ECO - Economia Online

ID: 90696110 16/01/2021

Visitas diárias: 126866
País: PT
Âmbito: Economia, Negócios e Gestão
OCS: ECO - Economia Online

Ciberataques aumentaram com a pandemia, mas empresas estão mais atentas

URL: https://pt.cision.com/cp2013/clippingdetails.aspx?id=B947E4BE-565D-44C7-86FD-CC9BA6623B77

Os cibercrimes aumentaram durante a pandemia e as empresas encaram ainda mais desafios tecnológicos e digitais para os combater. À Advocatus, advogados analisaram o panorama e deixaram alguns alertas.

Receber um email de um cliente. Mandar uma mensagem por Whatsapp à empresa. Reunião via Zoom. Todas as empresas têm contactos diários com clientes através da internet e o aumento da dependência do digital é hoje uma realidade. Mas com a massificação da digitalização as empresas e os clientes ficaram ainda mais expostos a ciberataques.

Um recente estudo da consultora Oliver Wyman revelou que Portugal encontra-se em 25.º lugar entre 50 países analisados no Índice Literacia e Educação em Cibersegurança, tendo os portugueses "ainda pouca consciência dos riscos cibernéticos e são poucos proativos na sua redução".

Segundo o Índice Literacia e Educação em Cibersegurança da consultora Oliver Wyman que analisou 50 países.

Segundo o mesmo, a 'Inclusão da População' e as 'Políticas Governamentais' são os parâmetros em que Portugal apresenta melhores resultados, por oposição à 'Motivação Pública' e ao 'Mercado de Trabalho', onde fica abaixo do meio da tabela. Com a pandemia Covid-19 o tema da cibersegurança passou a ser uma necessidade urgente para as empresas, dada a adoção do regime de teletrabalho que potenciou os ciberataques.

"Os ciberataques são potenciados, por um lado, pela oportunidade, por outro pela motivação. O trabalho remoto, ao aumentar a superfície de ataque, ou seja, o número de equipamentos e redes necessárias para trabalhar e que contém informação das empresas, aumenta a probabilidade da existência de vulnerabilidades, colocando em maior risco a informação empresarial", explicou à Advocatus João Gabriel, of counsel e encarregado de proteção de dados da GPA.

João Gabriel, of counsel e encarregado de proteção de dados da GPA

Também para Luís Neto Galvão, sócio da SRS Advogados, admitiu a possibilidade de o trabalho remoto potenciar os riscos de ciberataques. "A Cloud, em muitos aspetos, é uma solução mais segura do que o alojamento de ferramentas e informação intramuros. Mas também oferece riscos. O que sucedeu com a pandemia foi a explosão no uso destas ferramentas e um aumento significativo do grau de exposição a ameaças de terceiros, quer em termos físicos quer digitais", notou o advogado.

Apesar de considerar que as transformações tecnológicas que vamos assistindo no seio das empresas e mundo do trabalho potenciam desafios e oportunidades únicas, Gonçalo Gil Barreiros, associado sénior e responsável de propriedade intelectual e privacidade da PRA-Raposo, Sá Miranda e Associados, admite que também criam riscos na sua atuação.

Segundo o Índice Literacia e Educação em Cibersegurança da consultora Oliver Wyman que analisou 50 países.

"O caso paradigmático dos dados pessoais é exemplo disso mesmo. Efetivamente, não é por acaso

que se vem afirmando, de forma crescente que "os dados são o novo petróleo". Tal é o "novo" mantra de consultores e executivos, por todo o mundo", exemplificou o associado sénior da PRA.

Luís Neto Galvão acredita que estamos numa fase de transição para um modelo organizativo descentralizado, que requer uma "coordenação e segurança mais desafiantes". Para o sócio da SRS as empresas podem não estar capacitadas para oferecer soluções de remotização "eficazes" e "seguras", quer VPN's, quer aplicações na Cloud.

"Pode ainda haver por parte dos trabalhadores a tentação de uso no âmbito profissional de soluções de armazenamento gratuitas, do estilo Dropbox e dispositivos de memória não encriptados. Tudo isto traz consigo riscos para a confidencialidade", acrescentou Luís Neto Galvão.

"O que sucedeu com a pandemia foi a explosão no uso destas ferramentas e um aumento significativo do grau de exposição a ameaças de terceiros, quer em termos físicos quer digitais."

Luís Neto Galvão

Sócio da SRS Advogados

O advogado da SRS garantiu ainda que com o teletrabalho existe uma maior exposição a ciberataques como é o caso do phishing e malware.

Ciberataques aumentaram em Portugal em 2020

"Sinto na minha atividade profissional, mas as estatísticas também o dizem". Foi assim que Luís Neto Galvão começou por analisar a situação atual dos ciberataques em Portugal. "A Procuradoria-Geral da República refere ter havido um aumento exponencial das denúncias de cibercriminalidade em 2020, relativas aos clássicos malware e phishing e a extorsão por email, bem como um significativo recurso a fraudes no uso do MB Way", acrescentou.

Luís Neto Galvão, sócio da SRS AdvogadosHugo Amaral/ECO

De acordo com o Observatório de Segurança do CNCS, entre março e maio de 2020 verificou-se uma maior incidência de ciberataques, em relação aos meses anteriores e ao período homólogo do ano anterior.

"Este aumento pode ter tanto razões correlacionadas diretamente com a pandemia, como com a disponibilização de ferramentas de ataque que exploram vulnerabilidades que passaram a ser mais utilizadas - como o acesso remoto aos servidores da empresa -, como até circunstâncias geopolíticas relativas aos ciclos eleitorais", explicou à Advocatus, João Gabriel.

Ainda assim, para o of counsel da GPA é inegável a tendência crescente dos ciberataques. "Se a sociedade adota uma realidade digital, os criminosos também o farão", notou.

"A evolução tecnológica e a realidade digital, por regra, são sempre mais velozes que a adequação da legislação, nestas matérias."

Gonçalo Gil Barreiros

Associado sénior da PRA-Raposo, Sá Miranda & Associados

Setores da saúde, comunicações, energia, transportes, banca, fornecimento e distribuição de água potável, serviços e infraestruturas do mercado são alguns dos apontados como os mais vulneráveis de ciberataques.

"Nos dias de hoje, quer o mundo empresarial, quer os indivíduos na sua esfera pessoal, são alvos 'apetecíveis' para ciberataques", referiu Gonçalo Gil Barreiros. "O relatório elaborado pelo Centro

Nacional de Cibersegurança coloca os ataques aos organismos do Estado, empresas chave com dados sensíveis e confidenciais e bem assim sistemas de controlo industrial como os mais críticos, em termos de ataques", acrescenta o advogado.

Formação é a chave para diminuir riscos

O desafio de superar e combater as ameaças é complexo, mas a atenção que as empresas têm dedicado às questões de cibersegurança tem vindo a crescer. Gonçalo Gil Barreiras tem verificado um reforço das áreas de IT e das tecnologias seguras que as empresas utilizam, considerando este melhoramento e atualização das infraestruturas digitais um vetor principal para evitar ameaças.

"A adoção de sistemas e programas fiáveis e fortes de deteção e bloqueio de vírus e malware que permitam identificar e evitar ataques de ransomware, phishing e pharming, é outro dos pontos fulcrais para o reforço da segurança informática de uma empresa", referiu o associado sénior da PRA.

Gonçalo Gil Barreiros, associado sénior e responsável de propriedade intelectual e privacidade da PRA-Raposo, Sá Miranda & Associados

O reforço da utilização de sistemas e softwares de encriptação fortes, com a aposta em backups, a adoção de sistemas de gestão da segurança da informação, e a formação dos profissionais são alguns dos pontos enunciados pelos advogados contactados pela Advocatus.

Para João Gabriel não cabe às empresas evitar ameaças, mas sim reduzir o risco operacional através da mitigação do impacto das ameaças ou redução da existência de vulnerabilidades.

"A formação constante aos colaboradores sobre os meios a utilizar é fundamental para diminuir o risco, assim como a responsabilização e alocação de funções como a monotorização, capacidade de resposta e deteção", explicou o of counsel da GPA.

"Se a sociedade adota uma realidade digital, os criminosos também o farão."

João Gabriel

Of counsel da GPA

Também o sócio da SRS considera que as ameaças não podem ser evitadas, mas diz ser essencial o investimento em segurança da informação e no reforço da proximidade digital entre os colaboradores e a organização.

