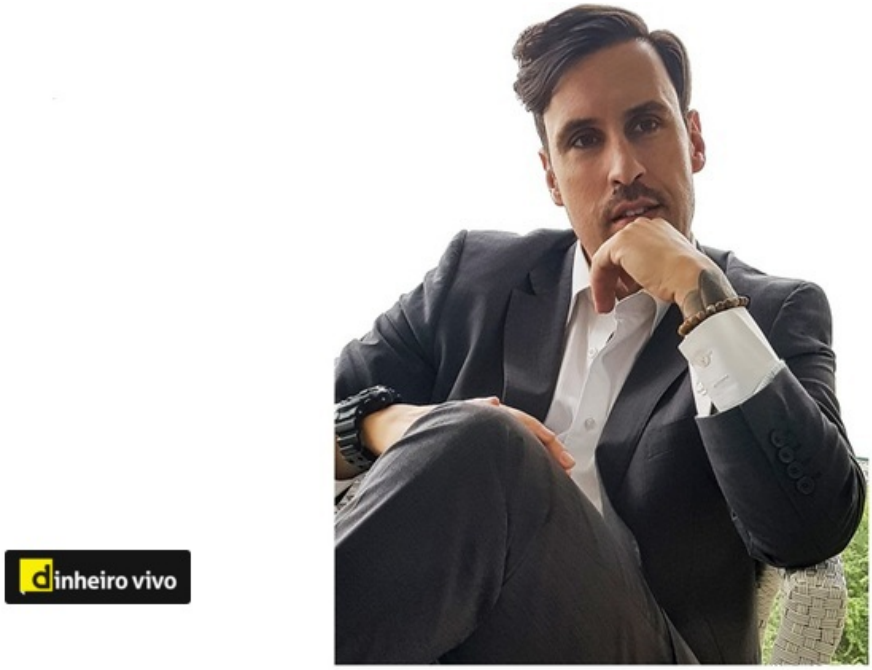
Análise forense: o que fazer se a sua empresa sofrer um ciberataque?

dinheirovivo.pt/opiniao/analise-forense-o-que-fazer-se-a-sua-empresa-sofrer-um-ciberataque-12811268.html

9 de setembro de 2019



Desde que haja exposição à internet, há risco de ciberataque, pelo que organizações de todos os setores, sejam elas públicas ou privadas, independentemente da sua dimensão ou geografia, devem estar alerta.

Um ciberataque é uma tentativa, muitas vezes bem-sucedida, de efetuar um crime orientado, tipicamente, para a comunidade cibernauta. As motivações são semelhantes ao crime tradicional, mas os meios utilizados estão associados à tecnologia. O roubo de identidade, propriedade intelectual ou informação, o assédio, a difamação, a extorsão, a espionagem, a fraude ou a manipulação representam crimes que podem igualmente ser cometidos virtualmente, mas com maior impunidade – dificuldade em identificar o criminoso – e com muito maior impacto, dada a "velocidade" do mundo digital.

Uma das vias preferenciais para atacar as empresas tem sido o correio eletrónico. Não é a única, mas é particularmente eficiente porque se faz valer da maior vulnerabilidade das organizações: as pessoas.

Os números indicam que os ataques cibernéticos só são detetados, em média, 90 dias depois de terem ocorrido. É essencial que, após ter detetado que foi alvo de um ataque, inicie, de imediato, um processo de investigação ou análise forense.

Primeiro, há que isolar e estancar o cenário do crime para que se possam analisar todas as "pegadas digitais", sem risco de contaminação. É essencial perceber quais foram os "alvos" do ataque, identificar os sistemas afetados e desconetá-los da rede, sem os

desligar. É fundamental envolver uma equipa especializada em análise forense para iniciar o processo de investigação.

Consoante a complexidade, a análise forense, que culmina com um relatório, pode ir de três dias a três semanas. Importa avaliar o cenário tecnológico e aplicacional afetado e, se possível, replicá-lo num ambiente de laboratório "isolado", para que, então, se possam desenvolver técnicas especializadas de recolha de prova.

Recolhendo informação sobre o impacto, evidências técnicas e linha do tempo, podemos decifrar qual o ataque e como foi realizado, quais os sistemas efetivamente atacados e qual o impacto e risco no momento atual.

Se possível, procede-se à identificação do autor do crime, analisando quais as ações a desenvolver junto e em coordenação direta com as autoridades - por exemplo, à luz do RGPD, se o incidente resultar na violação de dados pessoais, é necessário comunicá-lo no prazo de 72 horas. A equipa é ainda responsável pela tarefa particularmente sensível de acompanhar fornecedores e clientes, caso o incidente tenha repercussões nessas relações.

Ainda que o risco de incidente não possa ser eliminado por completo, é possível reduzi-lo preventivamente. A organização tem de ser capaz de avaliar regularmente o seu nível de segurança interno, através de auditorias, definir e implementar políticas de segurança que minimizem riscos na comunidade de colaboradores ou parceiros e, por fim, ser capaz de sensibilizar os seus colaboradores para o tema da segurança da informação – por exemplo, ensiná-los a identificar potenciais emails de *phishing* (ciberataque que implica a tentativa de "pesca" de um determinado tipo de informação por meios informáticos).

Afinal, como se costuma dizer na gíria da cibersegurança, não é uma questão de "se", mas de "quando" se vai sofrer um ciberataque. E, se a solução não passa por "desligar" do mundo digital, mais vale estar preparado!

Bruno Castro é CEO da VisionWare