Atuação do compliance na resposta aos ataques de ransomware

06.06.2022 4 minutos de leitura

Autores

Felipe Palhares

Assuntos

Compliance, Investigações e Direito Sancionador | Compliance | Proteção de Dados e Cybersecurity | Ransomware

▸ Ouça no Spotify — Atuação do compliance na resposta aos ataques de ransomware

Os ataques de ransomware têm ganhado cada vez mais destaque na mídia, especialmente no Brasil, onde diversas companhias tiveram que enfrentar as investidas recentes de grupos especializados de hackers que atuam na criptografia de sistemas de armazenamento de informações, tornando os dados corporativos inacessíveis até que o resgate exigido pelos criminosos seja pago.

Crimes cibernéticos dessa natureza se baseiam na utilização de softwares desenvolvidos especialmente para causar danos aos computadores, servidores e redes das empresas e têm como foco as falhas de segurança nos sistemas para transferência ou guarda de dados. É importante destacar que as falhas não se restringem aos sistemas informatizados das empresas, mas incluem também os protocolos de segurança que contemplam o fator humano, gestão de segurança cibernética e falha das organizações e seus colaboradores em subestimar ou não considerar certos riscos, especialmente os de cybersecurity.

Inicialmente, para que o ataque seja concretizado, o ransomware deve identificar e invadir as portas de acesso à rede do ambiente de tecnologia da informação da empresa, vencendo as barreiras tradicionais de firewall e antivírus, de modo que este possa transitar na rede livremente, ou se alocar conforme sua programação.

É neste primeiro passo que se impõe o maior obstáculo aos hackers. É também nesse passo que o elemento da falha humana se manifesta como crucial no enfrentamento de um ataque, uma vez que a abertura, por meio dos usuários dos sistemas, de sites, links, documentos ou páginas com conteúdos maliciosos, técnica conhecida como phishing, permite que o ransomware infecte o ambiente corporativo facilmente, ganhando acesso aos ambientes capazes de identificar, armazenar, encriptar e transmitir dados das organizações às redes criminosas mantidas pelos atacantes.

É essencial que os esforços das empresas não se concentrem exclusivamente no mapeamento, identificação e testes de potenciais falhas de segurança, usualmente solucionadas por meio de atualizações e investimentos nas ferramentas de monitoramento contínuo, e na manutenção de backups e redundância de dados, mas que sejam investidos recursos em treinamento e conscientização dos seus integrantes. Em outras palavras, a atuação da área de Compliance, em conjunto com as áreas de TI e Segurança da Informação, deverá se dar, inclusive, preventivamente, no desenvolvimento de estratégias que visem a capacitação dos integrantes das organizações, garantindo que estes sejam capazes de entender, localizar, reportar e distinguir situações

regulares daquelas camufladas e disfarçadas de legítimas, criadas como vetores de ataques.

No contexto de resposta aos ataques e incidentes de segurança cibernética, é primordial que as empresas possuam um plano de resposta a incidentes pré-estabelecido, e constantemente atualizado, preparado para este tipo de investida, que deve contemplar, pelo menos, (i) um canal de comunicação específico, fora da eventual rede infectada e (ii) um comitê de segurança de informação, composto por integrantes-chave da organização, que deve incluir as áreas de Compliance, Segurança da Informação, relações públicas, recursos humanos, alta gestão, finanças, logística, dentre outros, a título de estruturação de um gabinete de crises.

Em síntese, estabelecer este plano permite desenhar respostas imediatas a ataques, com atuação de neutralização e reestabelecimento de operação mais eficiente, e tem como objetivo prioritário a continuidade dos negócios, com o mínimo de interrupções, vazamentos de ativos digitais e danos, ou, ao menos, garantir a diminuição do tempo de inatividade. Além disso, o plano de resposta deve suportar medidas de investigação, eliminação, recuperação e remediação, uma vez que é essencial que o evento seja adequadamente investigado e que todos os artefatos maliciosos sejam identificados e excluídos, evitando-se a reincidência do ataque num futuro próximo.

Nessa trilha de iniciativas, a contribuição de consultores jurídicos externos e especializados é bem-vinda para ajudar as empresas a compreender os riscos legais, regulatórios e de Compliance da exposição de informações potencialmente confidenciais e, ainda, para direcionar as investigações internas, coletas de provas digitais, confirmação e aplicação de cadeia de custódia de eventuais vestígios identificados, dentre outras medidas de natureza extrajudicial, em antecipação aos procedimentos das autoridades competentes.

Adicionalmente, o trabalho conduzido por consultores jurídicos externos garante a confidencialidade do trabalho de resposta aos ataques, em face da aplicação do Estatuto da Advocacia e da Ordem dos Advogados do Brasil (Lei n. 8.906/1994), e demais regulações aplicáveis às relações entre clientes e advogados, e, ainda, evita situações potenciais de conflito de interesses, uma vez que a equipe de investigação não será a mesma que atuou na prevenção e contenção dos ataques.

Assim, a atuação coordenada e imediata das áreas de compliance, em conjunto com a área de cybersecurity e outras específicas a serem definidas por cada empresa, para formar um time de gestão de crises, deve ser planejada e treinada previamente, para que o fator humano e a gestão de segurança possam servir como elementos de resposta aos incidentes, e não a razão de sua causa.

>>> Este artigo foi escrito por nosso sócio Felipe Palhares, da área de Proteção de Dados e Cybersecurity e por nossos advogados Jean Jaldin e João Bonvicino, ambos da área de Compliance, Investigações e Direito Sancionador. Este artigo foi veiculado pelo Estadão no dia 30/05/2022.

Clique aqui e confira o conteúdo na íntegra.

OUÇA TAMBÉM!

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares