SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

Mecanismos de defesa

- Já vimos que temos que proteger as pessoas, os ativos e a informação propriamente dita.

- A segurança da informação deve proteger todos os elementos com seus mecanismos de defesa. Os mecanismos de defesa são os controles de segurança utilizados para a proteção do ambiente.

- A questão que surge é: o que é a defesa, a proteção ou a segurança? Uma forma de entender essa questão é analisando os princípios básicos da segurança da informação, que são a confidencialidade, a integridade e a disponibilidade. O que devemos buscar é que essas propriedades básicas sejam alcançadas. E, para isso, os mecanismos de defesa ou os controles de segurança, devem ser utilizados.


A informação existe
Na cabeça das pessoas
Em meios físicos
Em meios digitais
Controles de segurança
Devem garantir
Propriedades básicas da segurança da informação
Confidencialidade
Integridade
Disponibilidade

Mecanismos de defesa

- De acordo com uma das pesquisas condensadas por Neto (2015), o crescimento anual dos investimentos em segurança da informação no Brasil cresce a uma taxa de 30% a 40% anuais, chegando a US$ 8 bilhões, enquanto no resto do mundo a taxa é de cerca de 10% a 15%. Outra pesquisa citada pelo pesquisador mostra que, mesmo com os investimentos, as perdas resultantes de ataques cibernéticos chegam a números entre R$ 15 e R$ 20 bilhões anuais. Ainda outra pesquisa citada pelo mesmo autor indica que os crimes pela Internet provocam perda anual de US$ 445 bilhões para a economia mundial.

Controles de segurança ou mecanismos de defesa

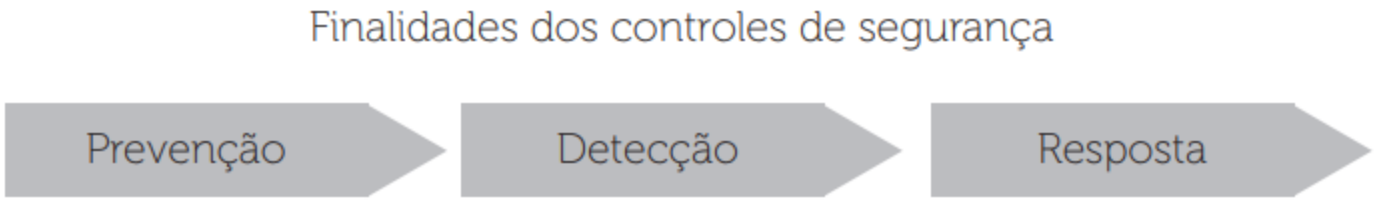
- Os controles de segurança são salvaguardas ou contramedidas que visam a:
  - Proteger as propriedades básicas de segurança da informação;
  - Cumprir um conjunto definido de requisitos de segurança, como a necessidade de manter uma comunicação segura entre matriz e filial de uma empresa para garantia de confidencialidade, por exemplo;
  - Cumprir requisitos de negócios, como o software que está sendo criado por uma empresa e deve seguir uma metodologia de desenvolvimento seguro para minimizar a probabilidade de ele ser a porta de ataques aos clientes que o utilizam;
  - Há um ciclo fundamental relacionado com controles de segurança que deve ser sempre cumprido;

Controles de segurança ou mecanismos de defesa

- O controle de segurança deve ser selecionado;
- O controle de segurança deve ser implementado;
- O controle de segurança deve ter sua efetividade avaliada;
- O controle de segurança deve ser monitorado;

Prevenção, detecção e resposta

- A segurança da informação deve atuar em prevenção, detecção e resposta.



- Controles de segurança são utilizados para a prevenção de ataques, para evitar que um risco se torne um incidente. Um exemplo desse tipo de controle é a criptografia, que protege a confidencialidade da informação, além da integridade.

- A criptografia, dessa forma, pode ser utilizada para a prevenção contra ataques como os que levam ao vazamento da informação.

