membros podem adotar disposições adicionais. "No caso português, a legislação já tinha introduzido diferenças em relação ao regime anterior", referem. Entre os exemplos da atual proposta está a definição de categorias de entidades públicas relevantes e um processo de notificação de incidentes mais detalhado, mostrando como Portugal ajusta as regras europeias à sua realidade.

A NIS2 não surge isolada, como aliás recorda Daniel Reis, "na prática, uma entidade poderá ter de responder em simultâneo a várias obrigações, como as do DORA ou do Cyber Resilience Act". O especialista acrescenta que esta representa "um quadro regulatório acumulado que exige das organizações uma estratégia integrada de *compliance*".

O QUE MUDA PARA AS ORGANIZAÇÕES

"Uma entidade que já faz uma gestão madura não tem de mudar o seu *modus operandi*. Uma entidade nova que passa a ser alargada pelo regulamento, tem uma receita nova para seguir", explicou o Coordenador do Centro Nacional de Cibersegurança (CNCS), Lino Santos, durante o C-Days 2025. O impacto será sobretudo sentido por organizações que até agora estavam fora do âmbito da diretiva e que passam a ter de alinhar-se com requisitos mínimos de segurança e gestão de risco.

O que também se confirma na análise de Daniel Reis, que acrescenta que as empresas até agora fora do enquadramento terão de definir políticas internas, nomear responsáveis e investir em tecnologia, "sob pena de enfrentarem sanções em caso de incumprimento". Catarina Mascarenhas e Catarina Rodrigues Rocha, da Abreu Advogados, sublinham ainda que os órgãos de administração passam a assumir responsabilidades diretas pelas infrações cometidas, "a título de dolo ou culpa grave", sendo exigido que frequentem ações de formação e as promovam junto dos colaboradores.

Segundo Lino Santos na mesma conferência, a aplicação da NIS2 também assenta no princípio da


MARTIM BOUZA SERRANO, CCA

A TRANSPOSIÇÃO DA NIS2 "IRÁ ALTERAR E OBRIGAR À REVISÃO DE VÁRIAS LEGISLAÇÕES NACIONAIS, INCLUINDO A LEI DO CIBERCRIME E A LEI DO CIBERESPAÇO"

> OS ÓRGÃOS DE ADMINISTRAÇÃO PASSAM A ASSUMIR RESPONSABILIDADES DIRETAS PELAS INFRAÇÕES COMETIDAS, "A TÍTULO DE DOLO OU CULPA GRAVE"


CATARINA MASCARENHAS, ABREU ADVOGADOS


CATARINA RODRIGUES ROCHA, ABREU ADVOGADOS

proporcionalidade. “O mesmo regime jurídico tem de ser aplicado a empresas de grande dimensão – com grande experiência e maturidade – e a pequenas empresas – que ainda não têm essa experiência”, afirma Lino Santos.

No plano regulatório, está previsto um reforço do quadro institucional, com várias autoridades competentes a poder fiscalizar e sancionar, incluindo aplicar coimas, suspensões temporárias da atividade ou sanções pecuniárias compulsórias. O quadro sancionatório é mais severo: no caso das entidades essenciais, as multas podem variar entre dois mil euros e dez milhões de euros, ou até 2% do volume de negócios global anual.

“O objetivo e aquilo que deve nortear o nosso trabalho é que haja uma coordenação entre autoridades competentes em cibersegurança e as autoridades setoriais para quando exigirmos uma determinada de cibersegurança estamos a cumprir com o regulamento NIS2 ou o regulamento do código da energia, por exemplo”, explicou o Coordenador do CNCS durante o C-Days 2025.

O responsável acrescentou que “o objetivo é que haja uma plataforma que evite a duplicação da informação”, lembrando o caso do ataque à AMA em outubro de 2024, que obrigou a comunicar a cinco entidades diferentes. Dessa forma, “as organizações


JOANA MOTA AGOSTINHO, CUATRECASAS

"UM DOS PRINCIPAIS DESAFIOS CONSISTE NA AMPLIAÇÃO SIGNIFICATIVA DO LEQUE DE ENTIDADES ABRANGIDAS, QUE OBRIGA A CLARIFICAR CRITÉRIOS DE IDENTIFICAÇÃO E A ARTICULAR ESTE REGIME COM OUTROS JÁ VIGENTES"

terão um trabalho mais simples e apenas tenham de notificar uma única entidade".

DESAFIOS LEGAIS E REGULATÓRIOS

Martim Bouza Serrano afirma que a transposição da NIS2 "irá alterar e obrigar à revisão de várias legislações nacionais, incluindo a Lei do Cibercrime e a Lei do Ciberespaço". Salienta ainda a "introdução de uma exceção à ilicitude penal para *ethical hacking*, ou seja, atividades de *hacking* ético realizadas sem fins lucrativos, respeitando a privacidade e comunicando as vulnerabilidades identificadas de forma responsável, que não serão punidas".

Já Joana Mota Agostinho, Sócia e Coordenadora da Área de Propriedade Intelectual e Tecnologia e Telecomunicações da Cuatrecasas, alerta que "um dos principais desafios consiste na ampliação significativa do leque de entidades abrangidas, que obriga a clarificar critérios de identificação e a articular este regime com outros já vigentes, nomeadamente o RGPD, a legislação sobre proteção de infraestruturas críticas e normas setoriais específicas".

A responsável sublinha ainda que será necessário "reforçar os poderes das autoridades competentes, como o Centro Nacional de Cibersegurança, ao mesmo tempo que se asseguram mecanismos eficazes de cooperação interinstitucional e de reporte de incidentes, evitando sobreposição ou conflito de obrigações".

É neste sentido que Lino Santos sublinhou que o objetivo é apoiar as organizações a desenvolverem a sua maturidade de cibersegurança e, simultaneamente, reforçar a resiliência de todo o país. Para isso, o CNCS "espera aumentar a resiliência e a segurança do país". "Queremos fazer este caminho com as comunidades. O objetivo é ajudar-vos a crescer na maturidade de cibersegurança", referiu o Coordenador.

DA CONSCIENCIALIZAÇÃO À REGULAÇÃO:

A VISÃO DA LAYER8 NA JORNADA DE SEGURANÇA CONJUNTA COM AS ORGANIZAÇÕES

MARTA QUARESMA FERREIRA

AS SOLUÇÕES DA LAYER8 ADAPTAM-SE AO TIPO DE MATURIDADE DE CADA CLIENTE: DESDE ANÁLISE DE MATURIDADE DE SEGURANÇA, SERVIÇOS DE CSIRT OU OFFENSIVE SECURITY – PARA CLIENTES QUE JÁ INVESTIRAM NA VERTENTE TECNOLÓGICA – ATÉ GESTÃO DE IDENTIDADES PRIVILEGIADAS E ADOÇÃO DE TECNOLOGIAS FOCADAS NA DETEÇÃO E RESPOSTA A INCIDENTES, PARA CLIENTES COM LACUNAS TECNOLÓGICAS.

Criada em 2011, a Layer8 dedica-se em exclusivo ao mercado da segurança da informação e da gestão da conformidade. Num momento em que a segurança já se figura como um ponto central nos processos de negócio, Fernando Cardoso, Chief Operating Officer da Layer8 considera que é "extremamente importante ver a segurança como parte de um processo e não meramente como uma componente técnica que se encaixa à *posteriori*".

A oferta da Layer8 inclui desde GRC, CSIRT, Offensive Security, Technology e Managed Services, garantindo que os clientes contam com uma visão 360º por parte do seu parceiro.

Ao dia de hoje, e quando falamos das maiores exigências dos clientes, Fernando Cardoso esclarece que as mesmas dependem sobretudo "do nível de maturidade de cada cliente". Por um lado, a organização conta com clientes que já investiram na vertente tecnológica de forma a assegurarem as melhores práticas, não só alinhadas com regulamentação, mas também que garantam a capitalização do investimento realizado. "Nesses casos, projetos como a análise de maturidade de segurança ou os serviços de CSIRT ou Offensive Security são os mais procurados", refere o COO.

Por outro lado, e nos clientes que ainda apresentam lacunas tecnológicas, "a procura tem-se focado em temas como a gestão de identidades privilegiadas (PIM/PAM) ou a adoção de tecno-

logias focadas na deteção e resposta a incidentes (XDR)".

O AUMENTO DA CONSCIENCIALIZAÇÃO DA CIBERSEGURANÇA

Quando olha para o mercado, Fernando Cardoso destaca dois fatores que têm "imprimido uma maior dinâmica na procura de serviços de segurança: consciencialização e regulamentação".

Com o crescimento do *awareness* ao longo das últimas décadas, o COO acredita que "o impacto, seja ele reputacional ou financeiro, de um incidente de segurança tem sido perspetivado de forma diferente desde que a imprensa começou a dar mais importância aos incidentes de segurança (ransomware, dataleaks, denial of service, etc.)".

O interesse pelo tema deixou de ser marginal, circunscrito a setores como a banca, as telecomunicações e os serviços online que dependiam da segurança, para passar a ser central para as organizações: "Raramente encontramos um negócio que não dependa de alguma forma dos sistemas de informação e, subsequentemente, da sua segurança".



FERNANDO CARDOSO, LAYER8

O COO aponta para "um aumento substancial em termos de regulação relativa à segurança de informação", como é o caso do DORA – para o setor financeiro – e da NIS2 – num contexto mais alargado –, que obrigam as empresas e instituições a manterem-se atualizadas e na linha da frente. A esta realidade da regulação "junta-se cada vez mais

> "O IMPACTO, SEJA ELE REPUTACIONAL OU FINANCEIRO, DE UM INCIDENTE DE SEGURANÇA TEM SIDO PERSPETIVADO DE FORMA DIFERENTE DESDE QUE A IMPRENSA COMEÇOU A DAR MAIS IMPORTÂNCIA AOS INCIDENTES DE SEGURANÇA"

a pressão de parceiros e fornecedores no sentido de assegurar relações de negócio seguras com partes terceiras, exigindo a conformidade com normas reconhecidas universalmente como, por exemplo, o ISO 27001".

