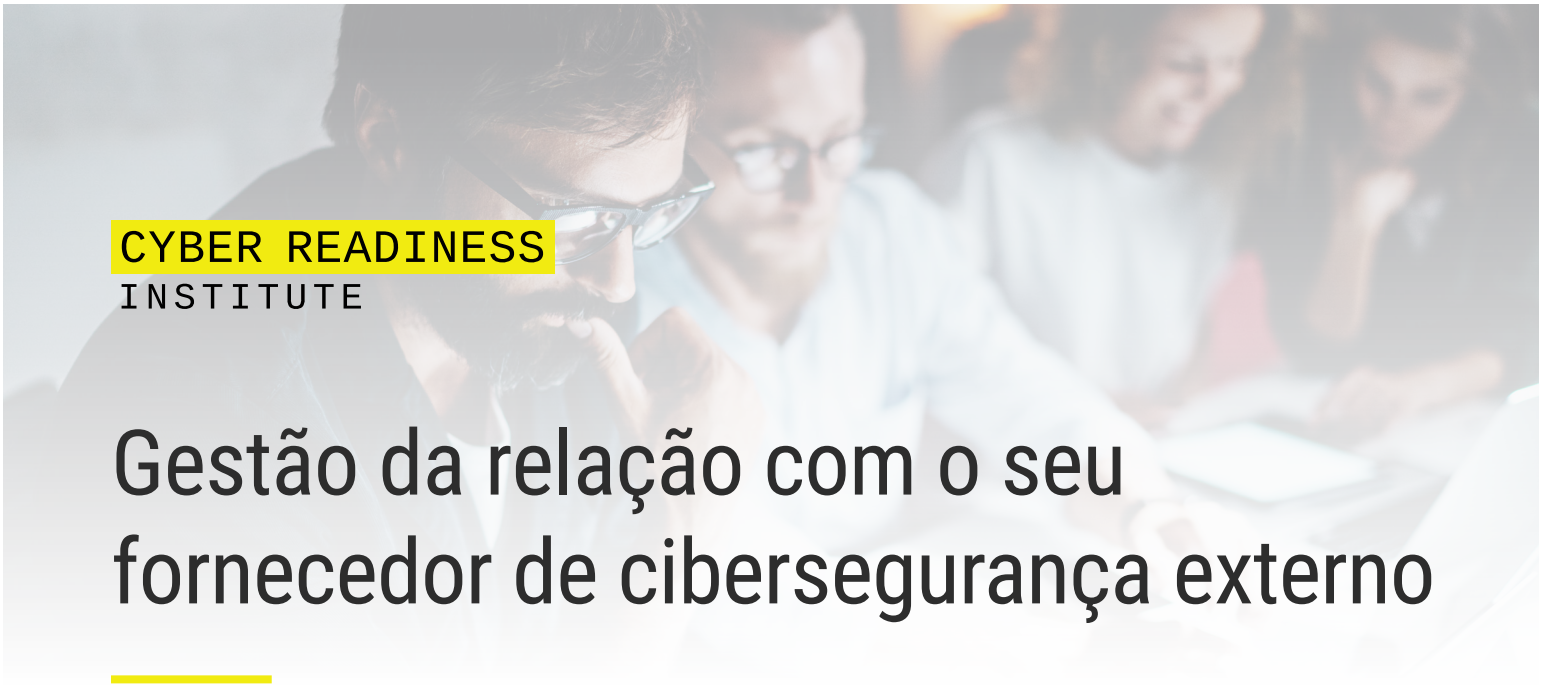

CYBER READINESS
INSTITUTE

Gestão da relação com o seu fornecedor de cibersegurança externo

Este é o último guia de uma série de cinco partes sobre como recorrer a empresas externas para reduzir o risco de cibersegurança.

No guia anterior, revimos o que deve ter em atenção num contrato com a sua empresa de suporte externa. Aqui, fornecemos orientações para uma boa gestão da relação. Hoje em dia, quase todas as empresas estão digitalmente ligadas aos seus clientes e a outras empresas. Os pequenos restaurantes dispõem de serviço de encomenda online. As pequenas empresas de contabilidade utilizam software baseado na cloud ou a partilha de ficheiros com os seus clientes. O e-mail e as mensagens de texto estão omnipresentes em todos os tipos de organização.

Como resultado, a relação que tem com a sua empresa de suporte de TI ou o seu fornecedor de serviços geridos (MSP) é tão importante para o seu negócio como a relação que tem com o seu contabilista ou banco. É do seu interesse tratar esta relação como uma prioridade e procurar que a empresa de suporte externa se torne um parceiro de confiança. A tecnologia está rapidamente a avançar e as ameaças de cibersegurança estão sempre a evoluir. É necessário estabelecer um canal de comunicação aberto e transparente com a empresa.

O primeiro ano é essencial para construir a base de uma relação a longo prazo. Não assine o contrato e depois arrume o assunto. Utilize o contrato como a base para estabelecer com clareza as respetivas responsabilidades no futuro. Recomendamos que marque reuniões mensais durante o primeiro trimestre e considere agendar uma chamada de seguimento pelo menos uma vez a cada três meses. Utilize a chamada de seguimento para se informar sobre o que estão a fazer na sua empresa e conhecer as novas tendências em termos de tecnologia e cibersegurança. Pergunte se há procedimentos que deve tomar para reduzir o risco cibernético e o que estão continuamente a fazer para ajudar a reduzir esse risco. Em última análise, lembre-se de que é responsável pelo comportamento humano na sua empresa. Ao definir uma revisão periódica com a cibersegurança na agenda, passa a mensagem de que a cibersegurança é importante para si. O objetivo é criar um canal de comunicação aberto e fiável para que a sua empresa de suporte externa se torne um parceiro.

Uma das ações que pode tomar para tirar o máximo partido da relação com o fornecedor é identificar um colega interno que se encarregue de gerir a relação. Peça a esse indivíduo (o líder cibernético) para obter a Certificação de líder cibernético do CRI, que inclui orientações sobre a gestão da relação com o fornecedor.

- ✓ Reveja as responsabilidades (deles e suas) para se certificar de que ambas as partes estão a fazer o que foi acordado.
- ✓ Avalie o seu fornecedor através de um inquérito de base anual. Considere uma avaliação semestral ou trimestral, consoante a importância crítica do software.
- ✓ Solicite informações atualizadas sobre a utilização do serviço (ou seja, número de pedidos de suporte de helpdesk, número de contas configuradas, data da última análise de vulnerabilidades de segurança, número de atualizações críticas abertas ou em falta, data do último teste de defesa contra o phishing e taxa de falhas da equipa, data e estado do último teste de resposta a incidentes, gestão de acesso remoto, utilização de autenticação multifator, etc.).

A relação que mantém com o seu suporte externo é uma das mais importantes para a sua empresa. Esperamos que esta série o tenha ajudado a identificar o nível adequado de serviço, a selecionar o tipo certo de empresa e a aprender a gerir a relação.

Sugestões para PMEs do Conselho Consultivo do CRI

- Nenhuma questão é irrelevante.
- Seja proativo.
- Defina uma sequência clara de pontos de contacto para estabelecer uma linha de comunicação com o fornecedor de serviços e validar se este sabe quem deve contactar dentro da sua empresa. Além disso, defina vários pontos de contacto, caso o seu contacto principal do fornecedor esteja fora do escritório.
- Faça um seguimento frequente e defina expectativas.
- Aceite sugestões sobre o que pode estar a faltar na sua empresa, especialmente considerando as relações do seu fornecedor com outros clientes.
- O seu fornecedor deve antecipar as suas necessidades e entendê-las de modo a que possa ajudá-lo antes de perceber que precisa da assistência dele.
- Compreenda os valores mútuos para estabelecer confiança. Estabeleça ligações pessoais na relação.
- A comunicação constante é essencial. Cimente a confiança investindo na comunicação bidirecional, mesmo se não houver proximidade física ou localidade.
- Seja claro sobre os limites de responsabilidade do cliente e do fornecedor. O cliente tem sempre um papel a desempenhar na cibersegurança.
- Não se deixe intimidar pela linguagem técnica. Se não compreender algo que o MSP lhe está a dizer, peça que o explique de uma forma menos técnica.

A lista completa de guias desta série:

Devo obter suporte externo para gerir o meu risco de cibersegurança?

Introdução aos tipos de suporte externo de TI e cibersegurança

Como selecionar o nível correto de suporte externo

Revisão e compreensão do contrato

Gestão da relação com o seu fornecedor de cibersegurança externo

(ESTE GUIA)

Autores que contribuíram

Agradecimentos especiais

- Marc Pillon, IT Ally
- Brian Kelly, EDUCAUSE
- Dawn Yankeelov, TALK
- Faye Francy, Auto-ISAC
- Ilene Klein, Cybercrime Support Network
- Jill Tokuda, CyberHawaii
- John Bryk, DNG-ISAC
- Michael Pritchard, Netchex
- Tanya Bolden, AIAG
- Walter Bran, ICC Guatemala
- Stan Stahl, SecureTheVillage
- Lisa McAuley, Global Trade Professionals Alliance
- Srinath Sogal, Cyber Academy for Kids through Empowerment
- Kathy Schultz, SUNY Cobleskill
- Sean Filipowski, SUNY Cobleskill
- Pam Hurt, NCMS
- Michael Fillios, TI Ally
- Lee Ann Lyle, TALK

Sobre o CRI

O Cyber Readiness Institute é uma iniciativa sem fins lucrativos que reúne líderes empresariais de vários setores e regiões geográficas para a partilha de recursos e conhecimento que informam o desenvolvimento de ferramentas gratuitas de segurança cibernética para pequenas e médias empresas (PMEs). Explore os blocos de construção de uma boa segurança cibernética com o nosso Kit de iniciação ou crie uma cultura de preparação cibernética na sua empresa com o Programa de preparação cibernética online. Os nossos recursos de teletrabalho e guias de local de trabalho híbrido oferecem sugestões oportunas para lidar com a evolução dos desafios cibernéticos da atualidade. Para saber mais, visite www.BeCyberReady.com.