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).