



CRISTINA CARDOSO, DIRETORA DE VENDAS ALIDATA

CASA ROUBADA, TRANÇAS À PORTA

'PORTUGAL É DOS PAÍSES COM MAIS VÍTIMAS DE PHISHING'. 'RANSOMWARE TORNA PÚBLICOS DADOS EMPRESARIAIS, ATRAVÉS DE EXTORSÃO'. 'ESPIONAGEM CIBERNÉTICA USA MALWARE DISFARÇADO EM APLICAÇÕES'. 'TRABALHO REMOTO SOBRE-EXPÕE EMPRESAS A CIBERATAQUES'

Estes, são apenas alguns exemplos de títulos de notícias que saíram nos últimos meses sobre os riscos a que as empresas estão expostas. O cibercrime não é um problema que vise exclusivamente grandes corporações e governos. As pequenas, médias e até microempresas também são alvos apetecíveis, independentemente do setor de atividade.

Diz a sabedoria popular que 'casa roubada, tranças à porta', mas, 'mais vale prevenir que remediar'. Nesse sentido, é importante proteger a sua empresa de ataques cibernéticos. Ainda que seja uma realidade preocupante, a verdade é que muitos empresários e gestores negligenciam esse investimento, na esperança de que aconteça apenas aos outros. Ora, estes ataques colocam em risco investimentos, dados e equipamentos de TI. Imagine que um hacker tem acesso a informação de gestão, dados bancários da empresa, listas e cartões de crédito de clientes, planos estratégicos, processos ou outra informação confidencial e que faz a diferença para a sua oficina.

Acresce que estes ataques não colocam apenas a sua empresa em risco. Podem usá-la como trampolim para redes de outras empresas, o que ainda complica mais a equação. É fundamental ter sensibilidade para a devastação que um ciberataque pode infligir na sua empresa. Segundo estatísticas recentes, 60% das pequenas empresas vítimas de um ataque fecham até seis meses após o crime. Embora esse possa ser o resultado mais devastador do ataque, outros terão de ser considerados, como prejuízos financeiros decorrentes do roubo de informações bancárias e do período de interrupção dos negócios, custos para livrar definitivamente a sua empresa das ameaças e danos reputacionais, assim que informar os clientes que as suas informações foram comprometidas. Quantos desses voltarão a depositar confiança na sua empresa e regressam como clientes?

Independentemente da dimensão da sua rede de oficinas, de ser uma oficina independente, empresa de peças ou outros serviços de aftermarket automóvel, o risco à exposição de um ciberataque está

sempre presente. Felizmente, e ao contrário do que a esmagadora maioria dos empresários e gestores pensa, estar protegido contra ameaças externas não depende de um avultado orçamento.

Pedir uma auditoria de análise de risco a uma empresa especializada e conhecedora do setor é um obrigatório primeiro passo. Os seguintes, poderão até parecer simples, mas o facto é que muitas empresas não os acautelam. Falo de formação de colaboradores e criação de boas práticas, implementação de software antivírus adequado, atualização de todo o software da empresa, criação de backups constantes, quer físicos, quer para a cloud, encriptação de dados, proteção de firewall, ferramentas/software adequados, ou criação de uma política de segurança da informação, entre outros. ●

A GARANTIA DE SEGURANÇA E PRESERVAÇÃO DO PATRIMÔNIO INFORMÁTICO DA MAIORIA DAS EMPRESAS DEPENDE DE PEQUENOS CUIDADOS E INVESTIMENTOS

