Este suplemento faz parte integrante do Jornal Económico Nº 2088 não pode ser vendido separadamente

9 abril 2021 | ESPECIAL

O Jornal Económico

ESPECIAL

CIBERSEGURANÇA E INTERNET DAS COISAS

AUMENTO DAS AMEAÇAS OBRIGA A MAIOR INVESTIMENTO

Se os ataques informáticos já eclodiam a cada segundo em todo o mundo, o acelerar da digitalização no último ano deu um novo ímpeto à necessidade de investir em cibersegurança e a procura pela posição de Chief Information Security Officer (CISO) - responsável pela segurança da informação e informática nas empresas – cresceu. No total, as autoridades portuguesas identificaram 6.525 incidentes em 2020, mais 93% do que no ano anterior, dos quais apenas 1.418 foram analisados e resolvidos.

TECNOLOGIA

Cibercrime vai custar à economia global 9 biliões de euros por ano ● II

CIBERSEGURANÇA

Covid-19 abriu porta a uma "pandemia cibernauta"

Especialista em cibersegurança diz ao JE que solução passa pela formação dos trabalhadores e implementação de planos de avaliação contínuos nas organizações. Especialista garante que só se ignoram os riscos "por opção". ● IV

EMPREGO

Pandemia acelera procura por responsáveis pela cibersegurança ● V

FÓRUM

As organizações estão preparadas para um aumento das ameaças? ● VI

TECNOLOGIA

Cibercrime vai custar à economia global 9 biliões de euros por ano

Especialistas alertam para a importância de as empresas atualizarem a estratégia de cibersegurança e formarem os colaboradores.

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt

O mercado da Internet das Coisas (IoT – *Internet of Things*) abrandou com o surgimento de um vírus que não atacou só computadores, mas prepara-se para crescer a dois dígitos este ano, de acordo com as previsões da consultora tecnológica IDC. As despesas globais com estes dispositivos cresceram a um ritmo mais lento que o esperado em 2020 – os analistas estimavam uma subida anual de 14,9% que acabou por ser de 8,2% – para 742 mil milhões de dólares (624 mil milhões de euros) e deverão retomar a taxa de crescimento anual composta de 11,3% até 2024. Porém, à medida que mais aparelhos eletrónicos são conectados e que os telemóveis, televisores, automóveis ou frigoríficos tornam-se (ainda) mais inteligentes acrescem preocupações com a segurança digital.

"Os dispositivos IoT podem ser uma fonte de ataques porque, devido à sua natureza, não é possível protegê-los no sentido habitual, ou seja, não é possível instalar-lhes um sistema de proteção *endpoint*. Por conseguinte, precisamos de um ecossistema que permita deteção e controlo para que, caso detetemos atividade maliciosa, possamos bloqueá-la", alerta ao Jornal Económico (JE) Alberto Rodas, sales engineer manager da empresa de antivírus Sophos Ibéria. Sem revelar o número de ataques que lhe foram notificados, o gestor admite que no último trimestre os ciberataques "se multiplicaram". "Temos visto ataques porque se publica o RDP (*Remote Desktop Protocol*) sem VPN [rede de comunicações privada] diretamente para a Internet. Utilizando ataques de força bruta ou falhas de produto (BlueKeep), os cibercriminosos têm levado a cabo ataques de maneira massiva", garante.

"Desde máquinas de lavar, aspiradores até um simples relógio, tudo hoje em dia detém funções que permitem *reporting*, gestão e controlo à distância a um determinado grau. Naturalmente que todas as oportunidades representam riscos e esta não é uma exceção. A maior preocupação, de um modo geral, deriva antes do mais pela massificação de dispositivos "ligados" que representam dificuldades de gestão integrada, mas também a confiabilidade de cada um destes dispositivos no que diz respeito à segurança e robustez do ponto de vista de conetividade", refere por sua vez Rui Shantilal, managing partner da Integrity. "Uma empresa que faça bons ténis de corrida, não é necessariamente uma boa empresa a introduzir tecnologia de conetividade nos ténis. Mas esses mesmos ténis, que podem nem dispor de informação muito sensível, podem conviver no mesmo contexto tecnológico com outros equipamentos de muito mais suscetibilidade e podem servir de porta de entrada para a rede e colocar todo o contexto tecnológico em risco", adverte.

Centro Nacional de Cibersegurança vai "muito breve" criar um quadro de certificação de produtos e serviços ciberseguros, alinhado com o quadro europeu

Quando se olha para a perda de riqueza mundial os valores são mais aterradores e podem causas danoso económicos equiparáveis a desastres naturais. O relatório anual da Sophos detalha que, pelo menos desde 2013, nenhuma ciberameaça teve um impacto mais danoso do que o *ransomware*, cujos até à data "já entraram nos biliões de dólares". Ademais, nesta década surgiram os famosos ataques informáticos Wannacry e NotPetya, uma continuação dos *botnets*, vírus, *spam* e das fugas de ciberarmas patrocinadas por nações. Já empresa de investigação Cybersecurity Ventures prevê que os custos globais do crime cibernético aumentem 15% todos os anos, nos próximos cinco, atingindo os 10,5 biliões de dólares (9 biliões de euros), o que é mais do dobro do que se perdia em 2015.

Logo, cidadãos e empresas têm um papel na reversão deste prejuízo. Na opinião da Unipartner, uma empresa de tecnologias da informação (TI), "as estratégias de cibersegurança passam por garantir que na organização exista capacidade tecnológica para lidar com potenciais riscos de segurança". "Todos os envolvidos devem possuir os conhecimentos necessários de prevenção e ação contra possíveis ataques, seguindo um conjunto de regras e processos de forma a evitar constrangimentos de negócio e processuais, as boas práticas existentes e os padrões de mercado. Uma das prioridades deste ano prende-se com a consciencialização constante sobre riscos e comportamentos, com o objetivo de garantir uma atitude preventiva, segundo a lógica

"Zero Trust" que consiste em nunca confiar e sempre verificar fonte, emissor, anexo, *link*, site...", explica Pedro Araújo, modern workplace e security services area leader da Unipartner. A estratégia acabará por, na sua opinião, levar a investimentos em diversas áreas, entre as quais a proteção e gestão de identidades, a *threat management*, *Endpoint Detect and Response* (EDR) e gestão de informação e eventos de segurança (SIEM), todos eles tirando do partido de componentes que têm por base a Inteligência Artificial. O mesmo investimento e consciencialização deve suceder nas entidades públicas.

Centro Nacional de Cibersegurança alerta para campanhas de 'phishing' com imagens de bancos ou empresas de encomendas

O *phishing* – quando os piratas informáticos criam mensagens/emails aparentemente reais para roubar *passwords* ou dados bancários – continua a ser o principal ciberataque em Portugal, mas a técnica tem-se tornado cada vez mais sofisticada, tirando proveito das alterações no comportamento dos consumidores. Ou seja, se as pessoas recorrem mais às plataformas de *streaming* e entregas é mesmo aí que os cibercriminosos vão imiscuir-se. "Desde março do ano passado em particular, realçam-se as campanhas de *phishing/smishing*, com um predomínio de narrativas que utilizam a imagem de entidades bancárias, mas também de empresas de serviços de *streaming* ou do sector dos transportes de encomendas. Destaca-se igualmente o impacto da remotização do trabalho e da diluição do perímetro de segurança das organizações nos incidentes de infeção com *malware"*, afirma ao JE o coordenador do Centro Nacional de Cibersegurança (CNCS).

Lino Santos destaca ainda as infeções por *malware* (vírus) e o compromisso de conta não privilegiada, que completam o pódio dos ataques informáticos mais comuns no país. "A infeção por *malware* é particularmente relevante, porque manteve-se como o segundo tipo de incidente mais frequente este ano. É também o tipo de incidente mais identificado através de observáveis. É relevante em todo o mundo, variando a sua relevância em função de um maior nível de articulação entre operadores de comunicações eletrónicas com as autoridades de cibersegurança na notificação dos clientes infetados e no apoio à limpeza dos seus equipamentos", explica o responsável do CNSC.

Apesar de os dados referentes aos primeiros três meses deste ano ainda não terem sido divulgados – sê-lo-ão no início do segundo trimestre no "Relatório Riscos & Conflitos 2021", o engenheiro Lino Santos lembra que os contextos de crise, como aquela que se vive em termos sanitários e económicos, são tradicionalmente "explorados por atores hostis no ciberespaço para sustentarem as suas campanhas de ciberataques na ansiedade social e na atenção mediática global sobre o tema".

É por esse motivo que o CNCS tem procurado criar um conjunto guias de apoio às organizações, para que estas beneficiem da transição digital sem pôr em causa a gestão do risco, como o Quadro Nacional de Referência em Cibersegurança ou Roteiro para Capacidade Mínimas de Cibersegurança, mais direcionado para as PME. O futuro (a curto prazo) passa por um certificado. "Para muito breve está a criação de um quadro de certificação de produtos e serviços em cibersegurança, alinhado com o quadro europeu homónimo e que pretende harmonizar e transmitir confiança nos produtos e serviços entro do mercado único digital", avança Lino Santos.

O CNCS lançou ainda este mês uma edição do curso online gratuito "Cidadão Ciberseguro", no qual os formandos serão confrontados com vários conteúdos e exercícios sobre comportamentos saudáveis – digitalmente falando – a adotar, tendo em conta o tema da navegação segura. O curso está dividido em três módulos (casa, trabalho e exterior), com quatro tópicos cada (identidade, redes e navegação, comportamento social e trabalho) e inclui uma avaliação final. "Temos desenvolvido atividades de índole mais pedagógica e de criação de capacidades, dirigidas a cidadãos e a empresas (independentemente da sua dimensão e sector de atividade), que assentam numa forte intervenção no domínio da sensibilização para comportamentos e atitudes mais seguras e responsáveis no uso das tecnologias digitais e no ciberespaço", garante o coordenador. "Na componente de reação a incidentes temos vindo a desenvolver capacidades internas, fazendo crescer a equipa quer em número, quer em competências, ao mesmo tempo que melhoramos a articulação com as restantes entidades com responsabilidades operacionais no ciberespaço e desenvolvemos capacidades de visualização", conclui. ●

LINO SANTOS
Coordenador do Centro Nacional de Cibersegurança

ALBERTO RODAS
Sales engineer manager da Sophos Ibéria

PEDRO ARAÚJO
Modern Workplace e Security Services Area Leader da Unipartner

RUI SHANTILAL
Managing partner da Integrity

CIBERSEGURANÇA

Covid-19 abriu porta a uma "pandemia cibernauta"

Bruno Castro, especialista em cibersegurança, diz ao JE que solução passa pela formação dos trabalhadores e implementação de planos de avaliação contínuos nas organizações. Especialista garante que só se ignoram os riscos da cibersegurança "por opção".

JOSÉ VARELA RODRIGUES
jrodrigues@jornaleconomico.pt

istock

A pandemia da Covid-19 não expôs apenas as fragilidades dos sistemas e dos serviços nacionais de saúde em todo o mundo. Os efeitos sociais e económicos do novo coronavírus também contribuíram para uma maior exposição das organizações (Estado e sector privado) às ameaças do mundo digital. Em Portugal, o último ano "foi inevitavelmente marcado, ao nível da cibersegurança, pela pandemia de Covid-19", afiança o Relatório Anual de Segurança Interna (RASI) de 2020, divulgado no final de março.

Em declarações ao Jornal Económico, Bruno Castro, o presidente executivo da VisionWare, empresa portuguesa especializada na análise forense de crimes informáticos, afirma que o contexto pandémico "também se traduziu numa pandemia cibernauta", tendo em conta "um crescendo enorme de ciberataques e de roubos de dados ou de dinheiro".

De acordo com os dados do RASI, no último ano, "notou-se um considerável aumento do número de incidentes, principalmente a partir do mês de março", época em que foi declarado o primeiro estado de emergência e em que as empresas iniciaram a transição para regime de teletrabalho. Ao todo, as autoridades portuguesas identificaram 6.525 (+93% face a 2019) incidentes de cibersegurança, dos quais apenas 1.418 foram analisados e resolvidos. Acresce os cerca de 183 milhões de observáveis (alterações discretas num dispositivo ou sistema cujo tratamento é automático), dos quais mais de 61 milhões "encontravam-se relacionados com o ciberespaço nacional".

Os incidentes encontram-se nas classes fraude, código malicioso, intrusão e segurança da informação *(ransomware)*, sobretudo. O *phishing*, o *SMS phishing* e o *spearphishing* foram os tipos de ataques mais comuns. As ações maliciosas simulavam vir de bancos ou outras instituições de serviços financeiros, serviços do Estado, bem como empresas de logística e de transporte, para obter indevidamente dados ou dinheiro. A estas somam-se as "operações cibernéticas ofensivas" contra o sector da saúde, incluindo ações de ciberespionagem, que procuravam a "exploração de oportunidades no contexto da pandemia".

Mas o crescimento do aumento de ciberataques explica-se como? "A partir do momento em que surge a pandemia, as empresas e o Estado tiveram que dar um salto, na maioria dos casos muito maior que a perna, para o entrar no digital", explica Bruno Castro. O especialista realça que adaptar as operações das empresas ao teletrabalho "foi um desafio tecnológico". Afinal, o trabalho remoto "era uma tendência para daqui a dez anos", não fosse a pandemia.

"Temos que partir do princípio que não existe uma vacina mágica ou um Ferrari das 'firewall'. Há que avaliar em contínuo as fragilidades e definir soluções caso a caso, e criar um plano de ação para combater fragilidades"

"A necessidade foi instantânea e foi necessário resolvê-la funcionalmente. Mas, na maioria dos casos, sem garantir a segurança", salienta o CEO da VisionWare.

A par da adoção do teletrabalho, as empresas cujas operações não passavam pelo digital tiveram de adaptar os negócios a um novo mundo. E "fizeram-no rapidamente", mas mais uma vez sem "pensar na segurança".

"Infelizmente, esse *hiato* entre adotar o teletrabalho ou adaptar os negócios ao digital e pensar na segurança foi demasiado longo e permitiu vários *tsunami* de ciberataques, que tiveram sucesso", resume o especialista.

Nesse hiato, o sucesso dos ciberataques foi determinado pelo fator humano, visto que, habitualmente, "os ataques são orientados especificamente para um determinado responsável da organização".

O problema da cibersegurança já não pode justificar-se com ignorância das empresas, tendo em conta o mediatismo do tema da cibersegurança, por via de notícias sobre a alegada interferência cibernética nas eleições norte-americanas de 2016, sobre *warfare* (guerra tecnológica), roubo de dados ou burlas informáticas. "Hoje, quem está nesse nível é por opção", refere Bruno Castro.

Então, o que justifica o crescimento dos ciberataques? A falta de de preparação aliada a uma "imaturidade tecnológica".

Na maior parte dos casos, os problemas terão surgido porque "as empresas não se preocuparam com o tema no passado, não avaliaram o nível de risco – isto é, o nível de maturidade de segurança da empresa". Assim, também "não se prepararam tecnologicamente" e, consequentemente, os trabalhadores "também não estavam preparados para ter de conviver de forma tão agressiva com o mundo digital". "Em contexto de teletrabalho, as pessoas não estão protegidas pela estrutura corporativa da empresa", acrescenta.

Solução passa por avaliação contínua dos riscos e ameaças

Apesar do aumento de ciberataques em Portugal, o país não compara com os "Estados Unidos, Israel, Itália, Espanha ou Inglaterra, que têm outro tipo de propensão a ser atacados". Mas Portugal "já começa a ter um nível de maturidade interessante", tendo em conta que o país avança na transição digital, uma tendência mundial.

Bruno Castro diz que "ainda há um caminho a percorrer, que é longo e tortuoso". Por isso, defende que as organizações devem procurar ter estratégias para a cibersegurança, tentando minimizar a exposição das operações.

Qual é a solução? "Temos que partir do princípio que não existe uma vacina mágica ou um Ferrari das *firewall*. Para se ter uma maturidade em termos de segurança reativa e preventiva há que avaliar em contínuo as fragilidades e definir soluções caso a caso", explica. Isto para perceber o nível de segurança e criar "um plano de ação para combater fragilidades". "Foi o que faltou em grande escala nesta pandemia cibernética. Quando as organizações eram atacadas nem sabiam por onde eram atacadas", diz.

Para minimizar o risco associado ao fator humano, o especialista diz que "é crítico" apostar na "formação e consciencialização" dos trabalhadores. ●


Unsplash

CISO

Pandemia acelera procura por responsáveis pela cibersegurança

Os Chief Information Security Officer tornaram-se uma realidade nas organizações, com o aumento do potencial de risco provocado pela crise pandémica.

JOÃO TERESO CASIMIRO
jcasimiro@jornaleconomico.pt

A procura pela posição de Chief Information Security Officer (CISO), i.e., responsável pela segurança da informação e cibersegurança, estava a crescer em Portugal, à medida que as organizações digitalizavam operações e que a perceção de risco associada aos sistemas também aumentava. A pandemia de Covid-19 veio acelerar esta tendência, ao obrigar a um recurso generalizado ao teletrabalho e à utilização de sistemas de uma forma mais aberta, aumentando o risco associado ao desenvolvimento das operações.

Num ecossistema virtual que inclui cada vez mais o Bring Your Own Device (BYOD), ou seja, em que cada pessoa utiliza os seus próprios equipamentos, e também a Internet das Coisas (IoT), as *firewalls* tradicionais não garantem total proteção e o risco humano, de quem interage com os sistemas, aumentou.

Se a segurança diz respeito à forma como as organizações protegem os dados, a privacidade é a forma como ela é usada. Dito de outra maneira, a privacidade não é uma questão sobre o que é legítimo fazer. Em vez disso, trata-se do que é eticamente correto, sendo isso cada vez mais definido por consumidores e utilizadores, segundo a consultora Korn Ferry.

O CISO tem como principal função aconselhar a equipa executiva sobre as necessidades da organização em atender aos requisitos de segurança para fazer negócios em determinado sector. Supervisiona uma equipa que, em conjunto, tem uma visão dos riscos que a empresa enfrenta e implementa as tecnologias e processos de segurança necessários para minimizar esses mesmos riscos para toda a organização. Tem autoridade para comunicar os riscos a quem toma decisões e agir de forma independente quando necessário. Também defende investimentos e recursos para garantir que as práticas de segurança recebem a atenção adequada.

Em Portugal, a Opensoft foi uma das primeiras empresas na criação do cargo, indo ao encontro das crescentes preocupações com a cibersegurança. Para Ricardo Anastácio, CISO da Opensoft, é "indispensável a criação de postos e cargos específicos para o efeito". Depois da União Europeia (UE) ter criado o Regulamento Geral de Proteção de Dados (RGPD), com o intuito de proteger as pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, foi introduzido um conjunto de novas regras, entre as quais se destaca a obrigação de designar um encarregado para a proteção de dados, regras sobre pseudonimização de dados, alteração das regras sobre obtenção de consentimento, novas regras sobre consentimento de menores, eliminação do sistema de notificações e autorizações, implementação do direito ao esquecimento, criação de obrigações acrescidas para os subcontratados, introdução de coimas de valor muito elevado e obrigações de informação relativas a quebras de segurança.

O CISO tem como principal função aconselhar a equipa executiva sobre as necessidades da organização em atender aos requisitos de segurança para fazer negócios em determinado sector

Neste sentido, Ricardo Anastácio considera que "há uma preocupação crescente, quer por parte das entidades governamentais, quer por parte das empresas, em segurar os seus ativos. Esta preocupação está a ser promovida em parte pelo RGPD e respetiva legislação portuguesa que o acompanha, mas também pelas incessantes notícias de informações expostas que têm impacto de milhões de euros no negócio das empresas.

O CISO da Opensoft sublinha que o número de empresas em Portugal que querem profissionalizar a área da cibersegurança ainda é reduzido, com "muitas empresas ainda em fase de adaptação, que acabam por delegar estas responsabilidades a técnicos internos com alguma apetência para a cibersegurança, ou a contratar empresas especializadas na área para gerir os seus ativos e implementar as medidas de segurança necessárias. Só as grandes ou médias empresas com previsão de crescimento sustentado, como a Opensoft, é que valorizam esta posição, definindo funções específicas que, por norma, estão incluídas na política de segurança de informação da empresa".

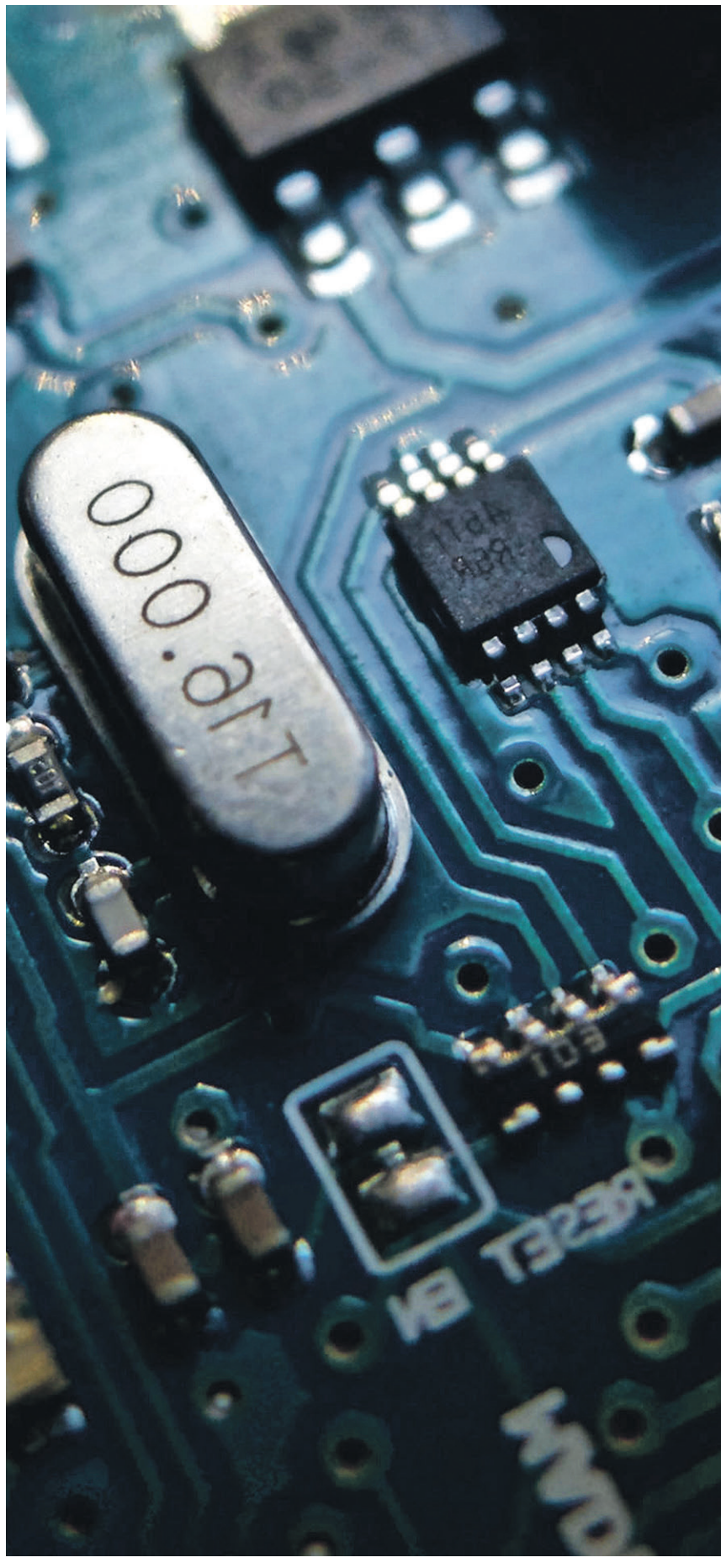
Nas empresas de recursos humanos também se nota a tendência para a necessidade de as organizações empresariais terem nos seus quadros um CISO. A Michael Page, através da sua consultora senior para informação tecnológica Tatiana Leitão da Silva, refere que a procura tem vindo a aumentar gradualmente, sublinhando que, "se há alguns anos não era uma posição que existisse frequentemente em Portugal, hoje em dia, com uma visão diferente em relação a dados e a tecnologia, começa a ser uma posição mais regular. Sobretudo em empresas de maior dimensão ou de sectores que podem representar riscos maiores, como a banca, seguros, indústria, mas não exclusivamente".

Tatiana Leitão da Silva destaca que, "numa altura em que o processamento de dados e de informação é cada vez maior, o papel do CISO torna-se indispensável de modo a proteger e a mitigar os riscos associados. Sobretudo numa altura em que o trabalho remoto é uma realidade indiscutível, os sistemas podem tornar-se mais vulneráveis a ataques e fugas de informação". ●

FÓRUM

CIBERSEGURANÇA AVANÇOU, MAS AINDA HÁ TRABALHO A FAZER EM PORTUGAL

A perceção que as organizações têm dos riscos cresceu e o investimento que foi feito em cibersegurança progrediu, mas os 11 participantes neste fórum consideram que ainda há muito caminho para fazer.



1 AS ORGANIZAÇÕES, ESTADO E EMPRESAS, TÊM INVESTIDO O SUFICIENTE PARA GARANTIR A CIBERSEGURANÇA?

RUI PEREIRA DA SILVA
CEO
da HCCM Consulting

É um facto que, ano após ano, o Estado e as Empresas aumentam os seus investimentos para se protegerem de ciberataques. Se há 10 anos atrás a notícia de um ciberataque era um acontecimento isolado, hoje é vista quase como habitual.
No contexto da atual pandemia, vários analistas reservam ainda mais importância à Cibersegurança.
Devido as alterações que aconteceram em muitas áreas, catalisadas pela transição "forçada" para um modelo de teletrabalho, o problema da Cibersegurança das empresas e organizações foi também levado do trabalho para dentro da casa dos colaboradores.
A complexidade aumenta, ainda mais, quando dentro das empresas e nas nossas casas assistimos a um aumento de dispositivos ligados à internet (IoT) o que indubitavelmente aumenta a vulnerabilidade a ciberataques.
Neste sentido, a minha perceção é que os investimentos por parte das empresas têm aumentado e que nos casos mais sensíveis (saúde, energia, etc.) é imprescindível para o seu progresso.
De igual modo, o Estado vem acompanhando estes investimentos, coadjuvados pelo admirável esforço que o Centro Nacional de Cibersegurança, tem tido não só na formação e sensibilização para que usemos o ciberespaço de uma forma livre e segura, mas também através de políticas transnacionais de cooperação face à possibilidade da ocorrência de ciberataques que ponham em causa as infraestruturas nacionais críticas.
Concluindo, a IoT é uma evolução com o objetivo de trazer benefícios às atividades das pessoas e das empresas, mas que aumentam o espaço de ameaça. A solução para este combate não passa apenas por investimentos em tecnologia, mas também por uma compreensão que do crescimento natural do problema terão de surgir políticas de avaliação de risco nas decisões de conectar um novo processo ou equipamento. Passando também pela consciencialização das empresas e organizações da necessidade de investir em formação e de definir políticas de aquisição de equipamentos seguros *by design*.

ANTÓNIO RIBEIRO
Cybersecurity Manager
da Claranet

1. De uma forma geral, temos visto que os investimentos têm aumentado nos principais pilares da cibersegurança: pessoas, processos e tecnologia. No que diz respeito a pessoas, ao existir mais formação, há uma maior consciencialização sobre as atuais ameaças; nos processos, vemos as organizações mais preocupadas com questões de conformidade, seja por um interesse natural ou com o propósito de evitar pesadas multas; e, na tecnologia, verificamos maior solicitação de serviços de especialistas nesta área para testar, monitorizar e proteger as suas infraestruturas e aplicações. No entanto, alguns dos setores mais tradicionais continuam a ter investimentos muito reduzidos face ao nível de ameaça a que estão expostos.

2. Estão mais preparadas – ou pelo menos mais conscientes das ameaças a que estão expostas. Se por vezes é impossível, por questões orçamentais ou outras, adquirirem serviços ou soluções que as possam deixar mais protegidas, observa-se um aumento progressivo da perceção dos riscos a que estão sujeitas. Naturalmente, nem todas as organizações têm formalmente um plano de continuidade de negócio com base numa análise de risco, no entanto e de forma por vezes mais informal, existe a perceção de como reagir a um incidente. Há que ter em conta que uma reação inadequada a um incidente poderá ter um impacto negativo superior ao próprio incidente e que todos os aspetos do ciclo de vida do incidente devem ser acautelados. Ou seja, estas informalidades podem vir a ter um custo muito superior mais tarde, como já vimos acontecer várias vezes.

2 AS ORGANIZAÇÕES, ESTADO E EMPRESAS, ESTÃO PREPARADOS PARA UM AUMENTO DAS AMEAÇAS?

JOSÉ CORREIA
Managing Director
da HP

Os indicadores dizem que os investimentos em cibersegurança cresceram em 2020, no entanto, muitos destes investimentos foram feitos de forma tática e não estratégica. O ano de 2020 registou um recorde nos ataques e as perspetivas para 2021 não são mais animadoras. Estima-se que mais de 70% dos incidentes tenham origem em algum tipo de dispositivo e o computador pessoal é hoje provavelmente, o principal equipamento das nossas atividades no mundo digital - é nele que trabalhamos, estudamos, e até desenvolvemos atividades de lazer. Foi também devido ao computador pessoal que muitas empresas conseguiram dar continuidade ao seu negócio, com o recurso ao teletrabalho. Pela tremenda transformação que estamos a ter no espaço de trabalho e na forma como trabalhamos, os computadores deixaram de estar de alguma forma protegidos pela tecnologia existente nos nossos escritórios e redes empresariais, por isso a segurança hoje tem de ser descentralizada.
A HP partilha desta visão, e tem investido em dotar os computadores pessoais de tecnologia de segurança integrada, que possa ser

Istock

adicionada às estruturas já existentes, reforçando assim os mecanismos defesa da empresa e individuais.
No que são os critérios de escolha de um computador pessoal, continua a ser a exceção, os clientes que discutem e valorizam sistemas de defesa integrados nos computadores. Este vazio diz-nos que temos ainda um longo caminho a percorrer, e apesar do Estado ter a responsabilidade de liderar pelo exemplo, a responsabilidade pertence também ao setor privado. Os computadores não são todos iguais, a avaliação de sistemas adicionais de segurança é uma responsabilidade de quem avalia e compra, e um passo crucial para a mitigação dos riscos e para a resiliência do negócio e das nossas organizações.

NUNO NOGUEIRA
Diretor de Pré-venda de Gestão de Projeto da Decunify

1. Dado que as ameaças e as vulnerabilidades persistem, é notório um investimento em cibersegurança por parte das organizações, ainda que varie um pouco de acordo com o segmento de tecnologia (segurança de dispositivos, segurança da rede, segurança web e email, segurança dos dados e as análises de vulnerabilidades e segurança) e, sem esquecer, as limitações orçamentais de cada empresa.
O teletrabalho em grande escala trouxe a necessidade de proteger não só os endpoints, mas também o fornecimento de um acesso seguro aos recursos empresariais e a ampliação das defesas para além do perímetro das redes corporativas. Isto significa mais desafios, a este nível, e ainda o incremento de encargos para colmatar as ameaças associadas à nova forma de dar continuidade aos negócios.

2. As organizações são o alvo preferencial para o crime informático e a grande maioria não está preparada para responder aos ataques. Com o acelerado crescimento do cibercrime, é imprescindível assegurar uma resposta às ameaças cada vez mais sofisticadas.
Nós, na Decunify, em conjunto com grandes parceiros da área da cibersegurança, ajudamos os nossos clientes a protegerem o seu negócio.
As empresas procuram soluções de cibersegurança para além das medidas básicas e querem otimizar as suas capacidades recorrendo a tecnologias avançadas como a inteligência artificial, automação de processos robotizados e analítica, entre outras.

CARLOS JESUS
Country Manager da Colt Portugal e VP Global Service Delivery da Colt

A pandemia obrigou as organizações a superarem inúmeros desafios, entre os quais a segurança das TI no contexto do trabalho remoto. As perturbações generalizadas nas operações que se fizeram sentir a nível da cibersegurança refletiram-se nas estratégias, nos investimentos e nas prioridades futuras das empresas e espera-se que o impacto venha a ser significativo.
O aumento do ritmo da transformação digital, fortemente acelerado pela crise sanitária, também provocou a emergência de novas vulnerabilidades de segurança. O trabalho remoto em particular tem sido uma área de grandes desafios, e os incidentes de *phishing* e outras ameaças têm vindo a aumentar, tanto que 71% das empresas indicaram que o apoio ao trabalho remoto é o maior desafio de segurança que enfrentam. Ainda assim, muitas empresas e organizações não estão a encarar esta questão tão a sério como deveriam. À medida que as empresas alargam os compromissos com as suas forças de trabalho remotas, as equipas de cibersegurança têm de enfrentar novos riscos e ajudar a criar novas mais-valias para os negócios no pós-pandemia. Os Chief Information Security Officers (CISOs) e as equipas dedicadas à cibersegurança terão de abordar o novo universo empresarial com uma dupla mentalidade: abordar os novos riscos decorrentes da mudança para um ambiente de trabalho digital remoto, assegurando a tecnologia necessária; e em segundo lugar antecipar a forma como as suas forças de trabalho, os seus clientes e parceiros irão trabalhar no futuro. Só desta forma a segurança poderá ser devidamente integrada nos novos contextos.

RUI CARVALHO
Head of Cyber Security na InnoWave

Não, na sua maioria, as empresas e estado não estão preparados para as ameaças que enfrentamos. Tem de facto havido algum investimento, nem sempre o mais adequado ou necessário, mas nitidamente insuficiente na maioria dos casos.
Os ataques têm-se diversificado entre ataques tecnológicos e de engenharia social, por vezes misturando os dois conceitos. O binómio de pessoas sem as bases para lidar com ataques de engenharia social e de tecnologia mal preparada ou mesmo inadequada, demostram fragilidades significativas.
A sociedade mudou perante a pandemia. As rotinas alteraram e as pessoas e empresas depararam-se com situações que misturam o pessoal, o profissional, o útil, o agradável e a necessidade de reaprender e converter muitas das nossas atividades para ambientes online. Esta realidade fez-se pela utilização mista de tecnologias, PCs pessoais, PCs de empresa, telemóveis, tablets, etc. A diversidade dos meios e circunstâncias abriram portas para o ressurgir, expandir e acumular das ameaças cibernéticas.
É necessário investir na formação das pessoas, na preparação da tecnologia, na criação de meios de prevenção e deteção das ameaças, assim como na valorização de verdadeiros profissionais de cibersegurança. Comportamentos devem ser adequados a cada vertente das nossas realidades, sejam elas profissionais, pessoais, de lazer ou de necessidade. A tecnologia permite uma liberdade que não é compatível com as ameaças evidentes e para as quais as sociedades e as empresas estão pouco preparadas.
A ciber-defesa monta-se de raiz e não de forma esporádica ou casuística, sem comtemplar os investimentos e os seus retornos efetivos. Dado o crescente aumento de ameaças em número e variedade, é cada vez mais importante não só investir em cibersegurança, mas principalmente fazê-lo de forma estruturada, planeada e com foco nos riscos específicos de cada entidade. É por isso crucial a identificação dos riscos, permitindo assim um investimento inteligente sendo que nem sempre mais tecnologia significa maior segurança.
A cibersegurança como, tudo na vida, tem que se ir adaptando às ameaças do dia a dia.

ESPECIAL CIBERSEGURANÇA E INTERNET DAS COISAS

CARLOS VIDINHA
Head of Cloud Infrastructure Services da Capgemini Portugal

Há um aumento geral da tomada de consciência das empresas face à cibersegurança, desde logo pela relevância mediática que certos incidentes e respetivas consequências têm merecido. Outro aspeto diferente é o nível de consciência sobre o risco para o negócio criado pelas ameaças de cibersegurança, que tem levado a um aumento da maturidade que permite a cada organização entender de forma estruturada e sistemática quais as ameaças de cibersegurança que pendem sobre os seus ativos e as vulnerabilidades que expõem, o impacto em termos de valor de negócio que a ocorrência de um qualquer incidente poderá provocar e as estratégias de gestão a adotar para alinhar o nível de risco dos seus ativos com o seu perfil de risco organizacional, numa lógica de melhoria contínua e eficiência operacional.
A mobilização de recursos para o desenvolvimento de estratégias de segurança mais efetivas ao serviço de interesses tradicionais (e.g. retorno financeiro direto, vantagem competitiva, danos na reputação), e de interesses emergentes neste domínio (e.g. confrontação geopolítica, disputas ideológicas, influência da opinião pública) será proporcional à criticidade da informação processada e armazenada.
O aumento da tomada de consciência sobre a relevância do tema, fará com que a cibersegurança seja cada vez mais encarada como um fator de risco com impacto estrutural na atividade de qualquer organização e, consequentemente, o nível de maturidade dos comportamentos dos indivíduos e dos mecanismos organizacionais e tecnológicos de proteção será maior.

NUNO CÂNDIDO
Senior Business Manager na NOESIS Portugal

O tema da cibersegurança é atualmente um dos grandes desafios que se colocam às organizações, independentemente do seu perfil, sector de atividade ou dimensão. A evolução tecnológica e a sofisticação dos ataques é cada vez maior, há cada vez mais ataques, que são cada vez mais complexos e diversificados. Só entre fevereiro e março de 2020, por exemplo, registou-se um aumento de 84% do número de incidentes de segurança reportados em Portugal, tendo-se registado um aumento de incidentes de mais de 150% em 2020, face ao ano anterior. Ataques *machine-to--machine* (M2M), ataques silenciosos, altamente personalizados, ataques de *phishing*, entre outros, colocam novos desafios de segurança, a que as abordagens tradicionais, não são capazes de responder.
Neste sentido, é materialmente impossível afirmar que uma organização está 100% preparada e protegida. O certo é que o tema da Cibersegurança está cada vez mais no centro das preocupações dos responsáveis das empresas e dos seus CIO. De acordo com o mais recente estudo da IDC –Security Market in Portugal, 2020 - A despesa com segurança da informação vai ultrapassar 197,3 milhões de euros em 2024, o que corresponde a um crescimento anual médio de 6,3% entre 2019 e 2024.
Assim sendo, nota-se no mercado uma atenção e um investimento crescente com os temas de segurança, tal como o surgimento de novas soluções de cibersegurança que apostam em novas abordagens, com recurso à inteligência artificial, *machine learning* e *Behaviour Analysis*, que se revelam mais eficientes, não só ao nível da deteção das ameaças, mas também na resolução e anulação das mesmas.

