5 dicas para evitar ataques de ransomware

24.02.2022 4 minutos de leitura

Autores

Felipe Palhares

Áreas relacionadas

Proteção de Dados e Cybersecurity

Assuntos

Proteção de Dados e Cybersecurity | Tecnologia e Negócios Digitais | Felipe Palhares | Ransomware | Incidentes de segurança

▸ Ouça no Spotify — 5 dicas para evitar ataques de ransomware

O aumento de ataques de ransonware e incidentes de informação é um dos grandes desafios para as empresas na atualidade. Nosso sócio da área de Proteção de Dados e Cybersecurity, Felipe Palhares, foi convidado pelo Bússula, do Portal Exame, para listar 5 ações que empresas devem tomar para se prevenir e evitar esse tipo de ataque.

Confira:

Time is of the essence

Para uma resposta adequada a um ataque de ransomware ou um incidente de segurança, todo segundo conta. Quanto mais o tempo passa sem que determinadas condutas sejam tomadas, mais difícil se torna resolver o problema com efetividade — principalmente pelo curto prazo de notificação da ANPD e pelos curtos prazos de "resgate".

Tenha ajuda externa

Não importa o tamanho da sua organização, nem a proficiência dos seus times internos: quando um ataque de ransomware acontece é essencial contar com suporte de assessores externos, tanto jurídicos, quanto técnicos.

O início não é o começo

Engana-se quem acha que um ataque de ransomware tem início quando os arquivos são criptografados e um dos colaboradores da organização encontra uma nota de resgate com informações sobre como recuperar o acesso aos dados. Para que um ataque possa ser adequadamente investigado, é fundamental que a organização guarde logs de forma apropriada e por períodos razoáveis. A adoção de um Siem pode ser medida extremamente benéfica nesse aspecto.

"Se não notificarmos, não acontecerá nada"

É óbvio que nenhuma organização gosta de notificar à Autoridade Nacional de Proteção de Dados ou a outros órgãos reguladores acerca da ocorrência de um incidente de segurança ou de um ataque de ransomware. Mas nos tempos atuais, é raro que um ataque de ransomware não seja noticiado em algum meio de comunicação.

A partir do momento em que o ataque se torna público, a ANPD envia um ofício à organização afetada, questionando sobre o ataque e pedindo

explicações sobre as razões pelas quais o incidente não foi notificado à Autoridade. Nesses cenários, perde-se a possibilidade de se argumentar que a organização atuou de boa-fé e com espírito de cooperação, aspectos atenuantes a eventual sanção que seja aplicada, estipulados nos incisos do § 1º do art. 52 da LGPD.

Documentar, documentar, documentar

Nos casos em que a decisão da organização for a de não comunicar à ANPD e aos titulares acerca do evento, por entender que não foi identificado risco ou dano relevante aos titulares, é fundamental que respectiva decisão seja documentada, incluindo o racional que levou até a decisão. A sugestão de produzir documentação não serve somente para a decisão acerca de comunicar ou não o evento à Autoridade Nacional de Proteção de Dados.

Todas as decisões relevantes que forem tomadas em relação ao evento (como realizar um boletim de ocorrência ou realizar ou não o pagamento de um pedido de resgate) também deveriam ser documentadas, especialmente quando a organização for uma Companhia Aberta, cujos diretores e membros do Conselho de Administração precisem comprovar que tomaram uma decisão desinteressada, refletida e informada, no melhor interesse da Companhia e de seus acionistas.

Segundo Palhares, pensar no pior cenário pode ser um bom caminho para mitigar os impactos, pois um incidente de segurança não é uma questão de "se", é uma questão de "quando".

Além disso, ainda de acordo com o advogado, um ataque de ransomware, nos dias de hoje, está muito longe de se limitar a criptografar os arquivos de uma organização, impedindo que eles sejam acessados sem a chave criptográfica, que somente é entregue mediante o pagamento de um resgate.

Por isso, antes que você seja vítima de um ataque de ransomware, é crucial fazer um exercício mental e imaginar qual seria o pior cenário para a sua organização caso um ataque acontecesse na data de hoje.

Pensar no pior cenário ajuda a, desde já, visualizar quais são as condutas que devem ser tomadas como precaução, antes mesmo que um ataque aconteça e a elaborar planos para o futuro. De nada adianta pensar nesse assunto só depois que o ataque ocorreu, quando já é tarde demais para remediar algumas fragilidades e as decisões se tornam menos flexíveis.

Clique aqui e confira a matéria na íntegra.

Quer saber mais? Baixe nossos e-books

E-book - Ransomware: como enfrentar ataques cibernéticos
E-book – LGPD
E-book – Incidentes de Segurança: Como Reagir

Ouça também:

DNA BMA Episódio #38 | "Ransomware e ataques cibernéticos"

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares