SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

Desenvolvendo uma política de segurança

- Cada organização é única e possui uma política de segurança única.

- As diretrizes de segurança da informação, normas e procedimentos devem seguir os objetivos de negócios, objetivos legais e os riscos daquela organização específica.

- A análise de riscos irá direcionar os principais controles de segurança necessários, que podem ser baseados em normas como a NBR ISO/IEC 27002, que define controles de segurança da informação.

Desenvolvendo uma política de segurança

- Algumas perguntas que a política de segurança deve responder são:
  - Os usuários sabem em quais links não devem clicar?
  - Os funcionários da empresa sabem o que devem publicar em redes sociais sobre a empresa?
  - Há preocupações sobre vazamento durante as discussões de novos produtos ou serviços?
  - Quais são as regras para uso de dispositivos móveis?

Objetivos de normas e padrões

- As normas e os padrões de segurança da informação exercem um papel importante para as organizações, sob dois pontos de vista principais. Primeiramente, as normas e os padrões auxiliam as organizações na definição dos controles de segurança e também no estabelecimento do sistema de gestão que, por sua vez, é o responsável pelo ciclo efetivo da segurança da informação.

- O segundo ponto de vista sobre a importância das normas e padrões é que elas demonstram a abordagem mais comprometida da organização com a segurança da informação, que é alcançada com a obtenção de certificação. A certificação mais conhecida em segurança da informação é a ISO/IEC 27001, que atesta organizações que possuem um sistema de gestão de segurança da informação.

Principais normas e padrões

- A segurança da informação faz parte de todas as organizações, e há um conjunto de normas (e padrões) que são mais utilizadas:
  - Segurança da informação: ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/ IEC 27002:2013.
  - Riscos: ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011.
  - Continuidade de negócios: ABNT NBR ISO/IEC 27031:2015 e ABNT NBR ISO 22301:2013.
  - Governança de TI: COBIT.
  - Serviços de TI: ITIL.

Principais normas e padrões

- **Norma de gestão de segurança da informação: ABNT NBR ISO/IEC 27001:2013**: define os requisitos para Sistemas de Gestão da Segurança da Informação (SGSI) e faz parte da família de normas ISO 27000, que possui o foco em segurança da informação.

- Uma característica da ISO 27001 é que uma organização pode ser certificada na norma, o que indica que ela possui e segue um sistema de gestão de segurança da informação.

Principais normas e padrões

- **Norma de código de prática para controles de segurança da informação: ABNT NBR ISO/IEC 27002:2013**: Os objetivos de controles da ISO 27002 incluem política de segurança da informação; conformidade; gestão de continuidade do negócio; gestão de incidente de segurança da informação; aquisição, desenvolvimento e manutenção de sistemas de informação; controle de acessos; gerenciamento de operações e comunicações; segurança física e do ambiente; segurança de recursos humanos; gestão de ativo; organização da segurança da informação.

Principais normas e padrões

- **Normas de gestão de riscos: ABNT NBR ISO 31000:2009 e ABNT NBR ISO/IEC 27005:2011**: tratam dos processos de gestão de riscos.
  - Identificação de riscos.
  - Estimativa e análise de riscos.
  - Avaliação de riscos.
  - Tratamento de riscos.
  - Comunicação e consulta de riscos.
  - Monitoramento, revisão e análise crítica de riscos

Principais normas e padrões

- **Normas de gestão de continuidade de negócios**: possui uma relação direta com a segurança da informação, com foco na disponibilidade, visando à manutenção e ao restabelecimento dos negócios após um incidente de segurança.

- **Norma e padrão de governança de TI**: O COBIT é um framework composto por ferramentas, recursos e guias para a governança e gerenciamento de TI. O COBIT é formado por duas camadas principais: a de governança corporativa de TI e a de gestão corporativa de TI.

Principais normas e padrões

- **Norma e padrão de gestão de serviços de TI**: O ITIL é um conjunto de cinco livros que definem processos para o gerenciamento de serviços de TI. Apesar de não ser focado em segurança da informação, estão relacionados ao assunto os processos de gerenciamento da continuidade do serviço e, também, o gerenciamento da segurança da informação.

Tendências

- De um lado, a segurança da informação é uma das áreas que mais crescem no mundo, com taxas ascendentes de 9,8% anuais, com estimativas de chegar a US$ 170 bilhões até 2020 (SEGINFO, 2016) ... Mas com certeza será atualizado com o cenário atual.

- Um dos maiores desafios na atualidade: como trabalhar de casa? E a Segurança da Informação?

- Se acessar a rede interna da minha empresa será que estou seguro?

O que é seguro hoje pode não ser seguro amanhã

- Novas vulnerabilidades são descobertas o tempo todo, o que leva ao fato de novos ataques passarem a existir.

- Uma nova forma de guerra, baseada não em bombas nucleares, mas em “bombas cibernéticas”, é discutida cada vez mais pelos países. Com as preocupações cada vez maiores com as infraestruturas críticas, como as de energia, de telecomunicações ou de transportes, que podem ser afetadas por ataques cibernéticos, a importância dos países com a proteção cibernética aumenta cada vez mais.

- Problemas atuais que envolvem nosso cotidiano: Internet das coisas, sinalizações.

Carros conectados

- Os carros autônomos e conectados avançam rapidamente, com vários experimentos sendo realizados ao redor do mundo.

- Com o controle remoto de veículos, já foram demonstrados ataques que controlavam funções críticas dos carros, como aceleradores, freios e mesmo direção.

EXERCÍCIOS

Resolução dos exercícios 1, 2 e 3 do Livro UNIDADE 4 SEÇÃO 3 e 4.

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.

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