SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

Aplicações de Criptografia – Transações

- Outra aplicação importante da criptografia é para a proteção de transações, que estão presentes em várias situações do nosso cotidiano on-line. Quando realizamos uma compra pela internet, por exemplo, temos que ter a tranquilidade de saber que o número do cartão de crédito está sendo transferido de uma forma segura até a loja. Além disso, uma vez que a transferência dos dados de cartão foi feita de uma forma segura, esses dados devem estar protegidos no servidor da loja virtual.

- Os protocolos de segurança para transações mais utilizados, também pelos bancos, para o transporte seguro dos dados são SSL (Secure Sockets Layer), TLS (Transport Layer Security) e HTTPS (HyperText Transfer Protocol Secure).

Aplicações de Criptografia – Transações

- Esse conjunto de protocolos é utilizado para transações web com a criação de um túnel seguro por onde trafegam as informações. Além de garantir a confidencialidade, eles podem visar também à integridade dos dados e à autenticidade das partes.

- Para o entendimento básico das diferenças entre SSL, TLS e HTTPS, o SSL evoluiu para o TLS, de modo que o SSL 3.1 é o TLS 1.0. Já o HTTPS é o HTTP dentro do SSL/ TLS. O túnel bidirecional do HTTP é criado entre duas entidades e, quando esse túnel é seguro por uma conexão SSL/TLS, então o conjunto é conhecido como HTTPS.

Novas frentes da criptografia

- A criptografia quântica é baseada na mecânica quântica, possuindo assim propriedades diferentes da criptografia tradicional (de chave pública e de chave privada) que a tornam mais segura.

EXERCÍCIOS

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

Aspectos não tecnológicos em segurança da informação

- Iremos discutir três categorias gerais de aspectos não tecnológicos (ISO 27001, 2013; ISO 27005, 2011) que são os aspectos físicos, humanos e naturais.
- Desastres
- Acidentes
- Falhas
- Engenharia Social
- Terrorismo

Política de segurança

- A segurança é de responsabilidade de todos, e não apenas da área de segurança da empresa. De fato, basta um incidente para que toda a empresa seja comprometida: vírus, vazamentos ou desenvolvimento de produtos vulneráveis que levam à má reputação.

- A informação pode estar em meios tecnológicos (já abordados) ou então na cabeça das pessoas ou armazenados em meios físicos. Para esses, é necessário a criação de uma política de segurança.

Política de segurança

- A política de segurança é composta por um conjunto de documentos ou capítulos que devem ser lidos, compreendidos e seguidos pelos respectivos responsáveis. A política em si, que possui as diretrizes gerais para a segurança da informação na organização, deve ser acessada e seguida por todos.

- Além disso, há as normas. Já os processos e procedimentos específicos, como o de desenvolvimento de software, ou o de administração de sistemas, por exemplo, devem ser seguidos pelos respectivos responsáveis, não sendo necessário, por exemplo, que o administrador de firewall tenha acesso aos processos e procedimentos de gestão de identidades.

Política de segurança

- Assim, a política de segurança é composta por diretrizes, objetivos, direcionadores e normas, enquanto os processos e procedimentos se destinam a aspectos específicos.

- Com isso, a política possui uma estrutura que deve facilitar o acesso de todos da organização para os documentos ou capítulos que são de responsabilidade de cada um.

- https://www.itau.com.br/_arquivosestaticos/RI/pdf/pt/CorporativaSegurancadaInfo.pdf?title=Pol%C3%ADtica%20Corporativa%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o

Política de segurança

- Uma política de segurança só possui utilidade se for conhecida de seus funcionários. Há três estratégias básicas para que todos da empresa tenham conhecimento da política de segurança:
  - Termo assinado de que o funcionário leu a política de segurança e que se compromete a cumpri-la;
  - Campanhas e tecnologias: as empresas podem criar quadros para enfatizar a política de segurança espalhadas em pontos estratégicos da empresa;
  - Treinamentos periódicos em segurança da informação: normas e procedimentos podem ser discutidos e trabalhados em grupos específicos.

Política de segurança

- Cada organização deve ter a sua própria política de segurança, que deve ser desenvolvida de acordo com suas próprias características, linguajares e contextos específicos.

- Assim, os seguintes aspectos devem ser utilizados para a definição da política de segurança de uma organização:
  - Análise de riscos;
  - Estratégia e requisitos de negócios: diferentes negócios requerem diferentes níveis de segurança;
  - Requisitos legais: alguns setores possuem obrigações legais a serem cumpridas.

Política de segurança

- Um dos principais fatores que resulta em proteção concreta da organização, em conjunto com uma política de segurança efetiva, é a cultura em segurança da informação.

- A cultura de segurança é importante porque é voltada para as pessoas, e não para as tecnologias.

- Em cultura de segurança da informação, a percepção de todos é fundamental. Caso o funcionário de uma organização tenha a percepção de que o presidente é de fato zeloso quanto à proteção da informação, naturalmente ele irá também agir com cuidado para proteger as informações.

Política de segurança

- A segurança deve começar pelo topo.
- A cultura deve buscar o engajamento de todos.
- Em cultura de segurança da informação, a percepção de todos é fundamental. Caso o funcionário de uma organização tenha a percepção de que o presidente é de fato zeloso quanto à proteção da informação, naturalmente ele irá também agir com cuidado para proteger as informações.

EXERCÍCIOS

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

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