ZERO TRUST "A crise sanitária económica que hoje vivemos criou restrições orçamentais"

COMPUTERWORLD

FROM IDG

COMPUTERWORLD.COM.PT | EDIÇÃO DIGITAL

ESPECIAL CIBERSEGURANÇA

CIBERSEGURANÇA na TRANSFORMAÇÃO DIGITAL

o que dizem os fabricantes

Ricardo Maté | Sophos

Carlos Vieira | WatchGuard

Rui Duro | Check Point

9 O Retorno do Investimento da perspetiva do Ciber-atacante, por Rui Shantilal, da Integrity.

11 O que é um ataque de bandeira?

17 Zero Trust.

24 Fabricantes - Check Point; Sophos e WatchGuard.

34 Opinião por Ricardo Neves, da WhiteHat.

35 Caso de Estudo: Águas do Norte.

Reportagem

O Papel da Segurança na Transformação Digital.

4

COMPUTERWORLD
FROM IDG

Redação
Redação Direto: +351 969 318 673
Endereço: Rua Braamcamp 84, 3º Drt.
1250-052 Lisboa

Diretora Editorial Mafalda Simões Monteiro
Editor Executivo João Miguel Mesquita
jmesquita@computerworld.com.pt

Colaboraram nesta edição
Josh Fruhlinger, Rafael García del Poyo, Rute Gomes, Stacy Collett.

Arte e Ilustração de capa Pedro Alves
pedroalves@toonstudio.pt

Publicidade e Eventos
Diretor Comercial: Paulo Fernandes
pfernandes@computerworld.com.pt

Propriedade
IDG, 492 Old Connecticut Path, Framingham, MA 01701

Editor
N.º contribuinte: 509967132
N.º de registo na ERC 112115

Periodicidade
A edição especial digital do Computerworld é parte integrante da edição diária online do www.computerworld.com.pt

Siga-nos em

Facebook.com/computerworldpt

Twitter.com/ComputerworldPt

Linkedin.com Computerworld Portugal

Soundcloud.com/techtalk-portugal

Youtube.com/ComputerworldPT

Não há transformação digital sem segurança

A pandemia COVID-19 paralisou o mundo em março do ano passado. Desde então, muitas coisas aconteceram, mas analisar o papel que está a desempenhar a tecnologia na construção de um novo mundo, merece uma análise de vários aspetos que exigem uma performance com uma visão realista do futuro, não nos deixando levar pelos "cantos das sereias". É verdade, como a maioria dos especialistas e analistas do mundo dos negócios e tecnologia afirmam, estamos perante a quarta Era real do desenvolvimento industrial e o nosso país não pode perder-se – como já aconteceu com as anteriores. Para isso, é necessário desenhar os eixos desta grande digitalização a nível nacional e não ficarmos pelos grandes projetos de grandes empresas e organizações, porque este segmento já estava - na maioria dos casos - no futuro estado de digitalização. Portugal é um país de PME e isso não pode ser ignorado. A nossa sobrevivência futura depende de sermos capazes de aumentar a eficiência e, para o efeito, devemos abordar os planos de digitalização urgentes de amanhã que, na sua maioria, dependem de uma gestão eficaz do Plano de Recuperação e Resiliência.

Embora possa parecer surpreendente, pode dizer-se que estamos no caminho certo para entrar no comboio da inovação, que desta vez não pode ser desperdiçado, se tal acontecer Portugal sofrerá em todos os setores e em vez de seguir em frente, volta para a casa de partida. Para entrar nesta "onda", há aspetos que precisam de ser eliminados o mais rapidamente possível, um deles, e o que consideramos o mais importante, é a abordagem ligeira que os gestores têm perante a cibersegurança. O risco de cibercrime emergiu como o risco número um, subindo drasticamente do quinto lugar observado em agosto de 2020. A boa gestão dos projetos e continuidade das PME portuguesas para o êxito da Indústria 4.0 passa pela abordagem que os gestores têm de ter perante as questões de vida ou morte que a cibersegurança traz. Não basta trancar a porta, é preciso monitorizar permanentemente, porque um incidente de cibersegurança por mais pequeno que seja, pode levar uma empresa à falência. CW

INTEGRITY

Securing your Business

Não consegue ler?

É assim que fica a sua informação após um ataque de Ransomware.

A cibersegurança é hoje um real risco de negócio. Não descure o seu.

Saiba mais sobre nós em:
www.integrity.pt

CONSULTING | AUDITING | ADVISORY | TRAINING

PAPEL DA SEGURANÇA NA TRANSFORMAÇÃO DIGITAL

Agora que a segurança está a recuperar a importância nas estratégias digitais, os CISO (Chief Information and Security Officer) querem partilhar a sua responsabilidade em toda a organização e trabalham para transformar a cultura de TI.

Até há poucos anos, as estratégias de transformações digitais aceleraram a uma velocidade vertiginosa com novos processos e o desenvolvimento de produtos avançados. Com a pandemia de Covid-19 essas estratégias passaram imediatamente para o plano operacional.

Enquanto as TI se desenvolveram tirando partido da utilização de metodologias como Agile e DevOps para acelerar a velocidade de marketing, as preocupações de segurança ficaram frequentemente para segundo plano.

Nessa altura, o Gartner previu que 60% das empresas digitais iriam sofrer falhas de serviço importantes em 2020, devido à incapacidade das suas equipas de segurança para gerir o risco digital.

Aconteceram de facto falhas de segurança de alto nível, como antecipado, mas é difícil especificar que projetos digitais foram a principal causa. "Estivessem as falhas previstas diretamente relacionadas ou não com a transformação digital, conseguiram que os líderes empresariais voltassem a pensar no risco e nas soluções capazes de o minimizar", afirma Pete Lindstrom, vice-presidente de investigação de segurança da IDC.

Cerca de 79% dos executivos globais classificaram os ciberataques e as ameaças como uma das principais prioridades de gestão de riscos na sua organização para 2020, de acordo com um inquérito da Marsh & McLennan. Em geral, o papel da segurança na transformação digital melhorou tanto na consciencialização como na participação nas fases iniciais do processo de design, mas os CISO ainda precisam lidar com a amplitude de projetos nos seus ecossistemas.

Desafio da Segurança: Manter o Ritmo

Os gestores de TI não incluem apenas a cibersegurança entre as suas principais preocupações quando se trata de transformação digital. É igualmente a segunda maior prioridade de investimento (35%), logo abaixo da computação em nuvem (37%), de acordo com um estudo recente da Altimeter.

Os investimentos em tecnologias transformadoras podem não fazer sentido se não puderem proteger a atividade, os seus clientes ou outros ativos vitais. E a complexidade e a velocidade do desenvolvimento continuam a ser um desafio, incluindo para as maiores operações de segurança.

"A batalha que está a ser travada avança mais rapidamente que o nosso ciclo de decisão. Se nos movemos

mais devagar, seremos irrelevantes de uma perspectiva de liderança", diz Abel Sánchez, diretor executivo e investigador do laboratório de fabrico e produtividade do Instituto Tecnológico de Massachusetts (MIT). Em segurança, é necessária agilidade, flexibilidade e rapidez na tomada de decisões, assim como durante o processo de desenvolvimento, acrescenta.

Na empresa de soluções globais Schneider Electric, a cibersegurança está no centro da estratégia de transformação. O CISO global, Christophe Blassiau, lutou para conseguir visibilidade em toda a organização, devido a complexas aquisições e às diferentes actividades da empresa que vão da investigação e desenvolvimento (I&D) à cadeia de abastecimento e aos serviços. A integração de TI e tecnologias operacionais (TO) é uma nova conexão, com fontes de dados e vulnerabilidades potenciais que necessitam protecção e a sua equipa deve conectar os pontos entre a segurança da empresa e o seu ecossistema de parceiros e fornecedores.

"Não tínhamos o nível adequado

de capacidade em todo o lado, quando começámos a projectar e a organizar uma nova governança para toda a empresa", assinala Blassiau. "Eu não queria equipas maiores, porque desse modo fica-se sempre com a impressão de que haverá outro que resolve o problema. Aqui, a segurança é responsabilidade de todos".

Em vez disso, a Schneider adotou uma abordagem dupla para a segurança digital e integrou profissionais de segurança digital (gestores de risco digital e CISO regionais) em cada caso e em toda a empresa para criar uma comunidade de líderes digitais treinados e focados em riscos de cibersegurança específicos.

A medida deu a Blassiau "um sentimento de controlo no espaço digital. Há um líder tecnológico que informa cada líder executivo sobre as práticas digitais e que me informa a mim", sublinha.

Equipas de Segurança também devem transformar-se

O desafio para as equipas de segurança continua a ser: como adicionar segurança à velocidade da transformação digital, garantindo que a segurança abrange cada novo processo digital interno e soluções desenvolvidas externamente ou oportunidades criadas na Internet.

Grande parte da solução resume-se à cultura de departamentos de TI e segurança, considera Sánchez.

"As equipas de segurança também têm de passar por uma transformação". Não é fácil, assinala, e muitos trabalhadores devem estar dispostos a aprender novas capacidades para poder interagir com a organização do negócio.

> "Em vez de não, diga 'vamos ver como podemos fazer isso o mais rapidamente possível e em segurança".

Isto só pode ser alcançado através de uma reorganização, diz Sánchez. Os testers, por exemplo, estão a desaparecer em muitos casos e os engenheiros de software estão agora a realizar os testes.

"Quem melhor sabe como proteger o produto do que aquele que o criou? O mesmo pode ser feito noutras áreas de desenvolvimento".

"Também podem ser necessários talentos diferentes ou que os talentos tenham de mudar. Podem perder-se muitas pessoas, mas pensem onde se podem encaixar. Precisará desse tipo de pessoa que pode trazer inovação e trazê-lo para a empresa", diz Sánchez. "O mundo está a mudar a velocidade acelerada".

A boa notícia é que as equipas de segurança como um todo estão a tornar-se mais acessíveis e são parte do negócio, o que leva a ter melhores relações, disse Matt Handler, CEO de Segurança para as Américas da NTT, uma grande consultora global e fornecedor de serviços de gestão de segurança que disponibiliza serviços de transformação digital.

"As equipas de segurança estão a aprender que não pode ser o "escritório do não" a toda a hora. Devem ser ágeis, flexíveis e ser vistos com um facilitador e não como um bloqueador", diz Handler. "Tudo isso aconteceu no último ano, mais ou menos.

O CISO deve também evoluir e assumir o papel de assessor interno e colaborador dos departamentos que estão a implementar as aplicações ou as novas tecnologias, acrescenta Handler. "Em vez de não, diga 'vamos ver como podemos fazer isto o mais rapidamente possível e de maneira segura'. Esta frase, por si, creio, representa uma mudança na estratégia de jogo de um CISO".

Cozinhando a Segurança

Os CISO têm vindo a promover, durante anos, que a segurança deve introduzir-se no início do processo de design". Agora, é mais fácil de se fazer, graças a componentes mais ágeis e dinâmicas. "Com a computação em nuvem, em particular" e as funções de segurança que se podem utilizar "podemos jogar para gerir riscos", diz Lindstrom, "e estamos a trabalhar mais na segurança baseada na aplicação, na camada de dados e aspectos relacionados com a identidade, em lugar de uma segurança assente no host e na rede".

Além disso, os investidores preveem que as empresas de cibersegurança que utilizem aprendizagem automática (machine learning) se devem destacar durante o corrente ano, à medida que se consolida o número de fornecedores de cibersegurança de nicho, embora tenham de enfrentar um elevado nível de incerteza sobre o que afirmam que a sua tecnologia pode fazer. As empresas com grandes quantidades de dados (big data) de segurança poderão combinar algoritmos, analítica e aprendizagem automática para identificar e reagir a novas ameaças à velocidade da luz, praticamente tão rápido como aquelas se produzem. As máquinas apenas podem ser tão boas como os humanos que as operam e tão precisas como os dados como os quais os seus padrões combinam e tudo isso levará tempo.

> O Gartner prevê que 60% das empresas digitais vão sofrer falhas importantes no serviço durante o corrente ano.

"Da perspetiva de um CISO, se pode proporcionar segurança a grande velocidade e ajudar a empresa a alcançar os seus milestones e objetivos e se consegue que a segurança esteja integrada no processo desde o início, tem o sucesso assegurado. Mas, isto é, por enquanto, algo para o futuro", conclui Handler.

Já chegámos?

Quando se trata de cibersegurança nas transformações digitais, Sánchez

diz que a cada dia que passa há mais empresas que "já percorreram mais de metade do percurso". Já passaram pelo processo de automação e estão a começar a olhar para a Inteligência Artificial e modelos preditivos.

"Estamos no caminho certo, mas isso não significa que, entretanto, não seja preciso fazer compromissos", acrescenta, Sánchez. "Tal como (antes da transformação digital), o desenvolvimento de software não estava integrado em todos os âmbitos e agora sim, o mesmo se pode dizer em relação à segurança. Tudo isto tem de unir-se. É uma questão de tempo". cw

As empresas duvidam que colaboradores consigam detetar ciberataques

Dados da S21sec mostram ainda que 38% das empresas reconhecem que foram vítimas deste tipo de ataques (de phishing) no último ano.

Cerca de um ano depois do primeiro confinamento em Portugal, o teletrabalho passou a ser uma realidade para muitas empresas e colaboradores. **Com o aumento do teletrabalho, registou-se também um aumento dos ciberataques** no último ano e, de acordo com a S21sec, 36% das empresas não têm a certeza se os seus colaboradores são capazes de prevenir e detetar um ciberataque.

O contexto atual trouxe riscos adicionais relacionados com os mecanismos de acesso remoto para teletrabalho, a proteção de informação nos sistemas e redes utilizados pelos colaboradores fora dos escritórios e a vulnerabilidade a ataques de negação de serviço. Em Portugal, a S21sec regista que os principais ciberataques são realizados com recurso ao phishing e à partilha e distribuição de malware, com técnicas cada vez mais aprimoradas pelos atacantes.

A S21sec conclui ainda que 38% das empresas reconhecem que foram vítimas deste tipo de ataques no último ano. Quando efetuados com sucesso, o impacto de um ciberataque traz consequências graves não só para o negócio de qualquer organização, mas também para a reputação da marca.

"Os novos modelos de trabalho obrigam a que estruturas de sistemas, aplicações e redes estejam preparadas para o acesso remoto e para uma nova força de trabalho dispersa pelos vários locais onde se encontram. É importante existir uma proteção eficaz dos endpoints que usamos diariamente, como os computadores portáteis por exemplo, mas também alertar os colaboradores para os riscos que existem atualmente e como devem proceder para os minimizar", explica José Luís Silva, Head of Integration da S21sec.

Recomendações para evitar um ciberataque

Face ao crescimento da possibilidade de se sofrer um ciberataque devido ao aumento do teletrabalho, a S21sec partilha seis recomendações importantes para diminuir o risco de um incidente interno:

- Pense antes de clicar: nunca abra um anexo e não clique num link de remetentes que não conhece.

- Não confie em promoções, ofertas ou sorteios: verifique sempre as páginas oficiais das empresas.

- Verifique a fonte: principalmente se o e-mail solicitar a confirmação de informações pessoais e/ou financeiras.

- Atualize as suas senhas: e não as reutilize nas suas redes sociais ou em sites potencialmente inseguros.

- Instale soluções de segurança nos seus dispositivos e mantenha-os atualizados.

- Tenha cuidado com as informações que publica nas redes sociais: não partilhe dados pessoais ou imagens que o possam comprometer ou à sua organização.

"Para além de alertar para os perigos que o teletrabalho em massa acarretou numa fase inicial, é também importante que as pessoas estejam sempre alerta. Uma desatenção ou descuido ao aceder a determinados sites ou clicar em determinados links, pode abrir a porta a um ciberataque que depois irá naturalmente ter diversas consequências, seja em termos pessoais ou, sobretudo, para a empresa à qual o trabalhador está associado", explica José Luís Silva, Head of Integration da S21sec.

O retorno do investimento da perspetiva do Ciber-Atacante

Por Rui Shantilal da INTEGRITY

O entendimento adequado da evolução do Cibercrime requer uma reflexão estratégica essencial para que se possa endereçar o tema de forma apropriada.

Atualmente a cibersegurança está tendencialmente na agenda dos gestores de praticamente todas as organizações, onde se procura de forma consistente avaliar as ameaças e definir estratégias de mitigação assentes em modelos de análise de risco, levando naturalmente em consideração o custo/benefício desses investimentos.

E quanto aos atacantes? Estes também terão uma abordagem de retorno de investimento à sua atividade? Quais são as variáveis a considerar, e mais importante: que lições devemos tirar desta análise?

Estarão as últimas tendências de crescimento e diversificação do cibercrime associadas a esta análise de retorno de investimento dos ciber-atacantes?

O que podemos esperar do futuro e quais as ações que devemos tomar?

Como pensa o atacante Variáveis a serem consideradas

Tal como acontece numa empresa, os atacantes também utilizam um modelo de custo/benefício e procuram obter o maior benefício possível dos seus investimentos.

Atuando maioritariamente em grupos organizados, estas são essencialmente as variáveis levadas em consideração pelos Cibercriminosos:

Receita líquida **–** É o resultado de quanto (ou o que) o atacante vai obter como resultado das suas ações. Esta variável calcula a projeção de potencial retorno considerando o cenário e alvo. Este valor terá que levar em consideração os custos de monetização da receita, que tipicamente envolve custos de branqueamento dos capitais obtidos de forma irregular.

Investimento **–** O investimento do atacante é essencialmente os recursos humanos com expertise e os meios tecnológicos necessários para levar a cabo um ataque de forma bem-sucedida.

Outra dimensão a considerar é o ***risco***. Não só o risco de poderem ser apanhados, mas o risco de que, apesar de investirem tempo e recursos, o ataque não ser bem-sucedido. Nesse contexto os atacantes levam em consideração a probabilidade de sucesso e o risco que correm de serem apanhados.

Depois de avaliar o ROI potencial e os fatores de risco, o atacante decidirá se vale a pena seguir em frente. Estes vão evitar situações como investir recursos e não ter sucesso, assim como, em qualquer outro modelo de negócio.

A evolução da maturidade da cibersegurança

A segurança cibernética já não é um tópico novo. Pelo menos, desde o início do milénio, as grandes empresas e entidades e mais especificamente o setor financeiro têm se concentrado sobre este tema.

Após 20 anos, espera-se que a sua maturidade tenha evoluído consideravelmente e atualmente não são amadores os que conseguem atacar com sucesso tais organizações.

Nos últimos anos, estas empresas criaram departamentos dedicados especificamente, com pessoas formadas, em Cibersegurança. Atualmente, estas organizações têm uma série de políticas, procedimentos, tecnologia e equipas que lhes permitem prevenir, detetar e responder apropriadamente a ameaças e incidentes. Muitos destas também executam um programa consistente de conscientização para os seus recursos humanos, com o objetivo de reduzir a tendência a ataques combinados de Engenharia Social.

As implicações para o cenário de ameaça

O crescimento da maturidade no setor da Cibersegurança também representou mudanças significativas para o cenário de ameaça, principalmente porque as oportunidades de sucesso num ataque contra empresas robustas ou entidade financeiras ficaram consideravelmente reduzidas, resultando numa projeção de ROI negativa para os atacantes.

Desta forma, os atacantes também estão a mudar o seu comportamento, a saber:

Diversificação de Target:

Sempre que alguém disser: "Mas nós não somos um banco !!" recorde-lhes que os invasores também estão conscientes desse facto e como tal sabem que, outras entidades não possuem o mesmo nível de controlo que um banco possui, facilitando-lhes assim a sua intrusão. Apesar de o lucro ser potencialmente inferior, estes diversificam pelos setores porque sabem que o investimento em cibersegurança é menor e que a probabilidade de sucesso é maior e isso resulta num ROI melhor. Hoje, vemos setores sob ataque, que não eram o principal alvo dos atacantes, como saúde, educação, retalho, indústria, hotéis, PMEs e até mesmo utilizadores finais, todos sob ataque utilizando abordagens de ameaças, como Card Skimming, Ransomware, Ceo Fraud, APT, Phishing, entre outros.

Ataques combinados e complexos:

os atacantes estão cientes de que obter quantias mais avultadas não é uma brincadeira de criança. Assim, sempre que estão dispostos a correr o risco para alcançar este tipo de alvo, naturalmente, também têm ataques mais sofisticados. Ataques combinados utilizando mais do que uma abordagem de ataque, como combinação de ameaça interna com hacking ou conluio são formas de ataques sofisticados que foram observados nestes tipos de alvo.

Que medidas tomar

A mentalidade de que não somos um alvo interessante já não é aplicável. Todos que utilizamos tecnologia somos um alvo interessante. E a ideia de que já estávamos prontos há 10 anos também está muito longe da realidade.

Quer seja ou não uma grande empresa ou entidade, com base neste cenário, todos os que utilizam tecnologia precisam de estar conscientes e preparados, porque os atacantes estão permanentemente à procura de novas e criativas formas de diversificar e lucrar.

É claro que um utilizador final ou uma PME não pode investir o mesmo

nível de recursos que uma grande empresa ou entidade, mas um esforço equilibrado e adequado deve ser considerado na sua estratégia de segurança da informação.

Regularmente, as organizações (e pessoas) devem:

- Estar conscientes e informados sobre as tendências de ataques cibernéticos.
- Avaliar os riscos e nível de exposição.
- Definir controlos apropriados (técnicos e processuais) para mitigar riscos quando adequados.
- Treinar as equipas, disseminar conhecimento e conscientização aos utilizadores.
- Definir planos de deteção e resposta adequados para minimizar o impacto no caso de um ataque bem-sucedido.
- Monitorizar e adaptar consistentemente, porque a Cibersegurança é dinâmica e a capacidade de observação e adaptação é um elemento chave neste puzzle.

Por fim, devemos estar cientes de que grandes oportunidades vêm sempre acompanhadas de grandes riscos. O incremento do cibercrime está para as tecnologias da informação, assim como a sinistralidade automóvel está para indústria automotiva. Os riscos são reais e dinâmicos, há que estar consciente e atuar sobre os mesmos para que se possa tirar o máximo partido das oportunidades, com o mínimo de risco possível. CW

O QUE É UM ATAQUE DE BANDEIRA FALSA?

ASSIM SE ENCOBREM OS ATAQUES DESTE TIPO DE PIRATAS INFORMÁTICOS

As bandeiras falsas são uma das técnicas preferidas dos ciber-atacantes relacionados com os serviços de inteligência russa, mas estes não têm o monopólio desta prática.

Fotografia de Alexis

Um ciberataque de bandeira falsa ocorre quando um hacker ou um grupo de piratas realiza um ataque que procura enganar as suas vítimas e o mundo sobre quem é responsável e quais são os seus objetivos.

As técnicas utilizadas neste tipo de ataques passam por simplesmente transmitir espalhar declarações de autoria falsa, simulando ferramentas, técnicas e até idiomas normalmente utilizados pelo grupo ou país pelo qual os atacantes se procuram passar por.

O termo "bandeira falsa" teve origem durante a primeira guerra mundial, quando navios britânicos e alemães utilizavam símbolos de outros países (os britânicos chegaram a utilizar bandeiras alemãs e vice-versa) para enganar os seus inimigos. O termo chegou a aplicar-se a atos enganadores mais elaborados, destinados a culpar politicamente os adversários e a permitir aos agressores passarem por vítimas. Por exemplo, nos anos 30, os japoneses começaram uma guerra com a China depois de executar um falso ataque chinês às forças japonesas, uma técnica que os alemães repetiram quando invadiram a Polónia. Tal como os soviéticos antes de começar a guerra contra a Finlândia. A partir daí o termo entrou no discurso dos teóricos da conspiração que, muitas vezes acreditam que ataques

terroristas ou tiroteios em massa são organizados ou perpetrados pelo próprio governo para alimentar o medo ou ganhar poderes ditatoriais.

