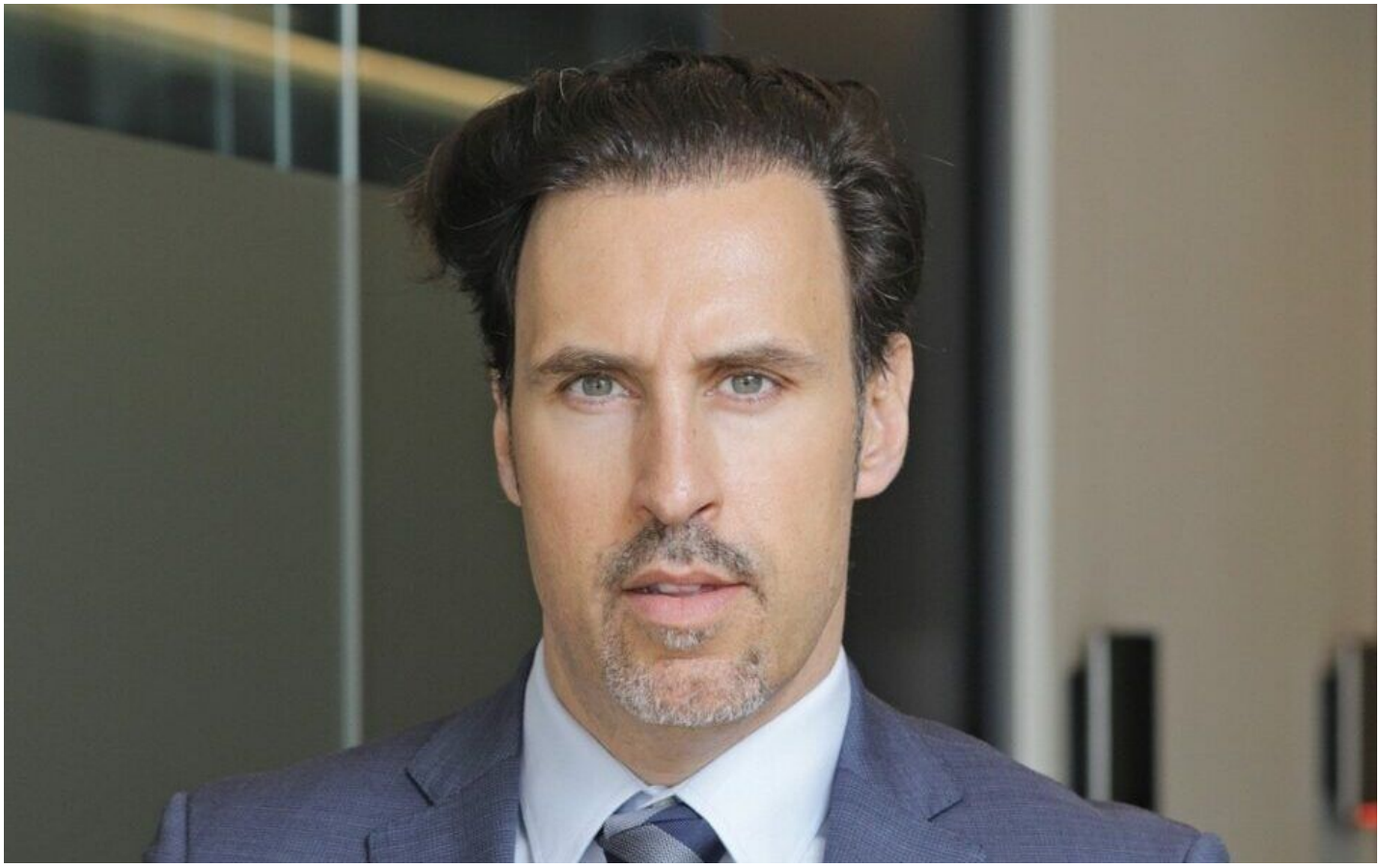
Dois anos do ciberataque à Vodafone. Teletrabalho trouxe “dos maiores desafios” de segurança informática



Cada vez mais ouvimos falar em cibersegurança e em ciberataques. Com o trabalho remoto e híbrido, estas duas palavras passaram a fazer parte do nosso vocabulário. Duas palavras que revelam ter um grande poder, uma vez que uma delas pode causar elevados danos numa empresa, enquanto a outra pode preveni-lo.

No dia 8 de fevereiro de 2022, a Vodafone Portugal foi alvo de um ciberataque que tinha o objetivo de causar danos e perturbações e que interrompeu os serviços da operadora durante algum tempo. De forma a reforçar a importância de estar em alerta constante e de ter uma boa segurança cibernética, Bruno Castro, CEO da VisionWare, empresa portuguesa que atua no sector da cibersegurança, TI, investigação forense, *compliance*, privacidade, formação e *intelligence*, falou ao JE sobre como é que os trabalhadores e empresas podem estar mais preparados para estas situações.

Desde que se iniciou esta mudança para o trabalho remoto/híbrido, quais têm sido os principais desafios que as empresas e os funcionários enfrentam tecnologicamente?

Indubitavelmente este novo paradigma social veio criar um dos maiores desafios de cibersegurança da atualidade, que reside no facto de o trabalho remoto vir expandir abruptamente a superfície de ciberataques. Os colaboradores estão conectados remotamente aos sistemas da empresa através de um número cada vez maior de dispositivos e assente muitas vezes em redes de comunicação inseguras que podem implicar a segurança da própria empresa. Com um maior número de dispositivos ligados entre si através da internet, existe um maior número de sistemas que podem ser atacados. Muitas vezes, estes dispositivos não estão devidamente protegidos nem as redes onde residem são seguras. É imperativo assegurar o acesso seguro aos sistemas corporativos fora do ambiente tradicional do escritório.

Mesmo quando se trabalha em redes domésticas conhecidas, é igualmente imprescindível que as mesmas estejam bem protegidas e, claro, que o próprio colaborador esteja consciente de boas práticas de cibersegurança. Estas passam, por exemplo, por realizar atualizações de *software*, utilizar *passwords* seguras, fortes, e que as mesmas sejam atualizadas regularmente. Outro desafio tem que ver com a maior suscetibilidade a golpes de *phishing*, muitas vezes através do *email*, com a intenção de roubar dados confidenciais da empresa. Os atacantes utilizam técnicas (cada vez mais sofisticadas e agora com o auxílio de Inteligência Artificial) para induzir colaboradores a revelar dados confidenciais ou mesmo a descarregar *malware* que infeta os seus sistemas individuais, e que através de conectividade com a empresa, são utilizados com *pivots* para atacar a empresa. Os colaboradores em regime híbrido e remoto, para além de não estarem debaixo do guarda-chuva de proteção da infraestrutura de segurança da empresa, podem não estar tão atentos aos riscos de segurança como aqueles que trabalham no escritório e é importante garantir um alto nível de conscientização sobre segurança cibernética, através de treino e consciencialização regular.

Como é que os trabalhadores podem estar mais preparados para detetar estas ameaças?

O importante é que exista uma cultura de cibersegurança, ou seja, *awareness* para os perigos da convivência no mundo cibernético. Conhecimento é poder e, efetivamente, um colaborador que esteja informado sobre as ameaças e sobre boas práticas será um colaborador mais bem preparado – é a primeira barreira de proteção de uma empresa. É importante que exista governação de segurança como pilar estrutural da empresa, e por inerência, formação e treino regular em cibersegurança no seio das organizações. Isto inclui formações internas, simulação de cenários de ataques (de engenharia social como *emails* de *phishing*) e desafiar os colaboradores a responder adequadamente a simulações de ataque, quer a nível individual, quer inclusive a nível corporativo com simulações, por exemplo, de resposta a desastre. Outras boas práticas que fazem toda a diferença passam por utilizar *passwords* seguras robustas e atualizadas, implementar autenticação de dois fatores sempre que possível, realizar as atualizações dos sistemas, fazer *backups* regulares e, claro, estar atento a comportamentos suspeitos nos dispositivos e redes corporativas e reportar quando verificados. É também vital implementar medidas rigorosas de segurança com o uso de VPNs, restrições de direitos de acesso a redes, dispositivos e dados da empresa e informar os colaboradores sobre a importância destas medidas. É crucial tornar a cibersegurança uma prioridade e um valor para todos os membros da organização.

É importante as empresas terem uma espécie de 'guião' para saberem o que fazer em caso de ataque?

