JE editors

·TALKS·

Em direto através do site **www.jornaleconomico.pt**
ou em **www.facebook.com/JornalEconomico**

Conheça os riscos, a legislação e os desafios que a internet enfrenta nos dias de hoje. A cibersegurança do futuro analisada por especialistas e líderes na indústria. **Esperamos por si!**

Powered by: DXC.technology | FREGO | MDS Group | gmv

Este suplemento faz parte integrante do Jornal Económico Nº 2036 não pode ser vendido separadamente

9 abril 2020 | ESPECIAL

O Jornal Económico

ESPECIAL

CIBERSEGURANÇA & IOT

(INTERNET OF THINGS)

EMPRESAS INVESTEM EM PROGRAMAS À PROVA DE 'HACKERS'

Os ataques informáticos, como os de 'ransomware', acontecem a todos os minutos e estão na agenda de decisores políticos e empresariais. Os especialistas defendem uma estratégia de cibersegurança transversal, que envolva fabricantes de dispositivos, distribuidores de software e utilizadores. A proteção dos sistemas tem ainda impacto na oferta das seguradoras.

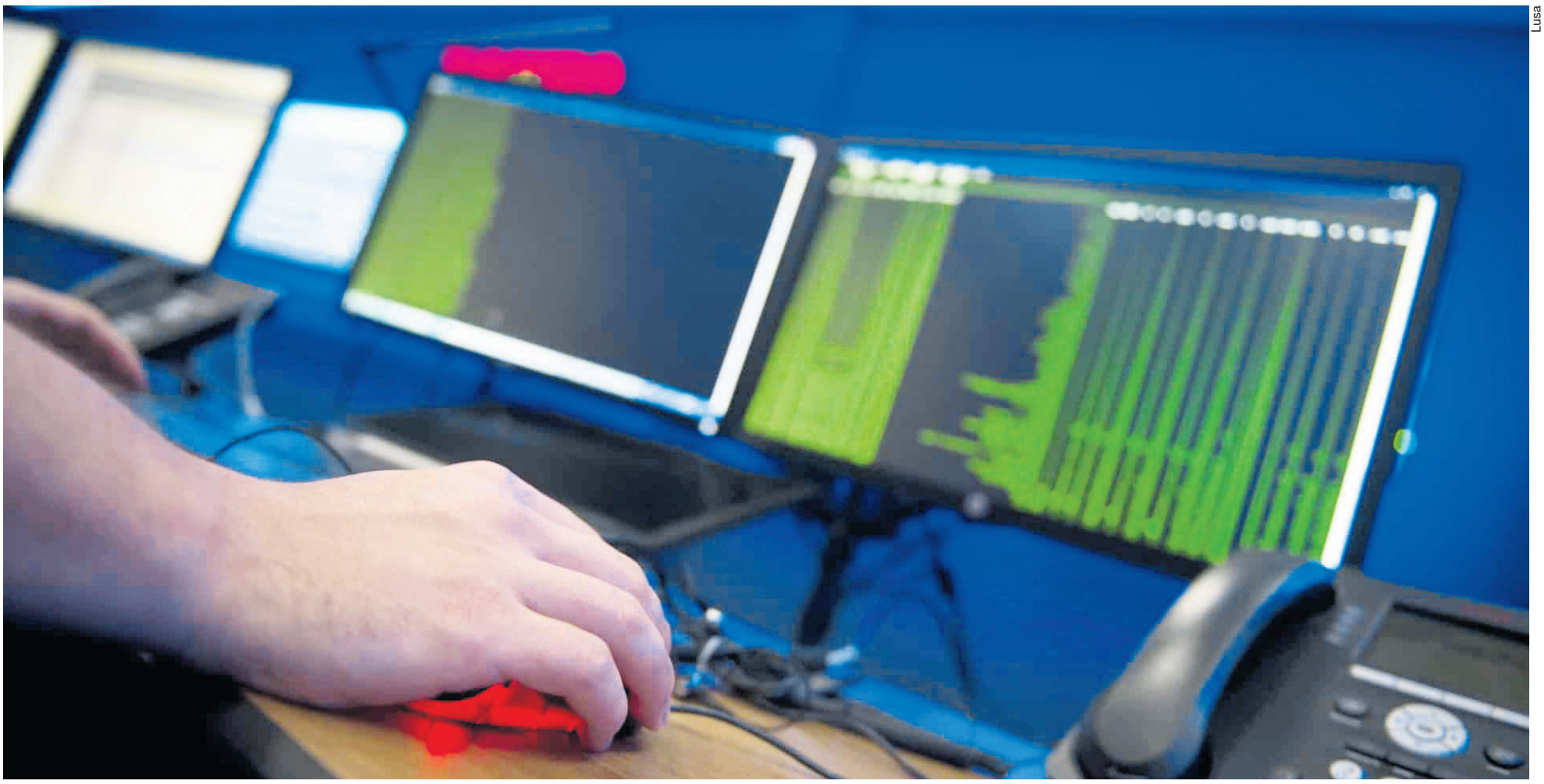
TECNOLOGIA
Internet das Coisas pressiona gestores a avaliar novos riscos ● II

ESTRATÉGIA
Gestão do risco cibernético deve ser transversal ● III

SOFTWARE
O que deve a sua empresa fazer em caso de 'ransomware'? ● IV

ORGANIZAÇÃO
Empresas compram seguros para proteger sistemas ● V

FÓRUM
Que exigências e despesas com cibersegurança trouxe o teletrabalho? ● VI



Lusa

TECNOLOGIA

Internet das Coisas pressiona gestores a avaliar novos riscos

João Madeira, partner da KPMG, lamenta que existam que normativos que orientam e estipulam regras de segurança para as tecnologias industriais apenas para determinados setores, como o automóvel.

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt

As empresas, os consumidores e os equipamentos tecnológicos vão estar cada vez mais conectados, nesta era da Quarta Revolução Industrial – ou Indústria 4.0. As previsões da consultora Bain & Company apontam para que o mercado da Internet das Coisas (IoT) valorize para os 520 mil milhões de dólares (cerca de 479 mil milhões de euros) já no próximo ano e os analistas da IDC antecipam que a despesa mundial com estas tecnologias chegue aos 1,2 biliões de dólares em 2022 (na ordem de 1,1 biliões de euros). Na prática, significa que os chamados "aparelhos inteligentes" vão tornar (ainda mais) casas e organizações também inteligentes, através de sensores, robótica/automação, assistentes virtuais, entre outros.

É neste contexto que as preocupações com a cibersegurança se tornam particularmente relevantes. Segundo Manuel Coelho Dias, especialista da Marsh Portugal, os grandes riscos prendem-se com a interconectividade das cadeias de distribuição. "Passam a estar verticalmente e horizontalmente integradas, ampliando os potenciais danos de um ato malicioso. Os sistemas isolados deixam de existir e a segregação é mais difícil", explica ao Jornal Económico (JE). O porta-voz da gestora de risco Marsh destaca até o facto de a agenda política também estar a ser marcada pela proteção dos sistemas informáticos. "Por parte das instituições governamentais dedicadas aos temas da segurança digital há já vários fóruns que tentam compilar as preocupações em relação a soluções tecnológicas já conhecidas, mas também face a todas as outras que se irão desenvolver, fruto nas novas possibilidades técnicas", realça Manuel Coelho Dias. Na sua opinião, há algum trabalho a fazer o levantamento detalhado destes riscos, mas mesmo qualquer prognóstico tem os seus limites.

Ademais, permanecem limitações orçamentais com as quais os CTO (Chief Technology Officer) se deparam, o que compromete a robustez e a segurança das redes.

'Chief Technology Officers' defendem mais regulação a nível europeu e maior investimento na análise e avaliação dos perigos informáticos

"No mercado atual, o principal fator é a redução de custo, fruto da integração de componentes eletrónicos e de código o mais baratos possível. Há pequenos fabricantes que muitas vezes compram tudo já feito, resultando em produtos que são autênticas mantas de retalhos, com inúmeros problemas de fiabilidade do software. O seu baixo custo também acaba por criar baixas expectativas nos compradores, que aceitam um funcionamento menos perfeito em função do custo. O preço a pagar poderá ser mais alto do que julgam", esclarece Pedro Fortuna, cofundador da Jscrambler. A seu ver, a única forma de solucionar ou atenuar este problema é a regulação. "Poderá ser feita de forma integrada para todo o mercado da União Europeia. Esta regulação deve definir patamares mínimos de qualidade do software, na totalidade ou por amostragem, identificando e vetando fabricantes associados a más práticas de desenvolvimento de equipamentos IoT", defende o gestor e CTO.

De acordo com os dados do Eurostat, em 2018, cerca de 8% das empresas portuguesas depararam-se com problemas de cibersegurança. A percentagem parece pouco significativa, mas os especialistas assinalam que o *gap* está na falta de reporte dessas falhas. Logo, mesmo com o melhor hardware e as questões regulatórias em dia, os piratas informáticos atacam todas as empresas, mesmo as mais bem preparadas para este tipo de crimes - nem todas optam é por admiti-lo.

E se tanto trabalhadores como consumidores não escapam aos *hackers*, o mesmo não se pode dizer das burlas online, nas quais apenas costumam 'cair' os menos informados.

Só nos primeiros três meses do ano, o Portal da Queixa recebeu 1.377 denúncias de esquemas de burla e fraude, o que representou um aumento de 34% em relação ao mesmo trimestre de 2019. O maior número de reclamações deveu-se a embustes relacionados com pagamentos online, esquemas maliciosos através de SMS, roubos de identidade, lojas online fictícias ou *phishing* (tentativa de obtenção de informação pessoal e financeira através de comunicações eletrónicas).

O perigo não é novo para os executivos, mas intensificou-se nas últimas semanas quando a grande maioria (ou mesmo a totalidade) dos funcionários entrou em regime de teletrabalho e, muitos deles, utilizam os computadores pessoais para trabalhar, com discos sobrecarregados e desprotegidos. Os empresários viram-se assim obrigados a reforçar a sensibilização para estes temas com os seus recursos humanos, que acabam por ser o 'calcanhar de Aquiles' nos seus esforços de cibersegurança e os consultores batem-se com alertas para a necessidade de os clientes implementarem novas tecnologias baseadas em Inteligência Artificial (IA) e *machine learning* para mitigarem vulnerabilidades.

"Embora para as tecnologias IoT também se verifiquem os principais riscos das redes TI, quando falamos da indústria 4.0 adicionamos riscos IoT e de segurança física. Desta forma, destacamos a maior premência para a obtenção de conhecimento técnico sobre matérias de segurança relacionadas com as tecnologias de suporte à Indústria", afirma João Madeira, partner da KPMG. "Embora existam à data normativos que orientem e estipulem regras de segurança para as tecnologias de indústria em sectores específicos – por exemplo o automóvel – estas obrigações e orientações ainda não abrangem toda a indústria", lamenta o sócio da área de Cibersegurança e Consultoria de Risco.

É uma ideia partilhada por Tomasz Jamroz, responsável de Analítica de Dados da CGI, que reforça a ideia de que as empresas que não forem capazes de assumir os riscos e investir perderão a vantagem competitiva e a oportunidade de liderar a transformação digital. "Requalificar os trabalhadores e permitir uma estreita colaboração entre pessoas e robôs é a chave. A introdução de novos modelos de negócio, processos de negócio, produtos e serviços interligados, transformam a maneira como os funcionários executam as tarefas diárias", refere ao JE.

ESTRATÉGIA

Gestão da cibersegurança deve ser transversal

As empresas devem ter em conta que a sua segurança informática depende de vários intervenientes, internos e externos.

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt

A gestão dos riscos cibernéticos é o processo de identificação, análise, avaliação e abordagem das ameaças informáticas dentro de uma organização. O ciclo passa ainda por monitorizar e priorizar esses riscos, mas a primeira missão dos executivos das empresas deve ser avaliá-los, porque permitirá automaticamente perceber a gravidade dos perigos e quais os que podem, de facto, comprometer a segurança informática dos seus sistemas.

José Casinha, *Chief Information Security Officer* da OutSystems defende que a melhor abordagem é ter em conta os padrões internacionais, tais como a norma ISO 27001 ou a NIST Cyber Security Framework (Estrutura de Segurança Cibernética do NIST) e estabelecer uma metodologia/estratégia para cada fase do risco: aceitá-lo e mitigá-lo ("reduzir o risco para um nível aceitável"), transferi-lo ("contratar um seguro, por exemplo") ou evitá-lo ("deixar de fazer algumas tarefas se for alto").

Resta a questão se essa gestão do risco informático deve ser centralizada na empresa ou distribuída entre quem desenvolve o software e quem produz ou fornece o hardware, ou mesmo transferi-la a 100% para seguradoras ou consultoras. "É uma das perguntas mais antigas em tecnologia. Tenho mais riscos se for tecnologia de muitos fornecedores (que, então, tenho que integrar) ou de um único (que vem integrado)? Existem muitas respostas diferentes. É fundamental testar implementações e ficar atento às informações de segurança dos fornecedores cujas tecnologias se escolhe", sugere Jonathan Sowler, vice-presidente de Engenharia da Unbabel ao Jornal Económico.

Concretamente para esta crise sanitária e económica, Jonathan defende que se mantenha os mesmos procedimentos pré-pandemia – até porque esses métodos já deveriam ser à prova de vírus (os que atacam online e os que levam ao teletrabalho de quase toda a empresa). "Os sistemas de segurança nunca devem confiar num único indivíduo, mas membros da equipa formados para desempenhar as funções se outro não estiver disponível", refere.

Quer Diogo Mendonça, diretor de Operações da Bee Engineering, quer Bruno Rodrigues, especialista em Cibersegurança da Noesis, são defensores de uma abordagem transversal, que compreenda todos os intervenientes para reduzir a exposição ao perigo, tendo em conta que hoje o cenário das TI é complexo, distribuído e envolve terceiros.

"Envolver o utilizador final apenas terá resultados práticos do ponto de vista do «antes», da prevenção. E mitigar uma vulnerabilidade que tem origem no hardware mais tarde acarreta custos elevados", completa António Ribeiro, *manager* de Cibersegurança da Claranet. No entanto, uma abordagem colateral da gestão não significa várias abordagens para cada um dos *stakeholders*. Segundo a Deloitte, cada vez existe maior necessidade de transparência e uniformidade na avaliação e no programa de gestão de riscos cibernéticos, porque as empresas não estratégica única.

"A análise de risco deve ter como base uma série de controlos, sejam NIST, ISO27k ou CIS, a ser aplicados nas três dimensões: utilizadores, fornecedores e fabricantes", diz Bruno Rodrigues, especialista em cibersegurança da Noesis

O seu desafio .
A nossa solução

*Há 40 anos que a proximidade e a cooperação são as palavras de ordem na **F. REGO**. Aplicámo-las em todas as relações. Com os nossos Colaboradores, Clientes, Parceiros e Stakeholders.*

Numa época cada vez mais tecnológica, a chave do sucesso reside na transformação das ameaças em oportunidades. Mais do que obstáculos, as novas tecnologias deverão ser percecionadas como ferramentas ao dispor dos mediadores para customizar e acrescentar ainda mais valor ao serviço prestado ao cliente, conservando o rigor e a proximidade exigidos.

A inovação tecnológica não impactará apenas a relação com o consumidor. O futuro reserva-nos novos riscos e, consequentemente, novas tipologias de seguros. De automóveis autónomos, à utilização de robôs para tarefas rotineiras, atravessamos uma revolução dos modos atuais de trabalho e de vida, em que o setor segurador terá, também ele, de acompanhar a própria evolução social e assumir uma posição de destaque pela liderança.

*Na **F. REGO** continuaremos a emprestar diferenciação a cada solução que nos propomos. Uma solução que salvaguarde e reflita os rostos que nos caracterizam: integridade, ética e responsabilização.*

com o apoio F·REGO CORRETORES DE SEGUROS · INSURANCE BROKERS

SOFTWARE

O que deve fazer a sua empresa em caso de 'ransomware'

É difícil recuperar os dados depois de um ataque desta natureza, que muitas vezes envolve criptomoedas. Rui Shantilal explica o que está em causa.

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt

O *ransomware* é um software malicioso que retira informação dos sistemas informáticos das empresas e dos utilizadores privados. No entanto, este tipo de ameaça online tem uma peculiaridade: recorre a uma chave digital que trava o acesso aos dados até que seja realizado um pagamento, por exemplo. Rui Shantilal, *managing partner* da consultora tecnológica Integrity, explica ao Jornal Económico que, muitas vezes, o dinheiro é facultado em moedas digitais.

