

AVALIANDO RISCOS DE SEGURANÇA DE DADOS



CYBERSECURITY
EXPERTS ON YOUR SIDE

Entendendo o processo de avaliação de riscos

A avaliação de riscos é a primeira fase do processo de gestão de riscos (discutido no Capítulo 2). Uma avaliação de riscos consiste em:

- Identificar seus ativos (ambos, tangíveis e intangíveis)
- Analisar ameaças (incluindo impacto e probabilidades)
- Avaliar vulnerabilidades (isto é, quais proteções ou controles estão ausentes ou insuficientes em um dado ativo)

De maneira similar, avaliar os riscos de segurança de dados envolve:

- Identificar suas operações de processamento de dados (para determinar como e onde seus ativos de dados são usados por seu negócio)
- Determinar o impacto potencial de negócios (se seus dados estiverem comprometidos)
- Identificar ameaças possíveis e avaliar probabilidades (de ocorrência, incluindo frequência)
- Avaliar riscos (para avaliar quais proteções ou controles devem ser implementados para proteger seus dados)

Passo 1

Identificar suas operações de processamento de dados

Os dados dentro de uma organização têm diferentes perfis de risco, não apenas baseado no conteúdo dos dados, mas também devido à maneira que os dados são usados dentro da organização. Portanto, é importante entender como os dados são processados dentro do seu negócio ao iniciar o processo de avaliação de riscos. Por exemplo, uma SME típica pode ter alguns ou todos os tipos seguintes de operações de processamento de dados:

Recursos humanos como gestão de folha de pagamento de funcionários, recrutamento e retenção, registros de treinamento, ações disciplinares e avaliações de desempenho.

Gestão de clientes, marketing e fornecedores como informações do cliente, ordens de compra e venda, faturas, listas de e-mail, dados de marketing e propaganda e contratos do vendedor.

Segurança pessoal e segurança física como registros de acesso de segurança do funcionário, registros de visitante e monitoramento por vídeo.

Para cada operação de processamento de dados, considere o seguinte:

- Quais dados pessoais estão sendo processados?
- Qual é o propósito do processo?
- Onde o processamento ocorre?
- Quem é responsável pelo processo?
- Quem tem acesso aos dados?



LEMBRE-SE

O princípio de menos privilégios é uma prática melhorada de segurança da informação na qual se concede aos usuários finais apenas o nível mínimo de acesso necessário para realizar uma função de trabalho específica.

Passo 2

Determinar o impacto potencial de negócios

A seguir, você precisa determinar o impacto potencial de uma violação ou comprometimento de dados. Uma violação ou comprometimento pode afetar a confidencialidade (por exemplo, acesso não autorizado) de dados, a integridade de dados (por exemplo, modificações não autorizadas) ou a disponibilidade de dados (por exemplo, um ataque de ransomware).



LEMBRE-SE

As organizações devem proteger a confidencialidade, integridade e disponibilidade de dados. Em segurança da informação, isso é conhecido como a tríade C-I-A.

Em uma avaliação de riscos típica, o impacto potencial de um dado risco é geralmente expresso em termos de danos à organização, como a perda ou destruição de um ativo físico (por exemplo, um servidor, uma máquina copadora ou um veículo).

O impacto de um risco para a segurança de dados e para o negócio é similar a outros impactos de riscos, mas o impacto pode ser indireto. No caso de dados pessoais sensíveis, o indivíduo cujos dados forem violados ou comprometidos é a vítima direta. Em tais casos, a identidade do indivíduo ou ativos financeiros podem ser roubados e/ou sua privacidade pode ser violada. O impacto para os negócios é menos direto, mas ainda muito custoso e pode incluir (dentre outros):

- Perda de clientes e receita
- Dano à marca e relações públicas negativas
- Multas legais e processos
- Notificações de violação e serviços de monitoramento ao crédito
- Análise forense e recuperação



TIP

O impacto de negócios pode ser classificado como Baixo, Médio ou Alto. Entretanto, a definição real de cada um desses níveis de impacto será única para cada negócio e deve envolver ambas, medidas objetivas (quantitativas) e subjetivas (qualitativas).

Passo 3

Identificar ameaças possíveis e avaliar probabilidades

Uma ameaça pode ser qualquer evento ou circunstância, seja natural ou humano, que tenha o potencial de afetar negativamente a confidencialidade, integridade ou disponibilidade dos dados pessoais ou sensíveis. Isso pode incluir ataques de cibersegurança, perda ou divulgação acidental, ameaças internas, incêndio e inundação, terremotos e tsunamis, tempo severo (como furacões e tornados), conflitos civis, processos trabalhista e outros. As empresas identificar possíveis ameaças a suas operações de processamento de dados e avaliar a probabilidade (incluindo a frequência de ocorrência) de cada ameaça possível. Garanta que você cubra ameaças em áreas bem-definidas, incluindo ameaças da rede e recursos técnicos (software/hardware) que são usados para o processamento de dados, ameaças de processos e procedimentos relacionados, ameaças que envolvam recursos humanos e ameaças na escala de processamento.



TIP

Para cada ameaça identificada, as probabilidades podem ser classificadas de uma maneira similar ao impacto de negócios: Baixo, Médio ou Alto. Ao avaliar a probabilidade de uma ameaça ocorrer, considere ambos, a probabilidade da ameaça ocorrer realmente, além da frequência com que é provável que ocorra durante um dado período (por exemplo, durante o período de um ano).

Step 4

Avaliar riscos

Assim que você tiver identificado todas as suas operações de processamento de dados (e os dados sendo processados), determinado o impacto de negócios potencial de uma violação ou comprometimento de dados, identificado as ameaças possíveis e probabilidades e frequência de ocorrência, você poderá avaliar os riscos associados a cada operação e determinar a tecnologia de controle de proteção de dados adequada e processo organizacional. De acordo com a avaliação de riscos, controles de processo e organizacionais devem ser implementados para assegurar adequadamente seus dados e operações de processamento de dados usando uma abordagem baseada em riscos.

A figura 3-1 mostra um modelo de avaliação de dados e um exemplo de uma avaliação de operação de processamento de dados.

		Nível de impacto			
		BAIXO	MÉDIO	ALTO	MUITO ALTO
Probabilidade de ameaça	BAIXA	RISCO BAIXO	RISCO MÉDIO	RISCO ALTO	
	MÉDIA				
	ALTA	RISCO MÉDIO			

Probabilidade de ameaça

Para uma operação particular de processamento de dados, analise a lista de possíveis ameaças de processamento de dados e avalie ou qualifique a probabilidade de ameaça. A probabilidade final deve ser baseada na soma da pontuação de todas as ameaças na lista de ameaças.

- **Baixa** – é pouco provável que a ameaça aconteça
- **Média** – existe uma possibilidade de que a ameaça aconteça
- **Alta** – é muito provável que a ameaça aconteça

Nível de impacto

Para a operação de processamento de dados, avalie o impacto possível na confidencialidade, integridade e disponibilidade dos mesmos. O maior impacto dos três é o nível de impacto final.

- **Baixa** – Inconvenientes mínimos que podem ser superados sem nenhum problema
- **Média** – Inconvenientes significativos que podem ser superados a pesar de algumas dificuldades
- **Alta** – Consequências significativas que podem ser superadas com dificuldades sérias
- **Muito alta** – Consequências significativas, ou até irreversíveis, que dificilmente poderão ser resolvidas

A operação de processamento de dados apresenta

- Risco baixo
- Risco médio
- Risco alto

Exemplo

Operação de processamento de dados: Marketing/Publicidade.

Dados processados: informações de contato (exemplo: nome, endereço, número de telefone, e-mail).

Classificação de dados: dados pessoais.

Objetivo do processamento: promoção de bens e ofertas especiais para possíveis clientes.

Dados pertencentes a: clientes atuais e clientes potenciais

Probabilidade de ameaça

Ameaças de rede e recursos técnicos (HW, SW): média

Processos e procedimentos de ameaças: baixa

Ameaças de recursos humanos envolvidos: média

Sector empresarial e escala de ameaças de processamento: média

Probabilidade final: Média

Nível de impacto

Confidencialidade da avaliação do nível de impacto: baixa, Integridade: baixa, Disponibilidade: baixa

Nível de impacto final: baixo

Operação de processamento de dados apresenta

- **Risco baixo** – o processamento dos dados de marketing e publicidade apresenta um risco baixo – Medidas Técnicas e Organizacionais adequadas para este risco devem ser implementadas.



CYBERSECURITY
EXPERTS ON YOUR SIDE

A 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 1992-2019 por ESET, LLC y ESET, spol. s.r.o. Todos os direitos reservados.

www.eset.com/br