Reforço da capacidade de cibersegurança
Caixa de ferramentas para organizações financeiras

Guia do nível do Conselho: Liderança de cibersegurança

Princípios Básicos da Governação do Risco Cibernético

Confirme que pode responder afirmativamente às seguintes perguntas:

1. A sua organização **cumpriu os requisitos estatutários e regulamentares relevantes**?

2. A sua organização **quantificou as suas exposições cibernéticas e testou a sua resiliência financeira**?

3. A sua organização tem um **plano de melhoria** para garantir que as exposições estão dentro da sua apetência pelo risco acordada?

4. O Conselho **discute regularmente informações concisas, claras e exequíveis relativamente à ciber-resiliência da organização fornecidas pela direção**?

5. A sua organização tem **planos de resposta a incidentes que tenham sido recentemente tratados a título de ensaio**, incluindo ao nível do Conselho?

6. As **funções dos responsáveis principais pela gestão do risco cibernético são** claras e estão em concordância com as três linhas de defesa?

7. Já obteve **validação e garantia independentes** da postura de risco cibernético da sua organização?

Supervisão

Como o nível mais alto da liderança da sua organização, o Conselho assume a máxima responsabilidade por controlar o risco cibernético e, por conseguinte, deve supervisionar a estratégia, políticas e atividades da organização nesta área. Especificamente, o Conselho deve:

⇒ Assumir a responsabilidade final pela supervisão do risco cibernético e da resiliência, seja como Conselho no seu todo ou através da delegação de supervisão numa Comissão de Conselho específica.
⇒ Designar um responsável da empresa, normalmente o CISO (Chief information security officer, [Diretor Executivo de Segurança da Informação]), para ser responsável por reportar a capacidade da sua organização de gerir a ciber-resiliência e o progresso na implementação dos objetivos da ciber-resiliência. Certificar-se de que este responsável tem acesso regular ao Conselho, autoridade suficiente, domínio do assunto, experiência e recursos para cumprir estes deveres.
⇒ Definir anualmente a tolerância ao risco da sua organização; garantir a consistência com a sua estratégia empresarial e apetência pelo risco.
⇒ Certificar-se de que é realizada anualmente uma revisão de ciber-resiliência independente e formal da sua organização.
⇒ Supervisionar a criação, implementação, teste e melhoria contínua dos planos de ciber-resiliência, assegurando conformidade em toda a sua organização e que o seu CISO ou outro responsável reporta regularmente os mesmos à administração.
⇒ Integrar a ciber-resiliência e a avaliação de riscos na estratégia global de negócio da sua organização, gestão de risco, orçamentação e alocação de recursos, com o objetivo de integrar totalmente o risco cibernético em risco operacional global.
⇒ Rever periodicamente o seu desempenho relativamente ao acima e considerar aconselhamento independente para melhoria contínua.

Manter-se informado

A supervisão eficaz do risco cibernético do Conselho depende do domínio dos membros sobre o tema e da informação atualizada.

⇒ Certifique-se de que todos os indivíduos que participam no Conselho têm competências e conhecimentos adequados e atualizados para compreender e gerir os riscos colocados por ameaças cibernéticas.
⇒ Solicite aconselhamento regular à direção sobre a exposição ao risco atual e futura da sua organização, requisitos regulamentares relevantes e referências da indústria e da sociedade quanto à apetência pelo risco. Além disso, envolva-se em briefings regulares sobre os últimos desenvolvimentos em relação ao cenário de ameaças e ambiente regulamentar, planeamento conjunto e visitas aos pares de melhores práticas e líderes em cibersegurança e trocas ao nível da Conselho no que se refere a governança e comunicação.
⇒ Responsabilize a direção por comunicar uma avaliação quantificada e compreensível dos riscos cibernéticos, ameaças e eventos como um elemento de ordem de trabalhos permanente durante as reuniões do Conselho.
⇒ Mantenha a consciencialização de desafios sistémicos contínuos, tais como vulnerabilidades da cadeia de fornecimento, dependências comuns e a lacuna na partilha de informação entre conselhos sobre a governação de risco cibernético.

Definir o tom

Juntamente com a direção sénior, o Conselho deve definir e exemplificar os valores fundamentais, a cultura de risco e as expetativas da sua organização relativamente à ciber-resiliência.

