

PROTEÇÃO DE DADOS

Advogados receiam tornar-se vítimas frequentes de ciberataques

Há medidas e meios para minimizar a ocorrência de ciberataques, mas para os especialistas inquiridos pelo Negócios, “não é possível a nenhuma organização garantir a segurança a 100%”.

JOÃO MALTEZ

jmaltez@negocios.pt

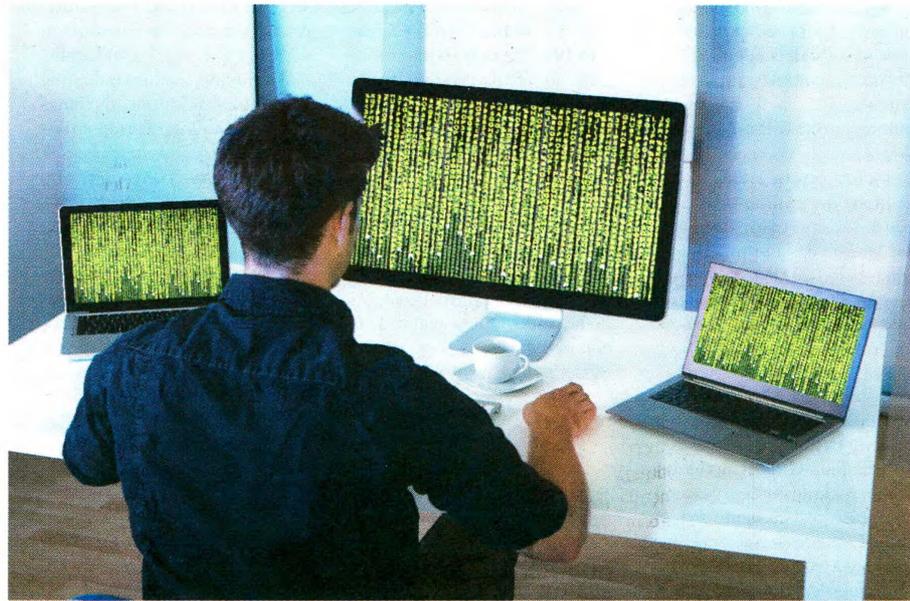
Os ciberataques a sociedades de advogados, à semelhança do caso que foi revelado esta semana e que envolveu a sociedade PLMJ, poderão repetir-se, com frequência, num futuro próximo, admitem especialistas contactados pelo Negócios. Tanto mais que nenhuma organização está a salvo e será até negligente afirmar que se está imune a este tipo de ataques, sustentam, por outro lado, vários atores do mercado da advocacia.

O caso veio a público esta semana, mas segundo a Polícia Judiciária, está em investigação “há já algum tempo”. Um ciberataque à PLMJ redundou no alegado roubo de quatro gigabytes de informação sobre alguns dos principais clientes do escritório. Estará aqui em causa pelo menos um crime de acesso ilegítimo, mas também a necessidade de colocar, no mínimo, uma pergunta: Em Portugal, as sociedades de advogados estão preparadas para resistir à investida dos hackers?

António Caeiro, encarregado de proteção de dados e responsável de comunicações da Abreu Advogados, defende que, “na generalidade, as sociedades têm vindo a adotar tecnologia e a implementar procedimentos para ajudar a prevenir, detetar e reagir aos ataques informáticos”.

No entanto, para este membro da direção da IT4Legal - Associação para as Tecnologias e Sistemas de Informação do Direito, “mesmo com toda a tecnologia, processos e equipas disponíveis e focadas na proteção dos sistemas e da informação, não é possível a nenhuma organização garantir a segurança a 100%”.

Para Martim Bouza Serrano, advogado associado e coordenador da



O roubo de quatro gigabytes de informação à PLMJ poderá corresponder a um crime de acesso ilegítimo, segundo a Lei do Cibercrime.

equipa de proteção de dados da CCA Ontier, “mesmo os sistemas informáticos tradicionalmente mais robustos, como aqueles associados à indústria financeira ou até o próprio Estado são alvo de constantes ataques”. Até por isso, sublinha ainda, “será um erro pen-

sar que existem sistemas sem vulnerabilidades e negligente afirmar que se está imune a estes ataques”.

Perdas reputacionais

O que fazer então para reduzir ao máximo eventuais fragilidades, que redundem no compromisso da informação privilegiada? “Não sendo possível eliminar o risco, as sociedades de advogados têm de estar bastante atentas às perdas financeiras e reputacionais que podem derivar de um ciberataque”, defende Luís Neto Galvão, sócio da SRS e especialista em privacidade e proteção de dados.

Sofia Riço Calado, da mesma firma de advogados e também especialista em proteção de dados, lembra que o início da aplicação do Regulamento

Geral Sobre a Proteção de Dados, em maio passado, veio reforçar a consciencialização quanto à importância da existência de uma política adequada, fazendo assentar a “tónica na formação das pessoas em matéria de segurança da informação”.

Fala-se aqui, também, tal como refere Martim Bouza Serrano, de adotar procedimentos internos “que limitem o acesso à informação”, bem como de apostar “no melhoramento da segurança das redes informáticas” de que as sociedades de advogados dispõem.

Quando se fala de uma sociedade de advogados e do que procuram os hackers, é preciso levar em linha de conta, sublinha Luís Galvão Neto, que estão em causa dados relativos

“A norma é dizer que vai acontecer [um ciberataque], só não sabemos quando”, afirma Elsa Veloso.



Cinco anos de prisão para acesso ilegítimo

Página online foi encerrada

O blogue “Mercado de Benfca” (mercado de benfca.blogspot.com) onde foram divulgados os ficheiros alegadamente roubados à PLMJ, foi ontem encerrado, passando a ler-se na local onde estava alojado a seguinte mensagem: “esta página foi encerrada por violar os nossos termos e condições”. A PLMJ, de onde terão desaparecido ficheiros relacionados com os casos E-Toupeira, Secretas, EDP e Operação Marquês, admitiu em comunicado que a segurança da sua rede “foi recentemente comprometida”, estando a “avaliar o impacto potencial desse acesso ilegítimo a informação”.

a “segredos comerciais, a direitos de propriedade intelectual ou informação sobre potenciais transações comerciais ou matérias em segredo de justiça”. Até por isso, adianta: “infelizmente, num futuro próximo, é expectável que ataques idênticos [ao do caso PLMJ] se repitam com frequência.”

A advogada Elsa Veloso, fundadora da DPO Consulting, frisa que “mesmo com todas as precauções ao nível da segurança da informação, ninguém está a salvo de um ataque informático”. Aliás, “a norma é dizer que vai acontecer, só não sabemos quando”, sentença esta especializada em proteção de dados. ■



É expectável que ataques idênticos [ao do caso PLMJ] se repitam com frequência.

LUÍS NETO GALVÃO
Sócio da SRS

Será um erro pensar que existem sistemas sem vulnerabilidades.

MARTIM BOUZA SERRANO
Advogado coordenador da CCA-Ontier

Qualquer ataque com repercussões fortes na operação de uma sociedade de advogados será decorrente de uma atividade criminosa.

ANTÓNIO CAEIRO
Responsável de comunicações da Abreu Advogados

O ataque informático de que terá sido alvo a sociedade PLMJ é suscetível de configurar os crimes de acesso ilegítimo a um sistema informático e de disseminação por meios eletrónicos da informação obtida, que se encontram previstos na lei do cibercrime, explicou ao Negócios Manuel Durães Rocha, sócio da Abreu Advogados responsável pelas áreas de prática de Propriedade Intelectual e de Tecnologias da Informação.

A moldura penal para estes crimes, segundo o mesmo advogado foi estabelecida entre um a cinco anos. “A aplicação da pena mais grave ocorre quando o crime visar a obtenção e disseminação ilícita de segredos comerciais da vítima ou de informações confidenciais protegidas por lei”, explica o mesmo advogado.

A lei atual, além da pena de prisão, também prevê a aplicação de penas acessórias, “nomeadamente a perda dos equipamentos que serviram para a prática do crime”, adianta Manuel Durães Rocha.

Por outro lado, e de acordo com a advogada da SRS Sofia Riço Calado, especialista em proteção de dados, quando ocorrer o acesso não autorizado a dados pessoais, haverá também “um crime de acesso indevido que, por ocorrer através de violação de regras técnicas de segurança, poderá dar lugar a uma pena entre prisão até dois anos ou multa até 240 dias”. Isto, tendo em conta o que prevê a Lei de Proteção de Dados Pessoais, que ainda está em vigor. ■

negócios

negocios.pt

Quinta-feira, 10 de janeiro de 2019 | Diário | Ano XVI | N.º 3909 | € 2,50
Diretor **André Veríssimo** | Diretor adjunto **Celso Filipe**

Exportações para Itália dispararam em 2018

Vendas cresceram cinco vezes mais do que a média à boleia do T-Roc da Autoeuropa. PRIMEIRA LINHA 4 a 6

Metro de Lisboa pode chegar a Santo Amaro

Construção da linha circular vai custar 210 milhões de euros e estará concluída em 2023.



Rafael Marchante/Reuters

EMPRESAS 22

Contadores de eletricidade inteligentes podem voltar a ter apoios

EMPRESAS 20

Viagens de estudantes de Erasmus não abatem no IRS

ECONOMIA 12 e 13

Direito de resposta de Augusto Santos Silva

OPINIÃO 30

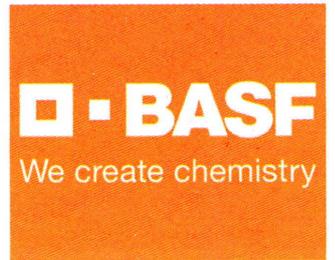
Gestora de fundos do GES alvo de coima pesada da CMVM

Falhas no combate ao branqueamento de capitais e prestação de informação falsa valeram à Gesfimo uma penalização de 300 mil euros.

MERCADOS 26 e 27

Créditos do BES só podem ser reclamados até 8 de março

EMPRESAS 24



Telecomunicações

Pharol deve ficar com 6% da Oi

Concretização do acordo está agora nas mãos do juiz e do administrador da Oi na Pharol.



A empresa liderada por Palha da Silva disparou ontem em bolsa.

PRIMEIRA LINHA 8 a 10

Lex

Advogados receiam tornar-se vítimas frequentes de ciberataques

ESPECIAL 16 e 17