

EXPLORANDO CONTROLES ORGANIZACIONAIS E DE PROCESSO



CYBERSECURITY
EXPERTS ON YOUR SIDE

A proteção de dados efetiva precisa de mais do que soluções técnicas. Você precisa estabelecer controles administrativos e organizacionais para garantir que controles técnicos sejam implementados adequadamente, configurados e operados em suporte a uma estratégia de gestão de segurança coerente. Alguns exemplos de controles organizacionais incluem:

Dados privados e pessoais sensíveis

Controles técnicos, como criptografia e software de prevenção de perda de dados (DLP), precisam ser usados com discrição devido a seus custos (tanto financeiros quanto relacionados ao desempenho). A criptografia precisa de processamento adicional para criptografar e descriptografar dados, e soluções DLP precisam fazer uma busca por palavras-chave e padrões para identificar dados privados ou sensíveis como números de cartão de crédito, informações de saúde e números do seguro social. Estabelecer um esquema de classificação de dados pode ajudar seus usuários a entender quais dados precisam ser protegidos, por que e como.

Documentação de dados e auditoria

LEmpresas que coletam, processam e/ou armazenam dados sensíveis precisam documentar o motivo pelo qual coletam esses dados, como são coletados (quais são as fontes), como são usados e como são protegidos. Documentar sua segurança de dados e políticas de privacidade de dados pode ajudar você a abordar essas questões e a satisfazer requisitos de auditoria, particularmente em relação a leis como o Ato de Responsabilidade e Portabilidade de Seguro de Saúde dos Estados Unidos (HIPAA) e a Regulamentação de Proteção Geral de Dados dos Estados Unidos (GDPR).

Política de segurança

As políticas não precisam ser livros extensos. Em muitos casos, podem ser necessários apenas alguns parágrafos. As políticas de segurança devem definir claramente os papéis individuais e responsabilidades já que eles se relacionam com a proteção dos dados pessoais. Exemplos de políticas de segurança importantes que toda empresa deveria criar incluem:

- Política de uso aceitável para e-mail e internet
- Política traga seu próprio dispositivo

- Política de acesso remoto
- Política de software autorizado

Recursos humanos

Isso inclui políticas e procedimentos para garantir que os dados pessoais (como aplicações de emprego, dados de folha de pagamento, treinamentos e registros disciplinares) que sejam coletados, mantidos e processados por recursos humanos sejam protegidos adequadamente. Isso também inclui processos como varredura pré-emprego, teste de drogas e rotatividade de trabalho.

Usando um modelo de maturidade de segurança

Um modelo de maturidade de segurança pode ajudar você a determinar suas capacidades de segurança em áreas específicas e identificar quaisquer intervalos entre onde você está e onde você precisa estar. Onde você precisa estar irá, claro, depender de muitos fatores como:

- Que você está protegendo – como dados sensíveis, informações financeiras, propriedade intelectual, equipamento médico ou infraestrutura crítica.
- Sua indústria – como médica, financeira, varejo, contratação de defesa ou utilidades públicas.
- Seus requisitos de conformidade regulatórios – por exemplo, se você está sujeito ao Ato de Responsabilidade e Portabilidade de Seguro de Saúde dos EUA (HIPAA), Regulamentação de Proteção de Dados Gerais dos EUA (GDPR), Ato de Documentos Eletrônicos e Proteção de Informações Pessoais do Canadá (PIPEDA), Normas de Segurança de Dados da Indústria de Cartão de Pagamento (PCI DSS) ou outros?
- Seu perfil de ameaça – você está localizado geograficamente em uma região hostil ou instável, cidade com muitos crimes, área industrial ou perigosa?

Treinando e testando seus funcionários

O treinamento de consciência de segurança para todos os seus funcionários é necessário para garantir que seus funcionários não sejam o elo mais fraco quando se trata de proteção de dados na sua organização. Você precisa cobrir tópicos como segurança de senha, spam e phishing, proteção de malware, requisitos de conformidade e proteção de dados (como classificação de

dados, tipos de dados sensíveis e tecnologias de proteção de dados). O teste pode ser feito de muitas formas para garantir que o treinamento seja atrativo e reforçado através do ano.

Realizando análise de impacto de proteção de dados (DPIA):

A DPIA é requerida pela GDPR para quaisquer operações de processamento de dados que tenham “probabilidade de resultar em um alto risco para os direitos e liberdades dos indivíduos”. Uma DPIA é similar ao processo de gestão de riscos básicos (discutido no Capítulo 2), mas ainda define parâmetros adicionais que sejam relacionados ao processamento de dados pessoais.

Implementando proteção de dados por design e por padrão

A GDPR requer “proteção de dados por design e por padrão”, o que significa que as organizações deveriam implementar medidas técnicas e organizacionais para minimizar que os dados pessoais sejam coletados, processados e armazenados por uma organização.



PROTEÇÃO DE DADOS DE A A Z (BEM... A F)

A seguinte abordagem sistemática para cibersegurança pode ajudar você a proteger dados valiosos na sua empresa. É simples como A, B, C... D, E, F!

AVALIE seus ativos, riscos e recursos

Liste todos os sistemas e serviços de computador que sua empresa usa. Afinal, se você não sabe o que tem, não saberá o que proteger. Lembre-se de incluir dispositivos móveis como smartphones e tablets que podem ser usados para acessar as informações da empresa ou cliente. Isso é particularmente importante porque, de acordo com o Instituto Ponemon, estima-se que 60 por cento dos funcionários contorna os recursos de segurança em seus dispositivos móveis, e 48 por cento dos funcionários desabilita as configurações de segurança requeridas pelo empregador. E não se esqueça de serviços na nuvem como Box, Dropbox, iCloud, Google Docs, Office365, OneDrive e Salesforce.

A seguir, revise sua lista e considere os riscos associados com cada item, além de avaliar se você realmente ainda precisa ou não do sistema, software ou serviço. Quem ou o que é a ameaça? Outra boa pergunta a fazer é: "O que possivelmente poderia dar errado"? Alguns riscos tem maior probabilidade de ocorrer do que outros, mas liste todos e então classifique pela quantidade de dano que poderiam causar e a probabilidade de ocorrência.

Você pode precisar de ajuda externa com esse processo, que é o porquê você precisa de outra lista: os recursos que pode utilizar para problemas de cibersegurança. Pode ser alguém da equipe que seja instruído e tenha e conhecimento de segurança, ou um parceiro ou fornecedor. Grupos de comércio nacionais e associações de negócio locais também tem recursos e podem fornecer conselho útil. A Aliança de Cibersegurança Nacional fornece materiais educativos gratuitos, folhetos com dicas e sugestões de treinamento de funcionário. Além disso, lembre-se de verificar informações com seu escritório de execução legislativa local (você deveria ao menos ter nomes de contato e números para ligar caso você seja a vítima de um cibercrime).

CONSTRUA suas políticas

Um sólido programa de segurança começa com políticas de segurança que tenham adesão executiva. Se você é o chefe, você precisa deixar que todos saibam que você leva segurança a sério e que sua empresa está comprometida a proteger a privacidade e segurança de todos os dados com os quais trabalha. A seguir, você precisa detalhar as políticas que você deseja aplicar, não pode haver acesso não autorizado a sistemas e dados da empresa e os funcionários não estarão autorizados a desabilitar as configurações de segurança em seus dispositivos móveis.

ESCOLHA seus controles

Você usa controle para aplicar políticas. Por exemplo, para aplicar a política de acesso não autorizado a sistemas e dados da empresa, você pode escolher controlar todo o acesso a sistemas da empresa com um nome de usuário, senha e token únicos.

Para controlar quais programas são permitidos executar nos computadores da empresa, você pode decidir não dar aos funcionários direitos administrativos. Para prevenir violações causadas por dispositivos móveis perdidos ou roubados, você pode requerer que os funcionários reportem esses incidentes no mesmo dia e especificar que tais dispositivos sejam bloqueados remotamente e apagados imediatamente.

No mínimo, você precisa de três tecnologias básicas de segurança:

- **Software anti-malware** que previna um código malicioso (como vírus e ransomware) de ser baixado em seus dispositivos.
- **Criptografia** que torne os dados em dispositivos perdidos ou roubados inacessíveis.
- **Autenticação multifatorial** para que mais do que um nome de usuário e senha (como uma senha única enviada para um telefone móvel registrado) seja necessário para obter acesso a seus sistemas e dados.

IMPLEMENTAR controles

Ao implementar controles, certifique-se de que funcionam. Por exemplo, você pode ter uma política que proíba softwares não autorizados em sistemas da empresa; um dos seus controles será um software anti-malware que busque código malicioso. Você precisa instalar e testar para que ele não interfira com

as operações de negócio normais, e documentar os procedimentos a seguir quando malware for detectado.

EDUCAR funcionários, parceiros e fornecedores

Seus funcionários precisam saber mais do que apenas as políticas de segurança e procedimentos da empresa. Eles também precisam entender porque eles são necessários. Isso significa investir em educação e consciência de segurança, que, frequentemente, é a única medida mais eficiente de segurança que você pode implementar.

Ao trabalhar com sua equipe, você pode levantar consciência dos problemas como phishing em e-mail. Um recente Relatório de Investigações de Violação de Dados (DBIR) da Verizon mostrou que 23 por cento dos e-mails de phishing enviados para funcionários foram abertos e 11 por cento dos recipientes abriram um anexo, sendo que ambos aumentam muito as chances de violação de dados e roubo de informações.

Eduque todos que usam seus sistemas, incluindo executivos, fornecedores e parceiros. E lembre-se de que violações de políticas de segurança devem ter consequências. A falha em aplicar políticas enfraquece todo o esforço de segurança.

Avaliar, auditar e testar MAIS

Para qualquer empresa grande ou pequena, a cibersegurança é um processo contínuo, não um projeto único. Planeje a reavaliação da sua segurança periodicamente, ao menos uma vez por ano. Mantenha-se atualizado sobre ameaças emergentes revisando notícias de segurança regularmente através de websites como WeLiveSecurity.com, KrebsOnSecurity.com e DarkReading.com.

Você pode precisar atualizar suas políticas e controles de segurança mais de uma vez por ano dependendo das mudanças da empresa, como novos relacionamentos com fornecedores, novos projetos, novas contratações ou funcionários saindo (incluindo garantir que todo acesso ao sistemas seja revogado quando qualquer pessoa sair da empresa). Considere contratar um consultor externo para realizar um teste de penetração e auditoria de segurança para descobrir onde estão seus pontos fracos e atacá-los.

Olhando para os controles de processo

Os controles de processo ajudam as empresas a minimizar o impacto de uma violação ou perda de dados. Por exemplo, um estudo recente feito pelo Instituto Ponemon descobriu que as empresas podem reduzir o custo médio por registro de uma violação de dados de uma média de \$141 para aproximadamente \$122 se um processo efetivo de resposta ao incidente for implementado para ajudar a reduzir o tempo que leva para identificar e conter uma violação de dados. Sua equipe de resposta ao incidente pode ser interna um parceiro terceirizado ou uma combinação de ambos. Para uma violação de apenas 10000 registros, que representa uma economia média de aproximadamente \$190000 – um investimento muito válido.

Ao criar os controles de processo, as empresas precisam:

Envolver pessoas

Esta não deve ser uma iniciativa de gestão de cima para baixo. Envolver as pessoas que realmente trabalham com os vários processos e tecnologia irá ajudar a garantir que os controles façam sentido e possam ser efetivamente implementados.

Definir responsabilidades

As responsabilidades individuais precisam ser claramente definidas e entendidas: todos precisam saber seu papel.

Explicar por que controles de processo são necessários

Medidas de segurança são frequentemente vistas como um fardo ou um impedimento. Ao fim, elas podem ser ignoradas ou contornadas se os funcionários não entenderem por que os controles são necessários e por que são importantes para a empresa.



LEMBRE-SE

De acordo com o Instituto Ponemon, o tempo médio levado para identificar uma violação de dados é de 191 dias, e o tempo médio para conter uma violação de dados é de 66 dias. A quantidade de tempo necessária para identificar e conter uma violação de dados diretamente impacta no tamanho da violação de dados e seu custo total.

Empresas que criam processos para transferência segura de dados também podem reduzir o custo de uma violação de dados ou perda de dados. Por exemplo, a criptografia reduz o custo médio por registro em \$16, de acordo com o Instituto Ponemon. Em muitos casos, criptografar os dados (e ser capaz de provar que eles foram criptografados adequadamente) pode ativar disposições de porto seguro para muitas regulamentações de privacidade de dados. Fazer isso permite que as empresas se esqueçam das notificações de violação, o que reduz significativamente o custo – ambos em termos de custos diretos (como notificações, serviços de monitoramento ao crédito e processos) e custos indiretos (como dano a marca e rotatividade dos clientes). Novamente, no caso de uma violação de dados de 10000 registros, a criptografia pode reduzir o custo total da violação em aproximadamente \$160000.

Controles de processo importantes incluem:

Políticas de controle de acesso

Define quem tem acesso a quais sistemas, aplicações e dados, e para quais propósitos.

Gestão de ativos/recursos

É importante saber o que você está protegendo e por que (seu valor ou risco para a organização). Além de manter um inventário preciso de recursos/ativos de dados e computacionais, as organizações precisam garantir higiene de segurança adequada – mantendo sistemas e aplicações atualizados com os patches de segurança mais recentes e excluindo imediatamente ou destruindo dados sensíveis que não sejam mais necessários de acordo com as políticas de destruição, arquivamento e retenção de dados estabelecidas.

Gestão de mudanças

Garante que mudanças nos sistemas e aplicações sejam documentadas, testadas e aprovadas, tal que o impacto de uma mudança seja compreendido já que se relaciona com a postura geral de segurança da organização.

Resposta a incidentes

Quando um incidente de segurança (como uma violação de dados ou ataque) ocorrer, as empresas precisam ter um plano de resposta a incidentes definido com clareza e bem compreendido. Isso ajuda a garantir uma resposta imediata e efetiva, incluindo contenção de danos, recuperação,

preservação de evidências, comunicações internas e externas e análise da causa raiz.

Continuidade dos negócios

Um plano de continuidade dos negócios minimiza o impacto de negócios de uma interrupção ou desastre, ajudando a empresa a continuar a funcionar até que as operações normais possam ser totalmente retomadas.

Finalmente, as empresas podem impulsionar serviços de segurança profissionais para suplementar capacidades internas. Isso inclui monitoramento diário e inteligência de ameaça, assim como detecção, escalção e resposta a incidentes. Isso é particularmente importante em atividades forenses e investigativas, serviços de avaliação e auditoria, gestão de crises na equipe e comunicações.



LEMBRE-SE

Os controles de processo e organizacionais que forem implementados devem ser adequados para o nível de risco.



CYBERSECURITY
EXPERTS ON YOUR SIDE

ESET é uma empresa pioneira em proteção antivírus que nasceu há mais de 25 anos com a criação do multipremiado software para detecção de ameaças ESET NOD32 Antivírus. Agora, o objetivo da ESET é garantir que todos possam aproveitar as grandes oportunidades que a tecnologia oferece. Hoje, nossas soluções de segurança permitem que as empresas e os consumidores em mais de 180 países possam aproveitar mais o mundo digital.

© Copyright 1992-2020 por ESET, LLC e ESET, spol. s.r.o. Todos os direitos reservados..

www.eset.com/br