Sim, é fundamental que exista um plano de resposta a incidentes bem como um plano de continuidade de negócio, que devem ser construídos no seio da organização, com todas as partes relevantes da empresa devidamente envolvidas, testados em ambiente de simulacro, e por fim, comunicados a todas as partes interessadas. Estes planos devem incluir medidas de resposta imediata e concretas para conter o ataque, conter uma clara definição de *owners*, os processos de comunicação interna e externa para informar as partes relevantes e quais os passos para restaurar a segurança e a integridade dos sistemas afetados. É importante que estes planos sejam comunicados de forma clara e transparente de modo a garantir que as equipas estão preparadas para essa execução e, ainda, que conheçam bem os seus papéis e responsabilidades durante um (ciber)ataque. É igualmente relevante que sejam realizadas simulações para garantir que o plano funciona adequadamente, bem como rever e a atualizar o mesmo, continuamente.

Além desses planos, é importante que a organização adote uma política de cibersegurança bem estruturada e que seja do conhecimento geral de todos os colaboradores. Ao compreender as políticas de cibersegurança, os colaboradores tornam-se mais conscientes das ciberameaças e das respetivas medidas de proteção necessárias – saber o que é permitido e o que não é, de acordo com as políticas, ajuda a evitar ações que poderiam levar a violações de segurança. O conhecimento das políticas promove uma cultura de segurança dentro da organização, que vai educar e, por sua vez, incentivar os colaboradores a aplicar as melhores práticas.

Em termos de tecnologia e cibersegurança, em que "nível" de conhecimento (saber o que fazer e deteção) é que os portugueses se encontram?

Um estudo do CNCS [Centro Nacional de Cibersegurança] relativo a 2022 revela que o tema de cibersegurança está na agenda das organizações portuguesas, sendo que 43% (empresas com mais de dez colaboradores e sem incluir o sector financeiro) já teriam revisto ou definido uma política de segurança corporativa nos últimos 24 meses.

É de destacar a viragem também em Portugal, ao nível do tecido empresarial, público e privado, com os ataques que tiveram maior impacto mediático em 2022, em particular aqueles feitos ao grupo Impresa e o super-mediático ciberataque à operadora Vodafone, algo inédito no nosso país, e que abriu um total precedente em todo o sector telco e no próprio mundo (ou submundo) da área da atuação da cibersegurança. Nunca se falou tanto da importância e dos impactos da cibersegurança como até essa altura (e ainda hoje), e esse é um fator e uma consequência altamente positiva, resultante de uma situação negativa e prejudicial para diversas empresas e inúmeros consumidores/particulares.

Adicionalmente, 54% do tecido empresarial nacional possui recomendações documentadas sobre medidas, práticas ou procedimentos de segurança das TIC. Estes dados revelam que a preocupação em relação à cibersegurança tem vindo a crescer, especialmente depois da pandemia e com o aumento dos casos de ciberataques. A notoriedade que a cibersegurança ganhou nos últimos anos em Portugal, também se percebe através do grande aumento do número de artigos nos media e a pesquisas *online* relativas ao termo e é realmente importante que continue a existir esse interesse e partilha de conhecimento e literacia digital. É importante realçar que há ainda um longo caminho a percorrer. As ameaças continuam a evoluir abruptamente e o aparecimento de novas tecnologias muitas vezes não é acompanhado por uma evolução de recursos e formação das equipas.

É notório que a transição digital veio aumentar a necessidade de conhecimento, no entanto, não podemos ignorar que uma das causas de incidentes, são erros humanos. Diria que os portugueses estão num bom caminho. Existe ainda uma grande necessidade de continuar a educar e a consciencializar os indivíduos, nunca é demais reforçar – é necessário literacia digital e literacia específica em cibersegurança. As táticas de ataques estão em constante evolução e, para estarmos preparados, também nós temos de nos atualizar e ser capazes de evoluir à mesma medida que o cibercrime o faz.

Pode-se dizer que os ciberataques estão cada vez mais "refinados". Euais as formas de ataque mais usuais?

O *ransomware* é sem dúvida um dos ciberataques mais conhecidos e até mediático da atualidade devido essencialmente ao impacto que causa na atividade da organização, tipicamente completamente disrupção, e agora, a posterior exposição e comercialização dos dados roubados no decorrer do ciberataque. Estima-se que os ciberataques de *ransomware* se tornem cada vez mais sofisticados nos próximos anos sendo que a Inteligência Artificial (IA) Generativa poderá constituir igualmente um fator impulsionador desta tendência através de *chatbots*, *malware* desenvolvido pela IA e algoritmos de *machine learning*. Estima-se que, globalmente, perto de 73% de todas as organizações foram vítimas de um (violento) ataque de *ransomware* em 2023. É um tipo de ataque bastante lucrativo e, como tal, podemos compreender porque que é bastante "popular" entre os cibercriminosos. Só no ano passado, o custo do cibercrime mundial ultrapassou os oito triliões de dólares.

Os ataques de *phishing* são também bastante usuais. A integração de IA Generativa poderá também levar a campanhas de *phishing* e/ou *spear phishing* mais avançadas com uma abordagem mais inteligente e personalizada, focada em alvos específicos. No fundo, a IA veio impulsionar as técnicas de identificação e exploração de vulnerabilidades de forma mais rápida e eficiente que os métodos tradicionais.

Outra tipologia de ataque muito comum são os chamados ataques de negação de serviço, isto é, ciberataques que impeçam a vítima, empresa ou instituição de ter atividade no ciberespaço. Estes ataques foram e continuam a ser utilizados, muito em particular, no contexto de ciberguerra, como é o caso do conflito entre a Rússia e a Ucrânia. Muitas vezes, estes ciberataques, para além de interromperem a presença da organização no ciberespaço, também têm o objetivo de colocar em causa a sua imagem institucional ao mediatizar a sua fragilidade de cibersegurança para o mundo.

Estes ataques têm tendência para irem aumentando?

Há uma tendência crescente de ciberataques, impulsionada pelo crescimento de número de atores no ciberespaço, a normal evolução contínua das tecnologias e pela sofisticação das táticas dos criminosos. Com o aumento da dependência da tecnologia e da conectividade, é expectável que os ataques continuem a crescer em número e complexidade. Um fator inovador, mas extremamente importante para o futuro da cibersegurança, é a IA que leva a uma ampliação da superfície de ataque híbrido. Os ciberataques podem tornar-se menos dispendiosos à medida que a IA é incorporada às tarefas atualmente executadas por pessoas. Isso permitirá que um número crescente de grupos (profissionais) cibercriminosos realize ataques com uma maior rapidez e direcionados a um maior número de alvos. A

tendência é que novas ameaças surgirão à medida que as soluções concebidas pela IA podem realizar tarefas que seriam complexas para seres humanos – operações ofensivas no ciberespaço suportadas por soluções de IA serão altamente eficientes, direcionadas com maior precisão e difíceis de atribuir.

O que é que as empresas devem fazer quando se deparem com um ciberataque?

Aquando de uma situação de ciberataque, ou até de desastre, são vários os processos que devem ser levados a cabo para restaurar a atividade e própria credibilidade da organização no ciberespaço. Para tal, é fundamental ter um modelo de governação de segurança implementado, conhecer perfeitamente qual a estratégia pré-definida de resposta a desastre, e ser capaz de agir rápida e organizadamente no decorrer do ciberataque. É um processo que deve ser acelerado tanto quanto possível, a fim de evitar tanto a perda de dados como a interrupção da sua atividade, mas deve ser devidamente concertada em ambiente de "sala de crise" com a devida organização e planeamento.

É importante ter em conta cinco ações imediatas: 1) ativar o plano de resposta a desastre com a convocatória da equipa de crise; 2) identificar os ativos críticos e desenvolver uma ação de recuperação dos sistemas (por criticidade) em ambiente fechado/seguro 2) identificar o ciberataque em curso e qual o impacto atual; 3) estabelecer procedimentos de análise, contenção e resposta ao ciberataque; 4) promover uma equipa responsável pelo processo de investigação forense; e, 5) ter o "buy-in" do *top management* e formação das equipas e *staff* interno.

Neste sentido, é importante que as empresas tenham documentados, e testados, três planos essenciais dentro do seu modelo de governação de segurança: (1) um Plano de Resposta a Incidentes bem definido; (2) um Plano de Continuidade de Negócio (framework abrangente que permite às organizações continuarem as suas operações face a incidentes imprevistos); (3) e por fim um Plano de Recuperação de Desastre (documento que descreve como uma organização pode retomar rapidamente as operações após um incidente).