O Jornal Económico

ESPECIAL

Cibersegurança

GUERRA E COVID-19 REFORÇAM PREOCUPAÇÃO COM SEGURANÇA INFORMÁTICA

Se a pandemia havia não só aumentado os ciberataques como os investimentos em tecnologia de proteção e prevenção dos sistemas informáticos das empresas públicas e privadas, o conflito militar que decorre no leste da Europa traz novos desafios para a Administração Pública, sector segurador, universidades e tecnológicas.

TECNOLOGIA

Investimento nacional em cibersegurança vai passar os 200 milhões em 2022

Especialistas acreditam que, ao nível da regulação, dificilmente a lei conseguirá acompanhar os desenvolvimentos tecnológicos ao ponto de ser também um obstáculo aos piratas informáticos.

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt

Os investimentos em tecnologia para cibersegurança em Portugal vão ultrapassar os 200 milhões de euros este ano, prevê a IDC. Apesar do aumento generalizado dos preços, os especialistas de mercado acreditam que as empresas não vão descurar os sistemas para travar o maior número de ataques de *hackers* possível - já que as tentativas de invasão, essas, não vão recuar. Na base do orçamento avultado para cibersegurança estará a consciência dos gestores de que, embora comecem a sair do caos provocado pela pandemia, guerra na Ucrânia gerou outros desafios geopolíticos e maiores ameaças informáticas, segundo a consultora norte-americana.

"O contexto geopolítico na Europa levou à intensificação da tendência de aumento da atividade maliciosa no ciberespaço europeu. A frequência e complexidade crescente destas atividades requerem cada vez mais investimento das empresas na segurança e resiliência dos seus produtos e serviços", afirma ao Jornal Económico (JE) Ricardo Pires, *manager* de Cibersegurança do .PT. "A adoção de mecanismos com duplos fatores de autenticação e utilização de passwords mais fortes, a garantia que os softwares utilizados são atualizados (focando-se naqueles com vulnerabilidades conhecidas), rever o acesso de terceiros às suas redes, efetuar cópias de segurança da informação crítica (*backups*) e sensibilizar os seus colaboradores para as matérias de cibersegurança são alguns dos principais fatores a reforçar pelas empresas", sugere o porta-voz da entidade responsável pela gestão, registo e manutenção de domínios sob .pt.

O canadiano Chester Wisniewski descarta falar de ciberguerra ao que está a acontecer, mesmo a nível tecnológico, no âmbito da crise na Ucrânia. "É «simplesmente» - e não o digo, de todo, de uma forma leve - uma guerra. Embora a Rússia se tenha envolvido em alguns ataques utilizando *malware* e *distributed denial of service* [DDoS ou ataque de negação de serviço], a maioria deles foi de natureza limitada e muito poucos tiveram impactos mais além da Ucrânia", esclarece. A seu ver, há um risco mais elevado para as infraestruturas críticas para o Ocidente, nomeadamente para o resto da Europa e os Estados Unidos [EUA], "pois muitas organizações reportaram um aumento na atividade de *scanning*, o que nos sugere que há adversários estrangeiros em busca de vulnerabilidades e métodos para entrar nos sistemas". "Os EUA atribuíram esta atividade à Rússia. Por outro lado, grupos criminosos, muitos dos quais baseados na Rússia, agora sentem-se também mais livres para atacar ativos ocidentais com pouco risco de serem presos pelo seu próprio país, o que pode resultar num aumento geral do cibercrime, principalmente do *ransomware*", argumenta o investigador da Sophos.

Para Daniel Creus, da equipa global de investigação e análise da Kaspersky, a segurança deve contemplar-se como uma "disciplina hiperdinâmica". "É essencial que qualquer entidade que se queira proteger, saiba como se adaptar a um ambiente de alta mudança. Qualquer entidade pode ter um modelo de riscos com base em ameaças teóricas, no entanto, o importante é ter um conhecimento contínuo e realista de ameaças específicas que as podem afetar", argumenta o investigador do GReAT.

Um pilar de conhecimento que tem sido fomentado no sector público e privado. A empresa portuguesa Claranet informou recentemente que, na sequência da parceria estratégica feita com a KnowBe4, proporcionou o acesso a

Daniel Creus
Investigador principal de Segurança do GReAT (Kaspersky)

David Grave
Consultor sénior de Cibersegurança da Claranet

Ricardo Pires
Manager de Cibersegurança do .PT

Chester Wisniewski
Investigador científico principal da Sophos


ThinkStock

simulações de *phishing* e consciencialização de segurança a mais de 40 mil utilizadores, que puderam aceder a ferramentas de simulação de *phishing* e a conteúdos formativos e de alerta face a riscos de segurança, reforçando as suas competências e alterando comportamentos, para dar uma resposta eficaz a um dos maiores tipos de ciberameaças da atualidade. Ao JE, David Grave, consultor sénior de Cibersegurança da Claranet, defende que o foco tem de passar para a cooperação internacional para se poder atuar sobre os grupos criminosos. "De outra forma continuaremos a observar um aumento deste tipo de criminalidade transfronteiriça, que apresenta riscos muito diminutos para os cibercriminosos, mas impactos significativos para as empresas", explica o responsável da empresa especializada em soluções de *cloud*, segurança, dados e workplace.

E a rede móvel de quinta geração (5G)? Daniel Creus, do GReAT (Kaspersky), crê que a sua implementação em maior escala facilite alguma ciberameaças, por causa da hiperconexão de dispositivos eletrónicos "com medidas de segurança fracas ou inexistentes de forma contínua, que podem supor um vetor de intrusão inicial para os atacantes". Por outro lado, David Grave, da Claranet, recusa que seja um problema da tecnologia, mas sim "do desenvolvimento de produtos centrados apenas da facilidade de utilização, que descuram muitas vezes a cibersegurança".

Ao nível da regulação, há unanimidade: dificilmente alguma vez a legislação – quer nacional quer europeia – conseguirá acompanhar os desenvolvimentos tecnológicos ao ponto de ser também um obstáculo aos piratas. Chester Wisniewski lembra ao JE que a Comissão Europeia propôs melhorar as comunicações e harmonizar as regras nos 27 Estados-membros, o que caracteriza como "uma melhoria", e que o RGPD foi uma mais-valia na proteção dos dados sensíveis, mas trata-se "apenas da base do que é necessário ainda fazer". "A partilha clara e abrangente de informações, como está a ser feito pela CISA [Cybersecurity and Infrastructure Security Agency] nos Estados Unidos, seria um enorme passo em frente, apoiando as regulamentações que começam a controlar melhor a utilização de criptomoedas para lavagem de dinheiro e pagamentos de resgates de *ransomware*. Precisamos de regulamentações que exijam relatórios precisos de cibercrimes que não tenham impacto claro na privacidade", recomenda.

Em Portugal, o mais recente passo foi o Regime Jurídico do Ciberespaço (decreto-lei nº 65/2021 de 30 de julho, tal como realça Ricardo Pires, da .PT. "Tem sido feito um grande esforço, a nível europeu e nacional, para acompanhar os desafios colocados à segurança no ciberespaço. Este regime trouxe uma base comum de requisitos de segurança para a Administração Pública, operadores de infraestruturas críticas, prestadores de serviços digitais e operadores de serviços essenciais, como é o caso do .PT", diz. ■

ENTREVISTA | HUGO NUNES | Líder de Threat Intelligence da S21sec em Portugal

"Acesso à 'dark web' aumentou consideravelmente na guerra"

Empresa ibérica de cibersegurança concluiu que os criminosos estão a utilizar cada vez mais mercados negros como o Genesis Market, o Russian Market ou o 2easy Market para vender dados bancários, a informação mais "apetecível".

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt

Foto cedida

A próxima mensagem é um alerta no sector financeiro: há cada vez mais dados bancários à venda na "deep web" ("internet profunda", que não se acede no Google). A conclusão consta no último relatório "Threat Landscape Report" da empresa ibérica de cibersegurança S21sec, que identificou os principais malwares bancários que marcaram 2021. Hugo Nunes, líder da equipa de Inteligência de Ameaças da S21sec em Portugal, conta ao Jornal Económico como, perante o aumento dos ciberataques, houve cada vez mais *hackers* a conseguir dados e acesso a computadores infetados para os colocarem à venda. A operação costuma ser feita em mercados negros na "deep web", como o Genesis Market, Russian Market e 2easy Market, onde, mediante pagamento, é possível aceder a equipamentos com vírus, credenciais e dados sensíveis. Em termos de *malwares* bancários, que se propagam através de campanhas de envio de emails com *phising*, destacaram-se o SquirrelWaffle, o Numando, o Guildma e o Infostealers.

Neste estudo, a que informações chegaram sobre Portugal?

É um estudo global, que envolveu 101 países. Não temos dados concretos sobre Portugal, mas digamos que Portugal não está imune e estará relativamente na média da União Europeia. Só fazemos essa divulgação de percentagens de afetação em relação ao tipo de ameaça, como o *ransomware*, porque temos maior visibilidade sobre as vítimas, o que aqui não se consegue aferir com tantas certezas. Infelizmente, o sector bancário em termos de risco é maduro, porque consiste numa fonte de rendimento constante, que movimenta volumes de dinheiro consideráveis e torna-se primordial em termos de ciberataques até devido à crescente utilização de telemóvel para tudo.

O sector bancário é o principal alvo?

É muito apetecível. As vítimas têm sempre uma componente financeira associada. A banca será sempre alvo constante e não acreditamos que vá acabar. Em relação aos bancos tradicionais e aos digitais, têm riscos diferentes. Será mais possível na banca online, porque o ataque poderá acontecer tanto de Portugal como de Espanha, França, Israel… Há uma multiplicação de potenciais agressores. Na banca tradicional, em termos físicos, se alguém quiser assaltar um banco tem muitos parâmetros que desconhece. A exposição à internet acarreta outros riscos. Mas as infraestruturas críticas, entre as quais logística, energia ou telecomunicações, são sempre alvos apetecíveis por cibercriminosos pelo volume de dados e de negócios.

"Vê-se como os constantes ciberataques entre a Rússia e a Ucrânia, mas o escalar desta situação poderá trazer também a NATO para jogo, para a guerra cibernética"

Segundo a NordVPN, há mais de três mil cartões bancários portugueses à venda na "dark web". É o mesmo número que têm?

Diria que três mil números de cartão de crédito de entidades portuguesas é um número perfeitamente viável. Esse valor não nos choca. Todos os dias nos deparamos com situações novas e faz parte dos nossos dos nossos serviços de *data leaks* para notificar as empresas, entidades bancárias ou empresas financeiras.

Sintetizando, o que é a "dark web"?

De uma forma simples, é a internet escondida, que requer ferramentas próprias e não é possível acederlhe através de um *browser* normal, pois precisa de um *browser* que tenha essa capacidade de interagir com plataformas que estão feitas para garantir mais anonimidade do que a "clean web". Não está indexada como a *web* clara. Se eu for ao Google pesquisar serviços de *homebanking* vai-nos aparecer a lista dos bancos. Na "dark web" não há essa capacidade, porque não é acessível de pesquisável. Mas depois nos fóruns criminosos vão aparecendo pequenos motores de busca direcionados ou páginas de venda de cartões de crédito, etc.

Existem mecanismos que bloqueiem esse acesso, se for malicioso?

Existem mecanismos que bloqueiem o acesso à "dark web", mas são difíceis. Por exemplo, um caso muito recente é do Twitter, que só estava na "clean web", e transportou a sua plataforma também para a "dark web", para permitir a cidadãos que estão na Rússia acederem sem monitorização ou possibilidade de o estado russo bloquear-lhes o acesso. É um protocolo encriptado sem rastreamento acessível ao comum dos mortais. No último mês os acessos à "dark web" até poderão ter estado com um aumento considerável nalgumas geografias, nomeadamente na Rússia, para circundar alguma censura em vigor. Estes últimos acontecimentos mostram que a imagem da "dark web" pode mudar, mas está sempre muito associada a atos ilícitos. É como uma autoestrada: tanto posso estar a andar de forma perfeitamente normal como a transportar droga. Dou-lhe um exemplo muito concreto: as bitcoins. As bitcoins não foram criadas para atos ilícitos mas, por vezes, estão associadas a tal, porque permitem a transferência de dinheiro anónimo.

Portugal está preparado para um contexto europeu de ciberguerra?

O que este conflito vem evidenciar é que uma guerra também passa pela parte online. Nunca estivemos nunca situação assim em que é tão válido um ataque físico como um cibernético. Isso vê-se neste conflito com os constantes ciberataques entre a Rússia e a Ucrânia, mas o escalar desta situação poderá trazer também, por exemplo, a NATO e os países aderentes para jogo, para a guerra cibernética.

O 'ransomware' vai continuar a ser dos maiores tipos de ataques?

Nos últimos três anos, o ransomware tem vindo exponencialmente a crescer porque também consegue ter retorno financeiro substancial. São organizações cibercriminosas bastante capazes e com volumes de negócios, digamos assim, muito elevadas. Temos também algumas tendências a crescer, nomeadamente o *malware* sobre o Android - sobre os nossos telemóveis, porque cada vez mais os estados a utilizar para mais coisas – e os *infostealers*, que são *malwares* específicos para recolha de dados de acessos. Ou seja, se eu tiver esse malware no computador ele vai guardar e transmitir para o seu dono os dados bancários que estou a digitar ou os meus *cookies* da Netflix ou do Continente.pt para depois serem vendidos. Não sei se a cibercriminalidade não terá já ultrapassado outra criminalidade como o tráfico de droga e de armas, porque consegue ser ter uma abrangência e desmaterialização tão grandes. ■

Portugal está na no mapa do cibercrime... mas não é de hoje

A cibercriminalidade tem atingido valores recorde um pouco por todo o mundo, com crescimentos nunca antes visto desde o início da pandemia e ameaças cada vez mais sofisticadas. O teletrabalho e o acesso remoto a redes empresariais são um grande impulsionador desta nova realidade e existe uma necessidade cada vez mais premente para a adoção de estratégias de cibersegurança integradas e robustas, a começar pela formação dos próprios colaboradores.

Portugal não é alheio a esta realidade, muito pelo contrário. Os ciberataques que fizeram manchetes nestas últimas semanas são, apenas, os mais mediáticos, pois este é um fenómeno que tem atingido fortemente as Pequenas e Médias Empresas.

Há já muito que se fala de cibercrime, mas, em Portugal, o flagelo – em particular os ataques de ransomware - tem atingido, sobretudo, as PME. Agora, o mediatismo dos alvos está, finalmente, a colocar o problema na agenda de todos. Porém, as empresas que hoje aparecem nas notícias têm dimensão e capacidade para investir em segurança, mas também a estrutura necessária para aguentar o embate. Infelizmente, nem sempre acontece o mesmo.

Embora não exista acesso a números oficiais, sendo operacionais e lidando com o mercado diariamente, estando no terreno como estamos, percebemos que só nos últimos dois anos foram muitas as PME portuguesas que se viram confrontadas com a dura decisão de terem de fechar portas, porque não conseguiram recuperar os dados sequestrados e tiveram os seus sistemas completamente paralisados; ou pagarem o resgate e ficarem financeiramente comprometidas, pagando a fatura até hoje.

CARLOS VIEIRA
Country Manager da WatchGuard Portugal e Espanha

Não vale a pena reagir precipitadamente na análise aos ataques recentes à Vodafone, Cofina ou aos Laboratórios Germano de Sousa. São diferentes ataques entre si, quer nas técnicas usadas, quer nas motivações por detrás dos mesmos.

O importante é perceber que não somos um país pequeno, ao qual ninguém liga e que escapa até aos radares dos denominados hackers. Não é verdade e, como disse, muito tem ajudado o mediatismo dos ataques, mas isto já acontece há muito.

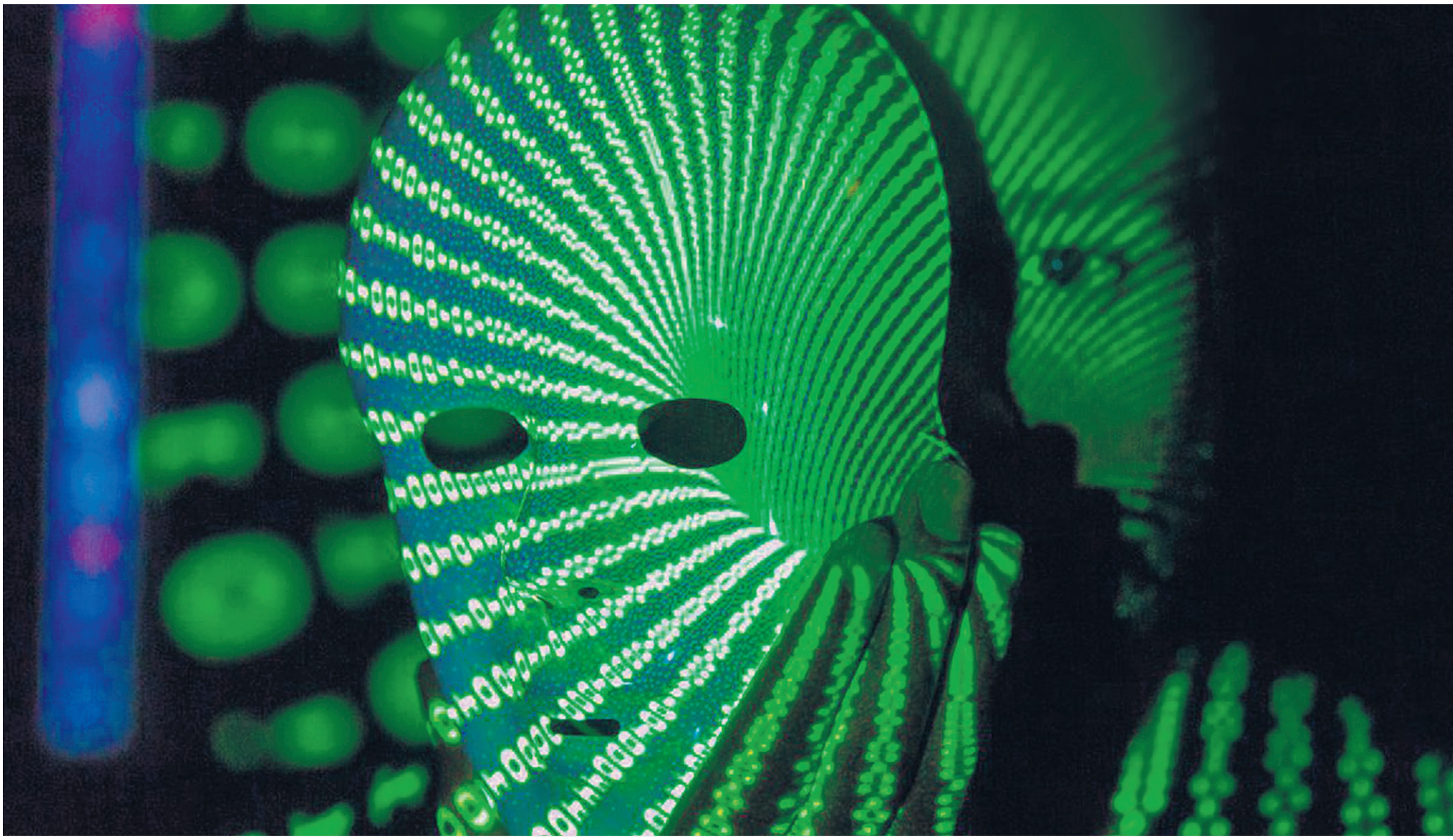
Temos de olhar para as nossas empresas e fazer um raio-x do seu parque tecnológico e informático, perceber as suas necessidades e delinear estratégias de cibersegurança que vão ao seu encontro, protegendo a continuidade e viabilidade do negócio.

Isto passa, nomeadamente, pela formação dos colaboradores em boas práticas e pela adoção de ferramentas e soluções tecnológicas, mas é essencial que haja uma mudança de foco coletiva do tecido empresarial, para que a aposta na segurança seja, cada vez mais, uma realidade e não um tema de debate.

Este é um assunto ao qual as próprias seguradoras estão atentas, como se vê no mercado norte-americano, onde já existe uma vasta oferta em termos de cyber insurance mas onde as empresas se comprometem a seguir escrupulosas guidelines para garantir a utilização de autenticação multi-fator, soluções robustas ao nível da proteção das estações de trabalho e do perímetro e outras: uma série de medidas preventivas que visam reduzir o risco do seguro poder vir a ser acionado.

Portugal está no mapa da cibercriminalidade. Mas pelo menos que algo de positivo saia destes ataques mais mediáticos e que sirvam de alerta para esta pandemia cibernética.

com o apoio WatchGuard



ANÁLISE

“Ciberrisco é encarado com realismo”

“A administração pública encara com realismo, sobretudo no atual contexto geopolítico, o tema da cibersegurança, afirma o contra-almirante Gameiro Marques, diretor geral do Gabinete Nacional de Segurança e membro do Observatório para a Segurança e Defesa da SEDES.

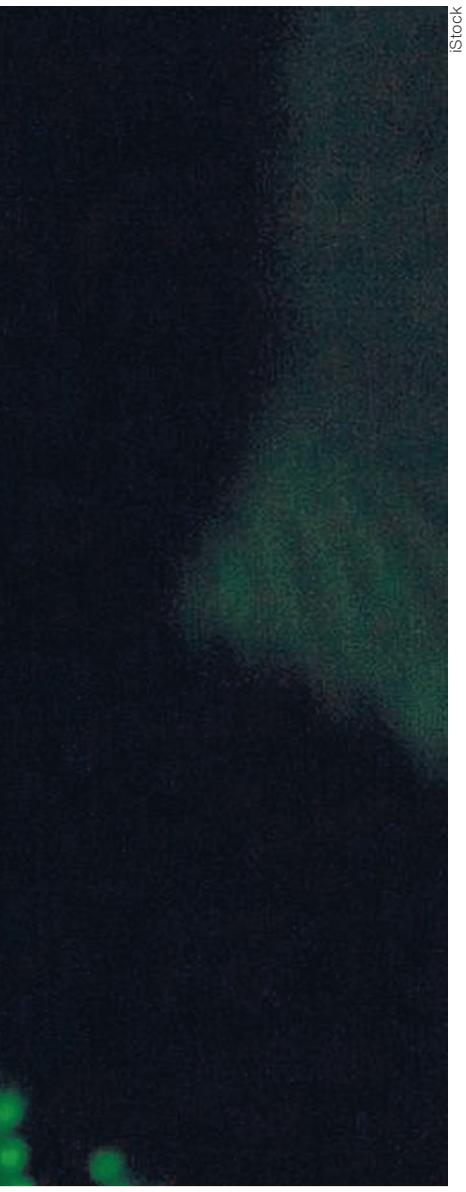
VÍTOR NORINHA
vnorinha@jornaleconomico.pt

O contexto geopolítico obriga a encarar o tema da cibersegurança com realismo. Refere o contra-almirante Gameiro Marques que o Gabinete Nacional de Segurança (que por inerência é a Autoridade Nacional de Segurança) tem vindo “a criar e a ajudar um conjunto de políticas públicas e a colocá-las em prática, através de um plano de ação e de estratégia com indicadores e metas”. Adianta que o Gabinete presta provas junto do parlamento todos os anos, são lançadas iniciativas de formação e de sensibilização, “comunicamos de forma regular através das redes sociais e trabalhamos em grande parceria com outros atores, caso dos serviços da Defesa Nacional relacionados com este tema, os Serviços de Informação da República e a Unidade de Cibersegurança da Polícia Judiciária”. Adianta que o tema da cibersegurança na administração pública é “demasiado complexo para não se trabalhar em parceria, é fundamental fazê-lo”.

Questionado sobre o tipo de trabalho que tem vindo a ser desenvolvido, o responsável pelo Gabinete Nacional de Segurança e membro do Observatório para a Segurança e Defesa da SEDES, salientou que o trabalho passa “pela divulgação de um conjunto de boas práticas reais”. Frisou que num recente evento onde estiveram todos os representantes de IT, “o engenheiro Lino Santos (Coordenador do Centro Nacional de Cibersegurança) divulgou um conjunto de boas práticas reais e que são também políticas públicas”. E adiantou não estar “apenas a falar na dimensão teórica, mas nas políticas públicas a nível de procedimentos, em assuntos tangíveis que as instituições têm de praticar para manter as estruturas protegidas”. Adianta que essas políticas são feitas “ao recomendarem boas práticas para o setor privado, em particular aquelas que por via da lei estabelece o regime jurídico do ciberespaço e que estão na nossa jurisdição. Refiro-me ao caso dos prestadores de serviços digitais, e que todos têm de cumprir normas que foram recentemente sujeitas a um exigente processo de divulgação dos mesmos e que estão a decorrer”. No início de abril os eventos decorrem no distrito de Évora, sendo que este processo de divulgação das melhores práticas começou a 14 de março e decorrerá até 27 de abril em todos os distritos do país, incluindo as Regiões Autónomas. Refere o diretor geral do Gabinete Nacional de Segurança que estão abrangidas mais de um milhar de pessoas, as quais são responsáveis pelo cumprimento legal no que se refere à implementação das boas práticas de cibersegurança. Adianta o quadro que neste mês e meio de formação serão abrangidos prestadores de serviços digitais, operadores de serviços essenciais e, em geral, toda a comunidade que está abrangida pela lei do ciberespaço. As normas sobre este tema são de 2018 e de 2021, sendo que o enquadramento normativo foi alvo de um novo regulamento em fevereiro último e que pormenoriza tudo o que é necessário fazer por cada uma das entidades envolvidas. A formação que está a decorrer “é focada nestes pormenores”, adianta a mesma fonte.

António Gameiro Marques
Contra-Almirante, Diretor Geral do Gabinete Nacional de Segurança

Relativamente a outros países europeus e no comparativo a nível de implementação de procedimentos o contra-almirante Gameiro Marques salienta que Portugal segue de muito perto todas as orientações com origem na União Europeia. Adianta que o crescimento que o país tem tido em termos de incidentes de cibersegurança ”acompanha de muito perto o que se tem passado no resto da UE”. E reforça que se registou um aumento de incidentes desde o início do ano, algo que considera expetável perante a situação geopolítica vivida na Europa. A nível de implementação de regras e procedimentos o país tem vindo a progredir rapidamente. Salienta a mesma fonte que neste ranking de cibersegurança e tendo em conta os dados da ITU – União Internacional de Telecomunicações, o país passou do 25º lugar na Europa para um 8º lugar. Gameiro Marques reconhece que “há um longo caminho a percorrer”, sendo relevante a aposta feita ao nível dos recursos humanos. Refere que no PRR foi possível inscrever projetos nesta área e que “vão ser estruturantes para a capacitação do país como um todo nesta matéria”. Adianta que o problema que recorrentemente se depara é a questão das pessoas. “Somos competitivos a atrair pessoas para trabalhar à saída das universidades, mas quatro ou cinco anos depois são convidadas por terceiros e embarcam em outros proje-


iStock

tos, quase sempre do setor privado. Estes têm mais capacidade atrativa do que nós na componente remuneratória. Mitigamos tudo isto investindo muito na formação e na qualidade a nível de cibersegurança e, desta forma, acabamos por conseguir reter muitos quadros de alto nível nas nossas fileiras".

Guardiões de informação

A temática do risco cyber para a administração pública é complexo, refere Carlos César, especialista em Sistemas de Informação, Segurança e Comunicações. Refere que "as organizações públicas são, por força da sua razão de existir, os guardiões de informação de qualquer pessoa e de qualquer organização pública, privada ou do terceiro sector. São elas que regulam o funcionamento de qualquer setor da economia e por vezes são elas que detêm o controlo operacional dos sistemas mais críticos para o funcionamento da sociedade, devendo por isso mitigar o risco com forte atenção em qualquer dos vetores acima referidos. Por vezes assistimos à contratação de verbas avultadas para "sistemas de segurança de acessos", mas as vulnerabilidades não se colmatam apenas injetando dinheiro nos sistemas pois a preparação dos colaboradores e dos dirigentes é essencial para o bom aproveitamento desses investimentos". Já Sérgio Sá, Associate Partner da EY, Cybersecurity, Consulting Services releva a adoção do Regime Jurídico da Segurança do Ciberespaço, um diploma de 2021. E a nível dos investimentos o mesmo quadro dá o exemplo do PRR e onde estão previstas verbas e metas para a administração pública. A Microsoft, através de Eduardo Antunes, Diretor Executivo do Setor Público da Microsoft Portugal, cita o "Relatório de Defesa Digital" da multinacional e destaca o facto de o cibercrime se ter tornado "uma economia madura, que representa uma ameaça à segurança nacional, à segurança económica e à saúde pública, apresentando um crescimento no número e na sofisticação dos ataques e sobretudo na taxa de sucesso, que passou de 21% para 32% em apenas um ano". Diz, relativamente à administração pública, ser "fundamental o esforço que tem sido feito pelo Estado português na área da segurança cibernética, através do investimento de 30 milhões de euros do PRR para apoio nesta área, contudo é um valor ainda residual dada a dimensão e escala do problema. Este esforço deve ser assumido e partilhado, em larga medida, tanto pelas organizações públicas como pelas privadas, garantindo que há um investimento transversal em cibersegurança para que possamos, assim, tentar minimizar o impacto que estes ataques podem ter na nossa economia e sociedade". E Carla Zibreira, Digital Trust Business Unit Manager na Axians Portugal, refere que "a escassez de quadros, a nível mundial e consequentemente na administração pública, com competências diferenciadas em matérias de segurança, a complexidade organizacional e a heterogeneidade na literacia dos utilizadores digitais em entidades públicas, são os grandes fatores inibidores do processo de gestão do risco de cibersegurança, que se entende cada vez mais exigente pela evolução permanente do contexto de ameaças e risco no ciberespaço". E reforça o papel da regulamentação que "obrigará a administração pública a endereçar as preocupações inerentes ao risco ciber, buscando o compromisso da gestão de topo, a reserva de fundos de investimento para a implementação de soluções estratégicas de segurança e a capacitação transversal de recursos com responsabilidades de segurança". E neste sentido o especialista em cibersegurança Carlos César conta um episódio recente quando se deslocou a um organismo de referência e que, para além de outras funções, assegura o alojamento de muitos equipamentos e servidores do Estado. Conta: "Após a creditação numa portaria de elevada segurança, dou por mim a entrar sozinho numa sala técnica recheada de servidores de organismos da administração pública. Nunca tal deveria ter acontecido, nunca um visitante pode ter acesso sem acompanhamento a um datacenter, certo? De quem foi a falha de segurança neste acesso físico? Onde falharam os procedimentos ou a supervisão e acompanhamento destas equipas? Mas se este exemplo ilustrativo se refere a um acesso de pessoa física, que ressalta à vista, o que se passará nas camadas invisíveis das redes de comunicação que interligam esses servidores?"

Como proteger

Quais são então os vetores de risco a que os organismos públicos devem dar atenção. Carlos César diz que a resposta é fácil mas a implementação dos modelos é mais difícil. Refere que "no processo de digitalização das suas atividades as organizações ficam cada vez mais expostas e as falhas transformam-se em problemas que passam a ser pontualmente noticiados. O acesso indevido a dados, sejam os tão falados dados pessoais, ou os dados de segredo industrial e empresarial, o sigilo bancário, os segredos de Estado, etc, é o que terá de ser protegido numa primeira fase, mas nunca descurando que o controlo do sistema não seja passado a personagens indesejáveis. Assim outro vetor a ter em conta é risco de controlo indevido de sistemas, controlos aéreos, sistemas de semáforos, distribuição de energia, comunicações, aparelhos de diagnóstico e de apoio à saúde, de gestão de recursos hídricos, e um universo de equipamentos que dependem de software e de conetividade, ou seja, praticamente tudo no momento atual, desde residências, empresas, fábricas, armazéns...". Carla Zibreira, da Axians, define um conjunto de pressupostos para a administração pública: "Definição de estratégia de segurança, contemplando, de modo integrado, os três vetores de influência: pessoas, processos e tecnologia; conhecimento dos ativos de informação a proteger; conhecimento das vulnerabilidades, ameaças e riscos a que está exposta no ciberespaço; definição de políticas de segurança, orientadoras dos requisitos de segurança a salvaguardar e implementar; reforço dos controlos tecnológicos de proteção da arquitetura de segurança quer ao nível da cloud, perímetro, rede e endpoint e nos acessos lógicos quer ao nível do controlo de acessos de utilizador final e utilizadores com privilégios". Outros pressupostos são "a deteção e monitorização de potenciais incidentes de segurança; e a capacitação de resposta e recuperação perante incidentes de segurança". Na opinião de Eduardo Antunes, da Microsoft, "a administração pública deve apostar em abordagens "zero trust" na delineação das estratégias de segurança, que se adaptem melhor à complexidade do ambiente moderno, compatíveis com modelos de trabalho híbridos e que protejam os cidadãos, os dispositivos, as aplicações e dos dados, independentemente da sua localização". E o mesmo quadro reforça a necessidade de atração de talento, algo que o contra-almirante Gameiro Marques já havia enfatizado. Na mesma linha responde Sérgio de Sá, da EY, ao afirmar que a administração pública "deverá estar atenta aos potenciais impactos da materialização dos riscos do ciberespaço, que poderão afetar direta e indiretamente cidadãos, empresas e instituições em larga escala". Carlos César acrescenta que a administração pública tem de "caminhar a uma só velocidade na proteção dos seus sistemas de comunicação e alojamento de serviços e dados. Qualquer porta de entrada numa rede do governo compromete todos os sistemas, direta e indiretamente, a ela ligados. Qualquer acesso indevido à informação de defesa de um Estado compromete a segurança de todos os Estados que a ele estejam interligados por ação e tratados bilaterais ou multilaterais".

Por último, Mauro Almeida, Head of Cybersecurity da NTT Data Portugal, frisa que está "demonstrado que as organizações que prepararam planos de recuperação de serviço e de continuidade de negócio, que incluam cenários de ciberataque, lidam com esses incidentes de uma forma mais eficiente do que as organizações que não têm estes planos. Embora muitas vezes, na realidade, o impacto de um incidente de segurança cibernética nunca reflita totalmente que foi planeado, a verdade é que a preparação e execução de simulacros, com base nestes planos, criam uma mentalidade de consciencialização e melhoram a cooperação das equipas numa situação de crise. Como diz um velho ditado militar - os planos são inúteis, mas o planeamento é indispensável". Conclui o gestor que é crítico que do lado das pessoas "compreendam e percebam o impacto que as suas ações terão dentro das organizações ou até mesmo nas suas vidas pessoais". ■

ANÁLISE

Seguradores com o dilema da complexidade das ameaças

Os riscos cibernéticos são realidades com diversidades e complexidades que constituem um desafio para os seguros e resseguros.

VÍTOR NORINHA
vnorinha@jornaleconomico.pt

Os desafios aos seguradores perante as ameaças cibernéticas são muito grandes e pelos exemplos conhecidos as perdas têm sido extraordinariamente elevadas. Refere Luís Sousa, Cyber Risk Specialist da Marsh Portugal que estes riscos ainda estão "em fase de amadurecimento". Refere Ricardo Azevedo, diretor técnico da Innovarisk, que "à imagem do mundo tecnológico, no crime informático a velocidade dos acontecimentos e as constantes mutações das diversas formas de perpretação desses crimes têm colocado imensos desafios aos seguradores, obrigando-os a fazer um acompanhamento muito rápido e constante da evolução do risco. Face à dimensão de vários ataques a empresas e organizações, as perdas têm sido elevadas". E Pedro Pinhal, Diretor Técnico e Sinistros da MDS Portugal afirma que a ameaça cibernética deixou de ser apenas emergente "para passar a ser, definitivamente, presente, global e em vias de se tornar sistémica. Esta ameaça afeta de forma transversal toda a sociedade, isto é, cidadãos, famílias e organizações, sejam elas de pequena, média ou grande dimensão".

Luís Sousa, por seu lado, acrescenta que este ramo recente dos seguros assenta "essencialmente em dois drivers: a vontade dos seguradores de fazerem crescer o seu portfólio nesta linha, por um lado, e a diversidade e complexificação das ameaças, por outro. Esta realidade encontra-se descrita no "The Changing Face of Cyber Claims 2021", relatório que a Marsh, em parceria com a Microsoft, a CMS e a Kivu, elaborou pelo segundo ano consecutivo e no qual se abordam as principais tendências de resposta ao crescente protagonismo do risco cibernético, sem esquecer a análise da crescente frequência e severidade dos ataques cibernéticos - com especial incidência para os eventos relacionados com ransomware.

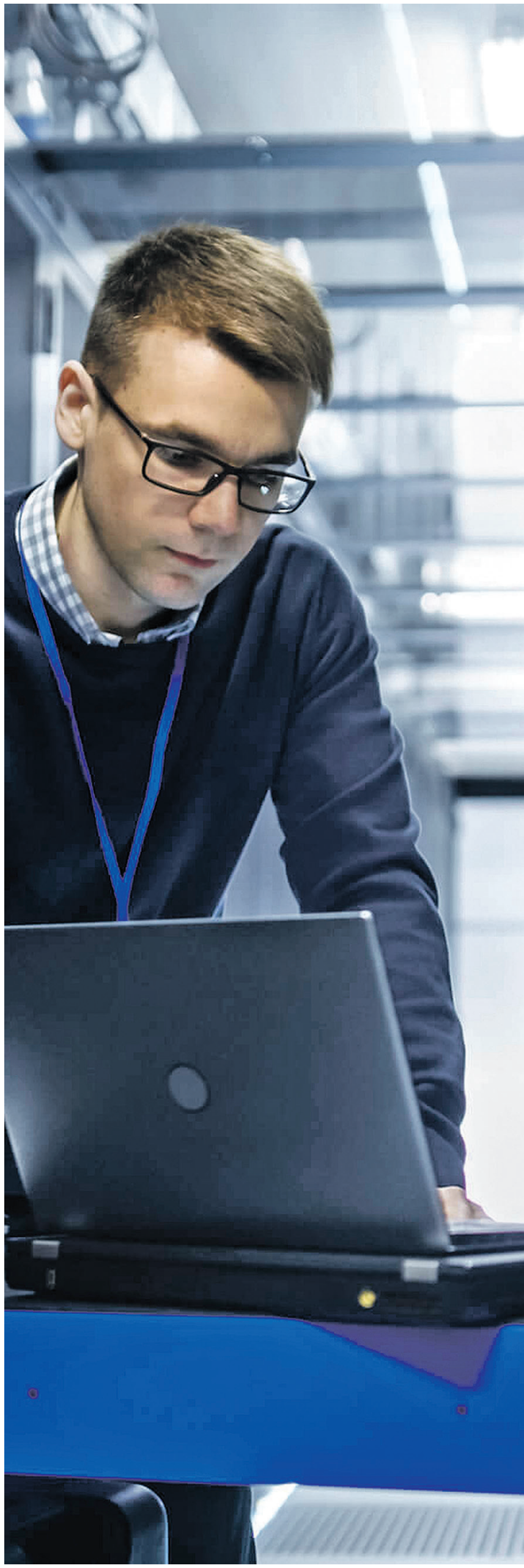
Em termos de evolução do risco, os analistas afirmam que os mercados estão a exigir maior maturidade por parte dos tomadores de seguros "e que é, na maior parte das vezes, acompanhada por um investimento crescente das organizações na robustez da sua infraestrutura digital", acrescenta Luís Sousa da Marsh Portugal. E Ricardo Azevedo salienta que perante mais do que expandir a oferta a nível de coberturas das apólices cyber, "os seguradores têm procurado essencialmente agir a dois níveis: desenvolvendo por um lado melhores mecanismos de compreensão do risco dos seus clientes; e por outro lado, "endurecendo" os termos de aceitação dos riscos que tomam, o que se reflete depois num nível de preços mais elevado, num nível de cobertura mais restritivo e genericamente num acesso mais difícil às próprias apólices". Na mesma linha está Pedro Pinhal que afirma estarem os seguradores "a aumentar o nível de rigor e cuidado das análises de risco e subscrição, solicitando um maior volume e detalhe de informação".

O que explica o aumento do risco cibernético é o avanço da transformação digital e a hiperconetividade associada à pandemia de Covid-19

Refere Pedro Rego, CEO da F. Rego, que "numa ótica de serviço, em caso de ataque, os seguros cyber cobrem as despesas inerentes à contratualização de especialista em cibersegurança, investigadores e auditores jurídicos, bem como advogados, consultores de relações públicas e demais profissionais necessários para o cenário de pós-crise. Em adição, a indemnização inclui, igualmente, as perdas de lucro líquido decorrentes da interrupção do negócio, bem como os custos de defesa por violações de privacidade". Por seu lado, Ricardo Negrão, Head of Cyber Risk da Aon Portugal, frisa que este seja um seguro "muito difícil e obter, muito pela limitação do capital existente no mercado de seguros para este risco e pela baixa maturidade das organizações do ponto de vista de cibersegurança". E dá o exemplo da guerra na Ucrânia onde "existe uma guerra cibernética e uma ameaça para o ocidente de ataques cibernéticos de retaliação", um cenário que está a originar "uma forte retração do mercado segurador para estes riscos, alterando a qualificação técnica do ponto de vista da cibersegurança, passando a ser mais exigente, o que leva a um consequente aumento dos prémios".

Risco aumenta

E o que explica o aumento do risco cibernético é, na ótica de Pedro Pinhal, "o avanço da transformação digital, a hiperconetividade associada à pandemia de Covid-19 e a incrível escalada de ataques cibernéticos, com especial predominância, nos últimos tempos, para os ataques de ransomware e os ataques aos supply chains digitais e às infraestruturas". O quadro da MDS reafirma que as organizações estão, mais do que nunca, dependentes da tecnologia e da informação, bem como interconectadas a ecossistemas digitais alargados e de digital supply chain (fornecedores, parceiros, etc). Esta dependência "gera vulnerabilidades, cujo controlo total é impossível de ter,




Shutterstock

aumentando significativamente as oportunidades para os cibercriminosos explorarem, de forma organizada e estruturada, causando disrupção e maximizando danos e lucros indevidos".

Onde está a proteção

E as empresas procuram proteger-se. Esta é uma área "onde se mantém um forte desconhecimento e assunções erradas do mercado", afirma Pedro Rego, CEO da F.Rego. Adianta que "as recentes ondas de ataques (o mais recente aconteceu com o grupo Sonae) em grandes empresas aumentou os níveis de alerta". A dimensão é relevante, assim como a existência, ou não, de meios próprios para a proteção digital. Refere Ricardo Azevedo da Innovarisk que a forma como as empresas encaram a gestão e risco "difere muito consoante a dimensão da empresa ou a área de atividade (…), o que ditará também o grau de prioridade que colocam em cima da mesa na altura de olhar para estas questões". Adianta que este tipo de visão se reflete, "não só na articulação dos vários instrumentos possíveis de mitigação do risco (por exemplo, a decisão de conjugar o investimento na segurança informática com a aquisição de uma apólice de cyber), como também no interesse com que olham para o seguro e para as diferentes componentes que o mesmo oferece. É natural que uma pequena empresa, sem um departamento informático próprio, possa ver um interesse particular em poder utilizar o serviço de assistência que tipicamente estas apólices oferecem. Por outro lado uma grande empresa que tenha meios próprios do ponto de vista da segurança digital olhará porventura com maior interesse para as coberturas de perda de lucros, na medida em que um ataque que possa paralisar a empresa é algo que pode sair de facto muito caro". Luís Sousa, da Marsh Portugal, refere que a nível de mitigação dos impactos financeiros perante um sinistro deste tipo, as empresas procuram "soluções de transferência de risco tailor-made, com clausulados adaptados à sua realidade, setor de atividade e modelo de negócio". Refere este técnico que é "essencial investir na formação das pessoas, na preparação da tecnologia e na criação de meios de prevenção, fornecendo acessos seguros aos recursos empresarias - proteção dos endpoints, dos dispositivos móveis e das ligações de rede, seja em casa ou nos escritórios. As empresas deverão ter os seus Planos de Continuidade de Negócio / Planos de Resiliência assentes numa estratégia de cibersegurança bem definida, com investimentos a médio e longo prazo e com recurso a mecanismos de transferência de risco por forma a aumentarem a probabilidade de serem bem-sucedidas na resposta aos possíveis impactos de um incidente cibernético. Não se trata, hoje, de um nice-to-have, mas antes de uma necessidade que exige respostas obrigatórias".

Diz ainda Pedro Rego que as preocupações das empresas "focam-se na transferência dos riscos decorrentes de uma tentativa de intrusão, mas igualmente na proteção dos dados de clientes e parceiros". Por seu lado, Pedro Pinhal, da MDS, frisa que "o investimento em planos de gestão de risco cibernético e em soluções de seguro não tem sido proporcional". Adianta: "Correndo o risco da generalização, temos a perceção de que as organizações de maior dimensão têm vindo a aumentar o investimento em cibersegurança e seguros cyber, no âmbito da implementação de estratégias de gestão do risco cibernético. Porém, esta realidade não se observa nas pequenas e médias empresas. De facto, a penetração do seguro cyber neste segmento é ainda muito reduzida, com investimentos pouco significativos. Existe ainda uma grande discrepância entre a ameaça que o risco cibernético representa e as ações que estão a ser implementadas pelas empresas, governos e outras instituições para a sua gestão. Para sobreviverem a esta crescente ameaça, as organizações têm de elevar a gestão dos riscos cibernéticos a um patamar estratégico e abordá-lo ao nível da gestão de topo". Já Ricardo Negrão, da Aon Portugal, diz que as empresas procuram essencialmente "o suporte na capacidade de resposta a incidente de segurança e análise forense, pois apesar de existirem em Portugal competências, não existem em quantidade suficiente". Alerta ainda que a apólice cyber cobre os incidentes que originam a paragem do negócio e que levam a perdas de exploração e de dados em terceiros. Por último, Ricardo Azevedo, da Innovarisk, afirma "ser natural para uma pequena empresa, sem um departamento informático próprio, possa ver um interesse particular em poder utilizar o serviço de assistência que tipicamente estas apólices oferecem. Por outro lado, uma grande empresa que tenha meios próprios do ponto de vista da segurança digital olhará porventura com maior interesse para as coberturas de perda de lucros, na medida em que um ataque que possa paralisar a empresa é algo que pode sair de facto muito caro". Um relatório recente produzido pela Deloitte e encomendado pela Vodafone (uma das entidades que foi recentemente alvo de ataque informático) revela o problema a nível de recursos humanos do país. Afirmam os analistas que o país precisa de mais de 270 mil especialistas de TIC para atingir os objetivos da "Década Digital" definidos pela Comissão Europeia, sendo que entre 2019 e 2020 o número desses especialistas aumentou apenas 9%. Adianta ainda o relatório que apenas 21% das empresas em Portugal usa serviços de comutação em cloud, o que fica 54 pontos percentuais aquém do objetivo de 75%, a atingir em 2030. Adianta o documento que "os serviços da cloud podem ajudar a aumentar a segurança de dados, contribuir para uma maior eficiência, ajudar as empresas a crescer, gerar conhecimento e reduzir custos". ■

A SUA EMPRESA ESTÁ PROTEGIDA?

As ameaças às infraestruturas das TI multiplicam-se. Há, assim, uma necessidade permanente de garantir a eficácia dos procedimentos de cibersegurança, de forma contínua, com especial atenção para a construção de uma verdadeira cultura de segurança transversal em todas as organizações.

SEGURANÇA NO ADN DOS PROCESSOS DE UMA ORGANIZAÇÃO

Ter uma estratégia de segurança eficaz e bem estruturada na empresa é um passo importante para a elaboração e implementação de ações e ferramentas mais eficazes e inovadoras. A prevenção e a preocupação com a cibersegurança devem estar presentes em todos os processos de uma empresa.

AUTENTICAÇÃO MULTIFATOR

É uma das ferramentas mais eficientes para melhorar a segurança no acesso às aplicações e, assim, proteger a empresa e os dados contra ameaças. É um método de autenticação seguro, que exige que os utilizadores provem a sua identidade, fornecendo duas ou mais evidências ao fazerem login.

SASE COMPLEMENTANDO SD-WAN

Secure Access Service Edge (SASE) é uma arquitetura de rede, que combina tecnologias de recursos VPN e SD-WAN com funções de segurança nativas na nuvem, como gateways da Web seguros, agentes de segurança de acesso à nuvem, firewalls e suporte de zero trust networking, que consiste no acesso baseado no utilizador, dispositivo e aplicação, e não na localização e endereço IP.

MICROSEGMENTAÇÃO

É um princípio fundamental de segurança dos sistemas de informação que permite isolar cargas de trabalho e protegê-las individualmente, pela criação de pequenos Data Centers virtuais dentro do seu Data Center e com a segregação de segmentos de rede.

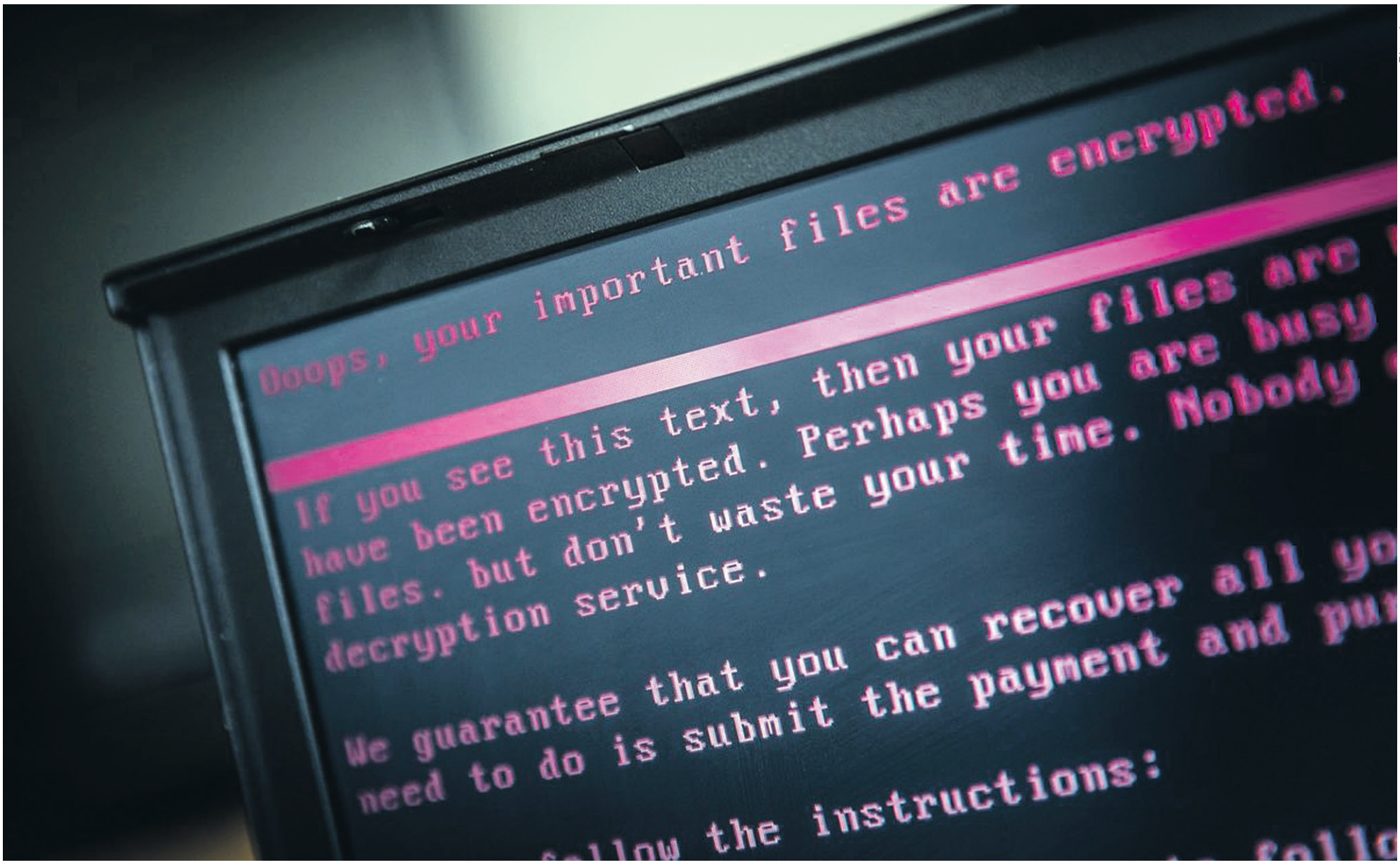
SENSIBILIZAÇÃO DOS UTILIZADORES PARA A PROBLEMÁTICA

Há uma necessidade imediata de especificar as medidas a serem adotadas em resposta aos incidentes, ameaças e vulnerabilidades.

VISIBILIDADE E ANALÍTICA NA MIGRAÇÃO PARA CLOUD

É fundamental dotar as organizações com soluções que forneçam proteção contra ameaças e informação sobre segurança contextualizada para a Cloud Pública, permitindo que as equipas de TI tenham acesso, a todos os ativos de IaaS, PaaS e SaaS e que controlem atividades realizadas na Cloud.

A segurança da informação resulta do conjunto de vários fatores dos quais se destacam as pessoas, as ferramentas e os processos. **O seu negócio não pode parar!** Saiba como podemos ajudá-lo, contacte-nos.



Bloomberg

UCRÂNIA

Número de ataques semanais a organizações portuguesas sobe 9% com guerra

A tendência de subida dos ataques informáticos a organizações é global, com os especialistas a falarem numa tentativa de aproveitamento por estes grupos do conflito na Ucrânia. Literacia digital é cada vez mais importante nas empresas.

JOÃO BARROS
jbarros@jornaleconomico.pt

A ameaça de ataques cibernéticos aprofundou-se com o conflito entre ucranianos e russos, observando-se já um aumento de 9% nas investidas desta natureza a nível global e nacional desde o início da invasão. Isto coloca um foco acrescido nas necessidades de cibersegurança do tecido empresarial português, onde não abunda a literacia digital e os recursos para fazer frente a estas ações organizadas são escassos.

A cibersegurança é uma das principais preocupações dos países europeus no contexto da guerra na Ucrânia, dada a probabilidade de retaliações russas na forma de ciberataques em larga escala aos sectores público e privado do Velho Continente. Esta era uma ameaça que já se verificava antes do conflito no leste europeu, como demonstra o aumento de 81% no número de ataques semanais médios que as empresas portuguesas sofreram no ano passado, mas os dados da Check Point Research confirmam um aumento desde o início do conflito.

Na semana passada, o número de ataques a organizações portuguesas foi 19% superior ao registado antes da guerra, sendo que a média semanal desde o início do conflito é 9% mais alta do que antes em Portugal e no resto do mundo. Esta é, portanto, uma tendência mundial com maior expressão nos países diretamente envolvidos no conflito: a Ucrânia regista um aumento de 39%, enquanto a Rússia verifica mais 22% de ataques, em média, por semana.

Rui Duro pede aos gestores nacionais que "se mentalizem que esta já não é uma questão de se vão sofrer um ciberataque, mas sim quando é que isto acontecerá"

Rui Duro, Country Manager da Check Point Software Technologies, refere que este cenário sugere uma tentativa de aproveitamento por parte de cibercriminosos de "todas as oportunidades que têm" e que têm crescido com a invasão russa da Ucrânia, o que coloca dificuldades acrescidas a um tecido empresarial dominado por micro e pequenas empresas como acontece em Portugal.

"Apesar de a cibersegurança ser cada vez mais uma preocupação junto dos gestores de TI, há ainda um desfasamento entre o avanço das ameaças e as capacidades de proteção das soluções de cibersegurança implementadas. Por outro lado, em Portugal, ainda existe muito aquela ideia de que, por estarmos no cantinho da Europa e sermos um país pequeno, não seremos visados", expõe.

Assim, Rui Duro pede aos gestores nacionais que "se mentalizem que esta já não é uma questão de se vão sofrer um ciberataque, mas sim quando é que isto acontecerá", falando num "trabalho de sensibilização para fazer, seja junto dos próprios gestores, como também das equipas, que muitas vezes não adotam as práticas de segurança necessárias no dia-a-dia".

Esta é uma das prioridades

enunciadas por vários responsáveis de segurança de empresas membros da Associação Portuguesa para o Desenvolvimento das Comunicações (APDC) contactados pelo JE, que colocam na formação dos recursos humanos e na literacia digital uma das principais prioridades para o incremento da resistência a investidas desta natureza. De resto, a própria associação tem apostado na oferta de formação em 'Gestão de Redes e Cibersegurança', no contexto do Programa UPskill, uma iniciativa nacional de requalificação profissional para a área das tecnologias digitais, conta Sandra Fazenda Almeida, diretora executiva da APDC.

Ricardo Negrão, Head of Cyber Risk da Aon Portugal, concorda que deve ser feito um forte investimento na sensibilização das pessoas. "É que o investimento em segurança está desproporcionado face aos investimentos grandes na tecnologia e muito poucos na consciencialização das pessoas, que são principal agente de segurança das organizações", argumenta, instigando as organizações a "fazer uma avaliação de risco e identificar os riscos cibernéticos que podem afetar a organização; fazer uma avaliação da maturidade da organização para os controlos de cibersegurança de acordo com os referenciais NIST, ISO 27001 e QNRCS; fazer um inventário dos seus ativos mais críticos; e fazer uma quantificação do impacto que estes riscos representam nos cenários que afetam os ativos críticos".

Por sua vez, Vítor Ventura, identifica outros dois vetores fundamentais. "Há que, tecnologicamente, apostar na adoção de soluções de autenticação fortes, que permitem debelar as consequências do compromisso de credenciais e a ativação inadvertida de software malicioso que pode ser defendida através soluções de defesa de *endpoint*. Por fim, e porque qualquer organização pode ser comprometida, é fundamental ter um plano de resposta a incidentes de cibersegurança testado e revisto periodicamente".

Esta última sugestão foi já tornada uma obrigação para as empresas nacionais, num esforço que Ricardo Negrão que classifica como "muito relevante para as infraestruturas críticas para o país, pois nestas organizações os impactos de um incidente de segurança extravasam o âmbito das organizações e afetam a sociedade de uma forma geral".

Ainda assim, esta tem de ser "uma ferramenta complementar a um Sistema de Gestão de Segurança da Informação (SGSI)", defende Luís Ferreira, Head of Cybersecurity da DXC Technology.

"A elaboração de um plano de segurança tem necessariamente de ser articulado com os objetivos de cada organização e complementado com a sua correta aplicação e constante validação, num processo permanente de melhoria contínua. Num SGSI, este processo tem o nome de PDCA (Plan-Do-Check-Act)", desenvolve. ■

OPINIÃO

Teremos sempre Budapeste

Pedro Latoeiro
Fundador do Center for Cooperation in Cyberspace

Filipe Domingues
Fundador do Center for Cooperation in Cyberspace

Ao mesmo tempo que milhares de soldados começavam, na Ucrânia, a devastar o mundo físico, duas centenas de diplomatas começavam, nas Nações Unidas, a regular o mundo digital.

De facto, e após vários adiamentos devido à pandemia, as negociações para a criação da primeira convenção da ONU contra o cibercrime arrancaram no mesmo dia que a Rússia agrediu a Ucrânia. E logo a Rússia, a principal promotora desta iniciativa diplomática, da qual o Ocidente desconfia profundamente.

Para os EUA e a UE o instrumento legal de referência para contrariar o cibercrime é a Convenção de Budapeste. Lançada pelo Conselho da Europa, foi negociada maioritariamente por procuradores, não por diplomatas, e conta já com 66 signatários, de todos os continentes – mas não com a Rússia.

Os países ocidentais temem que esta convenção seja apenas uma tentativa russa de policiar o ciberespaço, sem contrapoderes ou mecanismos de controlo sobre as ferramentas estatais de vigilância e acusação. Os procuradores europeus receiam que os dois textos não consigam coexistir e acreditam que o único objetivo de Moscovo é substituir a Convenção de Budapeste pela das Nações Unidas, onde a diplomacia russa consegue votos favoráveis de dezenas de países sobre os quais tem influência, também com a ajuda da China

As divisões que existiam à partida agravaram-se, naturalmente, com a invasão da Ucrânia. Na primeira vez que usou da palavra em Nova Iorque, o representante norte-americano perguntou: como querem que nos sentemos a negociar um tratado desta natureza com um país que acaba de violar tão grosseiramente o Direito Internacional e que sistematicamente lança ciberataques contra os seus vizinhos e rivais?

Mas a bipolarização não se esgota na Ucrânia. A fratura política materializou-se logo na definição dos objetivos da futura convenção. Uma vez mais, Washington, Bruxelas e até a Santa Sé defenderam que a proteção das Liberdades Fundamentais e dos Direitos Humanos tem de constituir uma prioridade firme do texto.

A Rússia, por seu lado, defendeu que esta negociação da ONU está mandatada para redigir um instrumento técnico e não uma nova Declaração dos Direitos Humanos. Para a China, a proteção dos Direitos Humanos deve ter em consideração as "diferenças culturais e políticas entre os países", visão partilhada por países como Singapura, Índia, Síria e Irão, cujos regimes beneficiarão de um reforço dos poderes dos Estados que permitam maior vigilância online.

Outro tema de divisão: incluir ou não obrigações para o sector privado. Pátria da Big Tech, os Estados Unidos defendem que a futura Convenção deve ser inteiramente voltada para a relação entre os Estados. Traduzindo: não interferir com os negócios de Silicon Valley. Em contrapartida, a Rússia alega que "sem as empresas, a Convenção não funcionará", já que a maior parte dos dados eletrónicos necessários para as investigações judiciais está nas mãos da indústria. Traduzindo: caros colegas, queremos mesmo acesso e meios de coerção sobre empresas como o Google e o Facebook.

Quanto às atividades cobertas, o mais provável é que a Convenção acabe por abranger tanto crimes dependentes (ataques que só possam ser cometidos com recurso a TIC, como o hacking) como crimes facilitados pelas ferramentas digitais (atividades tradicionais cuja escala ou alcance seja potenciado através de redes de computadores, como o roubo).

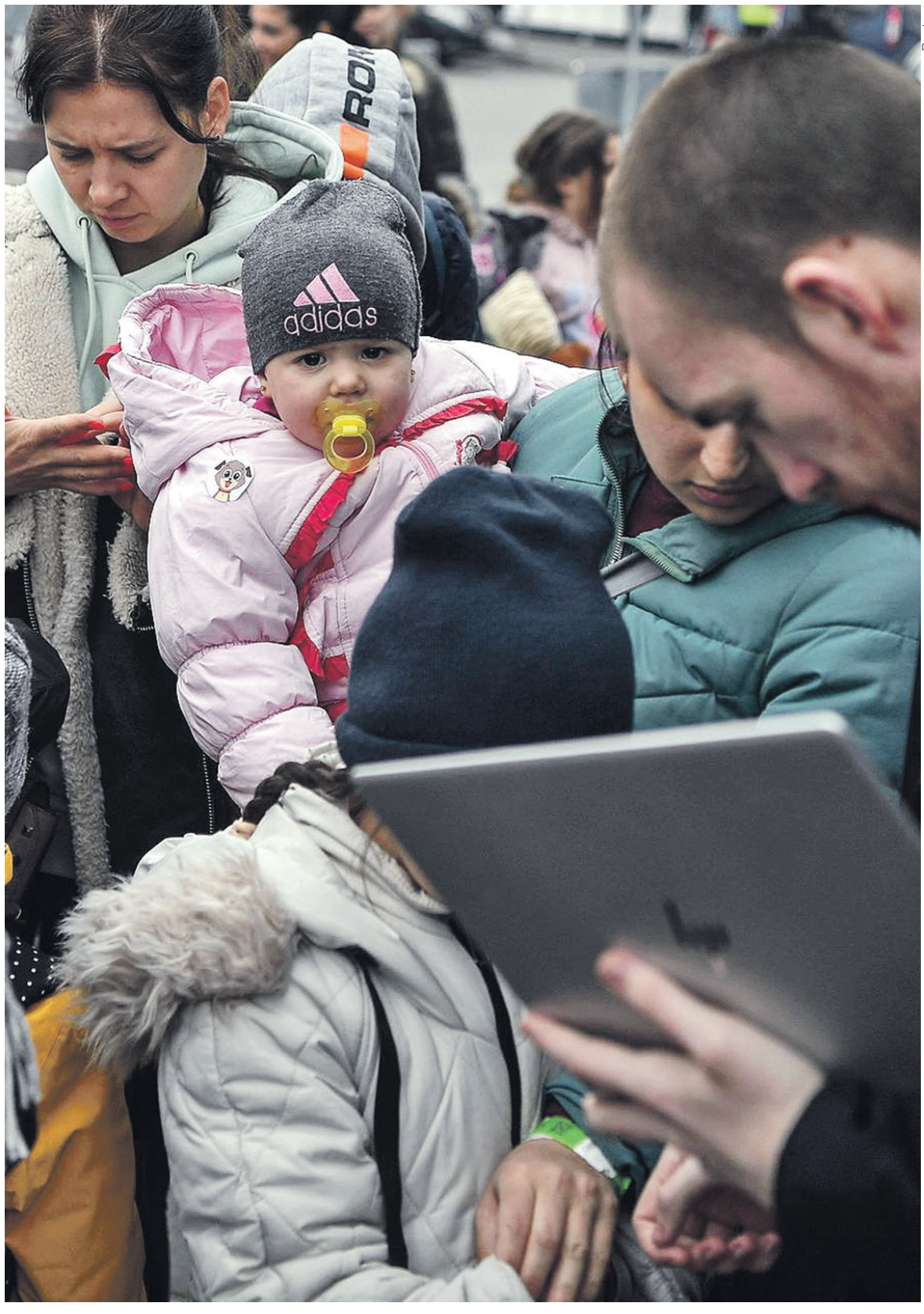
Apesar das divergências entre os negociadores, alcançou-se um consenso sobre os objetivos, o âmbito e a estrutura da Convenção. Contudo, à medida que as negociações forem evoluindo e a substância do tratado for discutida, será progressivamente mais difícil reconciliar as posições dos principais atores. ■

CRIME

Conflito é usado para esquemas de espionagem

Grupos criminosos mundiais estão a utilizar emails falsos de alegadas instituições oficiais e jornais de renome, sobre a invasão russa à Ucrânia, como isco para disseminar 'links' com vírus.

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt


Reuters

Pelo menos três grupos de cibercriminosos mundiais estão a utilizar documentos sobre o conflito entre a Rússia e a Ucrânia para distribuir malware (software malicioso) para incitar as vítimas a cair em esquemas de espionagem informática, concluiu a equipa de investigação da Check Point Software Technologies. A multinacional israelita de cibersegurança traçou, num relatório enviado ao Jornal Económico (JE), o perfil dos *hackers* da El Machete, da Lyceum e da Sidewinder, tendo-se apercebido de que os ficheiros partilhados variam consoante a região do globo e o sector visado. Onde está o isco? Alegadas notícias ou informações de fontes oficiais sobre a guerra na Europa ou mesmo ofertas de trabalho, que na prática são documentos para retirar informação sensível de instituições governamentais, bancos e empresas de energia.

"Neste momento, estamos a ver uma variedade de campanhas APT [Advanced Persistent Threat ou Ameaça Persistente Avançada] que aproveitam a guerra para distribuir *malware*. As campanhas são altamente direcionadas e sofisticadas, focando-se em vítimas de instituições governamentais, entidades financeiras e sectores energéticos. No nosso relatório mais recente, perfilamos e trazemos exemplos de três grupos APT diferentes, oriundos de várias partes do mundo, que apanhámos a orquestrar campanhas de *phishing* direcionado", começa por explicar Sergey Shykevich, *manager* do grupo Threat Intelligence da Check Point Software, no documento facultado ao JE. "Analisámos de perto o *malware* envolvido, e entre as capacidades encontramos desde o *keylogging* à captura de ecrã, e muito mais. Acredito vivamente que estas campanhas têm como motivação principal a ciberespionagem. As nossas descobertas revelam uma tendência clara em que o conflito Rússia-Ucrânia se tornou o tema de eleição dos grupos de cibercrime para ludibriar as vítimas", afirma o especialista.

Os três grupos a que se refere - El Machete (Espanha ou América Latina), Lyceum (Irão) e Sidewinder (Índia, provavelmente) - utilizaram *malware* capaz de: aceder a tudo o que é digitado no teclado (o chamado "keylogging" na linguagem técnica), furtar credenciais (obter as credenciais armazenadas nos *browsers* do Chrome e Firefox), recolher ficheiros (ou informação sobre os ficheiros em cada disco, acedendo a nomes e tamanhos de ficheiros, permitindo o roubo de ficheiros específicos), fazer capturas de ecrã (logo, aceder a imagens privadas, aplicações em utilização ou mensagens), recolher dados da área de transferência e executar comandos.

Check Point Software Technologies traça o perfil de três grupos internacionais: El Machete, Lyceum e Sidewinder

O departamento de investigação da Check Point, a Check Point Research, dá como o exemplo o facto de, em meados de março, uma empresa israelita do sector energético, que não foi identificada recebeu um email de um endereço de um suposto remetente "inewsreporter" (ou seja, como se fosse um meio de comunicação social, com o assunto "Crimes de guerra russos na Ucrânia". A mensagem eletrónica, que depressa se confundia com uma *newsletter* de um jornal conforme testemunhámos, continha algumas fotografias tiradas de meios de comunicação e um link para um artigo hospedado no domínio news-spot[.]live. O link levava o utilizador para um documento com o artigo do britânico "The Guardian" intitulado "Investigadores reúnem evidências de possíveis crimes de guerra russos na Ucrânia". O mesmo domínio servia de endereço para alguns outros documentos maliciosos relacionados com a Rússia e com a guerra Rússia-Ucrânia, como uma cópia de um artigo de 2020 do The Atlantic Council sobre armas nucleares, e uma oferta de trabalho para um agente de segurança privada na Ucrânia, tal como relatam os investigadores.

Nota ainda para a estratégia do grupo de ciberespionagem El Manchete, que enviava emails de phishing direcionados a organizações financeiras em Nicarágua, com um ficheiro Word anexado cujo título era "Planos obscuros do regime neonazi na Ucrânia". O documento continha um artigo escrito e publicado por Alexander Khokholikov, o embaixador russo em Nicarágua, que discutiu o conflito russo-ucraniano a partir da perspetiva do Kremlin. Por sua vez, o SideWinder utilizou como 'minhoca' para as vítimas um documento parecia advir do Instituto Nacional de Assuntos Marítimos da Universidade de Bahria em Islamabad, e apresentava como título "O impacto do conflito russo-ucraniano no Paquistão". Ambos confirmam a tese de que, se os piratas já eram sofisticados, estão agora a ver no conflito uma forma de ser ainda mais (ler páginas anteriores deste especial).

Sergey Shykevich, *manager* de Threat Intelligence, deixa ainda uma proposta para estados e privados: "A minha recomendação para os governos, bancos e empresas energéticas é que reiterem com as suas equipas a importância da cibersegurança, e implementem soluções de cibersegurança que protejam as redes a todos os níveis." ■

“As organizações têm de parar de financiar os cibercriminosos, pagando-lhes os resgates pedidos”

Nos últimos meses várias organizações de relevo em Portugal têm sido alvo de ciberataques. Como classificaria a preparação em Portugal para este tipo de ameaças?
Não podemos comentar nem, ao fazê-lo, generalizar a preparação de Portugal, enquanto país, nesta matéria – mas o que se tem tornado cada vez mais claro é que as organizações um pouco por todo o mundo enfrentam sérios desafios a nível de cibersegurança. A realidade é que, em praticamente todos os países, ainda demasiadas empresas não estão sensibilizadas nem preparadas para se prevenirem contra ciberataques, e menos ainda para lhes dar resposta. Isto é notório pelo sucesso contínuo e sustentado, nas últimas semanas e meses, dos operadores de ransomware e outros agentes de ameaças. Em Portugal, como bem dizem, empresas como o Grupo Impresa ou mesmo a gigante Vodafone provaram estar entre estas empresas que não se prepararam o suficiente – e sofreram as consequências. O seu exemplo tem de valer para as restantes empresas portuguesas se prevenirem a tempo.

A Sophos tem alertado para várias ameaças, como o esquema CryptoRom, ou sobre a crescente utilização do botnet Qakbot por parte de cibercriminosos. Qual é a importância da prevenção no combate ao cibercrime?
Como acontece em muitos outros âmbitos, a prevenção deve ser uma prioridade e pode evitar problemas de maior. Parar as ameaças antes que aconteçam será sempre preferível a ter de corrigir os danos de um ciberataque. Para isto, as organizações necessitam dos instrumentos de prevenção adequados e uma cultura de segurança robusta – as ferramentas podem bloquear as ameaças de forma automática, enquanto a cultura de segurança serve como uma segunda linha de defesa contra ameaças como os ataques de engenharia social. Contudo, como sabemos, a prevenção não é perfeita. Bem perto dela tem de estar a deteção, e logo em seguida a resposta. Os elementos que mencionei acima – não só as ferramentas adequadas, como o pensamento e ação prontos a agir e reagir – podem ajudar as empresas a minimizar e a conter as ciberameaças ativas, e um plano de resposta previamente preparado e testado garante uma recuperação rápida e completa dos sistemas.

Tem aumentado a preocupação com a cibersegurança por parte dos estados e organizações. A guerra da Ucrânia veio aumentar ainda mais o alarme, dado o historial da Rússia. Esta preocupação é justificada?
Existem sem dúvida preocupações relativas a possíveis ataques de retaliação, tanto da Rússia como de grupos criminosos pró-russos. Para além disto, devemos considerar que os cibercriminosos localizados naquele país são, também, menos suscetíveis de mostrarem contenção ou mesmo de serem impedidos pelas autoridades russas. Como membro fundador da NATO e apoiante da Ucrânia, Portugal deve ter isto em conta porque é um potencial alvo a atacar. Uma declaração recente do governo dos EUA alertou, precisamente, para que as organizações estejam preparadas para dar resposta a ataques que surjam neste contexto – e embora esse aviso seja mais dirigido às organizações norte-americanas, a verdade é que também se aplica aos seus aliados e parceiros e, diríamos, um pouco a todo o mundo no geral. Estamos numa situação sem igual e nunca antes vista, o que significa que estamos a percorrer caminhos potencialmente pantanosos. Para além disso, como vimos em 2017 com o NotPetya, os ciberataques têm potencial para causar um impacto muito maior do que apenas o alvo pretendido, pelo que podem ter consequências muito mais amplas do que agora imaginamos.

Diante do crescimento do cibercrime e do ciberterrorismo, que medidas devem as organizações adotar para garantir a segurança da sua instituição, assim como das suas pessoas?
Em primeiro lugar, as organizações precisam de avaliar o seu estado atual de preparação para enfrentar ciberataques, assim como analisar os seus pontos mais fracos. Isto inclui certificarem-se de que estão a aplicar os princípios básicos de TI, como patching, backups e fortalecimento do reconhecimento de identidade, e ainda outros controlos específicos de segurança como o threat hunting. A implementação de uma forte cultura de segurança dentro das empresas contribuirá também para que todos, desde o CEO até colaboradores em qualquer nível do organigrama, saibam porque é que a cibersegurança é essencial para a empresa e como podem reportar e reagir a possíveis incidentes.

Uma das grandes questões da cibersegurança é o que deve fazer a organização ou a pessoa que for vítima de um ciberataque? Há forma de reagir? E o que é que nunca se deve fazer?
A melhor maneira de reagir a um ciberataque é ter um plano. Este deve ser específico e completo, o que significa que provavelmente existirá até mais do que um para diferentes tipos de eventos. O plano deve, por exemplo, listar todas as pessoas que precisam de ser contactadas, como manter o acesso à rede, que sistemas individuais precisam de ser isolados e que ferramentas estão disponíveis para ajudar na recuperação. Também é uma excelente ideia manter cópias físicas desse plano, no caso de toda a rede deixar de estar disponível. As empresas devem, ainda, testar regularmente os seus planos, de modo a assegurar que tudo funcionará em caso de emergência – o que também ajuda a identificar quais as áreas a melhorar. Um bom recurso no geral, para dar os primeiro passos, é a iniciativa “Shields Up” da CISA, bem como o próprio Centro Nacional de Cibersegurança de Portugal. Finalmente, dizer que as organizações têm de parar de financiar os cibercriminosos, pagando-lhes os resgates pedidos, por exemplo. Embora possa parecer uma saída fácil, a verdade é que não resolve o problema de como o sistema foi violado, para começar. O dinheiro que estes criminosos conseguem é, muitas vezes, aplicado novamente nas suas operações, o que certamente piora o problema para todos nós.

ENSINO SUPERIOR

Formação e investigação de qualidade para enfrentar ameaça

Universidades portuguesas respondem aos desafios colocados pela cibersegurança com uma oferta estrturada, participação em projetos de investigação europeus e parcerias.

ALMERINDA ROMEIRA
aromeira@jornaleconomico.pt

O espaço cibernético europeu vai, em breve, ficar mais seguro e há expertise portuguesa envolvida. "É uma atuação inserida no projeto PANDORA", revela António Pinto, do Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência (INESC TEC) ao Jornal Económico. O investigador, que também é professor no Instituto Politécnico do Porto, adianta: "A mais recente atuação do INESC TEC insere-se na partilha segura, confidencial e controlada de informação relativa a ataques e ameaças cibernéticas, usando para tal mecanismos de cifras pesquisáveis."

O projeto envolve 15 parceiros de sete países, conta com um orçamento de 7,6 milhões de euros e ficará concluído em novembro deste ano. Objetivo? Reforçar a capacidade de defesa cibernética da União Europeia, através da conceção e implementação de uma solução aberta para a deteção de ameaças em tempo real e resposta a incidentes, com foco na proteção de postos de trabalho, bem como na partilha de informações.

"Decidir que estamos na presença de um ataque informático requer informação, muita informação, disponível atempadamente, de forma segura e de fontes confiáveis", salienta o investigador.

A União Europeia financia já o desenvolvimento e manutenção de uma plataforma de partilha deste tipo de informação — a plataforma MISP. Embora seja adequada a partilha de informação num contexto empresarial e institucional, a sua aplicabilidade é um pouco mais reduzida no contexto militar ou da Defesa. É justamente esse o contexto a que se destina, para já, o sistema PANDORA.

A solução será integrada e avaliada num ambiente pré-operacional contra dois casos relevantes de utilização: segurança de navios de guerra e segurança da rede de sensores militares.

A ferramenta utiliza técnicas de inteligência artificial e processamento automático para detectar em tempo real um ataque informático. "Ao mesmo tempo que sinaliza o ataque, procura saber mais sobre a sua origem, para fazer uma caracterização e partilhá-lo com outros países para que estes se possam proteger", diz António Pinto.

De acordo com o investigador do INESC TEC, o sistema PANDORA também visa detectar e classificar prontamente ameaças conhecidas e desconhecidas, impor políticas em voo para combater estas ameaças e trocar informações de inteligência de ameaças com terceiros, tanto a nível nacional como internacional.

Na lista de projetos de investigação europeia com contributo português há outro nome a fixar: Discretion. O Instituto Superior Técnico, maior escola de engenharia do país está envolvida num projeto pioneiro para desenvolver redes de comunicação quântica para a defesa e procura fornecer, pela primeira vez, serviços de encriptação de alta segurança de última geração. De referir que Discretion ("Disruptive SDN secure communications for European Defence") liderou a call de financiamento do Programa Europeu de Desenvolvimento Industrial no domínio da Defesa, tendo sido o primeiro classificada no tópico de "Cyber situational awareness and defence capabilities, defence networks and technologies for secure communication and information sharing".

ANTÓNIO PINTO
Investigador do INESC TEC e professor no Instituto Politécnico do Porto

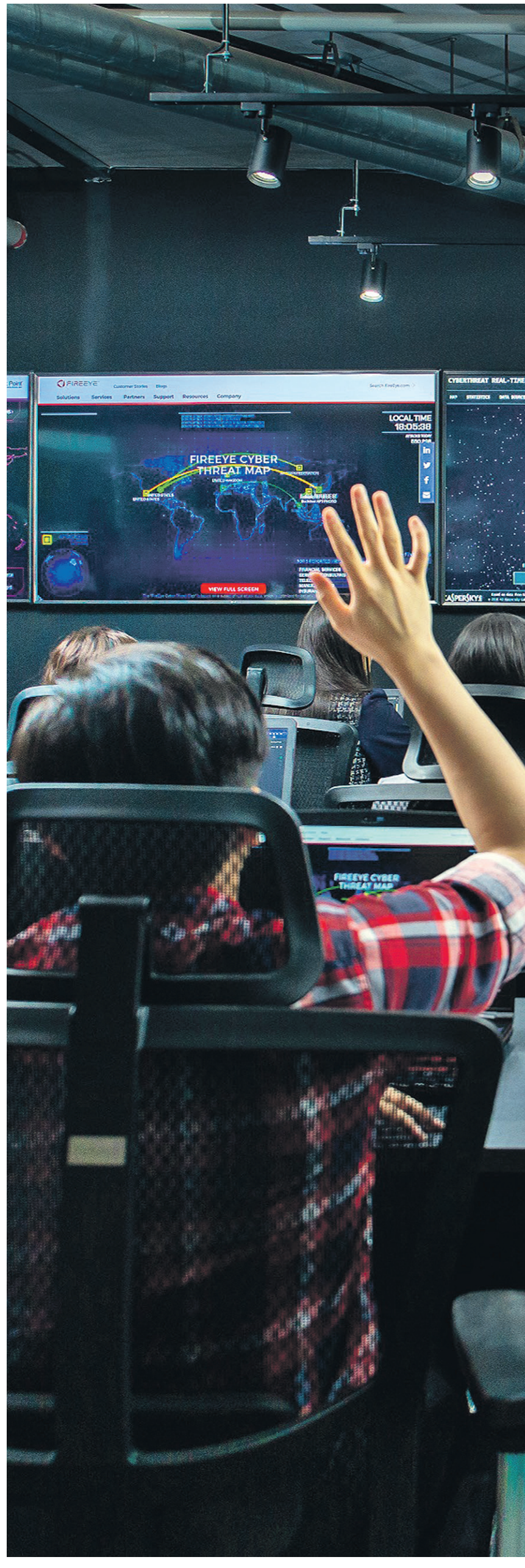
RUI RIBEIRO
Diretor Executivo da LISS – Lusófona Information Systems School

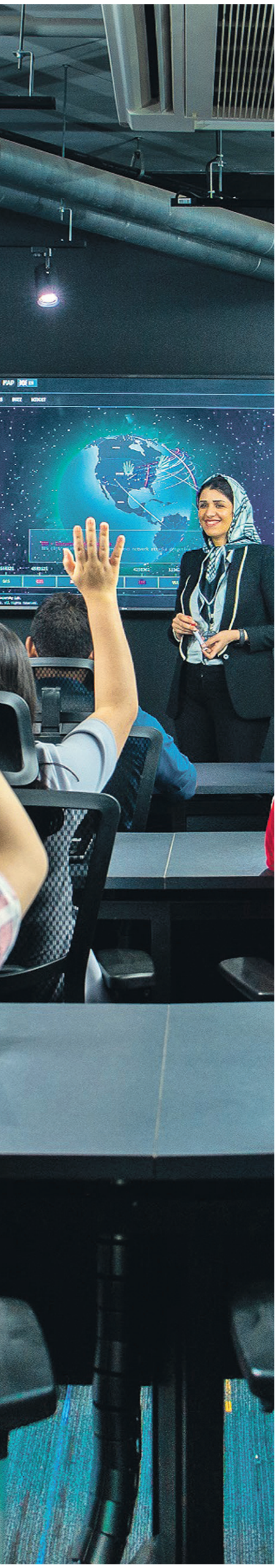
Ideias e negócios

Além do trabalho colaborativo que envolve os seus investigadores, a academia portuguesa é igualmente berço de muitas ideias e cada vez mais negócios nesta área.

A ADYTA é um exemplo. Esta startup focada na cibersegurança e em soluções de comunicação segura, teve a sua raiz num projeto de Investigação & Desenvolvimento realizado na Universidade do Porto, em cuja incubadora UPTEC – Parque da Ciência e da Tecnologia está sediada. A empresa tornou-se conhecida ao detectar uma vulnerabilidade que afetou a Galaxy Apps Store da Samsung a nível global. Para o seu palmarés também contribuiu a auditoria técnica das soluções Office 365 e Azure, da Microsoft, no âmbito do processo de certificação destas soluções pelo Gabinete de Segurança Nacional, o que lhe permitiu ser a entidade técnica a concretizar a primeira certificação cloud realizada em Portugal, concretamente da plataforma Azure.

"Desenvolvemos uma aplicação que permite a comunicação de voz e mensagem encriptada e estamos também a entrar na área das comunicações seguras em ambiente IoT (Internet das Coisas) para 'smart cities'", explicou Carlos Carvalho, CEO da empresa, recentemente na feira de tecnologia do Dubai, como o JE oportunamente noticiou.





Não é só investigação. Portugal tem instituições de primeira linha a ensinar matérias de cibersegurança. A Universidade Lusófona trabalha há mais de 10 anos no desenvolvimento de formações para o mercado empresarial, criando competências técnicas aos alunos dos cursos das áreas de Informática. "É um trabalho contínuo de longa data, que nos permite hoje ter uma consistência e conhecimento elevados na nossa equipa de docentes e parceiros", afirma Rui Ribeiro, diretor executivo da LISS – Lusófona Information Systems School, ao JE.

O professor diz que as parcerias são cruciais, em particular pela elevada velocidade a que as tecnologias e técnicas evoluem. A propósito, adianta: "Desenvolvemos parcerias empresariais para integrarem com técnicos seus como formadores especializados nos nossos cursos e workshops anuais aos alunos das nossas licenciaturas e mestrados, como a Cybers3c e a Layer8. Também estamos a apoiar a Academia Nacional de Cibersegurança nas suas formações de requalificação de profissionais de mercado em profissionais especializados de cibersegurança".

No campo da oferta formativa, a Lusófona tem uma pós-graduação em Segurança Informática e Ethical Hacking, que vai já para a 6ª edição; um MBA de Sistemas de Informação, onde os alunos dispõem de uma Unidade Curricular de ISO27001, que é referência do mercado em melhores práticas de procedimentos de Segurança de Informação; e a Unidade curricular de Segurança Informática nas licenciaturas e mestrados de Informática. Este ano está prevista a participação da equipa Security Team Lusofona, constituída por estudantes em concursos de cibersegurança universitária, e a criação da equipa de cibersegurança no centro de Investigação e Desenvolvimento COPELABS, onde o doutoramento em Informática da instituição está suportado. A realização de ações transversais de sensibilização de cibersegurança à comunidade universitária e o lançamento de cursos específicos para programadores e outro para administradores de sistemas, já no modelo europeu de microcredenciais são outras iniciativas previstas.

Grande parte da oferta em cibersegurança encontra-se no ensino superior público. Na NOVA IMS, nas Faculdade de Ciências e Tecnologia, nas Escolas de Engenharia, nas Universidades de Aveiro e do Minho só para citar algumas.

A UMinho é uma das principais instituições nacionais ao nível do ensino, investigação e interação na área da cibersegurança. Em duas licenciaturas e cinco mestrados existem disciplinas sobre o temática, a que se soma uma formação avançada em Cibersegurança, através da interface TecMinho. Nos últimos anos houve ainda uma pós-graduação em Cibersegurança e Ciberdefesa, em parceria com a Academia Militar de Lisboa.

Em termos de projetos I&D e ações de extensão, salienta-se o Centro de Investigação em Justiça e Governação (JusGov), afeto à Escola de Direito, que produziu o "Relatório Cibersegurança em Portugal – Ética & Direito", a pedido do Centro Nacional de Cibersegurança.

Na Universidade de Aveiro destacamos o Mestrado em Cibersegurança, cuja primera fase de candidaturas arranca dentro de quinze dias. O curso está alinhado com a oferta formativa interna da instituição no domínio da informática e com as estratégias nacional e europeia do sector. Pretende-se, entre outros objetivos, dotar o tecido empresarial da região, nacional e internacional de quadros superiores habilitados na área da cibersegurança e fomentar uma formação avançada centrada em inovação, desenvolvimento e investigação em cibersegurança.

No ISEG Executive Education tomamos como exemplo uma pós-graduação igualmente bem sucedida: Auditoria, Risco e Cibersegurança. A formação, cuja terceira edição arranca a 29 de abril, oferece ferramentas para o desenvolvimento de uma melhor capacidade de recolha, organização e análise de informação nas organizações, visando melhorar a tomada de decisão. Destina-se a profissionais de gestão, economia, contabilidade, sistemas de informação, auditoria interna e risco, que no final, deverão estar aptos a inovar e desenvolver metodologias eficazes de gestão do risco, de controlo de custos de contexto, além de prevenção, deteção e investigação.

"No cenário atual, a pós-graduação em Auditoria, Risco e Cibersegurança cria uma resposta a uma necessidade de mercado nacional e internacional, que apresenta escassez de recursos nesta área", afirmam os coordenadores Fátima Geada, diretora de auditoria do grupo TAP e presidente do Instituto Português de Auditoria Interna, e Sérgio Nunes, consultor nesta área da especialidade e membro fundador da AP2SI.

O talento qualificado é ainda escasso e as empresas enfrentam a necessidade de o reter. Já este ano foi criada a Academia de Cibersegurança da Critical TechWorks, formada entre a Critical Software e o BMW Group. Tem um propósito bem definido, como justifica Paulo Lourenço, Chief Information Security Officer: "O lançamento desta Academia de Cibersegurança reflete uma preocupação que tem ganho expressão nas empresas e, ao mesmo tempo, visa uma questão de retenção de talento, que também é muito importante para nós, uma vez que procuramos pessoas que tenham continuidade, façam carreira connosco e sintam que crescem com os desafios a que nos propomos".

Em Portugal, diversas organizações de primeira linha foram alvo de ciberataques particularmente violentos nos primeiros meses de 2022. Foi o detonador. A procura por especialistas disparou, o que faz aumentar as oportunidades de formação, deixando antever o lançamento de novos programas. ■

FÓRUM

Empresas devem preparar-se para recuperação rápida dos ataques

É inevitável o aumento do ciberrisco e das tentativas de entrada nos sistemas informáticos por parte de intrusos. Portanto, os especialistas defendem a procura de soluções que reponham, em pouco tempo, as operações impactadas.

Que aprendizagem ficou dos recentes ataques cibernéticos em Portugal que, além das repercussões internas, tiveram impacto nos consumidores e cidadãos em geral? O que devem fazer os gestores das empresas?

LUÍS SOUSA
Presidente da ASSOFT - Associação Portuguesa de Software

O cibercrime é hoje um espaço profissional, objeto de grandes investimentos por parte dos grupos criminosos, com objetivos muito concretos na geração de lucros. A maior vulnerabilidade das organizações ao cibercrime está nas suas pessoas, na maior parte dos casos, por ingenuidade ou ignorância. Se uma organização não tiver capacidade para investir em cibersegurança, no mínimo, treine os seus colaboradores nos cuidados a ter, nomeadamente habituando-os a verificar os endereços da correspondência que recebem e a nunca abrir ficheiros anexos. Mas há coisas simples que todas as empresas podem implementar: 1 - Treinar os colaboradores em cibersegurança. Sabendo que as pessoas são a principal vulnerabilidade das organizações ao cibercrime, torna-se imprescindível treiná-las, sem esquecer que, com a adoção do trabalho remoto, se torna vital estender esta formação além do local de trabalho, incorporando a mitigação de novos riscos como o acesso através de redes wifi publicas ou domésticas, a utilização correta de redes virtuais privadas (VPN) e o uso de computadores pessoais, normalmente com sistemas operativos domésticos, não geridos pela empresa. 2 - Defender-se do "phishing". O ataque denominado por "phishing" é talvez um dos tipos de ataque mais usados pelos cibercriminosos. Trata-se da tentativa de roubo de credenciais, normalmente através de um email aparentemente legitimo contendo um link ou um ficheiro anexo que despoleta a recolha das credenciais ou informações confidenciais. Os colaboradores das empresas têm de ser treinados por forma a conhecer quais são os meios oficiais de comunicação da empresa e aprendendo a tratar todos os emails com links e anexos como suspeitos bem como a ter atenção ao endereço dos sites web que normalmente necessitam de consultar. 3 - Garantir a segurança das ferramentas de colaboração. Temos percebido, pelos recentes ciberataques, que estas ferramentas também podem sofrer de vulnerabilidades, em particular se não estiverem atualizadas ou se forem incorretamente configuradas.

RITA MOURINHO
Responsável da Seresco em Portugal

O ano de 2022 iniciou com alguns ciberataques de grande envergadura e a empresas cruciais na nossa vida quotidiana e, por isso, também eles com maior visibilidade mediática. Naturalmente, quando assim é, a opinião pública reflete medo resultado da maior perceção da realidade que aumentou com a pandemia, o teletrabalho e ambientes mais vulneráveis. Mas que cresceu exponencialmente este ano e, especialmente, no último mês, face ao conflito armado da Rússia sobre a Ucrânia, mostrando uma espécie de guerrilha com unidades cibercriminosas que buscam anular o funcionamento de instituições e empresas. O facto de uma empresa estar ligada à Internet faz dela um alvo para hackers. Neste contexto, é fácil identificar que o ponto comum a todos ataques é a importância da exploração do fator humano, o elo mais fraco da cadeia da cibersegurança. Por razões óbvias, este é hoje a parte mais importante da defesa digital das empresas. Por este motivo, é vital que as empresas portuguesas tirem três grandes lições. Acima de tudo, devem concentrar-se na formação e prevenção. A melhor resposta a um ciber-incidente é aquela que não precisa de ser ativada. A segurança é um assunto de todos colaboradores, que devem estar conscientes das suas responsabilidades e capacidade de agir proactivamente para proteger a sua empresa. Deteção e monitorização: a cibersegurança absoluta não existe. Estamos mais ligados do que nunca e, portanto, mais expostos. É vital identificar precocemente as violações de segurança e ter uma equipa de monitorização dedicada para o garantir. Agilidade e robustez na resposta: quando tudo o resto falha, não deve haver espaço para improvisos. Temos de ter planos adequados de resposta e realizar uma análise prévia aprofundada do estado de maturidade da organização, percebendo os seus pontos fortes e, sobretudo, sobre as suas fraquezas. Para o criminoso, a forma mais fácil de comprometer uma organização tem sido sempre abrir as portas a partir do interior. O CEO, cada vez mais, precisará de se envolver.

RUI DURO
Country manager da Check Point Software Technologies

Em muito pouco tempo, vimos várias empresas e infraestruturas sofrer ciberataques. Apesar de não ser infelizmente um evento particularmente raro – se pensarmos que, em média, uma organização portuguesa é atacada 987 vezes por semana, percebe-se o porquê desta afirmação – a verdade é que talvez nunca antes tivesse havido uma sucessão tão pública e impactante deste tipo de incidentes. O derrube dos sites e plataformas digitais do grupo Impresa, a indisponibilização de serviços na Vodafone, o encerramento dos laboratórios da Germano de Sousa... Todos estes são exemplos de ciberataques cuja vertente pública e disruptiva não pode ser esquecida e onde esta tomou um papel muito importante. Numa primeira instância, há inevitavelmente uma descredibilização por parte dos consumidores face as marcas, muito devido ao receio de roubo de informação, à ideia de que houve um descuido para com a proteção de dados. Por outro lado, perante o impacto direto dos ataques na vida das pessoas, começa a instalar-se uma sensação de alarme que serve de lembrete para as proporções que um ciberataque pode tomar. Esta é uma realidade para a qual a Check Point Software tem vindo a alertar há longos meses. A monitorização das tendências de cibercrime da nossa área de investigação permitia antever que este fosse o cenário mais tarde ou mais cedo. Se, face a desconfiança dos consumidores, a melhor abordagem a tomar é a transparência, perante a sensação de alarme, há que agir (e esperar que não seja tarde demais). Esta onda de ataques é um belisque às organizações, na medida em que as incita a olhar para dentro e a fazer uma autoavaliação da segurança dos seus próprios sistemas. À medida que as redes e pontos de acesso de uma empresa ficam cada vez mais distribuídos, dispersam também os possíveis vetores de ataque. Estarão as organizações preparadas para acomodar uma força de trabalho híbrida? É esta a reflexão que deve pautar a agenda dos gestores.

RICARDO PINTO
Líder de Enterprise Security na V-Valley

A diferença nestes ataques foi o impacto que tiveram no dia-a-dia dos cidadãos e a consequente visibilidade nos media - isto em virtude de terem sido atacados serviços que são usados diariamente e que eram dados como adquiridos. Quando temos incidentes a esta escala, o importante é "parar" e avaliar a situação: perceber o ponto em que está, o espectro que pode estar em causa e traçar um plano em conformidade. Regra geral, o "bicho" já está na organização há muito tempo e aproveitou-se de uma vulnerabilidade para entrar. Até ao momento em que o ataque se torna visível podem passar meses. Nesse momento é importante ter a coragem para tomar decisões e, caso seja necessário, fazer uma paragem completa do serviço para evitar consequências mais graves como o comprometimento dos dados dos clientes. É certo que os recursos financeiros das empresas são finitos e é fundamental canalizar as verbas necessárias para garantir o core da mesma, mas nunca a qualquer custo. Há uma palavra importante nesta equação e que, cada vez mais é tida em conta pelo impacto que pode ter numa organização, a reputação. Esta pode ter um impacto devastador no seio da mesma. Contudo, é ponto assente que a exposição acarreta riscos, logo há que saber viver com isso e perceber que a segurança por si só não chega. Se a reputação é uma palavra de ordem, então a inteligência é crucial. É preciso dar olhos, ouvidos, tato e olfato às nossas soluções de segurança. Temos de conseguir fazer, com um grau de certeza elevado, que elas comunicam entre si e que são capazes de antecipar eventuais ameaças. Em suma, temos de continuar a viver com esta realidade que tende a ser cada vez mais sofisticada e agressiva, estando conscientes dos perigos e agindo com inteligência. É fundamental criar consciência, dentro das organizações, que o investimento em segurança é a espinha dorsal da mesma. Só desta forma se pode transmitir a confiança necessária aos cidadãos nesta caminhada da transição digital.

LUÍS MARTINS
Vice-presidente da Cipher em Portugal

Nos últimos anos, os ciberataques multiplicaram-se e tornaram-se num dos fatores de risco mais importantes para as empresas em todo o mundo. Neste sentido, o último relatório Global Cybersecurity Outlook 2022 do World Economic Fórum identifica como as três principais preocupações das organizações em termos de ciberataques, o ransomware, seguido de engenharia social e de actividades internas maliciosas. Atualmente, qualquer organização está exposta à possibilidade de sofrer um ciberataque, uma vez que a sofisticação e inovação dos cibercriminosos continua a crescer. Adicionalmente, o conflito no leste da Europa tem sido descrito como uma "guerra híbrida", no sentido em que os ataques ocorrem não apenas no plano bélico, mas também ao nível cibernético. A maior cobertura mediática dos recentes ataques tem contribuído para a sensibilização e preocupação das empresas, sendo que o tema começa a estar cada vez mais presente na agenda dos gestores. Muito valor é gerado através da transformação digital, mas isso introduz cada vez mais ameaças se o ecossistema não for protegido de forma eficaz. À medida que a digitalização continua a proliferar e novas tecnologias são introduzidas o ciber risco irá inevitavelmente crescer. Neste sentido, o fator humano continua a ser um dos mais importantes desafios no âmbito da cibersegurança, uma vez que os colaboradores continuam a ser um dos pontos mais vulneráveis. As organizações devem não só pensar em sistemas e redes integradas de monitorização de incidentes de segurança, mas também em ferramentas de sensibilização e formação para os seus colaboradores. E devem cada vez mais preparar-se para serem ciberesilientes, face a ciberataques que certamente ocorrerão, com capacidade de recuperar rapidamente o normal funcionamento das operações críticas do negócio face a esses eventuais ciberataques. Esta deve ser uma das prioridades da estratégia de cibersegurança de qualquer empresa ou organização.

ANTÓNIO PINTO
Diretor de Risco Tecnológico e Cibersegurança da BDO Consulting

Devido à elevada exposição mediática, os recentes ataques cibernéticos em Portugal colocaram, pelo menos brevemente, a questão da segurança da informação na agenda de todos. Estes tiveram um impacto direto e longo na disponibilidade de alguns serviços aos consumidores acentuando a consciência que, se os ataques cibernéticos estão a ter sucesso ao nível das maiores organizações do país e do mundo, quão expostas estarão outras de menor dimensão, leia-se, com menor orçamento para a segurança da informação.
Contudo, o relevo dado a estes incidentes não foi suficiente para alterar significativamente a nossa consciência coletiva sobre a enorme dimensão das nossas vulnerabilidades atuais, passíveis de serem exploradas com sucesso. De facto, sem uma cultura de segurança da informação onde, de uma forma natural, sejam tomadas decisões minimamente informadas destinadas a proteger a informação, os consumidores não irão alterar os seus hábitos informacionais. Esta baixa literacia digital, reside, essencialmente, na dificuldade que os cidadãos (e as organizações) têm em atuar sobre estes temas, devido à inexistência de programas curriculares que os abordem, à sua relativa novidade e à dificuldade na identificação de conteúdos já disponibilizados, como por exemplo o CNCS - Cidadão Ciberseguro.
Paralelamente, os gestores enfrentam, desde há muito tempo, um dilema entre a utilização da tecnologia e a segurança da informação. Os investimentos em segurança são, normalmente, baixos ou inexistentes, a sensibilização é, em muitos casos, residual e, estranhamente, existe a sensação de que somos invisíveis no espectro digital e de que os ataques só acontecem aos outros.
A segurança da informação deve sentar-se à mesa das decisões e fazer parte do risco inerente a fazer negócio utilizando tecnologia. Os gestores devem definir um apetite ao risco cibernético, avaliar a sua maturidade cibernética e implementar planos de ação para atingir uma resiliência alinhada com os objetivos de negócio.

LUÍS SOUSA
Especialista em Risco Cibernético da Marsh Portugal

Portugal viveu nos últimos dois meses uma onda de ataques cibernéticos que, pela primeira vez e numa escala nacional, geraram impactos económico-financeiros e também sociais afetando, de forma muito substancial, o funcionamento da estrutura digital da nossa sociedade. Estes recentes ataques cibernéticos vêm reforçar a ideia de que, de uma forma geral, as organizações não têm uma noção real do valor dos dados que detêm e dos impactos da inoperacionalidade dos seus sistemas. Embora assistamos, hoje em dia, a uma maior consciencialização por parte dos responsáveis das empresas no que a esta temática diz respeito, ainda falta alguma sensibilidade e maturidade para a compreensão do verdadeiro impacto, que um evento cibernético poderá ter nas suas operações. Destes recentes ataques cibernéticos em Portugal será importante reter que os mesmos podem acontecer a qualquer organização. A cibersegurança e a segurança da informação deverão, cada vez mais, ser encaradas como fatores de risco com impactos competitivos nas empresas e a gestão dos riscos cibernéticos deverá estar no centro das preocupações dos gestores de risco das empresas, e não somente dos responsáveis de segurança da informação. Não existem soluções 100% eficazes na prevenção do risco e, sendo fundamental o investimento em medidas e controlos de prevenção e mitigação de ataques cibernéticos é, por outro lado, absolutamente essencial à continuidade do negócio, ser capaz de reagir a um ataque ou evento desta natureza.
Entre outros mecanismos de prevenção e mitigação de riscos cibernéticos, é imperativo que exista, ou esteja pensado e pronto a acionar, um plano de continuidade da operação que possa ser imediatamente colocado em curso nas situações em que sistemas e redes sejam comprometidos e, também, um plano de resposta a incidentes e de gestão de crises que deverá considerar alguns procedimentos críticos por forma a garantir a melhor coordenação de recursos à sua disposição.

David Grave
Senior Cybersecurity Consultant

Cibersegurança e Inteligência Artificial, na prática

Em teoria, a Inteligência Artificial (IA) veio para revolucionar todas as atividades humanas - aparentemente está em todo o lado ou, pelo menos, o termo tornou-se ubíquo.
Apesar de alguns excessos e promessas quase a tocar a ficção científica, não podemos ignorar os exemplos práticos de aplicação em várias indústrias. A IA está a mostrar o seu enorme potencial e a acrescentar valor. E a cibersegurança é, claramente, uma destas indústrias, onde existem inúmeros exemplos da sua aplicação e das respetivas capacidades.
Na prática, onde é que estamos a aplicar a Inteligência Artificial na Cibersegurança? Neste momento, na área da cibersegurança – e tal como um pouco na restante indústria das tecnologias de informação -, vivemos uma falta enorme de recursos humanos. No caso da área da cibersegurança esta falta é mais acentuada, por se tratar, de alguma forma, de uma área "nova", em expansão muito acelerada.
Por outro lado, assistimos a uma evolução significativa, tanto em volume de ataques como da complexidade dos mesmos, resultante da profissionalização dos grupos de cibercriminosos. Assim, é improvável que um analista consiga identificar todas as ameaças que uma empresa enfrenta. Todos os anos os cibercriminosos lançam centenas de milhões de ataques com motivações diferentes, mas que podem causar danos significativos a uma organização.
Em cenários onde é necessário analisar uma quantidade massiva e crescente de dados, proveniente de inúmeras fontes, e onde as equipas de SOC (Security Operation Center) muitas vezes têm falta de pessoal qualificado, devido às dificuldades de contratação, a Inteligência Artificial está a ajudar a reduzir os tempos de resposta.
Com recurso às capacidades de Machine Learning são analisadas inúmeras fontes e indicadores de compromisso, bem como os dados oriundos de todos os sistemas de uma organização - sejam eles originários do endpoint, da Cloud ou de dispositivos de IoT. Isto permite reduzir o número de falso-positivos, identificar claramente novos padrões e ameaças complexas em fases mais iniciais do ataque, que de outra forma seria de difícil analisar.
A capacidade de usarmos os resultados destes processos de Machine Learning como uma fonte de informação para algoritmos de Inteligência Artificial, permite-nos dar o passo seguinte e, além disso, identificar os alertas de maior risco (entre inúmeros alertas diários), automatizar a respostas a incidentes e acelerar a investigação.
A automação da resposta a incidentes com recurso a IA pode desempenhar um papel crítico antes, durante e depois de um ciberataque. Permite definir cenários complexos e as respetivas ações, diminuindo drasticamente o tempo de resposta; mas também permite executar ações complexas imediatas e em tempo real, em múltiplos sistemas, que de outra forma poderiam ser morosas e repetitivas.
A automatização bem planeada reduz o risco global, ao proteger a integridade e disponibilidade dos sistemas e dos dados em toda a empresa.
A capacidade da IA para analisar grandes volumes de dados, de uma forma eficiente, permite acelerar e conduzir uma análise forense que, de outra forma, seria complexa e de difícil acompanhamento pelos analistas, usando apenas a ferramentas tradicionais. Recorrendo à Inteligência Artificial é possível correlacionar eventos passados, que dificilmente estariam no foco do analista. Esta capacidade permite que a análise tenha uma visão mais abrangente, muito para além do incidente atual.
A IA está, por isso, a tornar-se parte integrante da cibersegurança, com inúmeros benefícios. Está a ajudar as nossas equipas a identificar mais rapidamente os ataques, a investigar e a analisar de forma mais eficaz os incidentes de segurança e a responder mais rapidamente com automação.
Esta tecnologia não vai substituir as equipas de SOC e os analistas de cibersegurança, mas é mais uma ferramenta que permite aos profissionais tomar decisões mais informadas, de forma mais rápida e consistente, gerindo de forma mais eficiente as tarefas repetitivas.

Especial Cibersegurança

BRUNO CASTRO
CEO
da Visionware

Parece-me evidente que este período de terror cibernético que vivemos em Portugal nos últimos meses veio abanar um conjunto de certezas e mitos que havia face à nossa própria segurança, nomeadamente neste "pequeno" país que é Portugal, e que afinal, também pode cair na malha de interesses do cibercrime mundial, e por fim, até por consequência direta, veio finalmente colocar o tema da cibersegurança na agenda dos decisores. Hoje, a cibersegurança é um ponto de ordem obrigatório na agenda e estratégia da maioria dos decisores. Não há forma de não estar. O risco é enorme, e a conjetura atual veio alertar toda a sociedade desse mesmo risco. Qualquer gestor com responsabilidade, terá de colocar o tema da cibersegurança como prioritário. Contudo, continua a não existir uma receita mágica para o dilema, e portanto, a abordagem é sempre a mesma, ou seja, implementar um modelo de autoavaliação e melhoria contínua do seu nível de maturidade de segurança face às normas internacionais do setor. Parece-me ser um bom princípio.

LUÍS GAMA
Chief Information Officer
da Unicre

A crescente utilização da tecnologia e o acelerar da transformação digital no seguimento do contexto pandémico, responsável pelo alargamento do perímetro de rede para acessos remotos, deram origem a um ambiente digital profícuo em riscos cibernéticos e mais propício a tentativas de ataque do que em algum outro momento na história. A par deste contexto, a mais recente onda de ciberataques em Portugal resultou numa maior consciencialização das empresas e cidadãos em relação às vulnerabilidades a que estão expostos, e tornou a cibersegurança um tema-chave nas organizações em geral. A tendência em relação à intensidade e frequência de ciberataques não mostra sinais de abrandamento, e embora se verifique um investimento cada vez maior na segurança cibernética por parte das empresas, há ainda muito caminho a desbravar. Mais do que reagir para colmatar os danos de um ataque, ficou comprovada a importância de agir preventivamente, garantindo um nível de segurança adequado aos riscos emergentes. Mais do que nunca, os gestores devem considerar a cibersegurança como uma prioridade estratégica. Ao nível interno, importa investir na formação dos colaboradores, no sentido de fomentar boas práticas de cibersegurança no dia a dia de trabalho, ajudando-os a identificar possíveis ameaças e agir em conformidade. Ao mesmo tempo, é fundamental o desenvolvimento de uma estratégia de gestão do risco robusta que avalie as principais vulnerabilidades, riscos e consequências com impacto no negócio, apostando continuamente no desenvolvimento de mecanismos de prevenção e identificação de ameaças.

JOSÉ CORREIA
Diretor de Produto
da Samsung Ibéria

Com a proliferação dos chamados modelos híbridos de trabalho, acresce a necessidade de assegurarmos, em qualquer que seja o nosso ambiente, que estamos a aceder a redes de internet seguras e que fazemos um correto uso de sistemas como VPN. Este tema vem reforçar a importância de continuarmos a melhorar os nossos sistemas de segurança, nomeadamente a nossa plataforma Samsung Knox certificada pelo Gabinete Nacional de Segurança, e a necessidade de implementarmos medidas para evitar mais incidentes deste tipo, por exemplo, é fundamental um maior cuidado com os emails que recebemos e manter os nossos devices, sejam de trabalho ou pessoais, corretamente atualizados. O objetivo enquanto líder de mercado, passa por continuar a servir os nossos clientes sem perturbações, continuando a percorrer o nosso caminho em direção ao próximo patamar de inovação, fiéis aos nossos princípios, com tecnologia com propósito, e com a garantia de oferecer ao consumidor o máximo nível de segurança e qualidade possível. É nesse sentido que estamos a estender o nosso suporte ao nível de atualizações de segurança num período de 5 anos e de quatro anos ao nível de software, garantindo assim que os nossos utilizadores possam tirar o máximo partido dos seus devices com toda a segurança associada. Um propósito que é feito lado a lado com todos os amantes de tecnologia que confiam na Samsung para ir mais além na sua experiência móvel.

MAURO ALMEIDA
Responsável de Cibersegurança
da NTT DATA Portugal

Os ciberataques em Portugal não são um cenário inédito e muito menos singular. Estes ciberataques ocorrem diariamente e afetam empresas de diversos sectores e dimensão. A particularidade dos recentes ataques foi o mediatismo que tiveram, que se refletiu no impacto social que resultou destes ataques. Foi visível o impacto social que que resultou destes ataques, impossibilitando a realização de pagamentos, autenticações e operações em canais digitais ou a realização de chamadas ou SMS, colocando, inclusivamente, em perigo vidas humanas. A Gartner prevê que até 2025 os cibercriminosos terão criado com sucesso ambientes operacionais tecnológicos capazes de serem utilizados como armas capazes de causar, diretamente, dano físico em humanos, como por exemplo, interrupção do fornecimento de gás, interrupção da cadeia de fornecimento de bens de primeira necessidade ou redireccionamento de serviços de emergência médicos. Na minha opinião, a principal aprendizagem que fica destes recentes ataques, é que o ciberataque e o cibercrime trata-se de uma ameaça real e que impacta sociedade e organizações, independentemente do seu setor de atividade ou dimensão. Os gestores devem investir numa correta avaliação de risco, desenho e implementação de controlos de segurança, indexados a esse risco, e na preparação de planos de recuperação de serviço e de continuidade de negócio. Só desta forma, estarão as suas organizações devidamente preparadas para antecipar, identificar e mitigar possíveis ciberataques.