Mas os ciberataques de bandeira falsa não são uma teoria de conspiração. São um fenómeno bem documentado que se tornou cada vez mais frequente nos últimos cerca de cinco anos.

Num ataque de bandeira falsa, os ciber-atacantes, com base no próprio país, podem fazer passar-se por criminosos comuns, hactivistas motivados politicamente ou hackers apoiados por um país totalmente diferente. E, embora existam vários países envolvidos em tais ataques, o mais prolífico é, de longe, a Rússia, através do seu serviço de inteligência GRU e dos hackers a ele associados.

O objetivo de implementar um ataque de bandeira falsa pode parecer óbvio: não assumir a culpa pelos factos criminosos. Além disso, culpar os outros vai além do tradicional comportamento dos criminosos que estão apenas preocupados em ocultar a sua identidade.

Por exemplo, acredita-se que o ataque de Stuxnet contra o programa nuclear do Irão foi executado pelos EUA e Israel. Embora estes países não reivindiquem a autoria também não procuram culpar mais ninguém.

Num ataque de bandeira falsa, apontar o dedo alguém pode representar a criação de um alvo armado, além dos resultados diretos do ciberataque.

E ao incentivar um clima de caos e confusão dentro da comunidade de cibersegurança, as bandeiras falsas dificultam a tarefa de quem pretende manusear com segurança a realidade objetiva.

Como James Lewis, diretor do Programa de Tecnologias Estratégicas do Centro de Estudos Estratégicos e Internacionais, disse à revista Wired, os hackers querem criar um mundo onde ninguém, especialmente nos EUA, saiba com certeza quem é o responsável por um ciberataque. "Eles gostariam de criar uma contra narrativa: não se pode confiar nos americanos. Vejam, eles estavam errados", explica.

Seis ataques de Bandeira Falsa

Estes seis grandes ataques dos últimos anos, mostram como funcionam as técnicas de bandeira falsa e como evoluíram ao longo do tempo.

2014: Guardiões da Paz e o hack à Sony Pictures

A Sony Pictures foi pirateada, no final de 2014, com grandes quantidades de mensagens de correio electrónico embaraçosos, informações financeiras e, inclusivamente, filmes inéditos carregados em sites de partilha de ficheiros online.

A responsabilidade do ataque foi inicialmente reivindicada por um grupo intitulado "Guardiões da Paz". Embora o grupo não tenha revelado muito sobre si mesmo, o nome claramente sugere algum tipo de grupo ideológico. Ninguém levou esta teoria particularmente a sério e as listas de possíveis suspeitos incluíram cibercriminosos, mas também indivíduos descontentes.

No entanto, posteriormente os dedos começaram a apontar noutra direcção: a Coreia do Norte, cujo líder Kim Jong-Un foi provocado e finalmente foi "morto" na comédia da Sony, The Interview. O filme de Seth Rogan transformou-se no foco das comunicações dos Guardiões da Paz. Apenas algumas semanas após o ataque, o FBI responsabilizou o governo norte-coreano e a empresa de segurança CrowdStrike apresentou evidências do código associado ao ataque, incluindo erros de digitação,

que coincidiam com outros ataques da Coreia do Norte. A Coreia do Norte nunca assumiu a responsabilidade pelos ataques, embora a responsabilidade dos ataques seja universalmente reconhecida. A quantidade de desmentidos apresentados permitiu-lhes, no entanto, salvar politicamente a face.

> As técnicas utilizadas neste tipo de ataque podem passar apenas por difundir declarações sem autoria até emular ferramentas.

CyberBerkut

A revolução da Euromaidán na Ucrânia, que depôs um governo pró-russo e o substituiu por um pró-ocidental, desencadeou um conflito com a Rússia que deixou grandes regiões do país nas mãos dos russos e desencadeou uma guerra de poder no leste da Ucrânia. Com a própria população da Ucrânia polarizada em facções pró-ocidentais e pró-russas, não foi uma surpresa ver grupos de hacktivistas emergirem no extremo pró-russo do espectro.

O CyberBerkut foi um dos mais importantes. Lançou ataques DDoS em sites da NATO e pirateou computadores do Governo ucraniano para aceder e disponibilizar informações confidenciais sobre a participação secreta dos EUA no conflito.

A informação divulgada misturava documentos reais e manipulados, o que fez com que a União Europeia, os EUA e o governo ucraniano parecessem ainda piores, criando uma espécie de propaganda anti-ocidental.

A versão inicial do CyberBerkut da F-Secure referia que "eram ucranianos. Uma unidade voluntária de ciberataques não directamente associada a qualquer Governo".

No entanto, esta teoria não se manteve. Muitos dos ataques da CyberBerkut foram de phishing, através dos quais recolhiam as senhas das vítimas. Uma análise do Citizens Labs descobriu que os URL curtos usados nestas mensagens de correio electrónico eram semelhantes àqueles utilizados em ataques não associados ao conflito ucraniano, mas perpetrados pelos serviços secretos russos.

Muito provavelmente, o CyberBerkut é um grupo de astroturfing, uma operação do governo russo que aparenta ser um movimento orgânico ucraniano pró-russo.

2015: Cibercalifado

Em Abril de 2015, a emissão da cadeia de televisão francesa TV5Monde foi interrompida por um sofisticado ciberataque. Além da interrupção da emissão foram também danificados muitos dos computadores da estação. O site foi seriamente danificado e foram inseridas mensagens do autodenominado grupo do cibercalifado. A Cybernetic reivindicou o ataque.

Apenas alguns meses após o ataque ao Charlie Hebdo, e enquanto a França participava na campanha aérea contra o ISIS, a suposição inicial apontava para um ataque

lançado pelo Estado islâmico. No entanto, os investigadores rapidamente chegaram a uma conclusão diferente: o ataque foi lançado pela Rússia e estava de facto associado ao APT28, o mesmo grupo associado ao CyberBerkut.

Entre as pistas que apontaram para a Rússia, estava o código utilizado no ataque, digitado em teclados cirílicos, num dia útil, em Moscovo e São Petersburgo.

Porque atacaria a Rússia uma estação de televisão francesa ainda não é claro. Aconteceu no pico da crise ucraniana, pelo que a possibilidade de humilhar uma potência da NATO poderá ter sido uma ideia tentadora. O ataque também pode ter sido uma forma de baixo risco de testar algumas novas técnicas de ciberataques. Quanto ao aspecto de bandeira falsa do ataque, a Rússia também estava envolvida no conflito com o ISIS, pelo que desviar a atenção de um inimigo comum poderia ser uma forma de afastar os investigadores da cena do crime.

2017: NotPetya

Em 2016, equipas de TI de todo o mundo sofreram ou tiveram de lutar com um programa de ransomware denominado Petya. Apesar de ter algumas características inovadoras, o Petya era um exemplo típico do seu tipo: propagado através de mensagens de correio electrónico de phishing, se executado, cifrava o disco rígido da vítima e exigia um resgate em bitcoin. Não causou grande problemas. Mas, em meados de 2017, surgiu uma versão muito mais agressiva, suficientemente diferente do original para que os analistas de segurança o chamassem de NotPetya. O NotPetya poderia espalhar-se por si mesmo através da falha EternalBlue desenvolvida inicialmente pela NSA. E o mais estranho é que cifrava o computador da vítima e exigia um resgate em bitcoins, tal como o Petya, mas o endereço da carteira de bitcoin fornecido era apenas um número aleatório. Não havia forma de pagar de facto a alguém para restaurar o computador. O NotPetya é, por isso, uma bandeira falsa: um malware puramente destrutivo disfarçado de ferramenta de ransomware mais benigna. A identidade do autor tornou-se evidente quando se rastreou o vector de ataque inicial do NotPetya: acedeu ao ciber-ecossistema através de uma porta dos fundos instalada no M.E. Doc, uma aplicação de contabilidade extremamente popular na Ucrânia. Os investigadores consideram que foi um ataque russo que causou estragos nos sistemas da Ucrânia, disfarçando-se de uma versão de um malware já existente para não chamar demasiado a atenção.

Infelizmente, o NotPetya espalhou-se rapidamente e muito além do objetivo inicial, criando o caos em toda a Europa e colocando sob escrutínio a comunidade de segurança.

2018: Destruidor Olímpico

Embora tenha passado despercebido aos espectadores em todo o mundo, a cerimónia de abertura dos Jogos Olímpicos de Inverno de 2018, em Pyeongchang, Coreia do Sul, também enfrentou um desastre. A infra-estrutura de TI dos Jogos

> As bandeiras falsas dificultam a capacidade de gerir com segurança a realidade objetiva.

Os ciberataques de bandeira falsa não são uma teoria de conspiração. São um fenómeno bem documentado que se tem tornado cada vez mais frequente.

Olímpicos foi alvo de um ciberataque que derrubou a ligação Wi-Fi do estádio onde decorria a cerimónia. Os espectadores não conseguiam imprimir bilhetes nem os funcionários do estádio os conseguiam digitalizar. Apenas o esforço hercúleo da equipa de cibersegurança permitiu restaurar os sistemas para funcionarem no dia seguinte, quando os Jogos Olímpicos começavam de facto.

Quem esteve por trás deste ataque? O malware foi disfarçado deliberadamente sob várias camadas de bandeiras falsas, algumas das quais apontavam para a China, mas outras apontavam para dois países com rancores mais óbvios contra a Coreia do Sul e os jogos: a Coreia do Norte – vizinho do Sul com ambições de domínio sobre a Península – e a Rússia, cujos atletas se viram obrigados a competir sob uma bandeira neutra, devido a um escândalo de doping generalizado.

Finalmente, os investigadores de segurança chegaram à Rússia devido a duas pistas. Num caso, alguns dos metadados do cabeçalho do malware davam a entender que o código teria sido escrito na Coreia do Norte, mas o restante código não tinha essas características. E o arquivo Word contaminado, que tinha sido descarregado de correio electrónico phishing, usado inicialmente para infectar os sistemas dos Jogos Olímpicos, tinha fortes semelhanças com os documentos que tinham sido utilizados para atacar grupos LGBT ucranianos no ano anterior – um objetivo russo bastante óbvio.

2019: Turla e Oilrig

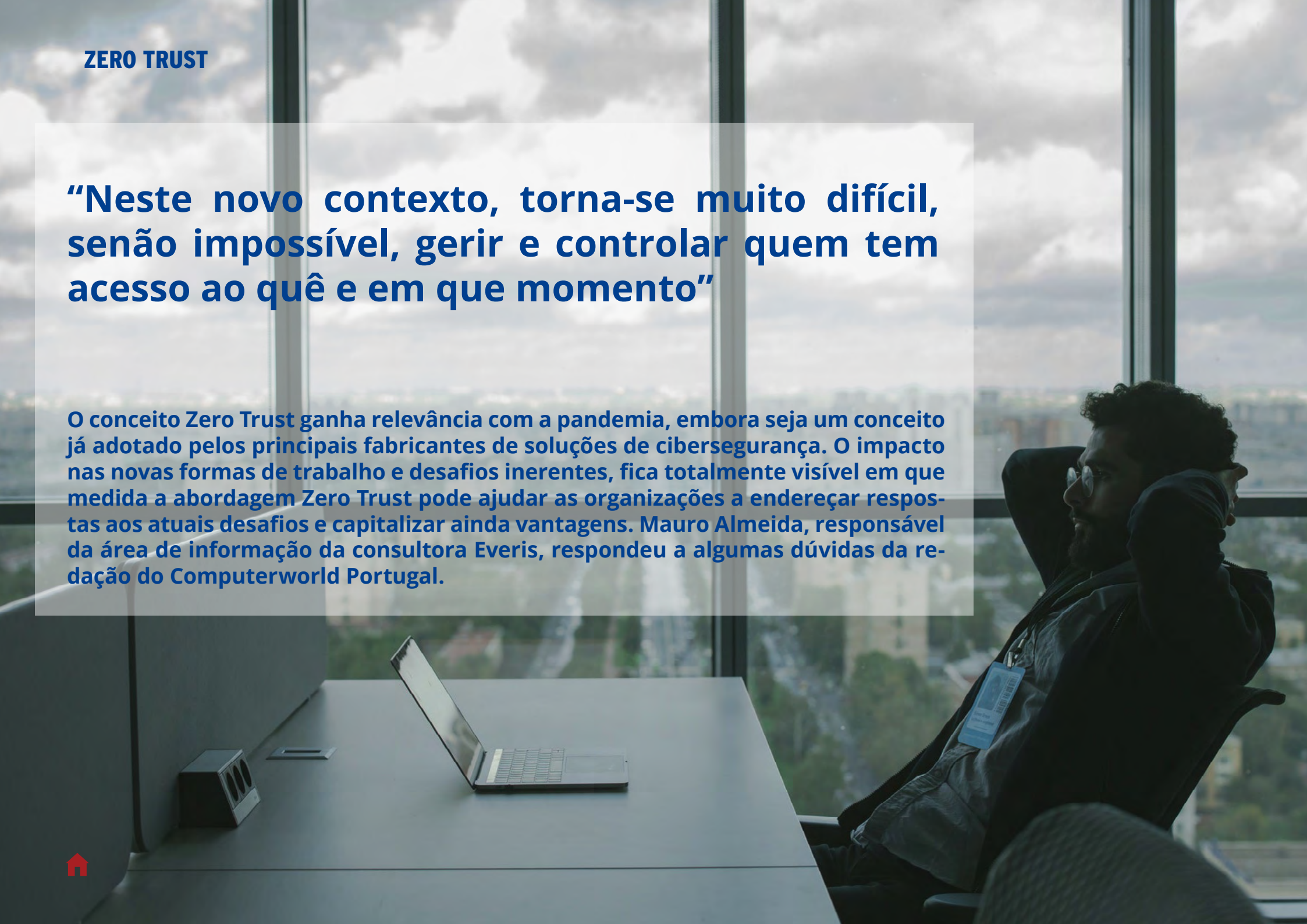
Anteriormente referimos que a Rússia se tinha feito passar por um grupo jihadista islâmico no ataque

a um canal de televisão francês. Um relatório publicado em 2019 revelou um movimento ainda mais insidioso: um grupo de piratas russo, conhecido por Turla, controlou muitos dos sistemas de um grupo de piratas iraniano conhecido como Oilrig, aparentemente sem o seu conhecimento ou consentimento. O Turla aproveitou as vulnerabilidades criadas pelo Oilrig para implementar as suas próprias portas das traseiras e outros conjuntos de ferramentas que posteriormente poderiam explorar a partir da própria infra-estrutura do Turla.

Esta é a derradeira bandeira falsa. Em vez de um navio ostentando as cores de outra nação, o navio iça a sua própria bandeira, mas o inimigo assume o controlo da navegação, sem que a tripulação saiba o que está a acontecer.

A Ponta do Iceberg

Centramo-nos nos ataques russos, porque, na realidade estão entre os mais conhecidos. Claramente, é uma prática popular na Rússia, mas estará sobrerepresentado na mente do público devido aos estereótipos associados aos russos. Porque não se estende a outras nações com tanta frequência? O mais provável é que existam outras nações capazes de realizar os mesmos tipo de ataques. Em 2017, a WikiLeaks revelou uma ferramenta da CIA, Marble, que podia alterar o código para parecer que tinha um país de origem não norte-americano, embora a maioria dos peritos em segurança esteja de acordo: o Marble é um programa que ofusca o código, mas que não poderia criar uma bandeira falsa de facto. Enquanto isso, em Dezembro de 2019, foi revelado que instalações nucleares na Índia tinham sido pirateadas por um código que parecia ser proveniente da Coreia do Norte. No entanto, a maioria dos peritos não sabe por que motivo a Coreia do Norte quereria piratear uma central nuclear na Índia. A única certeza que há em todo este tema, é quão assustador se está a tornar este panorama de ameaças. CW



“Neste novo contexto, torna-se muito difícil, senão impossível, gerir e controlar quem tem acesso ao quê e em que momento”

O conceito Zero Trust ganha relevância com a pandemia, embora seja um conceito já adotado pelos principais fabricantes de soluções de cibersegurança. O impacto nas novas formas de trabalho e desafios inerentes, fica totalmente visível em que medida a abordagem Zero Trust pode ajudar as organizações a endereçar respostas aos atuais desafios e capitalizar ainda vantagens. Mauro Almeida, responsável da área de informação da consultora Everis, respondeu a algumas dúvidas da redação do Computerworld Portugal.

Mauro Almeida, Responsável da Área de Comunicação da Everis

CW- Qual a abordagem correta que os CSO devem fazer para convencerem os CEO da importância do conceito?

Mauro Almeida - O principal fator que contribui para que se compreenda claramente a necessidade de uma abordagem Zero Trust à segurança de informação, e cibersegurança, é a correta compreensão dos problemas que esta abordagem vem endereçar e os riscos que pretende colmatar.

O parque tecnológico das organizações, em constante crescimento e mudança, a adoção de políticas de trabalho menos restritivas, aceleradas pela necessidade do teletrabalho na realidade de pandemia que vivemos atualmente e a migração para a cloud, fazem com que deixe de existir um perímetro de segurança nas organizações e a abordagem tradicional, de confiar no se encontra dentro desse perímetro de segurança, deixa de ser aplicável.

Neste novo contexto, torna-se muito difícil, senão impossível, gerir e controlar quem tem acesso ao quê e em que momento. A diversidade de acessos e a falta de visibilidade sobre os mesmos leva a níveis de confiança excessivos e perigosos para as organizações, com consequente aumento da exposição das organizações a ciber ataques e do impacto desses mesmos ataques.

Numa abordagem Zero Trust o acesso é baseado no mínimo privilégio possível e os equipamentos, redes e utilizadores são considerados maliciosos ou comprometidos até prova do contrário. Esta abordagem permite às organizações criarem os automatismos, políticas e arquiteturas necessárias para mitigar grande parte dos riscos associados a ciber ataques e prevenir que estes ataques tenham um impacto profundo e imediato nas organizações e nos seus negócios, equilibrando segurança e usabilidade.

CW - Onde, e como, é que a Everis pode ajudar neste processo?

MA - A Everis pode ajudar as organizações em 3 dimensões complementares: estratégica, desenho e implementação e comunicação e

> «A everis pode ajudar as organizações em trêsdimensões complementares: estratégica, desenho e implementação e comunicação e gestão da mudança.»

gestão da mudança.

Numa vertente estratégica, defendemos que a base de qualquer plano de segurança bem-sucedido é a correta identificação dos riscos aos quais a organização está exposta, bem como do real impacto e probabilidade destes riscos. Apoiamos organizações, nacionais e internacionais, através da realização de análises de ciber risco, assentes nas principais metodologias e normas, sistematizadas através de processos iterativos e que sejam transversais à organização. Estas análises, realizadas pelos nossos especialistas em ciber risco, permitem-nos identificar e priorizar os controlos críticos de segurança necessários, definir o plano de segurança a implementar e identificar as ferramentas que suportam a adoção de um modelo ou estratégia Zero Trust mais adequadas à organização.

Numa perspetiva de desenho e implementação, quando se fala de uma abordagem Zero Trust é imprescindível abordar o governo e gestão de identidades e o controlo de acessos. Neste domínio temos estabelecido sólidas parcerias com os principais fabricantes de soluções de Identity and Access Management (IAM) líderes de mercado e temos um vasto conhecimento e experiência no desenho e implementação destas soluções. Estes dois fatores, permitem-nos apoiar as organizações na adoção ou transição para estas tecnologias, desde a análise e desenho dos processos e arquitetura a implementar, até à instalação e integração das soluções com os repositórios, sistemas e aplicações. A implementação destas soluções permite uma gestão unificada e centralizada das identidades e controlo de acessos dentro da organização, com elevados mecanismos de automatismo, resultando em eficiência operacional, melhoria da experiência dos utilizadores e aumento da segurança.

Transversalmente à segurança de informação, acredito que para mudar comportamentos é necessário mudar convicções. São os colaboradores das empresas os principais agentes da mudança. E é nesta vertente que a Everis, através das suas equipas multidisciplinares, apoia as organizações na definição e execução de planos de gestão da mudança, e de comunicação, e na criação e execução de programas de sensibilização adaptados ao negócio e à cultura organizacional, contínuos no tempo, e que incluem mecanismos de avaliação da sua eficácia.

CW - Existem restrições orçamentais, nomeadamente com a crise económica adensada pela incerteza dos tempos que vivemos. Como se consegue convencer as empresas a investir em soluções de cibersegurança?

MA - Hoje, mais do que nunca, as organizações estão expostas a um elevado risco de ciber crime. A superfície de ataque às organizações aumentou exponencialmente. As empresas que não estão preparadas para atuar preventivamente sobre estas ameaças têm uma probabilidade muito maior de experienciar perdas financeiras, danos operacionais ou reputacionais. A segurança de informação, e ciber segurança, não podem, por isso, ser vistas como um custo para as organizações, mas sim como um investimento focado na redução dos riscos que ameaçam a organização e os seus ativos.

O acesso indevido a dados confidenciais das organizações, ou a sua adulteração, pode levar à perda de confiança por parte dos clientes, dano reputacional, perda de propriedade intelectual e à aplicação de multas pelo incumprimento de regulamentos ou normas, com as consequentes perdas financeiras. É por isso essencial que as organizações implementem preventivamente, por exemplo, soluções

e mecanismos de data loss prevention e de classificação e proteção de informação.

A falta de visibilidade sobre as redes e dispositivos da organização pode levar a que os atacantes perpetuem a sua atividade durante um elevado período, sem que esta seja detetada. É fundamental a implementação de soluções de monitorização de tráfego ou soluções de Endpoint Protection and Response (EDR) para que as empresas possam agir na deteção precoce de potenciais ameaças ou ciber ataques, evitando desta forma roubo de informação ou a quebra operacional incluindo interrupção dos serviços.

As ações não intencionais - ou falta de ação - por utilizadores podem desencadear vulnerabilidades que facilmente levam ao ciber crime. Estas ações podem ir desde a partilha inadvertida de credenciais de acesso, download de um anexo de um email infetado por malware até à utilização de passwords e credenciais fracas. Este risco humano pode ser reduzido através da criação de programas de sensibilização ou adoção de políticas de gestão de acessos ou de gestão de passwords mais restritivas. As políticas de gestão de acessos e gestão de credenciais, devem utilizar mecanismos de autenticação forte e adotar a abordagem do mínimo privilégio possível, conforme sugerido numa abordagem Zero Trust.

«A crise sanitária e económica que hoje vivemos criou restrições orçamentais, mas também mudou a nossa forma de trabalhar e a forma como as empresas se relacionam com os seus clientes, colaboradores e parceiros, expondo as organizações a novos riscos e ameaças de segurança. É por isso que investir em segurança é hoje mais importante que nunca.»

A crise sanitária e económica que hoje vivemos criou restrições orçamentais, mas também mudou a nossa forma de trabalhar e a forma como as empresas se relacionam com os seus clientes, colaboradores e parceiros, expondo as organizações a novos riscos e ameaças de segurança. É por isso que investir em segurança é hoje mais importante que nunca.

CW - Quais as situações de risco que as empresas mais devem ter em atenção tendo em conta o trabalho remoto?

MA - O principal risco ao qual o trabalho remoto veio expor as organizações é o facto de que os colaboradores deixam de estar no perímetro da organização e passam a utilizar as suas redes pessoais, de casa, para aceder a informação confidencial e sensível, ou a ativos da organização. Estas redes domésticas não têm os mesmos controlos de segurança que as redes corporativas e são mais uma superfície de ataque, não controlada pelas organizações. Com o trabalho remoto, esbatem-se as fronteiras entre o contexto pessoal e profissional, levando a que muitas vezes os colaboradores utilizem os seus equipamentos pessoais para fins profissionais ou que outros membros do agregado familiar acedam aos equipamentos profissionais.

Adicionalmente, grande parte dos colaboradores das empresas não está sensibilizado para o tema e por isso não toma as devidas precauções. A par da adoção de algumas medidas tecnológicas, como a segmentação de redes, a monitorização de dispositivos ou a implementação de mecanismos de multi-factor authentication (MFA), é essencial trabalhar a segurança na perspetiva da formação e sensibilização dos colaboradores. Não é suficiente investir nos melhores serviços, adquirir o melhor hardware e software e definir processos internos, se não houver investimento nos colaboradores, que são quem realmente vai estar na frente da batalha contra ciber ameaças. É errado pensar que os utilizadores são o elo mais fraco na segurança da informação das organizações, quando na verdade têm o potencial para ser o elemento mais forte de uma empresa na proteção contra ameaças de segurança.

CW - No mercado português quais os ataques mais comuns e os que têm vindo a aumentar?

MA - Em Portugal os ataques informáticos têm seguido a tendência mundial. Em ciber segurança não existem fronteiras, e é natural que se observe uma globalização dos

ataques informáticos, ganhando maior relevância aqueles que são economicamente mais atrativos para os atacantes.

Um aumento generalizado dos ciberataques é comum em tempos de crise, como se verificou em 2008 com a crise económica mundial. Os ciber criminosos procuram tipicamente as vulnerabilidades sociais como uma porta de entrada, explorando os receios dos indivíduos.

A crise pandémica que vivemos atualmente não é exceção. Alias, tem duas particularidades que a tornaram mais permeável a ataques: por um lado, atingiu a globalidade dos países de forma quase imediata, o que levou ao aumento de alguns tipos de ataques informáticos que tiraram partido da mudança de foco das organizações e dos governos para darem resposta à crise; por outro lado, como uma das respostas das organizações foi assegurar a continuidade dos seus negócios num formato de trabalho remoto, exponenciaram esse risco.

Em consequência, em Portugal assistiu-se a um aumento particular do registo de domínios da internet com termos associados à pandemia, como "coronavírus" ou "covid", com intenções maliciosas de envio de spam ou de ações de phishing.

Também os ataques de malware e ransomware tiveram um aumento considerável. Nos ataques de malware tem-se assistido ao aumento global da comunicação e informação relacionada com o vírus, com software malicioso embebido em mapas informativos da evolução da doença ou em emails maliciosos, que levam os utilizadores a carregar em links. Estes links descarregam, posteriormente, o malware para os computadores ou telemóveis dos seus utilizadores danificando os equipamentos ou recolhendo dados de forma ilícita. Os ataques de ransomware têm tido um maior foco nos setores que já se encontram sob pressão pela crise sanitária, como hospitais ou instituições públicas, e que não podem ver a sua atividade parar, tornando-se por isso nos alvos preferenciais dos atacantes. Neste tipo de ataque, um software ilícito torna "reféns" os dados do sistema infetado em troco de um resgate, tipicamente, em cripto moedas.

CW - A Everis não sendo fabricante de soluções de cibersegurança, quais os fabricantes com que trabalha e como os escolhe?

MA - Conjugamos o nosso conhecimento de segurança de informação, e ciber segurança, com os produtos líderes do mercado para criar soluções personalizadas e adaptadas à cultura organizacional e nível de maturidade dos nossos clientes. Para o efeito, estabelecemos sólidas parcerias com os principais fabricantes de soluções de cibersegurança nas nossas áreas de aposta, como é o caso da Sailpoint e da Microsoft.

Com a Sailpoint, líder no quadrante mágico da Gartner para governo e gestão de identidades, trabalhamos na área de IAM com soluções on-premises ou na cloud, pois acreditamos

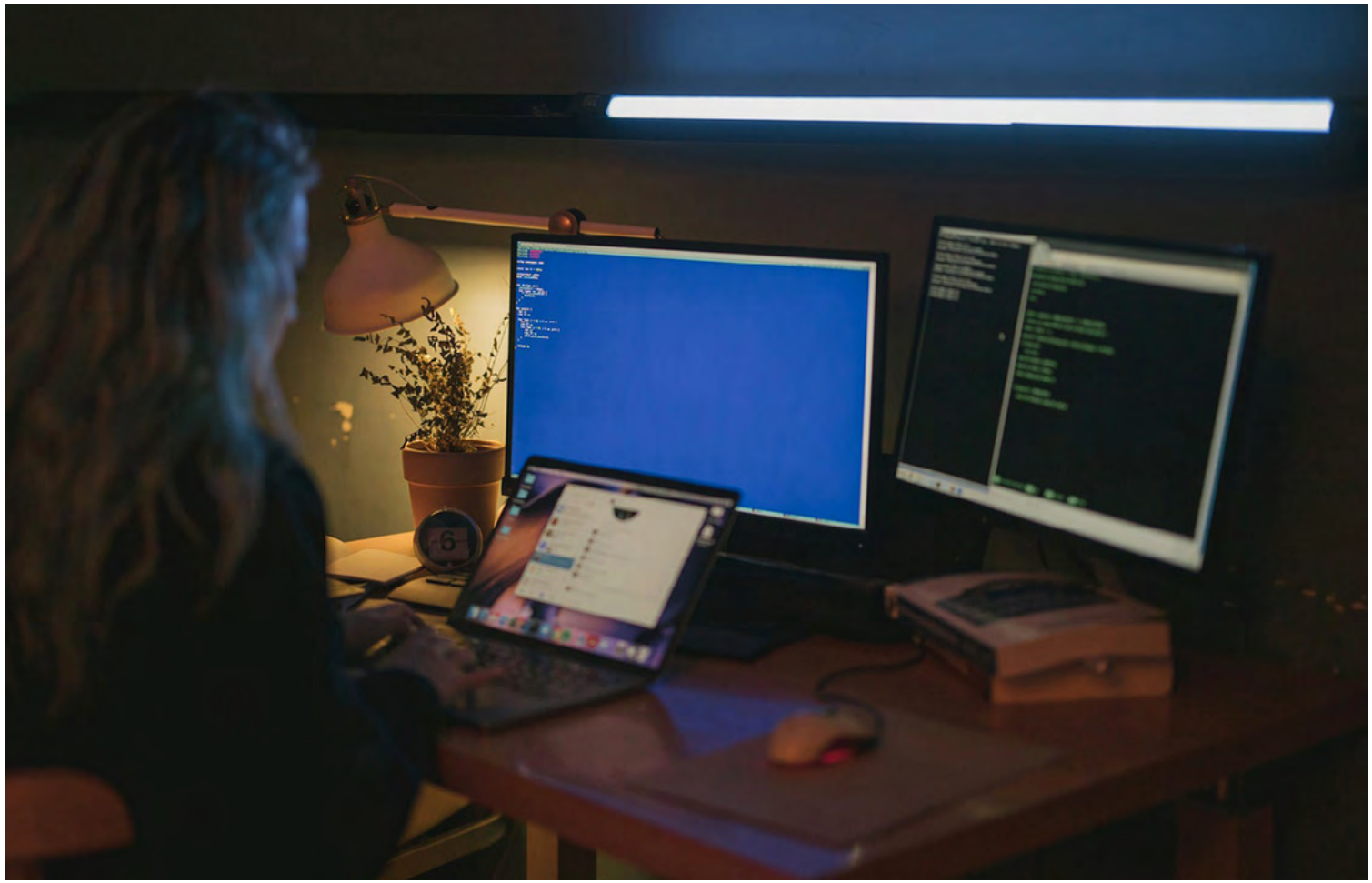
que para se ser bem-sucedido na implementação de uma estratégia, ou modelo, Zero Trust, as organizações devem ter a segurança centrada na identidade. Isto implica ter uma estratégia sólida de governo e gestão de identidades que inclua os necessários controlos de perfis e permissões, correta definição de políticas de atribuição de acessos, mecanismos automáticos e de self-service no aprovisionamento de utilizadores e um elevado nível de auditing e reporting.

Somos parceiros Gold da Microsoft para a área da segurança, o que nos permite um posicionamento estratégico na implementação e integração de soluções de segurança e compliance, complementando a oferta e know-how da everis com a tecnologia que a Microsoft Security oferece. Estamos a trabalhar com a Microsoft, junto dos nossos clientes, no desenvolvimento de soluções de gestão de acessos, gestão de vulnerabilidades, proteção e classificação de informação, suportadas em produtos que posicionaram a Microsoft como líder em 5 quadrantes mágicos de Gartner.

CW - No que diz respeito à defesa dos organismos do estado tem havido investimento e cuidado na proteção ou ainda há um longo caminho a percorrer?

MA - O trabalho realizado por entidades governamentais, como o Gabinete Nacional de Segurança, em particular o Centro Nacional de Cibersegurança, tem sido fundamental na promoção de uma cultura de segurança e no apoio aos organismos do Estado e operadores de infraestruturas críticas, quer na sensibilização e consciencialização para a segurança de informação, quer no aumento da sua resiliência a ciber ataques.

O Estado gere milhões de dados dos cidadãos, informação critica



dos múltiplos setores como a saúde, educação ou finanças. Além disso, hoje e cada vez mais, temos muitos serviços fundamentais para o funcionamento do país, e ao serviço do cidadão, suportados em sistemas informáticos. A responsabilidade para com a segurança de informação, e cibersegurança, dos organismos do Estado é ainda maior pela quantidade e criticidade dos dados que são tratados e armazenados.

Na verdade, ainda há um caminho a percorrer que não é específico dos organismos do Estado, mas transversal à sociedade e resultado da economia digital em que vivemos. A constante evolução tecnológica, um time to market cada vez mais reduzido e a pressão a que as empresas estão sujeitas para dar resposta às necessidades dos seus clientes, colaboradores e parceiros, em constante mudança, fragiliza-as e torna-as mais expostas a ciber ataques que, por sua vez, se tornam também cada vez mais rentáveis para os atacantes.

Tirar partido das novas tecnologias para dar confiança aos stakeholders e aos mercados, é fundamental para ajudar as organizações a liderar e inovar. Neste contexto, permanecer ciberresiliente e construir a confiança sustentada nas práticas de privacidade e segurança de informação das organizações, quer privadas, quer do Estado, é um imperativo estratégico. CW

Os clientes Everis têm procurado a consultora para fazer face às seguintes áreas específicas

Soluções de IAM

Análises de ciber risco, com especial foco na análise de risco de fornecedores, e implementação de soluções ou controlos de segurança ao nível dos canais digitais.

Uma resposta ao aumento da complexidade do parque tecnológico das organizações e à dificuldade que estas têm em gerir um crescente número de colaboradores internos e externos, parceiros, clientes e aplicações. Existe por isso um interesse crescente na procura por soluções que permitam gerir de forma eficiente estas identidades e controlar eficazmente os seus acessos. A everis tem apoiado os seus clientes na implementação destas soluções, com respetivas revisões das políticas de acesso, criando mecanismos automáticos que permitem às empresas simplificarem a experiência de utilização por parte dos seus colaboradores, parceiros e clientes, e diminuírem os riscos de segurança de informação.

Serviços de avaliação de risco de fornecedores

Estas avaliações permitem às organizações identificarem eventuais lacunas nos processos, procedimentos ou controlos internos dos seus fornecedores, potenciais ou atuais, e que representam um risco para a organização que os contrata. Na maioria das empresas este processo é ainda inexistente ou pouco eficiente e eficaz, representado um esforço acrescido para as áreas de compras. a everis trabalha num serviço de avaliação de ciber risco de fornecedores, baseado em modelos cognitivos, que integra fontes de informação, internas ou externas à organização, e permite aferir um nível de risco com elevados níveis de automatismos e reporting. A implementação deste tipo de soluções permite às organizações reduzir a sua exposição a ciberataques, que surjam da exploração de vulnerabilidades nos seus fornecedores críticos.

Implementação de controlos de segurança

Mecanismos de identificação, autenticação e controlo de canais que garantam um equilíbrio entre a experiência para os clientes finais e a segurança. Esta necessidade surge do maior volume de utilização dos canais digitais que se tem verificado como resultado da pandemia. Um caso interessante no qual a everis está a trabalhar é a utilização de mecanismos de identificação por biometria de voz para call centers e assistentes virtuais. Estes mecanismos de biometria de voz permitem identificar univocamente o cliente final, prevenindo ataques de man in the middle onde alguém mal-intencionado consegue, junto do call center, fazer-se passar pelo cliente e reunir um conjunto de informação que lhe permite mais tarde utilizar, de forma ilícita, os serviços ou aceder a dados confidenciais. Esta solução tem uma aplicabilidade direta em múltiplos setores, como por exemplo nos canais do setor bancário e de crédito ao consumo, impedindo este tipo de ataque e consequentes fraudes financeiras.

“As soluções de segurança mais solicitadas pelas empresas são as que permitam um acesso seguro às infraestruturas das organizações”

“Tem havido investimento e podemos ver pela própria atividade do centro nacional de cibersegurança, que tem sido muito proativo na deteção, apoio e divulgação dos diversos ataques que o nosso país e as nossas organizações têm sido alvo”.

Entrevista a Rui Duro, Country Manager da CheckPoint

Rui Duro, Country Manager - Portugal da Check Point

CW - Qual a importância da cibersegurança na transformação digital?
RD - Transformação Digital não pode ser feita sem ter em conta a cibersegurança. Tal como a reengenharia de processos, a adoção de novas tecnologias e reeducação das equipas para os novos métodos e processos de trabalho baseados na transformação digital das organizações, é de todo relevante ter em conta que estaremos sempre a trabalhar com dados e com informação quer da organização, quer dos seus clientes, e por isso teremos de estabelecer políticas de segurança conformes com a necessidade de proteção dos dados e dos acesso aos mesmos. Nenhum CISO, CTO pode planear um processo de transformação digital sem ter em conta a componente de segurança, pois esta é tão importante quanto dar acesso a ferramentas utilitárias de trabalho aos colaboradores.

CW - Passada a fase do susto e ainda com muitas incertezas ao nível da continuidade de alguns negócios tendo em conta a crise económica que aí vem, qual é o espaço da cibersegurança nas propriedades dos empresários portugueses?
RD - Com esta pandemia e crise, tornou-se mais claro junto dos empresários e gestores nacionais que é de todo relevante não só permitir o acesso de qualquer parte às ferramentas corporativas, como assegurar que estes acesso são efetuados em segurança. Temos visto um maior investimento nesta área e acreditamos que poderá ser reforçada cada vez mais.

CW - A segurança ainda é um entrave para a decisão de migrar para a Cloud?
RD - Podem existir ainda alguns medos, mas diferentes daqueles que existiam há 5, 10 ou 20 anos atrás. O medo já não se centra no "onde estão os meus dados", para passar a ser "como e quem é que consegue aceder aos meus dados".

É de todo importante não nos esquecermos que ao decidir-se utilizar uma solução cloud, não passamos todo o ónus de segurança para o fornecedor Cloud. É importante que os gestores compreendam que as plataformas de CLoud asseguram a segurança das infraestruturas, mas não dos dados em si, pois isso é algo que as organizações terão de manter sobre a sua responsabilidade com os acessos criados e sua tipologia de perfis de acesso. Na Cloud a Segurança é uma responsabilidade partilhada entre fornecedor e cliente.

CW - A Cloud é a base da transformação digital, quais as soluções mais procuradas?
RD - A Cloud é um forte motor de transformação digital que tem visto nas soluções de produtividade o maior valor de atração para as organizações, como é o caso das soluções Microsoft.

"A Cloud é um forte motor de transformação digital que tem visto nas soluções de produtividade o maior valor de atração para as organizações, como é o caso das soluções Microsoft".

CW - Quais as soluções mais solicitadas pelas empresas nesta fase?
RD - Nesta fase as soluções de segurança mais solicitadas pelas empresas são as que permitam um acesso seguro às infraestruturas das organizações, como é o caso das VPNs.

CW - Quais os principais riscos que as empresas nacionais correm no presente?
RD - As empresas nacionais ainda se mantém num estado muito rudimentar no que toca a segurança. Na sua maioria, continuam a proteger-se somente com soluções de anti-virus e noutros casos com firewalls. A não adoção de verdadeiras soluções de segurança que protejam todo o ecossistema das suas infraestruturas, e soluções híbridas que têm vindo a ser adotadas, criam enormes pontos cegos de segurança e que permitem aos ciberdelinquentes poder explorar com maior facilidade essas mesmas brechas.

CW - Quais os principais ataques que as empresas são alvo neste momento?
RD - Neste momento falamos de malware via campanhas de mail-spam. A engenharia social continua a ser o mais eficaz de todos os tipos de ataque, pois explora o ponto mais fraco em qualquer organização, mesmo aquelas que têm as melhores soluções de segurança, que são os seus recursos humanos. A falha humana é fácil de suceder, quando se ataca com base em engenharia social.

CW - E o Estado português Estado preparado para ataques cibernéticos por parte de outros Estados e de cibercriminosos?
RD - Os ataques estado-nação é algo extremamente complexo e que é muito difícil de indicar que algum estado, incluindo os mais desenvolvidos e sofisticados a nível de cibersegurança, se encontra devidamente preparado. Os últimos grandes ataques deste tipo foram efetuados de forma cirúrgica e extremamente criativa. Recordo a aplicação de telemóvel criada na altura do mundial de futebol, que infetou um conjunto de telemóveis de soldados israelitas com o intuito de obter dados sobre as suas localizações e outros dados pessoais que permitissem um ataque mais musculado a infraestruturas de segurança. Portugal não está imune a este tipo de situações, o que podemos dizer é que existe uma forte consciencialização por parte das forças de segurança nacionais para este tema.

CW - Tem havido investimento quer financeiro, quer estratégico, da parte do Estado portugues para se proteger do cibercrime?
RD - Tem havido investimento e podemos ver pela própria atividade do centro nacional de cibersegurança, que tem sido muito proativo na deteção, apoio e divulgação dos diversos ataques que o nosso país e as nossas organizações têm sido alvo. CW

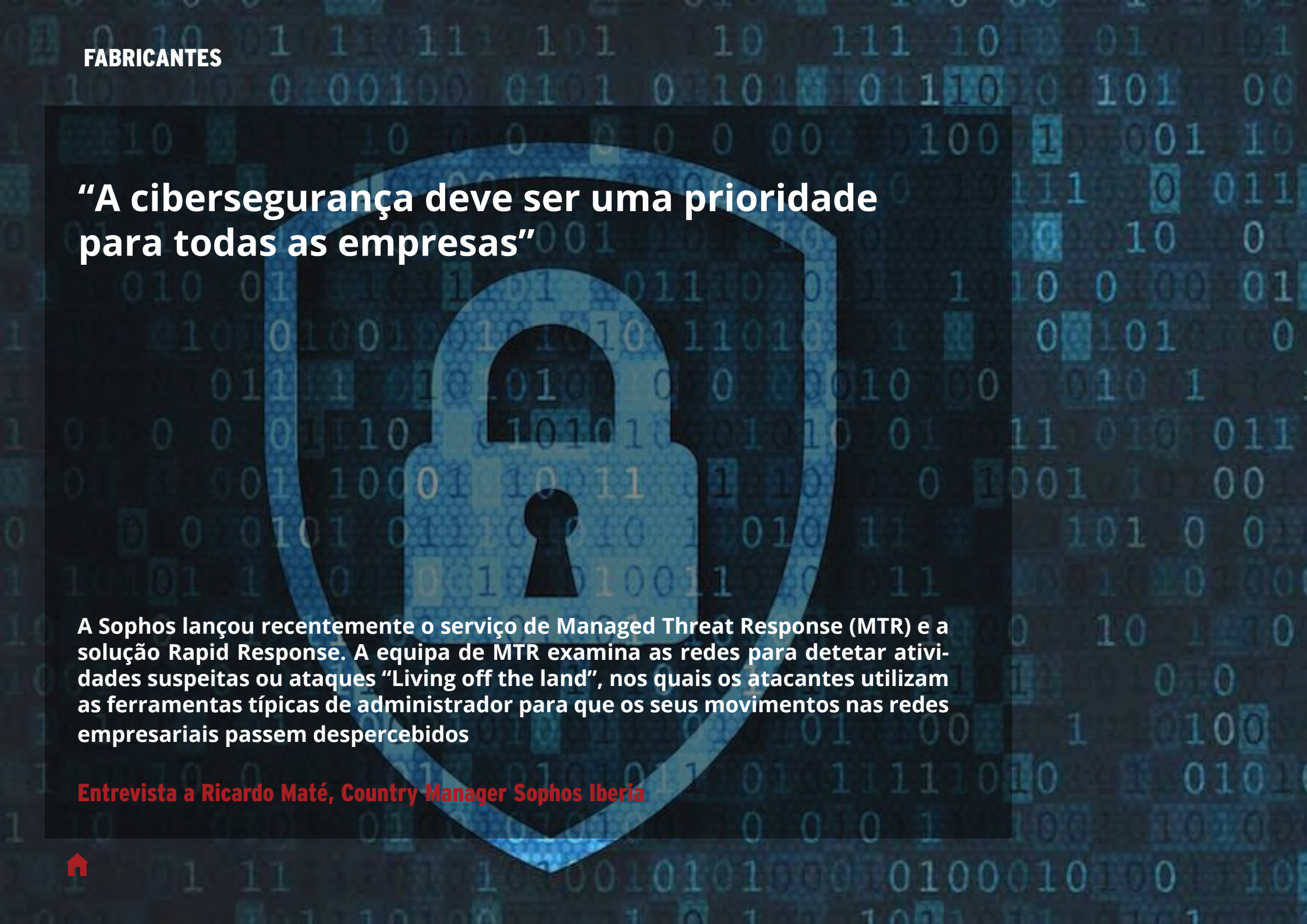
As soluções mais procuradas pelos clientes Check Point

Refresh das soluções de suporte a VPN para trabalho remoto
Solução para fornecer aos utilizadores um acesso seguro e contínuo às redes e recursos empresariais e corporativos quando se encontrar a trabalhar remotamente. A privacidade e integridade da informação sensível é assegurada através da autenticação de múltiplos fatores, verificação de conformidade do sistema de endpoints e via criptografia de todos os dados transmitidos.

Soluções para proteção de EndPoint e dispositivos (Beyond the Perimeter)
Solução para equipar todos os utilizadores com um acesso seguro através de qualquer dispositivo que utilizem para aceder à informação empresarial. Este acesso permite que os dados se mantenham sempre seguros através do seu envio encriptado, bem como ao verificar a permissão de cada dispositivo.

Soluções para proteção aplicações Cloud SaaS
As soluções Cloud Access Security Broker (CASB) fornecem proteção limitada. O Check Point CloudGuard SaaS protege os dados corporativos ao prevenir ataques objetivados em aplicativos SaaS em e-mail com base na nuvem.

“A cibersegurança deve ser uma prioridade para todas as empresas”



A Sophos lançou recentemente o serviço de Managed Threat Response (MTR) e a solução Rapid Response. A equipa de MTR examina as redes para detetar atividades suspeitas ou ataques “Living off the land”, nos quais os atacantes utilizam as ferramentas típicas de administrador para que os seus movimentos nas redes empresariais passem despercebidos

Entrevista a Ricardo Maté, Country Manager Sophos Iberia

Ricardo Maté, Country Manager Sophos Iberia

CW - Qual a importância da cibersegurança na transformação digital?
RM - A transformação digital converteu os utilizadores no coração das nossas redes de TI. Antes, as empresas construíam as suas redes e sistemas ao redor de um Data Center mas, com a proliferação da transformação digital e um ecossistema baseado em aplicações Cloud, o núcleo foi transferido para o posto de trabalho (endpoint), tendo os utilizadores como pontos finais, bem como os dados a que estes acedem e gerem. Cada utilizador comporta um risco e a ameaça do phishing, ou de um utilizador se tornar um vetor de ataque contra uma empresa, é mais real do que nunca.

CW - O pós-covid ainda tem muitas incertezas ao nível da continuidade de alguns negócios tendo em conta a crise económica que aí vem, qual é o espaço da cibersegurança nas prioridades dos empresários portugueses?
RM - A cibersegurança deve ser uma prioridade para todas as empresas, independentemente da sua dimensão ou setor. A crise de COVID-19 não fez mais que aumentar os riscos, o número e a intensidade dos ciberataques. A cibercriminalidade é um negócio muito rentável que pode destruir as empresas, e por isso é algo que não só não vai parar, como veremos ainda mais ataques e estes serão mais prejudiciais, solicitando resgates milionários mesmo a empresas de média dimensão.

CW - A segurança ainda é um entrave para a decisão de migrar para a Cloud?
RM - Desde o início da crise de COVID-19, as pessoas e os locais de trabalho começaram uma transição rápida e sem precedentes que continua até ao dia de hoje. É muito provável que a forma como trabalhamos, vamos à escola, assistimos a eventos e conferências e nos divertimos tenha mudado para sempre. A informática na Cloud é uma parte fundamental desta evolução veloz, mas apresenta um grande número de desafios. Permissões de acesso excessivas, visibilidade limitada sobre os recursos e ativos na Cloud e a falta de auditoria podem contribuir para criar ambientes Cloud mais vulneráveis a ciberameaças, e o malware é tão prejudicial na Cloud como em qualquer outro local. Além disso, muitas equipas que estão em trabalho remoto a partir de diversas localizações sofreram ataques, por exemplo, de ransomware, em que os cibercriminosos bloquearam a infraestrutura na Cloud da mesma forma que atacaram os dispositivos físicos... No final de contas, o ransomware pode encriptar um disco rígido ou um armazém virtual de objetos com a mesma facilidade do que um armazém físico. As empresas cuja infraestrutura na Cloud sofre um ataque de ransomware podem ter de enfrentar não só a fatura dos ciclos consumidos pela encriptação de dados, mas também um resgate ou um pagamento para que os seus dados não sejam publicados. Não obstante, as empresas de cibersegurança como a Sophos podem ajudar as empresas na sua transição para a Cloud pública, protegendo os acessos e os servidores implementados e verificando se a sua postura de segurança e de conformidade são adequadas.

CW - A Cloud é a base da transformação digital, quais as soluções mais procuradas?
RM - Conscientes de que as TI estão a migrar para a Cloud, a Sophos foi um dos primeiros grandes fornecedores a falar sobre CSWP (Certified Wireless Security Professional) e CSPM (Cloud Security Posture Management), graças tanto ao agente para servidores como ao Cloud Optix. Este realiza uma auditoria aos recursos que temos sobre fornecedores públicos da Cloud como AWS, Azure ou Google Cloud, bem como Kubernetes, tanto em qualquer um destes ambientes como outros locais. Adicionalmente, a Sophos proporciona as suas Firewalls de próxima geração, XG Firewall, para proteger a infraestrutura implementada nas Clouds públicas acima mencionadas, bem como a solução de Endpoint Detection & Response, o Intercept X EDR, para a proteção, deteção e resposta a ameaças nos servidores físicos ou virtuais implementados.

CW - Quais as soluções mais solicitadas pelas empresas na fase da pandemia?
RM - Hoje em dia, muitas empresas estão a fazer perguntas críticas sobre a sua segurança: se estão suficientemente protegidas, se têm planos de continuidade de negócio para poderem seguir em frente no caso de um ciberataque, ou mesmo a pensar e a testar os seus equipamentos de segurança para recuperar após um ataque. A cibersegurança entrou em pleno nas prioridades das empresas e, se sempre tinha sido um assunto crítico, agora é-o mais do que nunca e muitas empresas já estão conscientes disso. Lamentavelmente, a vulnerabilidade empresarial continuará a ser um risco para muitas empresas, já que os cibercriminosos não deixam de aperfeiçoar e sofisticar as suas táticas para se adaptarem e contornarem as medidas de segurança das empresas. É por isso que as empresas devem investir desde já em segurança avançada para se protegerem no futuro. A cibersegurança converteu-se num desporto interativo no qual as soluções tradicionais já não funcionam. As empresas já não podem atuar como meros espectadores e esperar que as suas defesas funcionem; devem contar com equipas de Threat Hunting e tecnologias de última geração que lhes permitam procurar proativamente as ameaças e manter-se realmente protegidas.

A Sophos lançou recentemente o serviço de Managed Threat Response (MTR) e a solução Rapid Response. A nossa equipa de MTR examina as redes para detetar atividades suspeitas ou ataques "Living off the land", nos quais os atacantes utilizam as ferramentas típicas de administrador para que os seus movimentos nas redes empresariais passem despercebidos. Para localizar este tipo de ataques é necessário contar com especialistas em deteção e resposta de endpoint (EDR) ou equipas de MTR humanas. Com o Rapid Response, proporcionamos às empresas uma equipa de respostas a incidentes, caçadores de ameaças e analistas, que trabalham 24 horas por dia para deter rapidamente os ataques avançados enquanto estão a ocorrer, bem como eliminar os cibercriminosos das redes empresariais.

Outras das áreas que está a ter grande procura são as soluções de acesso remoto baseadas em ZTNA (Zero Trust Network Access), já que o teletrabalho se converteu na forma de trabalhar para a grande maioria das empresas e Administrações Públicas, e as VPN começam a não ser a solução adequada – porque os utilizadores não só devem ligar-se a aplicações corporativas, mas também a dezenas de aplicações, muitas delas localizadas em fornecedores de serviços externos ou na Cloud.

CW - Quais os principais riscos que as empresas nacionais correm no presente?
RM - As empresas portuguesas estão expostas aos mesmos riscos que o resto dos países do ocidente. O aumento dos ataques de ransomware direcionados, com roubo de informação e sua subsequente encriptação e pedidos de resgate muito elevados, continuam a ser uma das principais ameaças para todas as empresas. O aumento do phishing como porta de entrada para estes ataques, bem como esquemas dirigidos por spear-phishing, continuam também a ser uma outra área de muita preocupação. Assim, a consciencialização dos utilizadores deve ser uma das prioridades para as empresas.

CW - E o Estado português está preparado para ciberataques por parte de outros Estados e de cibercriminosos?
RM - O Centro Nacional de Cibersegurança (CNCS) é o principal responsável por garantir que tanto os utilizadores como as empresas e a Administração Pública têm um acesso seguro e fiável ao ciberespaço, bem como por garantir a cibersegurança nacional. As Administrações Públicas em Portugal estão preparadas para os ciberataques, embora vejamos que as Câmaras Municipais e as Universidades devem fazer um esforço importante para atualizar as suas componentes de Cibersegurança para enfrentar melhor as atuais ameaças. CW

“A cibersegurança é a chave do desenvolvimento de uma estratégia de transformação digital de sucesso nas empresas”

O impacto financeiro, político e reputacional causados pelos ciberataques tem vindo a aumentar velozmente, o que veio a intensificar as preocupações com a segurança por parte dos consumidores particulares e das empresas em Portugal.

Entrevista a Carlos Vieira, Country Manager Espanha e Portugal, da WatchGuard

Carlos Vieira, Country Manager Espanha e Portugal, da WatchGuard

CW - Qual a importância da cibersegurança na transformação digital?

CV - Eu diria que a cibersegurança é a chave do desenvolvimento de uma estratégia de transformação digital de sucesso nas empresas. Hoje em dia, as empresas estão totalmente interligadas e procuram processos simples e produtos e serviços cada vez mais fáceis de usar, mais rápidos e intuitivos. Mas esta agilização de processos, movidos pela necessidade de um acesso imediato e direto, aumenta significativamente os riscos de segurança das organizações.

Com o intuito de proporcionar uma experiência de cliente de excelência, num mundo em constante transformação, a cibersegurança terá de ser forçosamente um elemento chave no desenho e gestão de produtos, serviços e plataformas.

Sugiro a todas as escolas de gestão que coloquem nos seus currículos, se ainda não o fizeram, módulos a explicar o que é cibersegurança, porque muitos gestores não têm a mais pequena sensibilidade para esta problemática e muitas empresas, seis meses depois de sofrer um ciberataque, simplesmente fecham. Começa a existir um aumento da sensibilização, mas continua a haver um longo caminho a percorrer.

CW - O pós-covid ainda tem muitas incertezas ao nível da continuidade de alguns negócios tendo em conta a crise económica que aí vem, qual é o espaço da cibersegurança nas prioridades dos empresários portugueses?

CV - As empresas são um dos alvos dos cibercriminosos e muitas delas acabam mesmo por sofrer sérios danos na sua reputação depois de um ataque, sendo que esta consequência é muitas vezes mais difícil e morosa de reparar do que uma perda económica direta.

Entre os riscos mais frequentes e danosos estão ataques de dia zero, campanhas de phishing e ransomware. Para minimizar os efeitos, o obviamente recomendável em qualquer situação é ter em conta a segurança desde o início de qualquer desenvolvimento e implementação. As empresas tendem a investir mais na prevenção de falhas e menos em estratégias desenhadas para detetar e antever futuros ataques.

É, por isso, essencial prevenir, detetar e responder a qualquer tipo de ciberameaças, bem como consciencializar os recursos humanos para as principais ameaças à segurança que podem afetá-los, especialmente quando estão fora do perímetro da rede da empresa, preservando a sua produtividade ao mesmo tempo.

A segurança deve estar presente como elemento fundamental desde o início e deve ser entendida como um processo – não um estado imóvel.

CW - A segurança ainda é um entrave para a decisão de migrar para a Cloud?

CV - A verdade é que apesar de todas as vantagens que a cloud traz para as empresas, as dúvidas acerca da sua segurança ainda são um entrave para as organizações fazerem essa transição.

À medida que empresas de todos os tamanhos e sectores de atividade migram as suas aplicações e dados para a cloud, esta começa a tornar-se na única forma de acesso à sua informação mais importante. É por isso que acreditamos que este porto seguro se desmorone com o ransomware a apontar as suas baterias aos ativos que lá moram e é também por isso que se torna mais fundamental do que nunca que os fornecedores de serviços cloud garantam a segurança integral dos ativos que alojam.

CW - A Cloud é a base da transformação digital, quais as soluções mais procuradas?

CV - Todas as que garantirem a continuidade do negócio e a manutenção da produtividade, mesmo em cenários tão atípicos e adversos como o que estamos a viver com esta pandemia.

Ou seja, ferramentas que permitam aceder aos dados e aplicações de uma forma imediata, sem perda de tempo, mas sobretudo de uma forma segura, de maneira que esse acesso facilitado às forças de

trabalho distribuídas não constitua, paralelamente, uma porta de entrada a hackers.

E é esse apelo que faço às empresas que estão – e bem – a agilizar a sua atividade com recurso à cloud: de nada adianta fazê-lo, é até contraproducente, se depois toda essa agilidade e continuidade do negócio se perder por uma estratégia de cibersegurança deficiente.

CW - Quais as soluções mais solicitadas pelas empresas na fase da pandemia?

CV - O impacto financeiro, político e reputacional causados pelos ciberataques tem vindo a aumentar velozmente, o que veio a intensificar as preocupações com a segurança por parte dos consumidores particulares e das empresas em Portugal. Há, por isso, um aumento da procura - quer global, quer no nosso país – de proteção avançada de EDR para endpoint, dispositivos móveis e ligações de rede. Além disso, com o objetivo de proteger o utilizador final, muitas vezes apontado como o elo mais fraco no que se refere à segurança das empresas, começamos também a assistir à procura por soluções de autenticação multifatorial.