PREPARAR PARA A REGULAÇÃO

A transposição da Diretiva NIS2, que recebeu, entretanto, luz verde após votação na Assembleia da República, está no radar da Layer8, que apresenta aos seus clientes uma "metodologia estruturada, faseada e totalmente adaptada às necessidades de cada organização".

"A Layer8 é parceira dos seus clientes em todo o processo de conformidade com a Diretiva NIS2, desde o diagnóstico inicial até ao acompanhamento contínuo, promovendo uma cultura de cibersegurança robusta e sustentável", reforça Fernando Cardoso.

A primeira fase conta com a nomeação de um responsável de cibersegurança e de um ponto de contacto permanente para assegurar "uma comunicação eficiente com as autoridades competentes". O objetivo, explica Fernando Cardoso, passa por garantir que "cada cliente cumpre integralmente as obrigações da Directiva NIS2 e aumente, progressivamente, a sua maturidade de cibersegurança".

O desenvolvimento dos documentos, nomeadamente do modelo de governo, da política de segurança, da metodologia de risco e dos procedimentos de notificação de incidentes fica a cargo da Layer8, que é ainda responsável por elaborar um plano de segurança personalizado, "baseado numa análise de maturidade que avalia o nível actual de cibersegurança de cada cliente e identifica oportunidades de melhoria".

A empresa procede a uma análise de risco detalhada junto do cliente, com a identificação e mitigação de ameaças e vulnerabilidades de ativos. Ultrapassada a fase inicial, a Layer8 apoia as organizações na "implementação das medidas do plano de segurança e das obrigações periódicas da Directiva NIS2, garantindo acompanhamento contínuo e especializado". Em caso de necessidade de resposta a incidentes, a equipa de CSIRT está munida de valências para realizar toda a gestão e resposta a incidentes pelo cliente, possibilitando que o mesmo se foque no mais importante: o seu negócio.

Como consequência, a abordagem permite aos clientes reduzirem os riscos de cibersegurança, aumentarem a confiança de clientes, parceiros e reguladores, alinharem práticas do setor e, desta forma, promoverem uma "maior resiliência operacional", evitando assim "sanções e coimas associadas ao incumprimento da Diretiva NIS2".

Na visão da Layer8, as organizações devem procurar olhar para a segurança "como (mais) um processo de negócio", através da implementação de medidas e considerações de segurança "diretamente no design" e "na execução dos principais fluxos e procedimentos operacionais, em vez de a tratar como uma função separada". ◀

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
COORDENADORA EDITORIAL: Marta Quaresma Ferreira
REDAÇÃO: Inês Garcia Martins, Flávia Gomes
BUSINESS DEVELOPMENT:
Beatriz Salzedas - (+351) 910 788 082 - beatriz.salzedas@medianext.pt
João Calvão - (+351) 910 788 413 - joao.calvao@medianext.pt
MARKETING & EVENTS DIRECTOR:
Rosa Bento - rosa.bento@medianext.pt
MARKETING COMMUNICATIONS:
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: Nuno Goes

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

PROPRIEDADES E DIREITOS

A propriedade do título "IT Insight Security" é de MediaNext Lda., uma empresa Jornalística registada da Entidade Reguladora da Comunicação Social com o nº 224011 e NIPC 510 551 866. Proprietários com mais de 5% de Capital Social: Margarida Bento e Pedro Botelho. Todos os direitos reservados. A reprodução do conteúdo (total ou parcial) sem permissão escrita do editor é proibida. O editor fará todos os esforços para que o material mantenha fidelidade ao original, não podendo ser responsabilizado por gralhas ou erros gráficos surgidos. As opiniões expressas em artigos assinados são da inteira responsabilidade dos seus autores.

O IT Insight Security e a MediaNext utilizam as melhores práticas de privacidade sobre dados pessoais e empresariais. Os dados fornecidos para uso exclusivo do serviço de assinantes do IT Insight Security não serão cedidos a qualquer entidade terceira. As informações sobre leitores constantes na base de dados de subscritores do site www.itsecurity.pt estão protegidos pelas melhores práticas de segurança informática.

IT Insight Security é membro de:

ASSOCIAÇÃO PORTUGUESA DE IMPRENSA · ACEPI ASSOCIAÇÃO ECONOMIA DIGITAL · CIWA COMPETITIVE INTELLIGENCE & INFORMATION WARFARE ASSOCIATION

Editado por: media NEXT STAY AHEAD • STAY RELEVANT