

SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS





PUC Minas
Virtual

UNIDADE I – A MUDANÇA NO TRATAMENTO DOS DADOS



PUC Minas
Virtual

1.1 Introdução à segurança da informação



PUC Minas
Virtual

1.1.3 Mercado de Tecnologia na nova abordagem

SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

- As transformações digitais aceleradas que permitiram a continuidade de muitas organizações também os abriu para uma série de ameaças antigas e novas e houve uma evolução rápida das ameaças.
- Os ataques direcionados ganharam popularidade entre diferentes tipos de agentes maliciosos, incluindo aqueles em grupos de *ciber-espionagem* e *ciber-mercenários*.
- Problemas de segurança continuaram a atormentar organizações que se tornaram adotantes da nuvem e a maioria dos desafios na segurança da nuvem são atribuídos a configurações incorretas na configuração da nuvem ambientes.

■ Conceito da ABNT é mais abrangente

“Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. A segurança da informação é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de hardware e software.” (ABNT,2013).

■ Novas responsabilidades, novos papéis!

- Com os papéis corporativo e estratégico da segurança da informação nas organizações abre-se espaço para o papel do **CISO** (*Chief Information Security Officer*) que é o diretor de Segurança da informação.
- **Quem então é responsável pela salvaguarda da informação?**
- É necessário que seja instituído um responsável pela segurança da informação organizacional. Este colaborador geralmente é nomeado como *Security Officer* (Gestor de Segurança da Informação).

■ Segurança em um sistema de TI

- Uma das coisas que mais ouviremos é a que a execução do assessment (como se fosse uma consultoria), é necessária para quaisquer ambientes que necessitam ser considerados seguros.
- Esta análise é pautada pelo batimento das regras de Auditabilidade baseada em critérios que são definidos por órgãos considerados como referência no assunto através de seus manuais de melhores práticas publicados.
- **Segurança é a capacidade de mitigar o impacto negativo de uma violação do sistema.**

■ Soluções de segurança e maturidade

- Um dos acontecimentos atuais em relação à investimentos em TI é a substituição dos orçamentos de CAPEX para OPEX.
- **Esta diretriz modifica basicamente como teremos acesso à soluções de TI inclusive as relacionadas à segurança da informação.**
- Uma das vantagens deste tipo de modalidade é ter a certeza que provedores de grande porte tem uma visibilidade maior de ameaças e vulnerabilidades do que uma oferta de serviços *on premise*, por exemplo.

■ Soluções de segurança e maturidade

- Se formos pensar no conceito de segurança e já adiantarmos que não há nenhum sistema totalmente seguro, a questão de fundamento passa a ser **identificação e recuperação de falhas** de forma rápida.
- *Como os provedores atendem a diversos clientes de forma compartilhada eles possuem a visibilidade de diversos tipos de ataques e identificam as vulnerabilidades muito rapidamente pois são responsáveis pela manutenção da disponibilidade das soluções.*

■ Soluções de segurança e maturidade

- Relatório da **Trend Micro** (2022) demonstra as previsões de segurança mostra as principais preocupações onde sugerem mais atenção à medida que os serviços vão evoluindo.

1. Ameaças na Nuvem

2. Ameaças de *Ransomware*

3. Exploração de vulnerabilidades

4. Ataques de malware de *commodities*

5. Ameaças no *IoT*

6. Ameaças na cadeia de abastecimento

■ Soluções de segurança e maturidade

- O motor de oferta destas soluções é o *assesement* que faz uma avaliação das proteções de segurança implementadas no ambiente.
- O processo se dá na análise da configuração da infraestrutura na conta do cliente e identifica possíveis problemas que o cliente pode corrigir posteriormente.
- Ele procurará coisas como portas abertas para a Internet e patches de segurança ausentes, bem como privilégios elevados.

■ Soluções de segurança e maturidade

- Uma violação pode afetar a confidencialidade, integridade ou acessibilidade de um sistema e um impacto em um sistema é o efeito negativo de um evento de segurança que pode ser classificado como baixo ou alto.
- As ações de mitigação/resolução das questões apontadas ficam a cargo de quem é responsável pela camada onde o problema foi apontado seguindo as melhores práticas e os *frameworks* de segurança já conhecidos.

■ REFERENCIAS BIBLIOGRÁFICAS

CORREA JUNIOR, H. E. Segurança de sistemas: conceitos básicos: material adaptado da Academia Latino-Americana de Segurança - Microsoft. 2011. Disponível em: <<https://pt.scribd.com/document/84971695/aula1>>. Acesso em: 20 ago. 2022.

DANTAS, L. M. Segurança da informação: uma abordagem focada em gestão de riscos. Olinda, PE: Livro Rápido, 2011.

BERNARDI, Fabio. Segurança da Informação – Conscientização. Disponível em: <<http://www.bluminformatica.com.br/SegurancadaInformacaoConscientizacao.html>>. Acesso em 10 Ago. 2022.

■ REFERENCIAS BIBLIOGRÁFICAS

IBR, 2015. Segurança contra ataques cibernéticos. Disponível em: < <https://www.grantthornton.com.br/insights/artigos-e-publicacoes/ciberespaco/> >. Acesso em: 24 Jul. 2022.

TREND MICRO, 2022. Em direção a um Novo Momento: Previsões de Segurança da Trend Micro para 2022. Disponível em: <<https://www.trendmicro.com/vinfo/br/security/research-and-analysis/predictions/2022>>. Acesso em: 17 Set. 2022.



PUC Minas
Virtual