"Creio ser fundamental apostar na formação dos trabalhadores em cibersegurança. O Centro Nacional de Cibersegurança oferece conteúdos inestimáveis para o efeito", acrescentou.

Lei a par e passo com o avanço tecnológico?

Com a evolução constante da tecnologia, a legislação necessita de um acompanhamento diário. "A evolução tecnológica e a realidade digital, por regra, são sempre mais velozes que a adequação da legislação, nestas matérias. Aliás, mostra-se, efetivamente, para esta difícil acompanhar tais evoluções que mudam e se alteram num "piscar de olhos"", começou por explicar o associado sénior da PRA.

Segundo Gonçalo Gil Barreiros, as legislações nestas áreas são mais "reativas" do que "preventivas ou antecipatórias", como é o caso da lei do cibercrime que data de 2009 (Lei n.º 109/2009, de 15 de Setembro).

"No plano da cibersegurança falta ainda a concretização dos requisitos de segurança e os requisitos de notificação de incidentes."

Luís Neto Galvão

Sócio da SRS Advogados

"Desde lá, muito mudou nestas temáticas com o surgimento de novas tecnologias e tipos de ameaças e ataques. Naturalmente que tais circunstâncias têm reflexos necessariamente na suficiência e/ou insuficiência da legislação que a regula e tutela. Certamente pontos existem a melhorar e aperfeiçoar na legislação nacional, nestas matérias", acrescentou.

Para o advogado da PRA é necessário definir caminhos comuns, nomeadamente a nível europeu, quanto às questões e políticas de cibersegurança, atento o caráter não-territorial das redes do ciberespaço.

"O legislador português tem tentado regular a área digital, olhando para cada assunto separadamente, e eventualmente através de noções e conceitos jurídicos pouco adequados para a realidade de um mundo digital", defendeu João Gabriel.

"Tornar o sistema judicial mais tecnológico e modernizado, por si só, não trará grande valor sem ser demonstrar uma capacidade digital num setor."

João Gabriel

Of counsel da GPA

Segundo o of counsel da GPA o resultado é uma regulação de assuntos como a privacidade, o cibercrime e a propriedade intelectual em "silos, com conceitos próprios de cada área, desligados entre si e não comunicantes com o panorama da cibersegurança".

"Existe um quadro legal robusto em termos de cibersegurança e de cibercrime, que o RGPD veio também, noutra perspetiva, reforçar. No plano da cibersegurança, embora tenhamos uma Estratégia Nacional do Ciberespaço e um importantíssimo Regime Jurídico da Segurança do Ciberespaço, falta ainda a concretização dos requisitos de segurança e os requisitos de notificação de incidentes", notou o sócio da SRS.

Com o confinamento obrigatório entre março e maio durante o Estado de Emergência, o sistema judicial teve que adotar uma postura mais modernizada e tecnológica. Desde julgamentos realizados através de uma câmara até a conversas entre arguidos e defensores, a Justiça reinventou-se.

"Nos dias de hoje, quer o mundo empresarial, quer os indivíduos na sua esfera pessoal, são alvos 'apetecíveis' para ciberataques."

Gonçalo Gil Barreiros

Associado sénior da PRA-Raposo, Sá Miranda & Associados

Mas será que Portugal, com o aumento do número de ciberataques, tem capacidade e segurança para tornar o sistema judicial mais tecnológico e modernizado?

"Tornar o sistema judicial mais tecnológico e modernizado, por si só, não trará grande valor sem ser demonstrar uma capacidade digital num setor", defendeu João Gabriel. Para o of counsel da GPA adotar tecnologia sem analisar os seus impactos, negativos e positivos, seria uma "má decisão de gestão".

"Caberá então verificar se é possível equacionar um sistema judicial mais justo, célere e eficaz através da tecnologia. Na medida em que a tecnologia permita a obtenção destes objetivos é imperioso que seja adotada", acrescenta.

Relembrando a postura mais digital adotada pelo ministério da Justiça face à pandemia, Gonçalo Gil Barreiras considera que muito caminho ainda terá de ser trilhado no sentido de existir um sistema "plenamente seguro" e "capaz de responder de forma adequada, rápida e eficaz e às exigências que a realidade tecnológica e digital, cada vez mais impõem".

Frederico Pedreira