SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE III – GESTÃO DE RISCOS EM AMBIENTES DA INFORMAÇÃO

PUC Minas
Virtual

3.3 – ANÁLISE DE RISCO NAS ORGANIZAÇÕES

NEGÓCIOS SOB RISCO

- A percepção sobre segurança de dados está frequentemente nos olhos de quem a vê. Lançamentos de ***patches*** de sistemas são identificados praticamente o tempo todo nos mecanismos de informação e distribuição de aplicativos.
- Temos também os profissionais de segurança de rede **exploram** redes com e sem fio para ver quais segredos podem ser peneirados dos pacotes à medida que avançam de nó em nó.

O QUE TEMOS DE TÉCNICO ENVOLVIDO?

- Uma **avaliação de risco** é simplesmente um esforço para identificar ameaças à sua organização, qual a **probabilidade** delas e as **consequências** dos **perigos**.
- A ideia principal da análise de riscos é utilizá-la para apoiar a **estratégia** de sua organização, fornecendo as informações necessárias para **implantar práticas** e **controles específicos** para lidar com os riscos identificados.
- **Em resumo você deve desenvolver medições objetivas de risco e proteger melhor os ativos em risco.**

O QUE TEMOS DE TÉCNICO ENVOLVIDO?

- Uma sugestão para o desenvolvimento de um guia para executar esta análise é responder as seguintes perguntas:
  - **O que é avaliado?**
  - **Quem precisa estar envolvido?**
  - **Quais os critérios para desenvolver os graus relativos de risco?**
- Esta sugestão pode ser utilizada como ferramenta para simplificar a questão!

O QUE TEMOS DE TÉCNICO ENVOLVIDO?

- Após estas definições podemos atuar em duas vertentes técnicas:
    - Utilizar **scanner de vulnerabilidades** - um software para identificar e reportar os problemas de segurança - nos sistemas da empresa.
        - **Scanner de vulnerabilidades** executa milhares de testes para encontrar falhas e coletar informações sobre potenciais riscos e problemas criando um inventário de tudo que está conectado à rede e executando uma série de testes de segurança em cada item inventariado.

O QUE TEMOS DE TÉCNICO ENVOLVIDO?

- Geralmente o próprio software utilizado para fazer o scanner faz a **triagem** dessas identificações produzindo o **ranking** que determina o quão a vulnerabilidade **perigosa** e qual **impacto** ela teria caso fosse explorada, e nível de facilidade para um hacker explorá-la.
- O software pode também sugerir medidas de segurança existentes para combater a vulnerabilidade, reconhecendo inclusive detecções de falso positivo.

O QUE TEMOS DE TÉCNICO ENVOLVIDO?

- Acompanhar os anúncios e executar as recomendações, geralmente aplicação de patches de segurança, para alertas de segurança dos fornecedores de soluções que a empresa possui.
    - Isto vai de sistemas operacionais e mecanismos mais sofisticados como *Web Application Firewall* **(WAF)** e Anti-DDoS.
- Executar periodicamente testes de penetração tecnicamente conhecidos como **Pentest** que podem ser: de rede **externa**, de rede **interna**, **aplicativos da web**, rede **sem fio** e teste de *phishing* **simulado**.

O RESULTADO DA ANÁLISE

- Além da possibilidade de construção da matriz de risco, ao fazer o scanner as ferramentas irão reportar formato de relatório parecido com este:

Severidades	Críticas	Altas	Medias	Baixas
Quantidade	0	0	4	1

CVSS Score	Nível de Severidade	Resultado do Scanner
0.0 – 3.9	Baixo	Aprovado
4.0 – 5.9	Médio	Reprovado
6.0 – 9.9	Alto	Reprovado
10	Crítico	Reprovado

Fonte: DEFENDER, 2021.

MAS COMO GERAR ESTA MATRIZ?

- O primeiro passo é classificar os tipos de informação que estão presentes no inventário da organização e uma sugestão é utilizar a classificação:

1. Informações públicas sobre a organização;
2. Dados internos não confidenciais;
3. Informações sensíveis (planos de negócios, por exemplo);
4. Dados disponíveis somente para determinados funcionários;
5. Informações confidenciais.

MAS COMO GERAR ESTA MATRIZ?

- Um método bastante conhecido e que pode apoiá-lo é o **STRIDE,** este método ajuda a categorizar as ameaças e funciona da seguinte forma:

S (*Spoofing of identity*): roubo de identidade ou falsificação;
T (*Tampering with data*): violação ou adulteração de dados;
R (*Repudiation of transaction*): repúdio de transação;
I (*Information disclosure*): divulgação não autorizada de informação;
D (*Denial of service*): ataques de negação de serviço;
E (*Elevation of privilege*): elevação de privilégio

ALCANÇAREMOS COM A ANÁLISE TÉCNICA

- Monitorar os sistemas e fazer inspeções regulares no ambiente;
- Reduzir a incidência de problemas como ransomware, senhas fracas e etc;
- Proteção dos ativos empresariais;
- Aumentar a conformidade com a LGPD;

REFERENCIAS BIBLIOGRÁFICAS

DEFENDER, 2021. Tipos de Pentest. Disponível em: <https://www.sitedefender.com.br/tipos-de-pentest/?gclid=EAIaIQobChMIg_G11KeQ-wIVyBOtBh217wWnEAAYASAAEgIg0fD_BwE>. Acesso em: 02 Nov. 2022.

MICROSERVICE,2022. O que é análise de vulnerabilidade e qual sua importância?. Disponível em: <https://www.microserviceit.com.br/analise-vulnerabilidade/>. Acesso em: 02 Nov. 2022.

SESTREM, Thatiana**.** Matriz de risco: o que é e como implementar na sua empresa. Disponível em: <https://qualyteam.com/pb/blog/matriz-de-risco/>. Acesso em: 25 Out. 2022.


PUC Minas
Virtual