85% das empresas já sofreram ataques virtuais, segundo a Kroll

Os benefícios dos meios digitais nas empresas são incontestáveis, mas a intensificação também abre maior espaço para a prática de crimes. Pesquisa da Kroll feita com 545 executivos de médias e grandes empresas pelo mundo constatou que 85% dessas companhias sofreu com ataques virtuais em 2016.

Essa foi a primeira vez que que a consultoria de riscos buscou informações a respeito desse tipo específico de crime. Entre os principais ataques virtuais sofridos por empresas estão infestações por vírus (citada por 33% dos entrevistados), *pishing* — e-mails coletivos com spam (26%), problemas de sistema (24%), violação de segurança (23%) e perda de dados por sistema corrompido por *malware* (22%).

Já as motivações são das mais diversas. Dentre as respostas, 26% dos entrevistados citou a vulnerabilidade do sistema que usam na companhia como culpada pelo ataque. Já 22% deles disseram que o episódio se deu por erro de um funcionário da companhia e 20% citaram roubo de aparelho com informações da empresa.

Dos efeitos dos ataques virtuais, o impacto na segurança e privacidade da empresa e de seus funcionários foi citado por 80% dos entrevistados. Esses mesmos quesitos, mas voltados aos parceiros dessa companhia, foram elencados por 74% dos executivos. Já os prejuízos na receita e na renovação dos negócios com clientes foi uma das respostas de 69% dos consultados. A reputação da corporação também foi lembrada, mas por 67% dos questionados.

Assim como nas fraudes físicas, ex-empregados (20% dos entrevistados), funcionários temporários ou autônomos (14%), agentes e intermediários (13%) e empregados da empresa (10%) foram apontados como os principais responsáveis pelos atos criminosos digitais. Os concorrentes foram citados por apenas 6% dos executivos.

Medidas de contenção
Para combater ou prevenir os ataques, as medidas mais tomadas pelas empresas atacadas para mitigar esses riscos foram melhorar o sistema de segurança dos dados, instaurar novas políticas de segurança, promover treinamentos sobre segurança virtual para funcionários e instalar sistema de detecção de intrusos.

A incidência de ataques virtuais por países é bem variada. Partindo de 73%, segundo os entrevistados indianos, até 95% entre os colombianos. Nos EUA e no Canadá, 88% dos executivos afirmaram terem sofrido com esses episódios. Já Reino Unido o resultado foi de 92%, sendo seguido pela África Subsaariana (91%), pelo Oriente Médio (90%), pela China (86%), por México e Rússia, ambos com 82%; Itália (79%) e Brasil (76%).

Entre os setores de atuação, as indústrias lideram com 91% das respostas. Depois estão os serviços financeiros (89%) e de venda e distribuição e de transporte e turismo, ambos com 87%; além do ramo de recursos naturais e o de saúde e biotecnologia (86%), serviços profissionais (84%), bens de consumo (83%). Por fim, com 77% cada um estão os mercados de construção, engenharia e infraestrutura;

tecnologia, mídia e telecomunicação.

Brasil virtual
Especificamente sobre o Brasil, onde 76% dos executivos disseram ter sofrido ataques virtuais, os principais responsáveis por esses delitos são os ex-funcionários das empresas, segundo 38% dos entrevistados. A média mundial nessa pesquisa foi de 20%. Apesar dessa discrepância entre os cenários interno e global, os principais tipos de ataque virtuais são os mesmos: vírus, violação de dados e problemas de sistema.

O especialista em segurança cibernética e diretor da Kroll no Brasil, Fernando Carbone, afirma que apesar do aumento nos investimentos em proteção digital no Brasil, os totais estão muito aquém do esperado por causa do surgimento de novas ameaças. O executivo da consultoria explica que entre os fatores que influenciam essas estatísticas está a falta de exigência, pelas leis brasileiras, de as empresas informarem as autoridades sobre esses ataques, mesmo que mal sucedidos.

“Outra informação relevante para a compreensão dos resultados da pesquisa diz respeito à demora em identificar uma invasão com potencial nocivo”, diz. Ele explica que esse ponto é muito importante, pois a ameaça pode permanecer imperceptível no sistema por um longo tempo.

Segundo Carbone, esse fato explica que no Brasil 38% dos casos envolveram ex-funcionários. Outra prática muito usada e destaca pelo diretor são os sequestros de dados. Nessa modalidade, as informações das empresas são criptografadas e o código para desfazer a ação só é concedido mediante pagamento. “Estão criptografando até o backup”, diz.

Ele lembra que o backup feito pelas empresas nunca deve ser guardado no mesmo lugar das informações, pois será sequestrado juntamente com os outros dados. “Ataques de *ransomware* ocorrem a cada 40 segundos. É um ataque em massa e eficaz”, alerta.

Carbone ressalta que a empresa precisa saber onde estão suas vulnerabilidades, pois, caso contrário, ela pode ser alvo do crime no dia seguinte. “Não há setor imune. Qualquer área que tiver vulnerabilidade, principalmente com exposição à internet, vai ser vítima desses fraudadores. Eles vasculham a internet, e onde acharem uma brecha, se aproveitarão dela”.

Date Created
20/02/2017