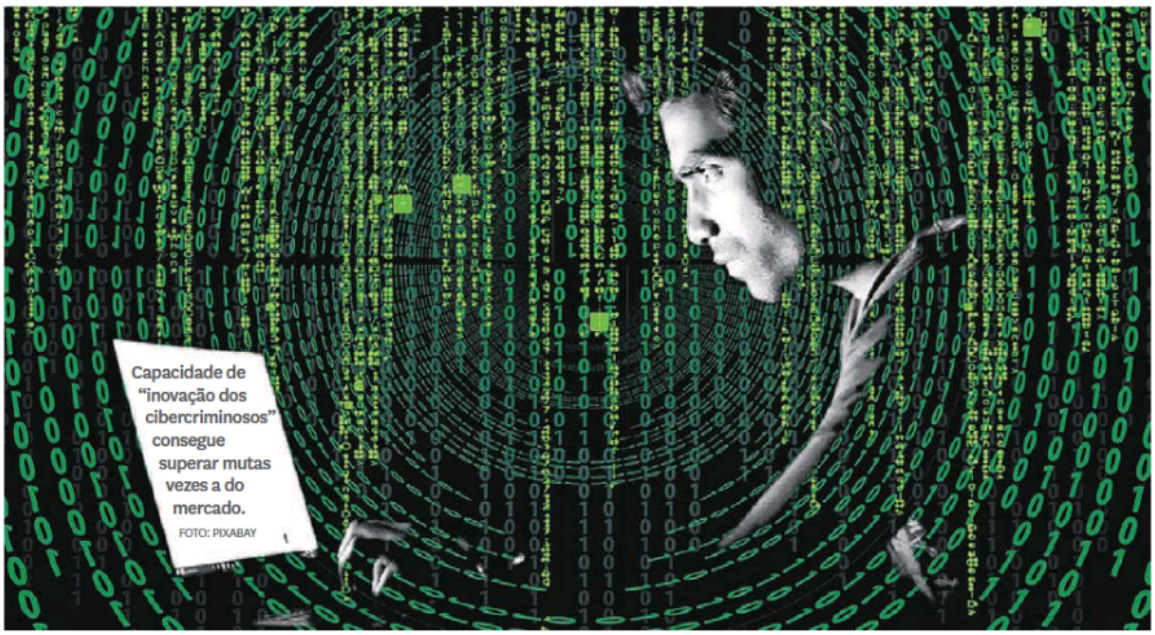
Cibercrime

Todas as empresas estão expostas. Impresa pode levar dois meses a recuperar de ataque



CIBERSEGURANÇA

Todas as empresas estão expostas a ciberataques

Especialistas explicam que não há empresas impenetráveis ou redes infalíveis. Perante o perigo, cautela é palavra de ordem. Estado, setor financeiro e saúde são alvos frequentes.

—JOSÉ VARELA RODRIGUES
jose.rodrigues@dinheirovivo.pt

O ataque informático à Impresa não só marcou o arranque de 2022, em Portugal, como voltou a mostrar que, a par das grandes empresas internacionais, as companhias nacionais também são alvos de redes de criminosos informáticos profissionais. Antes, ciberataques a grandes empresas, como a EDP e a Altice Portugal, já tinham evidenciado como os negócios em território nacional não estão imunes aos perigos da internet. Agora, a Impresa, pela exposição mediática, reacendeu a luz para um perigo que há muito os especialistas em cibersegurança alertam: o cibercrime é real e o risco de ciberataques é permanente.

"Todas as empresas do mundo estão expostas à possibilidade de sofrer um ciberataque", afirma ao Dinheiro Vivo Luís Martins, vice-presidente da Cipher em Portugal, a divisão de cibersegurança da Prosegur. Para este especialista, os ataques informáticos multiplicaram-se, nos últimos anos. Em 2020 e 2021, a pandemia acelerou a digitalização dos negócios e das rotinas de trabalho, criando novos desafios na segurança das redes. Resultado? Os ciberataques são hoje "um dos fatores de risco mais importantes para as empresas", diz Luís Martins.

Uma análise da Microsoft, divulgada em outubro de 2021, concluiu que a "economia do crime cibernético evoluiu para indústria criminosa madura". Já o 2021 Cyber Security Risk Report, da seguradora AON, à escala mundial, apontava que apenas duas em cada cinco organizações estão preparadas para enfrentar ameaças à cibersegurança. Em Portugal as ameaças informáticas às organizações nacionais têm crescido.

O último relatório de Relatório Anual de Segurança Interna (RASI), do governo, relativo a 2020, apontava que desde março desse ano – o primeiro mês de confinamento devido à covid-19 – se notava um "aumento do número de incidentes [de cibersegurança]". Os dados do RASI ganham força, tendo em conta que o relatório Riscos & Conflitos 2021 do Centro Nacional de Cibersegurança, revelou que o risco de uma entidade registar um ataque aumentou 94%, em 2020. A percentagem caiu para 86%, em 2021. O perigo permanece elevado.

Os especialistas afirmam que a cibersegurança é hoje um tópico prioritário para as empresas, que querem melhorar o nível de maturidade das organizações. "Além disso, a maior cobertura mediática dos recentes ataques está a aumentar a sensibilização das empresas e a segurança cibernética começa a estar presente na agenda dos gestores", afiança o gestor. "Creio que os portugueses em teoria já estarão mais sensibilizados para estas situações",

> Incidentes de cibersegurança começaram a aumentar desde o aparecimento da covid-19.

realça Luís Lobo e Silva, *managing partner* da Focus2Comply. Mas, diz o gestor, persiste a ideia "de que só acontece aos outros e que ainda se facilita no modo como se utilizam os meios digitais e equipamentos".

Não obstante, salienta o responsável da Focus2Comply, as empresas portuguesas começam a ter "diversos mecanismos, sejam tecnológicos, mas também de caráter técnico-organizativo, de paulatinamente irem adotando e implementando nas suas políticas e infraestruturas", em matéria de cibersegurança. "Não é por acaso que, em alguns setores, já existem orientações regulatórias para que o CISO [administrador com o pelouro da cibersegurança] tenha assento no conselho de administração das organizações, anota Luís Lobo e Silva.

A estratégia das empresas implica um plano de atuação. No fundo, "terem um levantamento documentado dos seus ativos de risco e uma análise de risco bem definida, por forma a definirem um plano de recuperação tecnológico para agirem de maneira concertada em caso de incidente", aconselha o gestor.

Esse tipo de atenção, investimento e ação preventiva das empresas já ocorre. Mas Luís Martins, da Cipher, alerta: "Apesar do crescente aumento do investimento em cibersegurança, a capacidade de inovação dos cibercriminosos é frequentemente maior do que a do próprio mercado. Significa isto que muitas organizações têm de repensar a sua estratégia de cibersegurança para garantir que possuem os protocolos e sistemas de segurança mais avançados, uma vez que os ciberataques estão a tornar-se mais numerosos e sofisticados".

"Os principais desafios serão proteger as organizações nas suas estratégias de transformação digital, principalmente na sua evolução para a *cloud*, o aumento do teletrabalho e a obsolescência de alguns dos seus ambientes. O fator humano continua a ser um dos mais importantes desafios a enfrentar e é prioritário estabelecer planos de sensibilização adequados, uma vez que este fator tem um papel crucial na ativação do *malware*. De acordo com as estatísticas, o fator humano é o ponto mais vulnerável nas questões relacionadas com a Segurança da Informação", acrescenta.

A falta de prevenção das empresas pode ter resultados negativos. Primeiro, na reputação, uma vez que os dados de clientes, parceiros, funcionários e outros podem ficar comprometidos. Em segundo, a falta de atuação pode contribuir para que um incidente se traduza em prejuízos financeiros para os negócios. "Estes custos costumam ser uma fração das perdas totais para os acionistas que implicam as possibilidades de fragilização da marca, perda da confiança do consumidor, dos credores e dos parceiros corporativos, custos legais por violação do sigilo do consumidor, bem como interrupção de serviços", afirma Luís Martins, da Cipher.

Ricardo Negrão, responsável pela área de análise ao risco cibernético da seguradora Aon, em Portugal, estimava, numa entrevista ao DV, em novembro, que os ciberataques podem custar às grandes empresas até dez milhões de euros. O impacto pode ser superior – a falta de dados não permite uma quantificação mais rigorosa. O cálculo foi feito só com base em ataques de *ransomware* – o que ocorre mais vezes –, com a certeza de que Portugal é cada vez mais "apetecível".

Quem são os principais alvos dos ataque? "O Estado de um modo geral, o setor da saúde (setor público e setor privado) e o setor financeiro. O relatório da AON aponta, ainda, as empresas de *media* e de telecomunicações – "grandes agregadores de dados" – como alvos comuns.

"Impresa pode levar mais de dois meses a resolver ataque informático"

Grupo de *media* sofreu um ciberataque. Especialistas alertam que o processo de solução é complexo e moroso.

A Impresa pode demorar mais de dois meses a resolver o ataque informático de que foi alvo no início deste ano. O ciberataque do grupo Lapsus$ que mandou abaixo os *sites* das marcas do grupo – *Expresso*, SIC, SIC Notícias, Blitz, Opto, ADVANCE –, bem como do jornal regional *O Mirante*, da revista corporativa *Energiser.pt*, da Galp, e do projeto de fotojornalismo *Olhares*, continua por resolver. O grupo de *media* lançou *sites* provisórios do *Expresso* e da SIC e está a trabalhar com a PJ, o Conselho Nacional de Cibersegurança e outras entidades para resolver a situação. Mas não há uma previsão para a conclusão do caso.

Ao Dinheiro Vivo, Bruno Castro, presidente executivo da VisionWare, empresa portuguesa especializada na análise forense de crimes informáticos, afirma que o ciberataque à Impresa pode "levar semanas e semanas" a resolver. "Cada caso é um caso", ressalva, certo que a solução para uma empresa com a dimensão da dona da SIC "pode ser complexa", assumindo que estão envolvidas "várias empresas, parceiros, funcionários". "Quanto mais dependências e aplicações houver mais difícil é a solução".

Ainda que seja difícil prever a morosidade de uma solução, Pedro Leite, administrador com pelouro das operações da S21sec, citado pela Lusa, diz que "existem alguns dados estatísticos que indicam que em média são precisos 78 dias [ou seja, cerca de dois meses e meio]", só para detetar e conter uma quebra de segurança. Só depois se entra no processo de resolver o problema.

Segundo Bruno Castro, da VisionWare, os responsáveis pelo caso estarão, agora, a procurar perceber "quem é o paciente zero". Isto é, por onde é que os *hackers* conseguiram entrar no sistema da Impresa, "se foi *phishing* ou uma falha aplicacional ou de infraestrutura", há quanto tempo estão (ou estiveram) no sistema, a que informação acederam e que "armadilhas podem ter montado". "Tudo isto, provavelmente, ao mesmo tempo que continuam a bloquear o ataque" detetado a 2 de janeiro.

E, identificado o grupo de *hackers*, consegue-se chegar até aos autores? "Para se conseguir rastrear os autores de um ataque informático é essencial a cooperação de vários ordenamentos jurídicos bem como a realização de grandes perícias", explica João Leitão Figueiredo, advogado e sócio de TMC da CMS Portugal.

O problema, nota o CEO da VisionWare, é que na internet "não existem geografias. Leitão Figueiredo diz que o caso enfrenta o desafio de as autoridades terem de fazer "perícias tecnologicamente rigorosas". Os resultados podem ter de ser cruzados com a lei de outros países.

O advogado diz que a legislação a recorrer é à Lei do Cibercrime, que "estabelece que, salvo tratado ou convenção internacional em contrário, a lei penal portuguesa é aplicável a factos: a) Praticados por portugueses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado; b) Cometidos em benefício de pessoas coletivas com sede em território português; c) Fisicamente praticados em território português, ainda que visem sistemas informáticos localizados fora desse território; ou d) Que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados".

Acresce a necessidade de recorrer, em simultâneo, aos "órgãos e mecanismos instituídos no seio da União Europeia para facilitar a cooperação entre as autoridades judiciárias dos Estados membros e a coordenação das respetivas ações". Tal é útil par a coordenação das ações necessárias.

"É essencial que os vários Estados-membros cooperem no âmbito da investigação, mas também no que diz respeito à competência dos tribunais, sendo tudo ainda mais complexo quando o autor em causa se encontra fora da União Europeia", conclui Leitão Figueiredo.

— José Varela Rodrigues