CARLOS VIEIRA
Country Manager da WatchGuard Spain & Portugal

1. De uma forma geral, as empresas não têm uma noção real do valor da informação que possuem, faltando sensibilidade para perceber o verdadeiro impacto de um roubo ou perda dessa informação. E, muitas vezes, só quando os desastres acontecem é que se tomam as medidas necessárias.
Isto porque, embora exista hoje uma maior sensibilização para o tema, quando se trata de investimentos para aumentar a maturidade da segurança das empresas, estas muitas vezes retraem-se, até ao dia em que é tarde.
No entanto, estando no terreno, assistimos como referi a uma progressiva consciencialização acerca dos riscos reais por parte das empresas, sendo que este despertar, embora tardio face ao avanço do cibercrime, é fundamental para "deitar mãos à obra" e preparar as empresas portuguesas para o combate à cibercriminalidade.

2. O aumento de incidentes de segurança conhecidos, o custo e impacto financeiro, político e reputacional por estes causados tem vindo a aumentar velozmente, o que veio a intensificar as preocupações com a segurança por das empresas.
Há, por isso, um aumento da procura e da sensibilidade para a temática, sobretudo no que diz respeito à proteção do *endpoint*, dos dispositivos móveis e das ligações de rede, complementado pela necessidade de uma maior consciencialização dos utilizadores, muitas vezes considerados o elo mais fraco e o principal ponto de entrada dos cibercriminosos nas redes das empresas. Ainda assim, devido às restrições orçamentais e também à falta de conhecimento técnico, muitas delas não estão protegidas com as soluções mais adequadas à sua realidade.

PAULO BARREIRA
Sales Director na TP-Link Portugal

O aumento do teletrabalho veio trazer também um aumento dos ciberataques. Em ambientes privados como os nossos lares e sem regulamentação laboral que possa permitir corrigir lacunas comportamentais, passamos a delegar a responsabilidade das nossas empresas serem atacadas para o colaborador ou utilizador e é aqui que todos temos que trabalhar muito e de uma forma aberta franca através de ações de formação e acima de tudo de consciencialização
Podemos fazer uma reflexão rápida para melhor entender a importância da segurança cibernética:
Que e quantos dados fornecemos às empresas com compras online? Pensemos no número de endereços, senhas, números de cartão de crédito, números de contribuinte, etc., etc.
Todas estas informações deveriam de ser confidenciais e devem ser protegidas com cuidado, longe de gente mal-intencionadas na internet.
O mesmo se aplica às informações comerciais de empresas e governos: os investimentos, as demonstrações resultados, objetivos estratégicos de cada uma delas devem ser mantidos a sete chaves.
É aqui que entra a cibersegurança, dando acesso e garantias desses dados sejam somente acessíveis apenas para aqueles que estão autorizados a fazê-lo.
Com o armazenamento na *Cloud* sendo integrado à realidade de cada vez mais empresas, a procura e importância da proteção também cresce, o que se reflete no mercado de trabalho.
Socorrendo-me de uma informação da International Data Corporation, o investimento mundial estimado para cibersegurança no ano passado foi de 134 Biliões de dólares e não vai parar de crescer. Em Portugal temos estado muito ativos em Fóruns, webinars e *trainings*, mas a mensagem tem custado a passar tendo em conta que o nosso aparelho empresarial é suportado basicamente por micro ou pequenas empresas e ainda não existem apoios libertados para a transformação digital através do PRR (plano recuperação e resiliência).
Portanto e em modo de conclusão; Formação, sensibilização e consciencialização do utilizador, autenticações de acessos – maior centralização, regime laboral e investimento contínuo... talvez seja necessário criar um novo Ministério no governo.
O número de ameaças não vai baixar, vão é ser diferentes.

JOÃO FARINHA
Head of Audit na S21sec em Portugal

Tem havido um significativo progresso na capacidade de comunicação sobre risco entre as áreas técnicas tipicamente responsável pela cibersegurança e os decisores dentro das organizações, o que tem resultado numa maior abertura para aumentar o investimento. No entanto, não podemos esquecer que Portugal tem ainda uma baixa maturidade no que diz respeito à cibersegurança e que fruto da Covid-19, grande parte das empresas (em particular as de pequena e média dimensão) atravessam um período de grande instabilidade, menos receitas e uma elevada incerteza quanto ao futuro, o que tem levado a que muitos orçamentos para a cibersegurança tenham sido revistos em baixa.
No entanto, esta redução do investimento em cibersegurança acaba por levar a um alargar do fosso entre o que está implementado e aquilo que deveriam ser os requisitos mínimos de segurança a cumprir. Não podemos esquecer que a mesma pandemia que levou ao corte dos orçamentos é a mesma que levou a que grande parte da força de trabalho tenha passado a modalidades de teletrabalho (que estão para durar), e nem sempre as soluções tecnológicas implementadas estão ajustadas aos riscos que representam para as organizações, quer do ponto de vista da confidencialidade dos dados, como da sua permanente disponibilidade. E o facto é que temos observado o aumento significativo de ataques a este tipo de fragilidades, com consequências por vezes desastrosas para as organizações atacadas.
Em suma, podemos dizer que há um aumento da perceção do risco cibernético, mas há ainda um longo caminho a percorrer e o investimento em cibersegurança tem de passar a ser uma presença constante em todos os orçamentos das organizações.