JOSÉ DUQUE
Diretor comercial
na Hardsecure

O primeiro é a evidência de que os ataques cibernéticos também acontecem em Portugal, tanto a organizações portuguesas como a organizações estrangeiras a operar em Portugal, e podem ter impacto significativo. O segundo é ter ficado claro que os ataques cibernéticos podem ter impacto na cadeia de valor das organizações, incluindo os terceiros que com elas fazem negócio (como fornecedores, parceiros ou clientes). Falamos não só de potenciais danos reputacionais, mas também, por exemplo, indisponibilidade de bens ou serviços ao longo da cadeia de terceiros que poderão ter consequências como a perda de negócio, para vários dos intervenientes nesta cadeia, seja essa perda de negócio imediata ou não. É necessário continuar a investir na sensibilização a todos os níveis da organização, é necessário diminuir o gap entre o estado real da organização e o que é recomendado pelas "boas práticas" de segurança. O risco cibernético constitui uma ameaça real que deve ser acautelada pelo adequado investimento em meios materiais e humanos, pela realização de análises de impacto no negócio, pela existência de planos de continuidade de negócio e pela análise do risco que terceiros podem representar para a produção e/ou comercialização de bens ou serviços. Além de ser importante prevenir, é importante monitorizar continuadamente o estado de segurança, e dispor de capacidade de resposta a incidentes de segurança informáticos, para diminuir a superfície de ataque, identificar as ameaças no seu estado inicial e reagir tão rápido quanto possível após a deteção de incidente. A segurança em sistemas de informação e cibersegurança são construídas diariamente, por pessoas, processos e tecnologias. Não se pode garantir segurança a 100% mas podemos preparar-nos o melhor possível.

MIGUEL COELHO
Diretor ibérico para Empresas e Sector Público da Lenovo

Criou-se uma maior notoriedade face às questões relacionadas com a importância de sistemas robustos de segurança cibernética e que permitam a privacidade de informações confidenciais, que é verdade tanto para a área empresarial como para os consumidores. Os gestores e responsáveis em empresas devem ter em atenção a necessidade de contar com soluções de ponta a ponta abrangentes de segurança. A segurança é uma parte fundamental do negócio da Lenovo, em qualquer etapa. A ThinkShield, por exemplo, é uma plataforma de segurança cibernética personalizável que fornece confiança completa de sistemas, incluindo dispositivo, identidade, online e dados, além de cobrir áreas essenciais de forma a evitar quebras de privacidade e ataques. Acreditamos, por isso, que é fundamental os utilizadores contarem com equipamentos que criam, por exemplo, um filtro no ecrã que impede que outras pessoas presentes no mesmo espaço consigam vê-lo nitidamente; a integração de tecnologia que permita um apoio rápido e eficaz da equipa de TI; que os equipamentos incluam tampa de câmara para o utilizador decidir quando quer ser visto; proteção das entradas de USB; sistemas de autenticação de vários fatores, inclusive de palavras-passe; segurança relacionada às redes de Wi-Fi; entre uma série de outras soluções fulcrais para garantir uma navegação e trabalho seguros. Para a Lenovo, Smart IoT significa, em primeiro lugar, que os equipamentos atuais se tornaram mais inteligentes – o que implica que estão sempre conectados, permitem colaboração facilitada, são adaptáveis às diferentes necessidades, com conexão contínua com a nuvem e segurança aprimorada, além da proteção de privacidade. É por isso que continuamos a lançar novas categorias de dispositivos inteligentes, como o Smart Clock, Smart Camera, Smart Lock, ThinkSmart Hub, dispositivos AR/VR e muito mais, adaptados à utilização doméstica e profissional.

NUNO NOGUEIRA
Diretor executivo de Tecnologia da Decunify

Os recentes ciberataques, demonstram que independentemente dos investimentos efetuados em segurança, todas as organizações são potenciais alvos de ataque, e a sua vulnerabilidade é posta à prova, diariamente, nesta nova era digital. Bastante relevante, foi a cobertura mediática aos mesmos, quer pelo grau de impacto nos serviços aos cidadãos, quer pela dimensão das organizações atacadas, o que veio incrementar a consciencialização de todos para esta ameaça global. Apesar de parecer inglório, é fundamental que as organizações continuem a investir em 3 pilares cruciais neste combate. Em primeiro, as pessoas, educar os colaboradores para comportamentos que possam pôr em causa a segurança das organizações, continua a ser uma das maiores necessidades nas nossas empresas. Segundo, capacitar as organizações com tecnologias de segurança inovadoras, que utilizem mecanismos de inteligência artificial e machine learning, garantindo maior celeridade na deteção e resposta a um ataque, pois já há algum tempo que a velocidade humana não é suficiente para analisar e reagir a uma ameaça. Continua a ser relevante alertar, que não basta instalar uma solução de segurança, mas mantê-la atualizada é crucial. Apesar de óbvio, por limitações orçamentais ou de recursos, muitas vezes os sistemas ficam obsoletos, dando apenas a ilusão de que existe segurança. Por último, definir processos de gestão de crise, para que em caso de ataque existam mecanismos de resposta adequados, com criação de planos de contingência e continuidade de negócio, minimizando o impacto à organização e aos cidadãos/consumidores que sejam seus clientes. Numa outra dimensão, apesar da Decunify participar em alguns fóruns, esperemos que o mediatismo destes últimos ataques cibernéticos permita alavancar mais iniciativas governamentais ou de setores empresariais, para a criação de grupos de trabalho de cooperação e partilha de conhecimento entre pares. Só assim, criamos sinergias para uma maior entreajuda, adequando uma resposta mais eficaz, em caso de ataque.

O Impacto da Covid-19 na Segurança da Informação

Rui Almeida
Incident Response
& Cyber Intel Manager na Hardsecure

O Covid-19 trouxe muitos desafios à operacionalização do negócio e funcionamento das empresas, levando a restrições impostas pelos governos como o isolamento e afastamento das pessoas, obrigando as empresas dependentes da tecnologia de informação, a criarem planos de contingência e a adaptarem-se de uma forma rápida e eficaz, para garantir a execução de um modelo remoto, tentando na medida do possível, minimizar o impacto nos seus negócios.

É verdade que no mundo de hoje, a nossa dependência no digital é maior, a tecnologia está presente no trabalho e nas nossas vidas pessoais, sendo que foi potenciado um incremento derivado da necessidade de tecnologia, quer por necessidades ao nível educacional que levou a crianças e jovens tivessem de se adaptar a um modelo remoto, ou por questões profissionais que conduziu ao investimento na aquisição de equipamentos para os colaboradores das organizações poderem realizar o seu trabalho a partir de casa.

Este aumento na procura pela tecnologia, veio expor um maior número de utilizadores aos riscos cibernéticos, criando também desafios e preocupações às organizações. A rápida adaptação, levou muitos a desconsiderar riscos, priorizando sobretudo a funcionalidade e necessidade urgente de colocar a mão de obra operacional.

De forma global, assistiu-se a um aumento dos ciberataques durante o período da pandemia, que, segundo um estudo da Swissinfo.ch do NCSC (National Cyber Security Center), indica que existiram mais de 350 ciberataques por semana em abril de 2020, muito acima do normal de 100-150 em relação ao mês anterior. Foram relacionadas as causas deste incremento como diretamente relacionadas com a pandemia e o aumento do trabalho remoto, concluindo que o nível de proteção não é o mesmo do ambiente de trabalho na organização. Os tipos de ataques maioritariamente incluem phishing, sites fraudulentos e ataques diretos a organizações, alguns dos quais sofisticados que tentam a extorsão, quer por via de 'data leaks' ou por ataques de ransomware, comprometendo a importante informação da organização.

A nível nacional, o relatório de 2021 do CNCS (Centro Nacional de Ciber Segurança) em Portugal, relativo ao ano de 2020, também constata um aumento de 55% do volume de dados fixos (fonte Anacom), um aumento 4% de agregados familiares com acesso à internet (fonte INE), mais 3% de utilizadores de internet (fonte INE) e 40% de confinamento social doméstico (fonte INE), que vem confirmar maior atividade digital, tendo-se verificado um aumento de atividades ilícitas online. As ameaças de phishing/smishing foram os ataques com maior prevalência, tendo criado oportunidades aos ciber-atacantes sobretudo no período do mês de dezembro, durante a época natalícia.

Com o aumento dos ataques a nível global, tem-se assistido à evolução e sofisticação dos próprios ataques. Técnicas usadas de evasão e camuflagem durante uma intrusão como o exemplo de ataques de intrusão camuflados com ataques distribuídos de negação de serviço (DDoS), dupla extorsão por roubo de dados (data leak) seguido de sequestro dos dados (ransomware), e a disponibilização de serviços de RaaS (Ransomware-as-a-Service) de suporte a atividades ilícitas.

À luz dos mais recentes ciberataques em Portugal, com grande impacto sobretudo no sector dos Media e Telecomunicações, é notório uma perceção geral do impacto e disrupção na sociedade, cada vez mais interligada, que afetou milhões de utilizadores e serviços essenciais. Estes problemas impactantes obrigam as organizações e seus responsáveis máximos a repensar e olhar para a cibersegurança de forma diferente, não só como um processo no IT, mas cada vez mais um processo de negócio que deve ser incluído nos planos de desenvolvimento de produto e de infraestrutura tecnológica. Estas oportunidades de melhoria não devem ser desperdiçadas ou ignoradas.

Algumas das medidas preventivas que podem ser adotadas, passam pela formação continua dos colaboradores sobre riscos das ciber-ameaças como o phishing/smishing/vishing, adoção e configuração de passwords robustas na organização com ciclos de expiração, fatores de múltipla autenticação (MFA) e encaminhar a organização para a adoção de uma política de cibersegurança Zero Trust. Para dispositivos com mobilidade, é igualmente importante ajudar e formar os colaboradores remotos a implementarem medidas básicas de segurança na sua rede em casa, como por exemplo a colocação de passwords robustas na sua rede wifi e garantir a implementação de firewall e antivírus de nova geração nesses dispositivos.

Em conclusão, a chave para a proteção de infraestruturas e produtos tecnológicos das ameaças cibernéticas passa pelo planeamento e a prevenção. Atividades continuas para procurar vulnerabilidades, realizar auditorias regulares para perceção do risco da organização, incluir no ciclo de vida dos ativos e dos produtos avaliações de segurança como parte de atividades de gestão de vulnerabilidades e do respetivo risco e implementar um programa de cyber intel para a organização estar um paço à frente na prevenção, são algumas das atividades fundamentais para a prevenção e limitação de danos que possam advir de ciberataques. As organizações devem procurar ter estes processos implementados e amadurecidos para melhor preparação e mitigação/bloqueio dos riscos associados às ameaças cibernéticas.

Estará a sua empresa exposta a um ciberataque?

A transformação digital representa mais do que uma transição, é uma realidade dinâmica que acarreta tanto enormes benefícios como desafios inesperados e muitas vezes súbitos.

Esta realidade em constante mudança exige uma resposta imediata aos novos desafios, de forma a evitar a todo o custo danos muitas vezes irreversíveis. Mais do que ter soluções para os problemas é necessário antecipá-los e dispor das ferramentas adequadas para os mais variados e adversos cenários.

Neste contexto, tendo em conta que o tecido empresarial português é composto por cerca de 99,9% de pequenas e médias empresas (PME), é importante sublinhar que muitas destas PMEs estão vulneráveis a ataques característicos da Era Digital: os ciberataques. Este é um tipo de ataque que pode afetar gravemente tanto grandes como médias, pequenas ou micro empresas.

OS IMPACTOS DE CIBERATAQUES

As consequências de um ciberataque são sempre negativas, variando a gravidade dos seus danos de acordo com a capacidade de resposta da empresa. Uma das estratégias, que qualquer empresa pode adotar para salvaguardar-se, é a incorporação de um sistema de cibersegurança capaz de minimizar ao máximo os prejuízos causados pelo ataque.

É neste universo cibernético, no qual inevitavelmente quase todos estamos diariamente imersos, que concluímos: o risco virtual é real. Como exemplo basta relembrar grandes empresas que foram vítimas de ciberataques ao longo dos últimos meses, o que leva a assumir que o risco será ainda mais elevado para uma PME.

Seja pela falta de conhecimento sobre o assunto, a irrelevância com que o tema é tratado internamente ou a ideia de que a empresa está protegida através de softwares que previnem a violação da privacidade, a realidade é que existe um enorme e agravado risco para as PMEs quando o tema é o cibercrime.

A VULNERABILIDADE DAS PMES

A cibersegurança está estreitamente ligada à proteção de dados, um dos grandes temas da atualidade, e é, portanto, de extrema importância que faça parte da política de cada empresa investir na 'segurança da informação'.

E porquê as PMEs? Porque são vistas como 'alvos fáceis', cuja literacia digital é ainda baixa, ignorando muitas vezes os riscos e prejuízos de um ciberataque e devido a uma lenta capacidade de diagnóstico e resposta – criando mais oportunidade para a prática do cibercrime.

Visto que o mercado português é maioritariamente comporto por pequenas e médias empresas, esta nova realidade representa um problema para qualquer gestor e empresário. É necessário que haja uma rápida consciencialização da importância de métodos de proteção e, acima de tudo, prevenção de ciberataques.

Se tempo é dinheiro, mais do que nunca, é fundamental investir na segurança digital para que face a um possível cibercrime, os negócios nunca parem.

COMO PROTEGER AS EMPRESAS

Garantir a proteção da informação de uma empresa passa maioritariamente pela prevenção que, aliada às boas práticas e identificação dos possíveis e comuns tipos de ataque (phishing, mensagens de remetentes duvidosos, entre outras abordagens), pode tornar a empresa menos vulnerável a um ataque.

Contudo a cibersegurança corporativa é complexa e exigente. Neste contexto, organizações competentes e certificadas estão preparadas para fazer um diagnóstico rigoroso e detalhado do grau de vulnerabilidade de cada empresa, de forma a apresentar um plano que garanta a segurança e que cubra possíveis danos originados por ciberataques.

A Fidelidade, empresa Nº 1 em seguros, assume que tem como missão ajudar as empresas portuguesas – nomeadamente as PMEs – na proteção contra os cibercrimes. Para o efeito a empresa criou o Fidelidade Cyber Safety, um seguro contra riscos cibernéticos.

FIDELIDADE CYBER SAFETY

A cada minuto cerca de 232 computadores são infetados por malware e ao longo dos últimos anos ¼ das empresas portuguesas já foi alvo de ciberataques, mas apenas 30% das empresas têm uma estratégia de resposta para este tipo de ataque. O Cyber Safety aposta na prevenção destes cibercrimes, tendo como objetivo proteger as pequenas e médias empresas.

Através de uma avaliação de cada PME e englobando situações como a invasão de terceiros em sistemas informáticos até à violação do direito de intimidade pessoal, este seguro é capaz de determinar se a empresa se encontra numa situação de Informação Vulnerável ou de Vulnerabilidades Críticas – uma escala que permite testar o grau de exposição da PME a riscos cibernéticos.

Como todos os seguros Fidelidade, a qualidade e segurança estão garantidas. Com mais de dois séculos de experiência, a seguradora aposta agora na proteção digital e compromete-se a entregar serviços como a oferta de diagnóstico RGPG (Regulamento Geral de Proteção de Dados), análise do website e das vulnerabilidades, assistência tecnológica, serviços de prevenção e backups informáticos.

As coberturas e garantias incluem a intrusão de terceiros nos sistemas informáticos, o incumprimento do dever de custódia de dados de carácter pessoal, as responsabilidades informáticas do segurado, a violação do direito à honra e intimidade pessoal de terceiros e a perda de lucros pela interrupção da atividade do segurado (opcional).

O CIBER RISCO É REAL

Este tipo de perigo, que pode afetar empresas de qualquer sector, representa cada vez mais uma preocupação para os portugueses. É imprescindível que, na Era da transformação digital, qualquer empresa – especialmente as PMEs – invista na prevenção deste risco.

O Fidelidade Cyber Safety representa uma solução preventiva, que mitiga as hipóteses de um ciberataque e minimiza os possíveis danos para o negócio.