Prevenção, detecção e resposta

- Podemos notar que controles de segurança são específicos para tipos de ataques. A criptografia, por exemplo, não protege contra os ataques de negação de serviço, que exigem outro tipo de mecanismo de defesa.

- Outro exemplo de controle de segurança de prevenção é o firewall. Sua função é limitar as conexões para o ambiente ou para o ativo a ser protegido, abrindo apenas as portas de serviços que podem ser acessados de uma forma legítima pelos usuários. O firewall, assim, faz a prevenção contra ataques que exploram serviços não legítimos e que, portanto, não possuem portas abertas. Porém, é importante você saber que o firewall não protege contra ataques ao serviço que está disponibilizado e tem a porta aberta que passa pelo firewall.

Prevenção, detecção e resposta

- O sistema de detecção de intrusão (IDS, Intrusion Detection System) é uma tecnologia que detecta, com base em padrões e assinaturas, ataques ao ambiente ou aos ativos.

- Os IDS atuam em diferentes camadas, como no host ou na rede, realizando detecções que, no entanto, não englobam toda a imensidão dos ataques existentes. Com isso, há falsos negativos (ataques que passam pelo IDS sem a emissão de alertas) e os falsos positivos (alarme falso).

Tipos de controles de segurança

- Segundo ISO 27002 (2013), os controles de segurança atuam em finalidades diferentes, que envolvem a prevenção, a detecção e a resposta. Essas finalidades podem ser alcançadas com o uso de mecanismos de defesa que são físicos, tecnológicos, processuais ou regulatórios.

- Controles de segurança podem ser:
  - Físicos, como um controle de acesso ao data center;
  - Tecnológicos, como um firewall para controle de acesso de rede;
  - Processuais, como uma política de senhas;
  - Regulatórios, como o Decreto nº 3.505 de 13 de junho de 2000, que institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal.

Tipos de controles de segurança

- A política de segurança é um controle de segurança do tipo processual e deve guiar toda a organização em busca dos objetivos de segurança, com definições de necessidades, regras e responsabilidades de todos para a segurança da informação.

EXERCÍCIOS

1) A segurança da informação é uma das áreas que têm apresentado maior crescimento em investimentos. As empresas investem como em segurança da informação?

a) Com ataques cibernéticos.

b) Em novas vulnerabilidades.

c) Implementado controles de segurança.

d) Em novos ativos.

e) Com comunicação.

EXERCÍCIOS

2) Os controles de segurança devem ser utilizados para cumprir algumas finalidades. Quais são elas?

a) Físico, regulatório e tecnológico.

b) Processos, resposta e regulatório.

c) Prevenção, detecção e resposta.

d) Resposta, detecção e físico.

e) Tecnológico, detecção e regulatório.

EXERCÍCIOS

3) Os controles de segurança podem ser de diferentes tipos. Quais são eles?

a) Físico e prevenção.

b) Processuais e regulatório.

c) Prevenção e detecção.

d) Resposta e físico.

e) Criptografia.

RESOLUÇÃO

1) C

2) C

3) B

PESQUISA

Elabore um relatório respondendo as seguintes perguntas:

O que é um firewall?

Qual sua finalidade?

Quais os tipos existem?

REFERÊNCIAS

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação: princípios e controle de ameaças**. [S. l.]: ÉRICA, 2014.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. [S. l.]: SARAIVA, 2007.

SMULDERS, André; BAARS, Hans; HINTZBERGEN, Jule; HINTZBERGEN, Kees. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [S. l.]: BRASPORT, 2018.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. [S. l.]: Cengage Learning, 2014.

REFERÊNCIAS

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. [S. l.]: Bookman Editora, 2013.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**: Princípios e práticas. 6. ed. [S. l.]: Pearson Universidades, 2014.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. [S. l.]: Record, 2001.


Anhanguera