A importância dos planos de resposta a incidentes de segurança

24.02.2021 3 minutos de leitura

Autores

Felipe Palhares

Áreas relacionadas

Proteção de Dados e Cybersecurity

Assuntos

Governança Corporativa | Proteção de Dados e Cybersecurity | LGPD | Felipe Palhares | Segurança Cibernética | Pandemia

Nos últimos meses, diversos **ataques cibernéticos** foram realizados, tendo como alvos tanto empresas, dos mais variados portes, quanto instituições governamentais, a exemplo dos recentes incidentes envolvendo uma série de tribunais brasileiros. Em agosto de 2020, a INTERPOL publicou um relatório[1] indicando um aumento alarmante no nível de crimes cibernéticos, incluindo ataques de *phishing*, de *ransomware* e de negação de serviço, os mais comumente utilizados por criminosos.

A elevação vertiginosa desses números coincide com a expansão da **pandemia de Covid-19** e a forte **digitalização** das organizações, em muitos casos realizada de modo abrupto, diante da necessária mudança imposta pelo contexto atual, sem que fosse possível realizar uma preparação adequada para a migração ao **trabalho remoto**.

Nessas circunstâncias, eventuais fragilidades tecnológicas ou vulnerabilidades relativas às práticas de segurança da informação podem abrir **brechas** relevantes para ataques e incidentes.

Ataques cibernéticos normalmente possuem um objetivo primordial: obter vantagem econômica indevida com a venda ou o uso de dados, sejam eles comerciais ou pessoais. No caso destes últimos, o **advento da Lei Geral de Proteção de Dados Pessoais (LGPD)** impõe a necessidade de cuidados redobrados com essas informações, sob pena de que eventuais violações à legislação resultem em sanções pecuniárias, ou, pior ainda, em danos incontornáveis à **reputação** da organização ou em ordens de proibição, parcial ou total, de tratamento de dados pessoais.

Para reduzir esses riscos, é fundamental que cada organização tenha um **programa de governança** em privacidade e proteção de dados, estabelecendo regras específicas para o tratamento de dados pessoais. Embora não seja uma obrigação legal, um programa de governança é reconhecido pela LGPD como uma boa prática, como prevê o artigo 50, § 2º, I, da legislação, e é capaz de servir como fator atenuante quando da aplicação de eventuais sanções administrativas.

Um dos pontos essenciais a ser contemplado no programa de governança é a **estruturação de um plano de resposta** a incidentes de segurança, estipulando os procedimentos a serem adotados quando da ocorrência de um incidente e determinando como os responsáveis devem agir frente a ele, para que haja clareza dos passos que devem ser tomados.

Em cenários caóticos, como o de um incidente que impede o acesso aos sistemas informáticos de uma empresa, é natural que os colaboradores não saibam exatamente como agir, perdendo-se no alvoroço do momento e ficando sem rumo, o que pode trazer consequências ainda mais complexas à organização. Quanto mais tempo passa sem que ações coordenadas sejam

tomadas para resolver o problema, mais se perde o **controle** da situação.

Um plano de resposta a incidentes deve servir de norte num momento de crise, dispondo sobre **aspectos práticos** relativos à identificação, contenção, investigação e comunicação de incidentes de segurança. Portanto, ainda que não seja um instrumento obrigatório, sua elaboração é altamente recomendável. Como já diz o ditado, é melhor prevenir do que remediar.

--

Notas de rodapé:

[1] Ver https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

*Esse artigo é parte da **BMA Review #70**. **Clique aqui** para ver todos os destaques desta edição.*

A Publicação também foi veiculada pelo portal Migalhas em 18/03/2021, clique aqui e confira o artigo na íntegra.

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares