PÓS EM COMÉRCIO EXTERIOR E ESTRATÉGIA

UNIVERSIDADE CATÓLICA DE PETRÓPOLIS

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

TECNOLOGIA DA INFORMAÇÃO

.:UNIDADE 5 - SEGURANÇA DA INFORMAÇÃO:.

PARTE 3 - FERRAMENTAS DE SEGURANÇA

VERSÃO: SETEMBRO DE 2018

Professor: Luís Rodrigo de O. Gonçalves
E-mail: luis.goncalves@ucp.br
Site: http://lrodrigo.sgs.lncc.br

(3) Ferramentas para Segurança

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

Assim como, a Segurança da Informação abrange várias áreas e formatos de dados, as ferramentas de segurança seguem o mesmo modelo.

Mas podemos identificar algumas de suas classes:

- Criptografia
- VPN
- Firewalls
- IDS / HIDS / IPS

CRIPTOGRAFIA

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Criptografia**
  - Do grego: kryptós, "escondido", e gráphein, "escrita"
  - Princípios e técnicas para comunicação segura na presença de terceiros;
  - Impedindo a leitura das mensagens trocadas
  - Largamente utilizada na Internet:
    - em sites e sistemas on-line
    - nos e-Commerce
    - nos e-Bussines

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Criptografia - Conceitos**
  - Texto Claro (plain text) – info. não cifrada
  - Segredo – Chave da Proteção
  - Cifragem – codificação do texto claro
  - Texto Cifrado - codificado
  - Decifragem – decodificação do texto codificado
  - Algoritmos Criptográficos
  - Criptologia e Criptoanálise;
  - Esteganografia e Esteganálise;
  - Criptovirologia

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Criptografia - Aplicações**
  - Certificados Digitais
  - Comercio e Negócio eletrônico
  - Cartões baseados em chip
  - Moedas Digitais (Bitcoin, etc)
  - Senhas Digitais
  - Troca de informações sigilosas (Civil ou Militar)

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

Criptografia - Técnicas

- Monoalfabeto e monogrâmica – caracteres são trocados um a um - Livro de Jerenias
- Cifra de Cesar – substituição de letras com avanço de casas
- Polialfabéticos
- Enigma – **1918** – Arthur Scherbius
- Enigma G – **1928** – Elétrico-mecânica, permitia a troca do segredo
- Diffie e Hellman – **1976** – Chave Pública – origem do **RSA**

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Criptografia - Técnicas**
  - Chave Simétrica
  - Chave Assimétrica
  - Hash
  - Criptografia Quântica

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Criptografia - Relaciona-se com**:
  - Confidencialidade: só o destinatário autorizado deve ser capaz de extrair o conteúdo da mensagem;
  - **Integridade**: ser capaz de verificar se a mensagem foi alterada durante o transporte
  - Autenticação: verificar se o remetente é realmente quem afirma ser.
  - **Não Repúdio ou irritratabiliade**: não deve ser possível ao remetente negar a autoria da mensagem

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Criptografia – de Arquivos**:
  - BitLocker: desenvolvido pela Microsoft; realiza a encriptação de unidades;
  - **VeraCrypt**: é o sucessor do TrueCrypt, pode encriptar todo uma unidade/volume ou gerar um arquivo de um tamanho determinado (Windows|Mac|Linux)
  - DiskCryptor: outra alternativa ao TrueCrypt, utilizado para encriptar unidades externas e partições inteiras (Windows)
  - **AxCrypt**, baseado na criptografia, individual de arquivos; sua interação com o Windows permite que o usuário clique sobre um arquivo codificado para que o mesmo possa ser aberto.

VPN

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **VPN – Virtual Private Network**:
  - Rede de comunicação privada montada sobre as redes públicas
  - Os dados fluem sobre uma conexão segura, como um túnel
  - Os dados são codificados na origem e decodificados no destino
  - Os protocolos de tunelamento seguro oferecem: confidencialidade, autenticação e integridade
  - Protocolos básicos:
    - Layer 2 Tnneling Protocol (L2TP)
    - Point-to-Point Tunneling Protocol (PPTP)
    - IP Security Protocol (IPSEC)

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **VPN – Tipos**:
  - **VPN PPTP**: solução mais comum; conexão de usuários; não exige hardware, podem ser oferecida pelo seu sistema operacional; não oferece criptografia;
  - **VPN L2TP**: Microsoft e Cisco; forma um túnel sem criptografia; o IPsec provê a criptografia do canal; fornece confidencialidade e integridade;
  - **SSL (Security Socket Layer) e TLS (Transport Layer Security)**: pode ser utilizada pelo navegadores e outros clientes (OpenVPN)

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **VPN – Pode ser usada para**:
  - Conectar Filiais geograficamente à rede da Matriz, de forma segura e transparente. (VPN Site to Site)
  - Prover segurança sobre conexões sem fio (WiFi)
  - Prover a troca segura de informações
  - Contornar geo-restrições
  - Conectar à servidores de proxy para proteger a identidade e a localidade
  - Permite acesso aos recursos da rede local da empresa sem estar fisicamente conectado à ela.

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **VPN – e seus usuários**:
  - Funcionário
  - Downloader
  - Em transito (viajando, cafeteria)
  - O que adora privacidade (manter o sigilo das conexões)

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **VPN – critérios de uso e contrato**:
  - Observe a política de privacidade
  - Observe a diferença entre a versão gratuita e a paga.
  - Protocolos: preferencia para o SSL (OpenSSL) e o TLS
  - Locais de Saída: várias localidades; o mais próximo do recurso; restrição de geolocalização
  - Registro de informações: verifique a Política de Registro de Informações
  - Controle de Malware: scanner de arquivos ativos
  - Clientes: Móveis, Desktop e Servidores

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **VPN – Soluções encontradas no mercado**:
  - ExpressVPN
  - NordVPN
  - CyberGosht
  - PrivateVPN
  - IPVanish
  - VyprVPN

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **VPN – Montando seu próprio servidor**:
  - Servidor VPS – Servidor Virtual Privativo
  - Hamachi Proxy -
  - OpenVPN – pode cobrir toda a sua rede local
  - OpenVPN+Privoxy – privacidade e anonimato
  - Winconnection
  - Windows Server Essentials – VPN
  - Outline VPN (Windows, Mac, Linux)

FIREWALLS

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Firewalls**:
  - São dispositivos de rede que aplicam políticas em determinados segmentos ou hosts;
  - Geralmente associados a pilha TCP/IP (Internet).
  - Na forma de um Software ou Hardware (Appliance)
  - Controla dos fluxos de Entrada e Saída
  - Primeiras soluções são de 1980, ainda na ARPNET.

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Firewalls - Gerações**:
  - 1ª Geração – Analise individual dos pacotes, sem o conceito de conexão; lista de acessos simples (ACLs); alguns ativos possuem suporte a este recurso
  - 2ª. Geração – orientados a conexão; Statefull; baseados nas tabelas de conexão do TCP/IP (New, Established e Related)
  - 3ª. Geração – Firewall de Aplicação ou Firewall Proxy; combinavam ambas as funcionalidades.
  - 4ª. Geração – Stateful Inspection; inspeciona pacotes e tráfego baseado no perfil das aplicações
  - Next Generation

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Firewalls - Tipos**:
  - Firewall de Pacotes: análise individual dos pacotes; camada de Rede e Transporte
  - Proxy Firewall ou Gateways de Aplicação;
  - Statefull Firewall: de estado sessão; Stateful Inspection; Deep Packet Inspection (analise em todas as camadas);
  - Firerall de Aplicação: análise de protocolos específicos; atuam junto do servidor onde a aplicação está hospedada; camada de verificação antes de chegar à aplicação.

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Firewalls – Soluções para empresas:**
  - Cisco Asa X
  - FortGate UTM
  - Paloalto Next-Generation Firewalls
  - Checkpoint Firewall
  - Intel Security
  - Juniper
  - Linux – iptables
  - BSD - pfSense

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **Firewalls – Soluções Servidores e Desktop**:
  - Linux – iptables
  - BSD – pf / ipfilter / ipfw
  - Windows Firewall
  - TinyWall (Windows – Free)
  - Comodo Firewall (Windows – Free)
  - Windows Firewall Control – Controle do firewall do Windows.
  - Zone Alarme Free Firewall

IDS/IPS – NIDS/HIDS

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

- **IDS/IPS/HIDS**
  - IDS – Intrusion Detection System
    - NIDS – Network IDS
    - HIDS - Host IDS
  - IPS – Intrusion Prevention System

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

IDS - Intrusion Detection System

- Sistema Passivo
- Examina os fluxos de rede
- Identificar acessos (externos/internos) não autorizados;
- Monitoram os cabeçalhos e o campo de dados dos pacotes
- Informa sobre possíveis ameaças
- **Falsos Positivos e Negativos**
- Detecção baseada em (i) assinatura, ou (ii) anomalias estatísticas

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

IPS - Intrusion prevention System

- Sistema Ativo
- Conectado em linha, logo apos o firewall.
- Inicialmente eram IDS que se comunicavam com o firewall
- Foram implementadas soluções de bloqueio dentro do próprio IPS
- Libera ou bloquei os acessos baseado no conteúdo do pacote e da aplicação associada.
- Pode ser baseado em rede ou em host.

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

NIDS e HIDIS

- Os IDS e os IPS podem ser de dois tipos, dependendo de sua "localidade"
  - Network IDS
  - Host IDS
- OS **HIDS** examinam o sistema hospedeiro, ou o sistema final, onde estão instalados os serviços e os ativos
  - Acesso aos arquivos
  - Acessos aos aplicativos
  - Informações dos Logs

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

NIDS e HIDIS

- OS NIDS examinam o fluxo de informações que transita pela rede;
  - Busca comportamentos suspeitos
  - Geralmente instalado: (i) atrás/após do firewall; em (ii) sub-redes importantes onde os usuários internos podem ter acesso; (iii) nas redes dos servidores

Segurança da Informação

FERRAMENTAS PARA SEGURANÇA

IDS/IPS - Soluções

- Snort – Windows e Unix Like
- Tripwire – Unix Like - HIDS
- The Bro Network Sec. Monitor – Unix Like
- Suricata – Windows e Unix Like
- Malware Defender – Windows – IPS – Free
- OSSEC – Open Source HIDS SECurity – Unix Like
- Sagan – Unix Like
- Secutity Onion – Unix Like
- AIDE – Unix Like
- Open WIPS-NG – Unix Like

SEG. INFO. – FERRAMENTAS DE SEGURANÇA

PÓS EM COMÉRCIO EXTERIOR E ESTRATÉGIA

UNIVERSIDADE CATÓLICA DE PETRÓPOLIS

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

TECNOLOGIA DA INFORMAÇÃO

.:UNIDADE 5 - SEGURANÇA DA INFORMAÇÃO:.

PARTE 3 - FERRAMENTAS DE SEGURANÇA

VERSÃO: SETEMBRO DE 2018

Professor: Luís Rodrigo de O. Gonçalves
E-mail: luis.goncalves@ucp.br
Site: http://lrodrigo.sgs.lncc.br