

LISTA DE VERIFICAÇÃO: PROTEGER LIGAÇÕES A TERCEIROS

ESCOLHER FORNECEDORES COM CIBERSEGURANÇA EM MENTE

Sempre que avaliar um potencial fornecedor, verifique as seguintes perguntas:

- ☐ Que experiência têm os fornecedores na prestação de serviços a clientes semelhantes à sua organização?
- ☐ Documentaram a sua conformidade com os padrões de cibersegurança conhecidos (como o Quadro NIST ou ISO 27001, ou podem fornecer um relatório SOC2)?
- ☐ Quais dos seus dados e/ou ativos irão precisar para realizar os seus serviços e estão a solicitar qualquer acesso aparentemente desnecessário?
- ☐ Como planeiam proteger os ativos e dados da sua organização que estão na sua posse?
- ☐ Como gerem o seu próprio risco cibernético de terceiros e podem fornecer informações sobre a segurança da sua cadeia de abastecimento?
- ☐ Qual é o seu plano para recuperação de desastres e continuidade de negócios no caso de um incidente ter impacto na sua organização?
- ☐ Como irão manter a sua organização atualizada em termos de comunicação de tendências, ameaças e alterações dentro da sua organização?

IDENTIFICAÇÃO DE RISCO ATRAVÉS DE TERCEIROS

Realizar uma avaliação de risco cibernético de terceiros, incluindo os seguintes passos:

- ☐ Crie e mantenha uma lista atualizada de todas as relações com fornecedores e os ativos e dados expostos em cada uma.
- ☐ Realizar uma revisão dos dados que cada fornecedor ou terceiro tem acesso, garantindo que cada nível de acesso adere ao princípio de “menos privilégio”.
- ☐ Classifique o seu fornecedor e as relações com terceiros (baixo, médio, alto) com base no impacto que uma violação dos seus sistemas teria na sua organização.
- ☐ Começando pelos fornecedores de maior risco, avalie as capacidades de cibersegurança e compliance de cada fornecedor.
- ☐ Desenvolva um plano para realizar avaliações regulares, tendo em mente que pode querer ocasionalmente realizar avaliações no local de fornecedores com o maior risco e/ou maior acesso aos dados do cliente.

GESTÃO DE SEGURANÇA DE TERCEIROS

- ☐ Realizar diligência devida rigorosa. Estabeleça expectativas de cibersegurança nos pedidos da sua organização para propostas, contratos, continuidade do negócio, resposta a incidentes e acordos de nível de serviço com fornecedores. Acordar responsabilidades e obrigações em caso de acidente cibernético.
- ☐ Inquirir sobre as práticas de cibersegurança das organizações financeiras e outras entidades com as quais realiza transações ou partilha dados, tendo em mente que os seus fornecedores e terceiros devem igualmente cumprir quaisquer requisitos de cibersegurança que a sua organização deve cumprir.

- ☐ Utilize medidas estabelecidas e acordadas para monitorizar a conformidade dos seus fornecedores com os padrões de cibersegurança.
- ☐ Consulte os seus fornecedores que lidam com dados sensíveis para ver se oferecem autenticação de dois fatores, encriptação ou outras medidas de segurança para quaisquer contas que tenha com os mesmos.
- ☐ Certifique-se de que todo o software e hardware de terceiros que instalar têm um aperto de segurança para que os processos de arranque sejam protegidos através de códigos de autenticação e não serão executados se os códigos não forem reconhecidos.
- ☐ Se encontrar produtos de fornecedores que sejam falsificados ou não correspondam às especificações, trabalhe no sentido de negociar uma resolução ou outra estratégia de saída.
- ☐ Avalie anualmente contratos de fornecedores e certifique-se de que estes continuam a cumprir os requisitos de segurança de dados regulamentares e da direção. Após a rescisão do contrato, inclua estipulações sobre a obtenção dos seus ativos ou dados e verifique que os ativos ou dados são totalmente apagados no lado do fornecedor e desativam o acesso aos seus sistemas ou servidores.

INFORMAÇÃO RESUMIDA

- ☐ Certifique-se de que tem canais de comunicação claros e pontos de contacto para comunicar sobre questões de segurança com os fornecedores e contrapartes da sua organização.
- ☐ Verifique que se envolve de forma a garantir a partilha atempada de informações de cibersegurança fiáveis e acionáveis com partes interessadas internas e externas (incluindo entidades e autoridades públicas dentro e fora do setor financeiro).
- ☐ Monitorize as atualizações relevantes sobre o que outras organizações estão a experienciar com os seus terceiros em termos de ameaças, vulnerabilidades, incidentes e respostas fazendo parte das organizações de partilha de informações como o FS-ISAC e procurando outras fontes de informação de ameaças.