⇒ Promova uma cultura em que o pessoal a todos os níveis reconheça as suas responsabilidades importantes em garantir a ciber-resiliência da sua organização. Liderar dando o exemplo.
⇒ Supervisione o papel da direção na promoção e manutenção da cultura de risco da sua organização. Promova, monitorize e avalie a cultura de risco, considerando o impacto da cultura na segurança e solidez e proceder a alterações quando necessário.
⇒ Torne claro que espera que todo o pessoal atue com integridade e que remeta rapidamente a não conformidade observada dentro ou fora da sua organização.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

Reforço da capacidade de cibersegurança
Caixa de ferramentas para organizações financeiras

Guia ao nível do CEO: Liderança de cibersegurança

Governança

A segurança cibernética da sua organização começa e termina ao nível mais elevado da gestão. O CEO, juntamente com o Conselho, deve manter a compreensão dos riscos e assumir a responsabilidade final e responsabilidade pelas atividades e pessoal de cibersegurança da organização. Deve:

⇒ Contratar um Diretor Executivo de Segurança da informação (CISO), caso não exista, ou, se os recursos forem demasiado limitados, nomear alguém dentro da sua organização para desempenhar a função de um CISO.
⇒ Trabalhar com o CISO ou outro pessoal técnico para estabelecer e manter uma estratégia e estrutura de cibersegurança adaptada aos riscos cibernéticos específicos da organização, utilizando normas e diretrizes internacionais, nacionais e da indústria.
⇒ Articular funções e responsabilidades claras para o pessoal que implementa e gere a cibersegurança da organização.

- Trabalhar com o CISO para identificar as funções de cibersegurança adequadas e direitos de acesso para todos os níveis de pessoal.
- Supervisionar a comunicação e colaboração para garantir que a gestão de cibersegurança é holística, principalmente se as responsabilidades de cibersegurança forem partilhadas por vários funcionários ou divisões dentro da organização (como, por exemplo, ter informações de segurança da informação, risco e tecnologia).

⇒ Certificar-se de que o CISO tem uma linha direta e clara de comunicação para relacionar ameaças de forma atempada para si e para o Conselho.
⇒ Convidar o CISO ou outro pessoal técnico para informar regularmente a alta direção.
⇒ Certificar-se de que as políticas de segurança, normas, mecanismos de aplicação e procedimentos da organização são uniformes em todas as equipas e linhas de negócio.

Avaliação e gestão de riscos

Garantir que uma forte consciencialização e preparação de cibersegurança depende da análise contínua baseada no risco. Para melhorar a cibersegurança da sua organização:

⇒ Estabeleça a avaliação e gestão do risco de cibersegurança como uma prioridade nos processos de controlo e gestão de riscos mais amplos da sua organização. Trabalhe com o seu CISO ou outro pessoal técnico num plano para realizar uma avaliação de risco que envolva:

- Descrever os ativos da sua organização e os seus vários níveis de dependência tecnológica,
- Avaliar a maturidade da sua organização e os riscos inerentes associados às dependências tecnológicas dos seus ativos,
- Determinar o estado desejado da maturidade da sua organização,
- Compreender onde as ameaças de cibersegurança se encontram na lista de prioridades de risco da sua organização,
- Identificar lacunas entre o seu estado atual de cibersegurança e o estado alvo pretendido,
- Implementar planos para atingir e sustentar a maturidade,
- Reavaliar continuamente a maturidade, os riscos e os objetivos da segurança cibernética da sua organização, e
- Considerar a utilização de testes de invasão de terceiros ou red-teaming,
- Considerar medidas de proteção como a compra de um seguro cibernético.

⇒ Liderar os esforços dos funcionários durante o processo de avaliação de riscos para facilitar respostas atempadas de toda a instituição.
⇒ Analisar e apresentar os resultados da avaliação de risco para a supervisão executiva, incluindo os principais intervenientes e o Conselho.
⇒ Supervisionar quaisquer alterações para manter ou aumentar a preparação da cibersegurança pretendida da sua organização, assegurando que quaisquer medidas tomadas para melhorar a cibersegurança são proporcionais aos riscos e acessíveis para a sua organização.
⇒ Supervisionar o desempenho da monitorização contínua para se manter ágil e flexível no tratamento de risco cibernético em evolução.

Cultura organizacional

A cibersegurança da sua organização não é um processo único ou o trabalho de alguns funcionários; é um fator a considerar em todas as decisões e operações comerciais e uma prática que deve ser mantida por todos os funcionários. Para incentivar a cibersegurança contínua e holística dentro da sua organização:

⇒ Inicie discussões sobre cibersegurança com a equipa de liderança e comunicar regularmente com o pessoal responsável pela gestão de riscos cibernéticos.
⇒ Faça com que a formação de cibersegurança faça parte de toda a integração dos funcionários, assegurando que todos os funcionários estão atualizados – e assinaram documentos em que concordam em cumprir – as políticas de cibersegurança da sua organização e que o seu departamento de TI ou outro pessoal técnico os tenha informado sobre as melhores práticas.
⇒ Institua formação de cibersegurança recorrente para todo o pessoal relativamente às suas responsabilidades de segurança a curto e longo prazo.
⇒ Certifique-se de que a cibersegurança é sempre considerada quando a sua organização avalia potenciais fornecedores e partilha dados com terceiros.
⇒ Reveja anualmente as políticas de cibersegurança da sua organização.
⇒ Incentive a partilha voluntária de informação sobre ameaças de cibersegurança e incidentes dentro da sua organização e com contrapartes de confiança.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

Reforço da capacidade de cibersegurança
Caixa de ferramentas para organizações financeiras

Guia do nível CISO: Proteger a sua organização

Desenvolver um Programa de Segurança de Informações Baseado no Risco

1. Identificar os tipos de informação que o seu negócio armazena e usa
⇒ Listar todos os tipos de informação que o seu negócio armazena e usa (por exemplo, nomes e endereços de correio eletrónico de clientes).

2. Definir o valor da sua informação
⇒ Coloque perguntas-chave para cada tipo de informação:

- O que aconteceria se esta informação fosse tornada pública?
- O que aconteceria ao meu negócio se esta informação estivesse incorreta, por exemplo, a integridade dos dados tivesse sido manipulada?
- O que aconteceria ao meu negócio se eu/os meus clientes não conseguíssemos aceder a esta informação?

3. Desenvolver um inventário
⇒ Identifique que tecnologia entra em contacto com as informações que identificou. Isto pode incluir hardware (por exemplo, computadores) e aplicações de software (por exemplo, e-mail do navegador). Inclua a marca, o modelo, os números de série e outros identificadores. Controle o local onde se encontra cada produto. Para software, identifique em que máquina(s) foi carregado o software.
⇒ Quando aplicável, inclua tecnologias fora do seu negócio (por exemplo, "a nuvem") e quaisquer tecnologias de proteção que tenha instaladas, como firewalls.

4. Compreenda as suas ameaças e vulnerabilidades
⇒ Reveja regularmente as ameaças e vulnerabilidades que o sector financeiro pode enfrentar e calcule a probabilidade de ser afetado. (As informações podem ser encontradas através do seu CERT nacional, FS-ISAC, o seu capítulo local da InFragard e outros.)
⇒ Realize um scan ou análise de vulnerabilidade, pelo menos, uma vez por ano.

5. Criar uma política de cibersegurança
⇒ Trabalhe com a alta direção da sua organização para estabelecer e manter uma estratégia de cibersegurança que seja adaptada aos riscos acima e informada pelas normas e diretrizes internacionais, nacionais e da indústria. Orientações como o Quadro NIST, a Ferramenta de Avaliação de Cibersegurança da FFIEC e a ISO 27001 fornecem modelos para reforçar e melhorar estas políticas.
⇒ Dê formação a todos os funcionários sobre os detalhes da política e peça-lhes que assinem os documentos reconhecendo o seu papel na manutenção contínua da cibersegurança da sua organização aderindo à política.

Prevenir danos de malware

⇒ Ative a sua firewall e definir listas de controlo de acesso (ACLs) para criar uma zona de tampão entre a sua rede e a Internet. Restrinja o acesso utilizando uma definição de lista branca, não colocando em lista negra determinados endereços ou serviços de IP.
⇒ Utilize software antivírus e anti-spyware em todos os computadores e computadores portáteis.
⇒ Atualize todo o software e firmware aplicando prontamente as atualizações de software mais recentes fornecidas pelos fabricantes e fornecedores. "Atualização automática", quando disponível.
⇒ Restrinja a instalação de novos programas a pessoal de TI com direitos administrativos.
⇒ Mantenha e monitorizar registos de atividade gerados por hardware de proteção/deteção ou software. Proteja os registos com proteção e encriptação de palavra-passe.
⇒ Mantenha todos os relógios de anfitrião sincronizados. Se os dispositivos da sua organização tiverem definições de relógio inconsistentes, a correlação de eventos será muito mais difícil quando ocorrem incidentes.
⇒ Controle o acesso a suportes amovíveis tais como cartões SD e pens USB. Incentive o pessoal a transferir ficheiros por e-mail ou armazenamento na cloud. Eduque os funcionários sobre os riscos de utilizar os USBs de fontes externas ou ao entregar os próprios USBs a outros.
⇒ Configure a segurança de e-mail e filtros de spam nos seus serviços de e-mail.
⇒ Proteja todas as páginas nos seus websites de contactos públicos com encriptação e outras ferramentas disponíveis.
⇒ Considere contratar um serviço de teste de invasão para avaliar a segurança dos ativos e sistemas da sua organização.