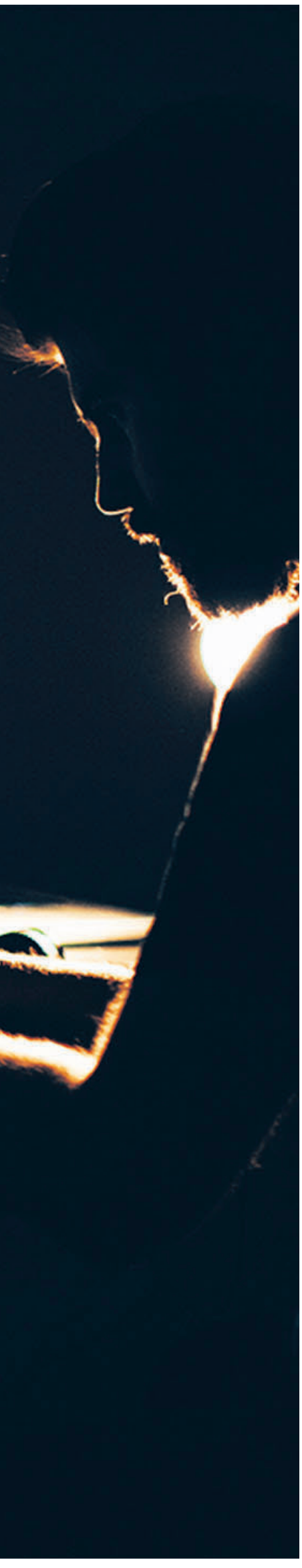
Como acontecem estes ataques?
Este tipo de ataque acaba por ser bastante prejudicial para quem é vitimado pelo mesmo, imagine-se uma empresa que fique sem acesso aos seus dados vitais, registos, dados de clientes ou dados financeiros, ou o exemplo de um fotografo que no dia seguinte à reportagem de um casamento acaba por ficar sem acesso às fotografias dos momentos únicos dos protagonistas. Para que um ataque de *ransomware* seja bem-sucedido, é necessário que um software malicioso concebido para esse efeito seja instalado ou executado no computador da vítima. Esta execução pode ser facilitada porque determinado software está inseguro, por exemplo por falta de instalação de uma atualização ou através do recurso ao engano do utilizador, levando-o executar determinada ação como instalar ou a facilitar a execução deste software. Os casos práticos mais típicos são a exploração de falhas de software facilitadas pela falta de instalação das atualizações de *browser*, do sistema operativo ou os ataques de *phishing* nos quais leva-se o utilizador a executar determinada ação como seguir um *link* ou efetuar o *download* e instalação de um software. Este tipo de ataques não está limitado aos computadores, os dispositivos móveis também têm vindo a ser alvo deste tipo de ataques, por exemplo, através da instalação de aplicações, que embora possam parecer fidedignas aos olhos do utilizador, não o são. Um exemplo muito atual deste ataque tem sido o caso dos utilizadores que instalam aplicações maliciosas de *ransomware* que usam a "máscara" de uma aplicação legítima com o intuito de suportar a luta contra a pandemia da Covid-19.

Quem está por detrás destes cibercrimes?
Trata-se de uma indústria ilícita com um custo estimado em 10 biliões de euros este ano e como tal, salvo exceções, quem está por detrás destes ataques são verdadeiras organizações bem estruturadas com os meios humanos e tecnológicos que podem estar a operar ao virar da esquina, mas mais frequentemente situados em países do Leste ou na Ásia.

> "Há utilizadores que instalam 'apps' maliciosas que usam a 'máscara' de legítimas para suportar a luta contra a Covid-19", exemplifica o CEO da consultora tecnológica Integrity

Qual é a solução para resolver este tipo de *malware*?
Infelizmente, na grande maioria dos casos não é possível ter acesso à informação em tempo útil a não ser com a chave correta. E, infelizmente, mesmo pagando não é garantido que o atacante disponibilize a chave. Portanto o melhor é efetivamente não chegar sequer a ter que resolver, ou seja, chegar à fase da remediação, atuando na prevenção de que este tipo de ataques venha a ocorrer.

Há forma de prevenção?
Estes ataques previnem-se através da conjugação de um conjunto de boas práticas que os utilizadores devem seguir, nomeadamente: evitar instalar software sem confirmar a sua confiabilidade; não seguir *links* que o podem conduzir para levar a cabo ações inseguras; manter os seus dispositivos e aplicações devidamente atualizados – não esquecer que estas atualizações resolvem vulnerabilidades de segurança no software que acabam por ser exploradas pelos atacantes -; apostar em software de prevenção (*firewall*, software *anti-malware*) para ajudar a detetar e prevenir a execução do programa malicioso em tempo real e garantir que dispõe de cópias de segurança atualizadas dos seus sistemas e informação, pois poderá ser a solução mais viável em caso de ser alvo de um ataque bem-sucedido. ●



ORGANIZAÇÃO

Empresas compram seguros para proteger os sistemas

Ainda que a maior parte das soluções de seguro existentes no mercado se dirija às empresas, a procura por este tipo de produto estruturado para pessoas singulares tem vindo a aumentar.

CARLOS CALDEIRA
geral@jornaleconomico.pt

Com o constante aumento do número de dispositivos eletrónicos existentes (IoT) e dos seus utilizadores, assim como dos negócios realizados online e das informações guardadas em rede, a segurança no ciberespaço tornou-se definitivamente uma preocupação muito séria para as pessoas, empresas, governos e nações, interferindo diretamente com a confiança nos sistemas.

Segundo Pedro Moura Ferreira, diretor de Negócio Global da MDS, o risco cibernético "é um assunto que mina de forma significativa a credibilidade das organizações, faz retrair a confiança dos clientes e testa a capacidade das empresas em conseguirem resistir às contantes falhas de segurança (*data breach*) e aos crescentes ataques às suas operações/negócios". O responsável explica que esta guerra virtual (e muitas vezes silenciosa) é capaz de "causar danos financeiros e reputacionais gigantescos às empresas e, por esse motivo, o risco cibernético é hoje um assunto debatido em todos os conselhos de administração. Sem dúvida, as empresas colocam hoje as ameaças cibernéticas no topo das suas preocupações". Para a consultora e gestora de risco e seguros, a interrupção do negócio, as perdas financeiras, a perda de informação confidencial, o ataque à integridade de dados, a extorsão, o roubo de identidade e os danos reputacionais são alguns exemplos do impacto que um *data breach* poderá ter numa organização.

"Uma vez mais, e porque estamos perante um risco que não é passível de ser totalmente eliminado, a transferência do mesmo para uma apólice de seguro assume um papel crítico no 'risk governance' de uma empresa", diz Pedro Moura Ferreira.

O seguro cyber dá cabal resposta a isto mesmo, garantindo a proteção do negócio e os custos relacionados com os danos e prejuízos sofridos na própria empresa, bem como as responsabilidades perante terceiros. Daí que a procura por esta solução esteja a crescer.

Particulares preocupados com perdas financeiras

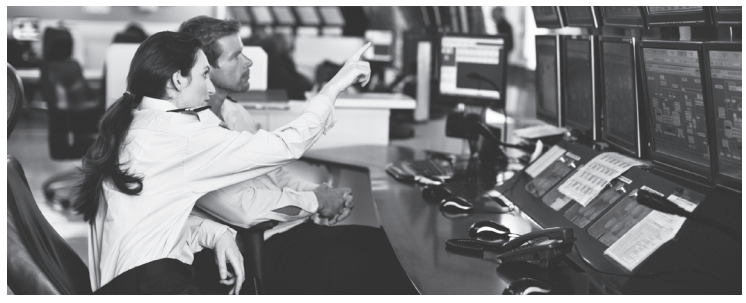
A procura por este tipo de seguro é maior por parte das empresas. No entanto, ainda que a maior fatia das soluções de seguro existentes no mercado se dirija às empresas, existe uma crescente procura deste tipo de produto estruturado para pessoas singulares. "Obviamente, a tónica do seguro estará mais voltada para a proteção contra a perda financeira que individualmente as pessoas poderão sofrer em virtude de um problema de cibersegurança", explica o executivo MDS. E acrescenta: "Mas, tal como nas empresas, também neste prisma existem soluções que garantem cabalmente a responsabilidade perante terceiros, bem como os demais e essenciais serviços de aconselhamento técnico, jurídico e resposta a incidentes".

Especialista defende coberturas que garantam acesso de emergência a equipa de consultores legais e tecnológicos, resposta a perda de lucros e serviços especializados na monitorização da base de dados e identidades

Segundo Pedro Moura Ferreira, "existem muitos produtos nesta área oferecidos pelas seguradoras clássicas e generalistas. A abordagem que temos realizado junto do tecido empresarial em Portugal revela que cada caso é um caso e, por isso, as soluções *taylor-made* gozam naturalmente de maior eficácia e eficiência na resposta aos incidentes. A exposição ao risco é inevitavelmente diferente de empresa para empresa". Genericamente, a grande maioria dos seguros cyber que encontramos no mercado "dão hoje um considerável nível de conforto no que respeita à amplitude de cobertura e ao financiamento dos custos que advêm de falhas de segurança (*data breaches*) e ataques cibernéticos", diz ainda o consultor.

DXC Technology avalia cibersegurança de sistemas e infraestruturas

Empresas necessitam de analisar a maturidade de cibersegurança dos seus ambientes OT e IoT.



As organizações estão a transformar digitalmente os seus negócios, beneficiando das oportunidades de inovação oferecidas pela Internet das Coisas (IoT – Internet of Things). Esta tecnologia apresenta-se como uma das grandes impulsionadoras da transformação e abre um novo mundo ao desenvolvimento dos negócios.

"As organizações que melhor souberem aliar a tecnologia ao negócio estarão melhor posicionadas para liderar no mercado. No entanto, as empresas precisam de se preparar corretamente e acautelar os riscos inerentes, pelo que é fundamental que realizem uma análise à cibersegurança dos seus sistemas e infraestruturas", afirma Miguel Mendonça, Cybersecurity Offering Lead da DXC Technology Portugal.

Por exemplo, no sector industrial, a OT – Operational Technology, que inclui os sistemas de controlo desenhados para monitorizar e controlar um conjunto de máquinas industriais, está a abraçar a IoT para aumentar a eficiência e diminuir o tempo de inatividade das operações.

Mas à medida que estes ambientes se interconectam, a tradicional segregação das infraestruturas OT e assunção de segurança por obscuridade ("Security by obscurity") já não protege os sistemas dos altamente sofisticados e avançados ciber criminosos. O grande desafio é que estas infraestruturas OT historicamente não foram expostas ao mesmo nível de ameaça do que as tradicionais (de IT) e, devido a isso, no presente necessitam de um maior nível de segurança e visibilidade dentro de uma organização.

Como não é possível proteger o que não se vê ou conhece, a DXC está a ajudar os seus clientes a montar a fotografia completa das suas organizações de forma a priorizar os seus investimentos em segurança em IoT e OT.

com o apoio DXC.technology

VULNERABILIDADES DO REMOTO

O teletrabalho colocou centenas de trabalhadores a trabalhar a partir de casa. O tráfego de emails aumentou, o controlo dos colabradores que estão a utilizar computadores próprios diminuiu e o apetite dos piratas informáticos aguçou-se.

O REGIME DE 'HOME OFFICE', AO QUAL A PANDEMIA OBRIGOU CENTENAS DE EMPRESAS A ADERIR, TROUXE MAIS EXIGÊNCIAS/DESPESAS DE CIBERSEGURANÇA AOS SEUS SISTEMAS INFORMÁTICOS? SE SIM, QUAIS?

ANTÓNIO RIBEIRO
Manager de Cibersegurança da Claranet

MAIS EXIGÊNCIAS

Acima de tudo o regime remoto traz mais exigências, face a uma monitorização mais apertada dos riscos cuja origem parte – agora praticamente na totalidade – para o exterior do nosso perímetro. E, tal como numa pandemia, sem cuidados trata-se uma exposição - agora constante - a ameaças em contextos tipicamente desprotegidos. Obriga não só a constantemente assegurar a integridade (postura) e comportamento dos equipamentos que se ligam, remotos, a infraestuturas corportativas, bem como a aumentar todo o detalhe e a capacidade de processamento desta monitorização detalhada de integridade e de comportamento. O maior custo é o de lidar com quantidade acrescida de situações detetadas, e que carecem de análise, já que a infraestrutura facilmente consegue lidar com este novo volume.

BRUNO RODRIGUES
Especialista em Cibersegurança da Noesis

VULNERABILIDADE DESMASCARADA

Não se pode afirmar que a rápida (e descontrolada) adesão ao teletrabalho trouxe por si uma maior despesa no orçamento de segurança às organizações. O que acontece é que o teletrabalho desmascarou uma série de vulnerabilidades e ameaças para quais as empresas nacionais não estavam despertas. De certa maneira, esta pandemia forçou a mudança digital e trouxe as questões de segurança informática para a ordem do dia, tornando-se neste momento um dos assuntos mais preocupantes no panorama atual. É evidente que as organizações terão de alocar mais recursos para esta temática, pois estão confrontadas com uma nova realidade, mas na verdade estão apenas a cobrir áreas onde eram mais vulneráveis e ainda não as tinham identificado. A Noesis tem vindo a trabalhar com os seus clientes e parceiros naquilo que podemos designar como uma segunda vaga de intervenção nesta pandemia – em primeiro lugar foi necessário colocar as pessoas em segurança em suas casas – nesta segunda vaga temos de garantir a segurança dos utilizadores, da informação e dos sistemas. Para isso, dispomos neste momento de duas parcerias muito fortes, Darktrace e Microsoft, que nos permitem, através de modelos de 'machine learning' e 'behaviour analysis', implementar rapidamente as ferramentas que as organizações necessitam para detetar e mitigar as ameaças de uma forma transversal, incluindo os utilizadores/informação que se encontram em teletrabalho.

EDGAR PIMENTA
Diretor de Segurança de Informação da Talkdesk

REFORÇO DO ALERTA AOS FUNCIONÁRIOS

Evidentemente, houve algumas necessidades de ajuste, pois este cenário específico e a sua duração trouxe desafios inesperados. O facto de a Talkdesk, além de ser um produto 'cloud', também utilizar ela própria vários serviços 'cloud', torna (e, neste caso, tornou) a ativação dos planos de continuidade de negócio bastante fácil, não implicando grandes custos adicionais. O principal é, obviamente, o fator humano e aí temos feito um investimento em reforçar junto dos colaboradores as boas práticas de segurança, com dicas concretas de boa utilização de ferramentas. Sabemos que este momento é propício a ataques dirigidos às pessoas e, como tal, temos também reforçado a monitorização das ameaças existentes e, quando aplicável, algumas medidas de segurança. Ou seja, diria que o regime de 'home office' trouxe mais exigências em termos de cibersegurança, mas não obrigatoriamente em termos de despesas.

TOMASZ JAMROZ
Responsável de Analítica de Dados e IA da CGI

RISCO DE 'HACKERS' SOCIAIS

As organizações e as redes já estão bem preparadas para o trabalho remoto. Os maiores desafios vêm dos próprios funcionários. Os colaboradores que se ligam através de Wi-Fi não seguras ou que são alvos fáceis de hackers sociais são os dois problemas mais críticos que aumentam os riscos de uma violação de dados atualmente. Embora o primeiro possa ser mitigado pelas empresas que garantem a conexão VPN da empresa com as suas redes, o último é muito mais complicado. A quebra de segurança mais recente do Marriott Group aconteceu quando os hackers obtiveram acesso ao sistema através de duas contas de funcionários, o que permitiu o acesso às informações de 5,2 milhões de clientes da cadeia de hotéis. A maioria das trocas e comunicações ocorre agora por email, ao contrário do que acontece quando se está no escritório, em que pode comunicar com o colega que está sentado ao seu lado. Como resultado, o tráfego de emails é significativamente maior. É muito fácil para os hackers enviar um email que possa parecer relevante e que se mistura com os restantes, dando início a uma reação em cadeia de consequências potencialmente muito perigosas. Infelizmente, os hackers aproveitaram-se do facto de existirem mais funcionários a trabalhar remotamente devido à Covid-19. As empresas devem por isso, e cada vez mais, considerar a utilização de plataformas de colaboração, permitindo assim que as pessoas troquem informações com opções de vídeo e imagens, pois isso pode ajudar a mitigar o risco. Em particular as equipas de segurança interna, precisam de aumentar os esforços na verificação das redes e de considerar a utilização de soluções avançadas de análise e de IA.

SÉRGIO AGRELOS
Chief Operating Officer da F3M

FALTA DE MONITORIZAÇÃO

O mundo tem-se deparado com algo inédito para muitos de nós, levando a que as prioridades, tanto em termos pessoais como profissionais, tivessem mudado de forma brusca e inesperada. As empresas de TI foram chamadas, como que num contrarrelógio, a criar condições para que tanto os seus colaboradores como os colaboradores dos seus clientes pudessem passar a trabalhar de forma 100% remota a partir dos seus lares, tendo acesso a toda a informação que necessitassem no âmbito das respetivas funções de cada um. Surge, no entanto, um problema acrescido com esta nova realidade, a necessidade de, mais do que nunca, serem reforçadas todas as medidas no âmbito da cibersegurança. A partir do momento em que os colaboradores das organizações passam a trabalhar a partir de locais não controlados pelas mesmas, e muitas das vezes, passam a utilizar computadores também eles não monitorizados pela organização (pessoais sem anti-vírus ou com versões atualizadas, por exemplo), novas vulnerabilidades passam a surgir. As organizações devem garantir que estão devidamente protegidas contra ameaças externas e que o acesso aos seus recursos é devidamente controlado através de 'firewalls' e outros mecanismos de controlo de acessos. Infelizmente o cibercrime não conhece fronteiras ou códigos de ética e uma altura como esta potencia crimes dessa natureza.

JOÃO SEQUEIRA
Diretor de Secure e-Solutions da GMV Portugal

PARTILHA DE INFORMAÇÃO

Desde o início da crise provocada pela pandemia da Covid-19, a GMV tem vindo a monitorizar de perto a sua evolução e seguido as recomendações das autoridades de saúde internacionais, nacionais e locais. Em consequência, ativámos de forma gradual uma série de medidas preventivas com o objetivo de assegurar a saúde dos colaboradores e suas famílias, o que até à data não nos impediu de continuar a funcionar com quase completa normalidade. No dia 13 de março a GMV ativou o seu plano de continuidade de negócio Covid-19 assente no nosso Sistema de Gestão da Continuidade do Negócio, certificado segundo a norma ISO 22301 desde 2010, aplicável a todas as nossas sedes em todos os países em que estamos presentes. Desde a ativação do plano que podemos considerar que praticamente a totalidade das nossas atividades em todas as nossas sedes internacionais e em todos os países onde operamos, têm-se realizado remotamente, pelo que a maior parte dos nossos projetos e serviços prestados aos nossos clientes prossegue dentro dos parâmetros normais. Para dar suporte a um número maior de acessos à rede da GMV foi necessário monitorizar de perto a infraestrutura já existente tal como as ligações à internet, 'desktops' virtuais utilizados, e acessos concorrentes à VPN tendo sido criado um 'scorecard' para fornecer esta informação a todos os colaboradores da GMV. Por outro lado, e em particular na situação atual, mantivemos o especial cuidado com os aspetos da cibersegurança que caracteriza as nossas operações. Ataques de 'phishing', 'malware', engenharia social e ataques externos que têm naturalmente um aumento elevado e podem afetar a continuidade do negócio. Além da normal monitorização constante da rede pelo nosso SOC, a empresa reforçou a partilha de informação de algumas medidas a ter em conta junto dos colaboradores para que possam estar mais alerta e menos vulneráveis.

DIOGO MENDONÇA
Diretor de Operações da Bee Engineering

MATURIDADE TEM INFLUÊNCIA

Sem dúvida, ainda que depende do estádio de maturidade tecnológica de cada organização. Quer isto dizer que a própria adaptação da tecnologia à dinâmica remota, veio forçar as organizações a se adaptarem, por exemplo, a aceder informação partilhada numa rede pública. Isto significa que as organizações podem precisar de serviços externos para o fazer, caso não tenham essa competência. Foi precisamente a pensar nisso que lançámos uma iniciativa de apoio a PME, a que chamámos de Tech Guidance, em que nos podem consultar e receber apoio tecnológico, sem qualquer custo associado. Foi uma das formas que encontrámos de ajudar o tecido empresarial, usando a nossa experiência e capacidades internas.

JOÃO MADEIRA
Partner de Cibersegurança da KPMG

SENSIBILIZAÇÃO PARA A SEGURANÇA

Sim, as organizações tiveram que redirecionar a sua atenção para a disponibilização de infraestruturas e acessos remotos em larga escala, antecipando algumas atividades e investimento que estavam preconizados mais a médio ou longo prazo. Ao mesmo tempo, ficam igualmente mais expostas a vulnerabilidades e riscos de cibersegurança, pelo que o investimento em atualização de processos relacionados e a sensibilização e cultura de segurança são igualmente áreas de foco e investimento.

JOSÉ CASINHA
Chief Information Security Officer da OutSystems

EMAILS MALICIOSOS

O 'home office' expõe alguns riscos para a organização, no sentido que as pessoas passam longas horas sozinhas e, por isso, mais isoladas na sua tomada de decisão. Isto torna-as mais vulneráveis a ataques cibernéticos, como seja o seguimento de emails maliciosos, o acesso a sites na internet que podem conter vírus, etc. Nem todas as empresas têm sistemas de proteção adequados para trabalhar remotamente quando a sua atividade é maioritariamente desempenhada nas suas instalações, o que as obriga a investimentos que permitam o trabalho remoto, como sejam o uso de tecnologias de rede privada virtual, sistemas de colaboração seguros, etc.

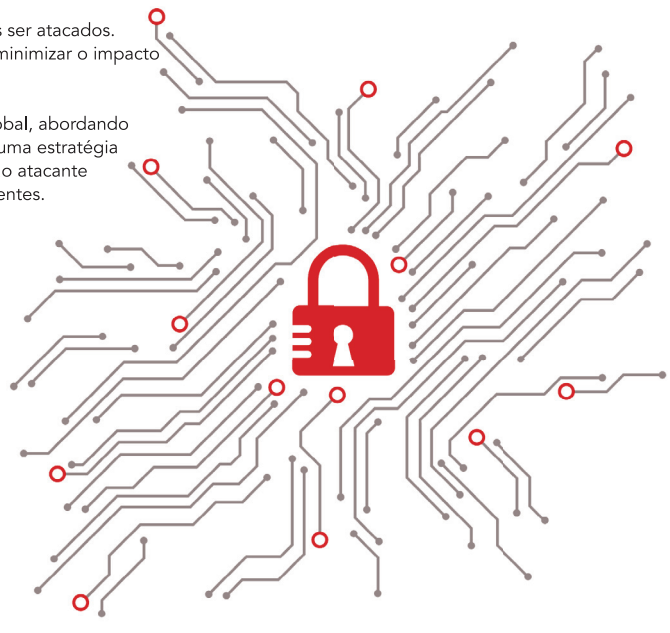
PUB

O NOSSO OBJETIVO
A SUA CIBERSEGURANÇA

Estamos cada vez mais conscientes do risco a que todos estamos expostos.

Devemos assumir que mais tarde ou mais cedo vamos ser atacados. Por isso, devemos aumentar os nossos esforços para minimizar o impacto destes ataques nas nossas infraestruturas.

Na GMV apostamos numa aproximação proativa e global, abordando a cibersegurança em todas as suas formas: definindo uma estratégia operacional, protegendo os ativos, antecipando-nos ao atacante e estabelecendo a normalidade perante os ciberincidentes.



GMV
www.gmv.com/pt/ marketing.portugal@gmv.com

www.facebook.com/infoGMV
@infoGMV

gmv®
INNOVATING SOLUTIONS

AERONÁUTICA | ESPAÇO | DEFESA | SAÚDE | CIBERSEGURANÇA | ITS | TELECOMUNICAÇÕES | TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

PEDRO REGO
CEO
da F.Rego

CONFIDENCIALIDADE DE DADOS

O setor segurador, à semelhança da própria sociedade, depara-se com novos desafios provocados pela pandemia da Covid-19. Para a maioria das organizações esta é uma situação sem precedentes, que lhes coloca desafios imediatos e de urgente resolução. O repto é desafiante para todos, que subitamente, se veem confrontados com novas dinâmicas e urgências, obrigando a uma aceleração evidente dos processos de transformação digital. Na F.Rego, de maneira a manter a qualidade no atendimento que nos é característico e preservar a segurança dos dados dos nossos clientes e parceiros, reforçamos a infraestrutura tecnológica que nos suporta para garantir que as ferramentas que já dispúnhamos, e necessárias para que toda a nossa equipa tenha acesso a canais de comunicação que lhes permitem a partir de suas casas tratar diligentemente e atempadamente de todos os assuntos e necessidades dos cliente, estão em pleno funcionamento e sem falhas. Ao nível da segurança, uma preocupação central da nossa organização, seja pela confidencialidade dos dados que tratamos, seja pela recente regulação relativa à proteção de dados, não podemos afirmar que a atual situação trouxe custos adicionais mas evidenciou a importância dos investimentos anteriormente efetuados.

PUB

Conquistar o mundo sempre foi um risco. E essa é a nossa especialidade.

DE PORTUGAL PARA O MUNDO.

A MDS lidera o mercado português de corretagem de seguros há cerca de 15 anos. Contamos hoje no mundo com mais de 800 colaboradores, 10 nacionalidades, gerindo mais de 600 milhões de euros em prémios. Com forte presença no Brasil, Angola e Moçambique, somos o grande corretor de referência do espaço lusófono. Atuamos em todo o mundo através da nossa participada Brokerslink, uma global broking company, presente em 110 países. A MDS é o único Lloyd's Broker de capital português.

Brokerslink Partner

Broker at LLOYD'S

MDS Global Insurance & Risk Consultants

PEDRO MOURA FERREIRA
Global Business
Director da MDS

RISCOS NAS REDES DOMÉSTICAS

Não há dúvida de que o mundo está diferente após a explosão da pandemia da Covid-19. Com a imposição pelos governos do distanciamento social como forma de combate à propagação do novo coronavírus, foram implementadas medidas exigentes que obrigaram a que muitas empresas tivessem de encerrar ou, sempre que possível, recorrer ao modelo de 'home office' para manter "a máquina a funcionar". Assistimos a uma mudança do paradigma de comunicação entre pessoas e organizações, comunidades e sociedade em geral. O novo normal são as reuniões e conversas por videoconferência, utilizando as mais variadas plataformas digitais, que se tornaram hoje o principal veículo de comunicação e interligação entre todos nós. As empresas, para responderem a estas necessidades, tiveram de providenciar aos seus colaboradores o uso de ferramentas de trabalho remoto, a extensão das licenças de VPN ou VPN-SSL, e linhas fixas externas para acessos remotos ou aplicativos acessíveis, para além da criação massiva de novos utilizadores e perfis com acesso remoto; entre outros. Neste novo cenário, muitas barreiras de segurança e políticas corporativas, outrora sagradas, terão sido levantadas e as boas práticas recomendadas temporariamente esquecidas. Para os cibercriminosos, esta pandemia é propícia à exploração e procura de lucro. Temos assistido a um aumento dos ataques cibernéticos para explorar todas as vulnerabilidades e comprometer a segurança dos sistemas e da informação das empresas que, agora, dependem em muito da segurança instalada nas redes das casas dos seus colaboradores. Nestas redes domésticas existem muitas novas ameaças que estão a ser aproveitados pelos "digitais amigos do alheio" para violações de privacidade, confidencialidade e roubo de informações das empresas. São várias as lições que podemos tirar desta nova realidade. Seja a importância de planos de contingência e de continuidade - não apenas desenvolvidos mas também testados- seja uma maior consciência da segurança cibernética na cultura da organização, mas, "last but not least", a importância da contratação de um seguro cibernético para ajudar a mitigar este tipo de riscos.

MIGUEL MENDONÇA
Cybersecurity Offering Lead
da DXC Technology Portugal

NOVOS PROCESSOS E TECNOLOGIAS

Com a pandemia atual, a nossa forma de trabalhar mudou, mas os sistemas mantiveram-se. Assim, é inevitável que as empresas tenham de reagir rapidamente e dotar-se de outro tipo de soluções e sistemas para enfrentar a situação. Mas mais do que isso, têm de prepararem-se para que as novas formas de trabalho se transformem no novo normal. Embora o teletrabalho não seja algo recente, a maioria das organizações não estava preparada para praticá-lo em larga escala e com as condições de produtividade adequadas. Muitas das soluções existentes estavam desenhadas para funcionar dentro da empresa de uma determinada forma que hoje se percebe que não é aplicável quando fora da mesma. A partir do momento em que um colaborador leva um computador para casa, e/ou se liga remotamente aos sistemas corporativos, o contexto muda e o seu perfil de risco torna-se completamente diferente do que estamos habituados. Outro exemplo acontece de aumento de risco acontece quando as empresas possibilitam o uso de dispositivos pessoais para acesso a sistemas e dados corporativos (tipicamente referenciados como dispositivos BYOD – Bring Your Own Device). Ou seja, o risco cibernético aumenta sempre que os níveis de segurança baixam, o que pode ser um cocktail bastante perigoso. Esta alteração de paradigma atrai atores maliciosos e produz novos vetores de ataque, empurrando a responsabilidade da segurança da informação para além das fronteiras das empresas. Nunca foi tão importante para as empresas adotarem uma postura forte de cibersegurança, com especial atenção ao treino e sensibilização dos seus colaboradores, para que sejam capazes de detetar e reagir perante comportamentos anómalos ou suspeitos, e à proteção dos dispositivos e serviços para teletrabalho e acesso remoto, que pressupõe a adoção de novos processos e tecnologias. Tudo isto se materializa num investimento - e não em despesa - que possibilitará a adoção de teletrabalho seguro e poderá trazer benefícios económicos no futuro, como redução de custos com despesas pessoais ou com escritórios físicos. A DXC encontra-se a trabalhar com os seus clientes nessa transformação, seguindo uma metodologia assente na análise e adaptação das três dimensões: pessoas, processos e tecnologia.