CW - Quais os principais riscos que as empresas nacionais correm no presente?

CV - Como muitos especialistas têm vindo a sublinhar, o trabalho remoto veio para ficar, pelo que os hackers vão continuar a explorar no próximo ano o cenário das empresas distribuídas para ter sucesso nos seus ataques de phishing. Desta forma, tal como em 2020, as empresas que ainda não o fizeram vão a ter a necessidade de estabelecer uma política de zero-trust com soluções que as protejam dos diversos vetores de ataque, pelo que terão igualmente que recorrer a empresas especializadas, particularmente MSSP, principalmente as que não contam com recursos próprios de TI.

CW - Está o Estado português Estado preparado para ataques cibernéticos por parte de outros Estados e de cibercriminosos?

CV - É um facto que o cenário de pandemia fez disparar os casos de ransomware e outros ciberataques a empresas e a infraestruturas críticas, algumas estatais. Temos visto inclusivamente isso a acontecer no nosso país e a organizações que, pela sua dimensão, não julgaríamos ser possível que se tornassem vítimas destes ataques.

A verdade é que, com Covid-19 ou sem ele, o cibercrime se tornou um negócio extremamente lucrativo, havendo aumento do investimento dos grupos criminosos para o desenvolvimento de novas formas de ataque. As organizações têm de continuar a reforçar a sua cibersegurança para estarem cada vez menos vulneráveis ao cibercrime.

> "As empresas são um dos alvos dos cibercriminosos e muitas delas acabam mesmo por sofrer sérios danos na sua reputação depois de um ataque, sendo que esta consequência é muitas vezes mais difícil e morosa de reparar do que uma perda económica direta".

CW - Tem havido investimento quer financeiro, quer estratégico, da parte do Estado português para se proteger do cibercrime?

CV - Existe da parte das organizações estatais, principalmente no que respeita à administração central, uma maior consciencialização da necessidade de se proteger contra o cibercrime e temos visto algum investimento, ainda que tímido, neste domínio.

Quando falamos de administração local, este investimento varia não só de acordo com os orçamentos disponíveis, mas também com o grau de especialização e consciencialização dos responsáveis pela gestão dos parques informáticos. Todos temos de perceber que o cibercrime utiliza técnicas cada vez mais avançadas e que as estratégias de segurança devem acompanhar essa mesma evolução. As soluções de segurança utilizadas há 10 anos já não são suficientes para responder a este avanço tecnológico, pelo menos quando utilizadas de forma isolada. As organizações estatais, mas não só, tem de começar a pensar a cibersegurança como um todo, protegendo diversos vetores, sensibilizando recursos humanos e definindo não só políticas de proteção, mas também de mitigação de riscos perante um ciberataque.

Portugal continua a ser, segundo um estudo publicado no site do Gabinete de Estratégia e Estudos do Ministério da Economia, um dos países europeus com menor volume de investimento em cibersegurança. Este cenário é preocupante quando, de acordo com o mesmo estudo, somos um dos países europeus mais vulneráveis ao cibercrime. CW

Recreio TIC

Uma reflexão sobre o compromisso da educação com a sociedade digital

João Miguel Mesquita

Paulo Lopes

COMPUTERWORLD
FROM IDG

[PODCAST]

PARA OUVIR EM COMPUTERWORLD.COM.PT/TECHTALK

A Cibersegurança faz parte do processo

Ricardo Neves, Marketing Manager na WhiteHat

É necessário garantir que pessoas e empresas estão seguras no uso da tecnologia e que conseguem desempenhar cada vez melhor todas as suas atividades, contribuindo para um processo de transformação digital consistente, com a máxima confidencialidade e a segurança da informação.

A verdade é que os consumidores e as empresas vão estar cada vez mais expostos a riscos face a uma maior dependência da tecnologia e à constante transformação dos processos digitais. O volume e a diversidade das ciberameaças será cada vez maior e a adoção de medidas e tecnologia de segurança serão determinantes para um crescimento seguro e sustentável.

Em Portugal, um mercado essencialmente composto por pequenas e médias empresas, é crucial que as organizações procurem profissionais especializados e soluções tecnológicas adequadas às suas necessidades. É facto que muitos gestores não dão prioridade à segurança e a falta de medidas cria custos enormes às organizações.

A visibilidade que temos através de indicadores fornecidos pelos nossos parceiros e clientes é que neste segmento empresarial, domina também a escassez de acompanhamento focado em Cibersegurança e a tecnologia adotada não é suficiente ou é incorretamente implementada. Um problema, sobretudo em tempos de elevado risco.

O recente relatório Anual de Segurança Interna 2020 (RASI) demonstra que o CERT.PT (serviço integrante do Centro Nacional de Cibersegurança e que tem a responsabilidade de coordenar a resposta a incidentes no ciberespaço português) processou 6.525 notificações. Um número 90% superior ao ano transato (2019), tendo-se verificado um aumento nas tipologias de incidentes, nas classes de fraude, código malicioso, intrusão e segurança da informação. No que respeita aos ataques de phishing, registou-se um aumento na ordem dos 260%. De acordo com o relatório, os aumentos nos números devem-se ao incremento do teletrabalho e à consequente diluição da tradicional segurança de perímetro das organizações, tendo havido um claro aproveitamento da temática da COVID19 para a elaboração de diferentes tipos de ataques.

As empresas e os seus decisores devem estar cientes destes números e perceber que o risco é enorme e que devem desde logo considerar a Cibersegurança nos seus planos de negócios e de investimentos. É importante que as empresas garantam diversas medidas, entre as quais:

- Criar uma estratégia documentada e alinhada com o setor e processos de negócio da organização de forma a dar resposta aos potenciais riscos existentes;
- Ter recursos humanos com conhecimentos e qualificação na área de forma a garantir a segurança de todo o parque informático;
- Facultar formações internas regulares aos colaboradores. A sensibilização é uma ação determinante dado que o erro humano ainda é responsável por muitos dos ataques efetuados às organizações;
- Devem ser adquiridas soluções que mitiguem os diferentes vetores de ataque a que a organização está exposta. Para além das soluções de proteção anti-malware, a segurança de dados nos endpoints deve ser reforçada com tecnologia de encriptação e autenticação de dois fatores (2FA). Soluções como Unified Threat Management (UTM), Data Loss Prevention (DLP), Cloud Sanboxing e Backup e Disaster Recovery, entre outras, devem fazer parte da equação;
- Ter parceiros tecnológicos especializados que facultem o suporte necessário ao nível formação, escolha e implementação tecnológica é determinante para o sucesso da estratégia.

A WhiteHat tem como missão, enquanto distribuidora de tecnologia na área da cibersegurança, consciencializar todos os utilizadores para a importância da segurança. Queremos que o nosso canal de parceiros e mercado tenham acesso às melhores soluções tecnológicas, dando respostas eficazes. Na WhiteHat, desde 2003 que a Cibersegurança faz parte do "processo" e esperamos que todas as organizações façam o mesmo para garantirem um futuro seguro e sustentável.

A WhiteHat possui em portefólio as principais tecnologias de Cibersegurança a implementar em qualquer tipo de organizações, nomeadamente: Anti-malware, Anti-spam, segurança Microsoft 365, 2FA - Two-factor Authentication, Cloud Sandboxing, Encriptação, DLP - Data Loss Prevention, Backup e Disaster Recovery, SD-WAN, Balanceamento de Tráfego, UTM, entre outras. CW

CASO DE ESTUDO

Águas do Norte inicia implementação de um Security Operations Center

Trata-se de um projeto de cibersegurança encarado pela Águas do Norte como transversal, onde todas as áreas de negócio são clientes e altamente dependentes dos sistemas de informação, pelo que devem encarar os riscos de cibersegurança como algo inerente a uma realidade de negócio cada vez mais digital.

A avaliação de risco da cibersegurança nos últimos anos e a realização de alguns processos de auditoria, internas e externas, evidenciaram algumas oportunidades de melhoria neste domínio na Águas do Norte. Embora já fossem usadas algumas ferramentas de auditoria, a Águas do Norte teve ao longo dos últimos anos uma abordagem interna e muito pontual à cibersegurança. A falta de capacidade, tanto de conhecimento como de disponibilidade das equipas internas, para a cibersegurança, tanto a nível técnico como processual, acabou por concluir que era necessário endereçar a esta área um maior foco e dedicação.

Por outro lado, a Águas do Norte foi identificada pelo Centro Nacional de Cibersegurança (CNCS) como um operador de serviço essencial no sector do fornecimento e distribuição de água potável, de acordo com a legislação em vigor.

Para atingir o nível de segurança compatível com o serviço que presta, a Águas do Norte candidatou-se ao programa Connecting Europe Facility – Telecom, para apoio ao desenvolvimento de capacidades operacionais na área da cibersegurança e implementação da Directiva SRI. Concluído este processo, foi aprovada a atribuição de um incentivo não reembolsável de 75% das despesas elegíveis, num projeto que se prevê ter um custo global de cerca de 300 mil euros.

Nesse sentido foi elaborado um plano de cibersegurança em água (WCSP), que visa proteger toda a rede e infraestrutura da Águas do Norte, a fim de garantir a continuidade dos serviços de abastecimento de água e de saneamento de águas residuais. Como resultado desta ação, a Águas do Norte iniciou um processo de implementação de ferramentas inteligentes para lidar com a maior parte da monitorização de eventos e resposta a incidentes, com tecnologia de autoaprendizagem incorporada, com capacidade de reconhecer padrões de eventos e bloqueios automáticos de ameaças.

Através deste plano de cibersegurança, a Águas do Norte pretende criar um Centro de Operações de Segurança (SOC) com base nas plataformas SIEM (Security Information and Event Management) e inteligência cibernética artificial (AI). O Objetivo é que o sistema consiga brevemente monitorizar todo o ecossistema, identificando e adaptando-se continuamente às ameaças cibernéticas mais evoluídas, melhorando as capacidades técnicas e operacionais da Águas do Norte. A vantagem de recorrer a um SOC com estas características é a possibilidade de monitorização ativa e

mais inteligente de todas as infraestruturas, mantendo a orientação dos sistemas de informação para os serviços que considera que podem trazer mais valor para o negócio. Além desta adoção estão a ser preparadas outras atividades internas que visam a realização de testes regulares, tanto técnicos como comportamentais, e também ações de sensibilização e formação dos utilizadores. O entendimento da Águas do Norte é que a abordagem à cibersegurança deve tentar ser holística.

A Águas do Norte pretende ainda que solução tenha a capacidade de fornecer informações relevantes para as partes interessadas em segurança cibernética, nacionais e internacionais. Consequentemente espera-se que a maturidade da segurança tecnológica da Águas do Norte aumente em coerência com a aposta estratégia que esta Concessionária do sistema multimunicipal de abastecimento de água e de saneamento do Norte de Portugal tem vindo a implementar no âmbito da digitalização dos serviços. Trata-se de um processo evolutivo de afinação que demorará vários meses.

Trata-se de um projeto de cibersegurança encarado pela Águas do Norte como transversal, onde todas as áreas de negócio são clientes e altamente dependentes dos sistemas de informação, pelo que devem encarar os riscos de cibersegurança como algo inerente a uma realidade de negócio cada vez mais digital. A Águas do Norte não encara a cibersegurança como uma corrida com uma meta a atingir, mas sim como um exercício continuo que faz com que esteja cada dia mais capaz. CW


WhiteHat
desde 2003
A sua ponte para a cibersegurança
Distribuição de soluções:
• Anti-malware
• Segurança de Perímetro
• Reforço de Autenticação
• Backup e Disaster Recovery
• Encriptação e Protecção de Dados
www.whitehat.pt
eset
untangle
Macriumsoftware
Your image is everything
peplink
Infrascale
safetica
XOPERO
WORKS, SO YOU CAN TOO!