Formar funcionários

⇒ Realize formações obrigatórias de cibersegurança durante a admissão de novos funcionários e a intervalos regulares para todos os funcionários atuais, pelo menos, uma vez por ano. Exija que os funcionários:

- Utilizem palavras-passe fortes em todos os dispositivos e contas profissionais e incentive os mesmos a usar o mesmo procedimento para dispositivos pessoais e a utilizar um gestor de palavras-passe,
- Mantenham todos os sistemas operativos, software e aplicações atualizados em todos os dispositivos,
- Utilizem autenticação de dois fatores em todas as contas,
- Mantenham os detalhes da conta e os cartões de acesso seguros e bloqueiem os dispositivos quando se ausentarem,
- Não partilhem detalhes da conta ou outros dados sensíveis através de e-mail não encriptado ou outras comunicações abertas,
- Evitem abrir imediatamente anexos ou clicar em ligações em e-mails não solicitados ou suspeitos,
- Verifiquem a validade de um e-mail suspeito ou uma caixa pop-up antes de fornecer informações pessoais e prestem muita atenção ao endereço de e-mail, e
- Comuniquem quaisquer incidentes de segurança internos ou externos, ameaças ou manuseamento incorreto de dados ou dispositivos ao pessoal técnico da sua organização e/ou a uma diretor superior.

⇒ Teste regularmente a consciencialização dos funcionários através de problemas simulados, tais como enviar e-mails do estilo phishing de contas falsas. Use quaisquer falhas como oportunidades de aprendizagem ao invés de punição.

Proteger os seus dados

⇒ Efetue cópias de segurança regulares dos seus dados importantes (por exemplo, documentos, e-mails, calendários) e teste que podem ser restaurados. Considere fazer cópias de segurança para à nuvem.
⇒ Certifique-se de que o dispositivo que contém a sua cópia de segurança não está permanentemente ligado ao dispositivo que contém a cópia original, nem fisicamente nem através de uma rede local.
⇒ Instale protetores contra surto, utilize geradores e certifique-se de que todos os seus computadores e dispositivos de rede críticos estão ligados a fontes de alimentação ininterrupta.
⇒ Utilize uma solução de gestão de dispositivos móveis (MDM).

Manter os seus dispositivos seguros

⇒ Ligar o PIN e proteção de palavra-passe para dispositivos móveis. Configure os dispositivos para que, quando perdidos ou roubados, possam ser monitorizados, limpos remotamente ou bloqueados remotamente.
⇒ Mantenha os seus dispositivos (e todas as aplicações instaladas) atualizados, usando a opção 'atualizar automaticamente', se disponível.
⇒ Ao enviar dados sensíveis, não se ligue a hotspots públicos Wi-Fi públicos – utilize ligações celulares (incluindo "tethering" e dongles sem fios) ou utilize VPNs.
⇒ Substitua os dispositivos que já não são suportados por fabricantes com alternativas atualizadas.
⇒ Defina procedimentos de comunicação para equipamento perdido ou roubado.

Utilizar palavras-passe

⇒ Certifique-se de que todos os computadores utilizam produtos de encriptação que necessitam de uma palavra-passe para arrancar. Ligue a palavra-passe ou a proteção de PIN para dispositivos móveis.
⇒ Utilize palavras-passe fortes, evite palavras-passe previsíveis (como passw0rd) e identificadores pessoais (como nomes de família e animais). Instrua todos os funcionários a usar o mesmo procedimento.
⇒ Sempre que possível, utilize a autenticação de dois fatores (2FA).
⇒ Altere as palavras-passe predefinidas emitidas pelo fabricante em todos os dispositivos, incluindo dispositivos de rede e IoT, antes de serem distribuídos ao pessoal.
⇒ Certifique-se de que o pessoal pode repor as suas próprias palavras-passe facilmente. Pode também desejar que o pessoal altere a sua palavra-passe em intervalos regulares (por exemplo, trimestralmente, semestral ou anualmente).
⇒ Considere utilizar um gestor de palavras-passe. Se utilizar um, certifique-se de que a palavra-passe "principal" (que fornece acesso a todas as suas outras palavras-passe) é uma palavra-passe forte.

Controlo de permissões

⇒ Certifique-se de que todo o pessoal tem contas de identificação exclusiva que são autenticadas sempre que aceder aos seus sistemas.
⇒ Ofereça apenas privilégios administrativos ao pessoal de TI de confiança e pessoal-chave e revogar privilégios de administrador nas estações de trabalho para utilizadores padrão.
⇒ Faculte aos funcionários apenas acesso aos sistemas de dados específicos de que necessitam para os seus trabalhos e garanta que não podem instalar qualquer software sem permissão.
⇒ Controle o acesso físico aos seus computadores e crie contas de utilizador para cada funcionário.

Proteger as suas redes e dispositivos Wi-Fi

⇒ Certifique-se de que o Wi-Fi do seu local de trabalho está seguro e encriptado com a WPA2. Os routers vêm muitas vezes com encriptação desligada, por isso certifique-se de que a liga. A palavra-passe protege o acesso ao router e certifique-se de que a palavra-passe é atualizada a partir da predefinição predefinida. Desligue quaisquer funcionalidades de "gestão remota".
⇒ Configure o seu router ou router sem fios para que não transmita o nome da rede, conhecido como Identificador do Conjunto de Serviços (SSID).
⇒ Limite o acesso à sua rede Wi-Fi permitindo apenas dispositivos com determinados endereços de controlo de acesso ao media. Se os clientes precisarem de Wi-Fi, crie uma rede pública separada.
⇒ Ative o Dynamic Host Configuration Protocol (DHCP, [Protocolo de Configuração Dinâmica de Host]), iniciando sessão nos seus dispositivos de rede, para permitir um seguimento fácil de todos os dispositivos que estão na sua rede.
⇒ Termine a sessão como administrador depois de ter configurado o router.
⇒ Mantenha o software do router atualizado. Saiba mais sobre as atualizações registando o seu router com o fabricante e inscrevendo-se para receber atualizações.

Evitar ataques de phishing

⇒ Certifique-se de que os funcionários não navegam na Web ou verificam e-mails em servidores ou de uma conta com privilégios de Administrador.
⇒ Configurar filtros de e-mail e web. Considere bloquear funcionários de visitar websites normalmente associados a ameaças de cibersegurança.
⇒ Ensine os funcionários a procurar sinais óbvios de phishing, como má ortografia e gramática, ou versões de baixa qualidade de logótipos reconhecíveis. O endereço de e-mail do remetente parece legítimo?
⇒ Verifique malware e altere palavras-passe logo que possível se suspeitar que ocorreu um ataque. Não penalize a equipa se esta se tornar vítima de um ataque de phishing (desencoraja as pessoas de comunicarem no futuro).

Reforço da capacidade de cibersegurança
Caixa de ferramentas para organizações financeiras

Guia do nível CISO: Proteger os seus clientes

Aconselhamento individual para clientes e funcionários para proteger dados financeiros

Aconselhe os seus funcionários e os seus clientes a seguir as orientações de cibersegurança abaixo no seu comportamento pessoal para aumentar a sua preparação e proteger os seus dados financeiros contra ameaças cibernéticas.

1. Implemente práticas básicas de higiene cibernética nos seus dispositivos.
⇒ Utilize palavras-passe fortes em todos os dispositivos pessoais e profissionais e considere utilizar um gestor de palavras-passe.
⇒ Mantenha os sistemas operativos e outros softwares e aplicações atualizados nos seus computadores e dispositivos móveis.
⇒ Instale software antivírus, anti-malware e anti-ransomware que previne, deteta e remove programas maliciosos.
⇒ Utilize um programa de firewall para impedir o acesso não autorizado ao seu computador.
⇒ Utilize apenas produtos de segurança de empresas conceituadas. Leia comentários de publicações de computadores e consumidores e considere consultar o fabricante do seu computador ou sistema operativo.

2. Tenha cuidado com informações sensíveis.
⇒ Não envie palavras-passe de contas bancárias ou outros dados de contas financeiras sensíveis por e-mail não encriptado.
⇒ Seja inteligente sobre onde e como se estabelece a ligação à Internet para comunicações bancárias ou outras comunicações que envolvam informações pessoais sensíveis. As redes e computadores Wi-Fi públicos em locais como bibliotecas ou centros comerciais de hotéis podem ser arriscados.

3. Resistir ao phishing.
⇒ Não abra imediatamente anexos de e-mail ou clique em ligações de e-mails não solicitados ou suspeitos. Pare. Pense. Clique.
⇒ Suspeite se alguém o contactar inesperadamente online ou por telefone e pedir a sua informação pessoal. Mesmo quando comunica com endereços conhecidos, minimize a partilha de informações pessoais por e-mail.
⇒ Lembre-se de que nenhuma instituição financeira irá enviar-lhe um e-mail ou contactá-lo e solicitar informações confidenciais que já tenha sobre si.
⇒ Assuma que um pedido de informações de um banco onde nunca abriu uma conta é um esquema fraudulento.
⇒ Verifique a validade de um e-mail de aspeto suspeito ou uma caixa pop-up antes de fornecer informações pessoais. Preste muita atenção ao endereço de e-mail.

Administrar contas

⇒ Peça aos clientes que utilizem ID de utilizador e palavras-passe fortes para iniciar sessão nos seus serviços. Aconselhe-os a não utilizar a mesma palavra-passe como o fazem para outras contas.
⇒ Utilize a verificação instantânea, verificação em tempo real, verificação de "trial deposits", verificação da identidade e/ou perguntas pessoais para validar clientes reais e reduzir a oportunidade de fraude.
⇒ Ofereça, idealmente peça, autenticação de dois fatores para os clientes utilizarem ao iniciar sessão nos seus serviços.
⇒ Verifique regularmente as contas do utilizador para sinais de fraude.

Proteger dados

⇒ Considere quais os dados de clientes que a sua organização *deve* recolher para prestar os seus serviços e seja cauteloso na recolha de quaisquer dados de clientes que possam ir além dessa finalidade.
⇒ Definir e distribuir políticas de retenção de dados. Elimine os dados do cliente quando já não forem necessários.
⇒ Encripte os dados do cliente em trânsito e em repouso.
⇒ Implemente políticas de segurança de dados para esclarecer quais os métodos de transferência de dados aprovados versus restritos e para especificar o que é aceitável para todos os funcionários ao lidar com dados de clientes. Certifique-se de que estas políticas são documentadas, comunicadas, aplicadas a todos os funcionários e revistas e atualizadas periodicamente.

Proteger aplicações Web públicas

⇒ Implemente HTTPS na(s) aplicação(ões) Web direcionadas para o público da sua organização e redirecione todo o tráfego HTTP para HTTPS.
⇒ Utilize uma política de segurança de conteúdo no(s) seu(s) website(s) para evitar ataques de scripting entre sites, clickjacking e outra injeção de códigos.
⇒ Permita a fixação de chaves públicas no(s) seu(s) website(s) para impedir ataques de intrusos.
⇒ Certifique-se de que a(s) sua(s) aplicação(s) de rede pública nunca utiliza(m) cookies para armazenar informações de clientes altamente sensíveis ou críticas (tais como palavras-passe) e que têm prazos de validade conservadores para cookies (melhor mais cedo do que mais tarde). Considere encriptar as informações armazenadas nos cookies que utiliza.
⇒ Considere contratar um serviço de teste de invasão para avaliar a segurança da sua aplicação de rede pública, pelo menos, uma vez por ano.

Formar funcionários

⇒ Ensine a responsabilidade e as estratégias dos seus funcionários para minimizar o erro humano que possa expor os dados dos clientes. Isto significa aconselhá-los a:

- Minimizar o seu acesso e transmissão de dados de clientes apenas para o que é necessário para desempenhar as suas funções profissionais,
- Manter fortes práticas de segurança em todos os dispositivos e contas que lidam com os dados do cliente utilizando palavras-passe fortes, permitindo a autenticação de dois fatores, mantendo o software atualizado e não clicando em ligações suspeitas, e
- Comunicar quaisquer potenciais incidentes de segurança internos ou externos, ameaças ou manuseamento incorreto de dados ao pessoal técnico da sua organização e/ou a direção superior.

⇒ Certifique-se de que os seus funcionários compreendem e assinaram documentos para aderir às políticas de proteção de dados e segurança da sua organização, para que não os violem, para que sejam fluentes ao lidar com os clientes e que não comuniquem com os clientes de forma desprotegida.

Notificar clientes

⇒ Compreender o ambiente regulamentar da sua organização no que diz respeito ao tratamento de violações de dados dos clientes para garantir que está preparado para cumprir quando ocorrem incidentes.

⇒ Quando a sua organização toma conhecimento de um incidente de acesso não autorizado a informações sensíveis do cliente, investigue para determinar de imediato a probabilidade de a informação ter sido ou ser usada indevidamente. Siga as melhores práticas de notificação e notifique o(s) cliente(s) afetado(s) assim que possível com:

- Uma descrição geral do incidente e a informação que foi violada,
- Um número de telefone para mais informações e assistência,
- Um lembrete “para permanecer atento” nos próximos 12 a 24 meses,
- Uma recomendação para que os incidentes de suspeita de roubo de identidade sejam comunicados imediatamente,
- Uma descrição geral das medidas tomadas pela instituição financeira para proteger a informação de acesso ou utilização não autorizados,
- Informações de contacto para agências de informação comercial, e
- Qualquer outra informação que seja exigida pelos regulamentos com os quais a sua organização deve cumprir.

Reforço da capacidade de cibersegurança
Caixa de ferramentas para organizações financeiras

Guia do nível CISO: Proteger ligações a terceiros

Como escolher fornecedores com cibersegurança em mente

Coloque as seguintes perguntas de potenciais fornecedores para avaliar a sua preparação e consciencialização cibernética e, consequentemente, o impacto que teriam no perfil de risco da sua organização:

1. **Que experiência têm?** Saiba mais sobre a história do fornecedor que serve os clientes. Já serviram clientes semelhantes à sua organização?
2. **Documentaram a sua conformidade com os padrões de cibersegurança conhecidos** como o Quadro NIST ou ISO 27001, ou podem fornecer um relatório SOC2?
3. **Quais dos seus dados e/ou ativos terão de aceder para prestar os seus serviços?** Estão a solicitar algum acesso aparentemente desnecessário?
4. **Como planeiam proteger os ativos e dados da sua organização que estão na sua posse?**
5. **Como gerem o seu próprio risco cibernético de terceiros?** Podem fornecer informações sobre a sua cadeia de abastecimento?
6. **Qual é o seu plano para recuperação de desastres e continuidade de negócios** no caso de um incidente ter impacto nos ativos e/ou dados da sua organização?
7. **Como irão manter a sua organização atualizada?** Qual é o seu plano para comunicar tendências, ameaças e alterações na sua organização?

Identificação de risco através de terceiros

⇒ Crie e mantenha uma lista atualizada de todas as relações com fornecedores e os ativos e dados expostos em cada uma.
⇒ Reveja os dados a que cada fornecedor ou terceiro tem acesso. Certifique-se de que este nível de acesso adere ao princípio de "privilégios mínimos".
⇒ 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 de cada fornecedor. O cumprimento das normas relevantes é um bom ponto de partida. Desenvolver um plano para avaliação de segurança regular. 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 expetativas 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 de outros terceiros, tais como organizações financeiras com as quais realiza transações ou partilha dados. Quaisquer requisitos de cibersegurança aos quais a sua organização devem aderir deve também ser seguidos pelos seus fornecedores e quaisquer outras organizações com as quais partilhe dados ou exponha ativos.

⇒ 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.

Partilhar informações

⇒ 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.
⇒ Envolva-se na 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 para melhorar as defesas da sua organização, aumentar a perceção das situações e alargar a aprendizagem. Fazer parte das organizações que partilham informações, por exemplo, o FS-ISAC, facilitará estar atualizado.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

Reforço da capacidade de cibersegurança
Caixa de ferramentas para organizações financeiras

Guia de resposta ao incidente

Preparação

⇒ Trabalhe com a liderança sénior da sua organização e outro pessoal relevante para desenvolver um plano de resposta a incidentes e continuidade de negócios com base nos riscos mais urgentes que foram identificados na avaliação de risco cibernético da sua organização.

- Desenvolva cenários de ameaças para os tipos de incidentes relacionados com os riscos cibernéticos mais prioritários da sua organização. Concentre-se na capacidade de construir a resposta a esses cenários.
- Identifique, registe e disponibilize na sua organização uma lista de pontos de contacto para a resposta ao incidente.
- Identifique e registe informações de contacto para as autoridades e agentes policiais locais e federais.
- Estabeleça disposições especificando que tipos de incidentes devem ser comunicados, quando devem ser comunicados e a quem.
- Estabeleça diretrizes escritas que definem a rapidez com que o pessoal deve responder a um incidente e que ações devem ser realizadas, com base em fatores relevantes, como o impacto funcional e de informação do incidente, e a provável recuperação do incidente.
- Informe todos os funcionários para contactarem a sua equipa técnica – mais frequentemente, será pessoal de TI e/ou CISO/CIO/outro gestor comparável – quando ocorre um incidente.
- Implemente soluções para monitorizar as ações dos funcionários e para permitir a identificação de ameaças e incidentes.
- Inclua planos de continuidade de negócios para coordenar como a sua organização irá trabalhar com fornecedores e clientes principais durante uma emergência empresarial, incluindo a forma como conduziria o manual ou operações empresariais alternativas, se necessário.
- Inclua procedimentos escritos para encerramento e reinício do sistema de emergência.
- Desenvolva e teste métodos para recuperar e restaurar os dados de cópia de segurança; teste periodicamente os dados de cópia de segurança para verificar a sua validade.
- Tenha acordos e procedimentos estabelecidos para realizar operações comerciais numa instalação/local alternativo.
- Tenha um canal de difusão claro implementado para todos os clientes.

Exercício

⇒ Organize pequenos exercícios de mesa com todos os funcionários ou representantes de todos os níveis de pessoal, incluindo executivos da organização, pessoal de PR/comunicações e equipas legais e de conformidade.
⇒ Identifique e participe idealmente em exercícios de simulação de toda a indústria relevantes para a sua organização.
⇒ Estabeleça o processo para garantir que as lições aprendidas a partir dos exercícios são incorporadas e abordadas na estratégia de cibersegurança da sua empresa.

Responder

⇒ Implemente ações do plano de resposta a incidentes para minimizar o impacto, incluindo o que respeita a danos na reputação.
⇒ Identifique sistemas afetados/comprometidos e avalie os danos.
⇒ Reduza os danos removendo (desligando) os ativos afetados.
⇒ Comece a registar todas as informações assim que a equipa suspeitar que ocorreu um incidente. Tente preservar a evidência do incidente ao desligar/isolar o ativo identificado afetado, por exemplo, recolha os registos de configuração do sistema, rede e deteção de intrusão dos ativos afetados.
⇒ Notifique as partes internas apropriadas, fornecedores terceiros e autoridades e solicite assistência, se necessário.
⇒ Inicie as atividades de notificação e assistência ao cliente em conformidade com as leis, regulamentos e orientações interagências.
⇒ Utilize plataformas de partilha de ameaças como a FS-ISAC ou a MISP para notificar a indústria sobre a ameaça.
⇒ Documente todos os passos que foram tomados durante o incidente para rever mais tarde.

Recuperar

⇒ Restaure os ativos recuperados para “pontos de recuperação” periódicos, se disponíveis, e utilize os dados de cópia de segurança para restaurar os sistemas para o último estado “bom” conhecido.
⇒ Crie cópias de segurança “limpas” de ativos restaurados e certifique-se de que todas as cópias de segurança de ativos críticos são armazenadas num local física e ecologicamente seguro.
⇒ Teste e verifique se os sistemas infetados estão totalmente restaurados. Confirme que os sistemas afetados estão a funcionar normalmente.

Rever

⇒ Realize uma discussão de “lições aprendidas” depois de o incidente ter ocorrido – reúna-se com o pessoal sénior, consultores de confiança e o(s) fornecedor(es) de suporte informático para rever possíveis vulnerabilidades ou recomendar novos passos a implementar.
⇒ Se possível, identifique as vulnerabilidades (quer em software, hardware, operações comerciais ou comportamento pessoal) que levaram ao incidente e desenvolva um plano para mitigar as mesmas.
⇒ Desenvolva um plano de monitorização para detetar incidentes semelhantes ou adicionais relacionados com os problemas identificados.
⇒ Partilhe lições aprendidas e informações sobre o incidente sobre plataformas de partilha de ameaças, como o FS-ISAC.
⇒ Integre as lições aprendidas nos protocolos de resposta a incidentes da sua organização.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE