PÓS EM COMÉRCIO EXTERIOR E ESTRATÉGIA

UNIVERSIDADE CATÓLICA DE PETRÓPOLIS

CENTRO DE CIÊNCIAS SOCIAIS APLICADAS

TECNOLOGIA DA INFORMAÇÃO

.:UNIDADE 5 - SEGURANÇA DA INFORMAÇÃO:.

PARTE 2 - AMEAÇAS A SEGURANÇA

VERSÃO: SETEMBRO DE 2018

Professor: Luís Rodrigo de O. Gonçalves

E-mail: luis.goncalves@ucp.br
Site: http://lrodrigo.sgs.lncc.br

(2) Ameaças a Segurança

Segurança da Informação

AMEAÇAS A SEGURANÇA

Vulnerabilidade

- ✗ Pode ser uma falha: (i) no projeto, (ii) na implementação ou (iii) na configuração de determinado software ou sistema operacional.
- ✗ Quando explorada por um "atacante", resulta na violação da segurança.

Segurança da Informação

AMEAÇAS A SEGURANÇA

Negação de Serviço

- DoS - Denial of Service
  - Ocorre quando o "atacante" usa apenas UM host realiza o ataque sobre outro computador ou serviço conectado à Internet.
- DdoS – Distributed Denial of Service é um ataque distribuído
  - VÁRIOS hosts são no ataque à um ou mais serviços e computadores.

Segurança da Informação

AMEAÇAS A SEGURANÇA

Phishing

- ✗ É um tipo de fraude que acontece através do envio de mensagens ou solicitações.
- ✗ O conteúdo recebido parece ter sido enviado por uma fonte conhecida;
- ✗ Todavia direcionam o usuário ao acesso de páginas falsas, que são utilizadas para obter dados privilegiados.

Segurança da Informação

AMEAÇAS A SEGURANÇA

Malware

- Códigos maliciosos, usados para realizar ações ilícitas em um host ou serviço
- Tipos:
  - Virus (Arquivo/Macro/Boot)
  - Cavalos de Troia
  - Adware / Spyware
  - Backdoor
  - Worms (Vermes)
  - Keyloggers
  - Spam Relays

Procedimentos de Segurança

Segurança da Informação

PROCEDIMENTOS DE SEGURANÇA

Os Procedimentos de Segurança dependem:

- ⚠ Dos controles que fazem parte da Política;
- ⚠ Do tipo do sistema operacional e das aplicações
- ⚠ Do valor do ativo
- ⚠ Mas recomenda-se que um grupo básico de controles seja aplicado sempre que possível (vide ISSO /IEC 27002)

Segurança da Informação

PROCEDIMENTOS DE SEGURANÇA

Monitoramento e Registro de Acesso:

- ⚠ O par Login e Senha é um dos mecanismos mais antigos de proteção digital, mesmo assim é um dos mais utilizados
- ⚠ Alguns processos de invasão começam com o teste de quebra de senha baseado na "***força bruta***"
- ⚠ Devemos monitorar, registar e alertar sobre tentativas de acesso autorizados e negados
- ⚠ Validar o horário, a geolocalização e a detecção de dispositivo

Segurança da Informação

PROCEDIMENTOS DE SEGURANÇA

Identificação/Análise/Verificação de Arquivos

- Varredura periódicas podem alertar sobre:
  - presença de arquivos pesados ou com tamanhos suspeitos
  - presença de diretórios/pastas com nomes estranhos
  - extensões incomuns ou desconhecidas.
- Gerenciadores de arquivos e HIDs podem ser utilizados para identificar, verificar e remover estes arquivos.

Segurança da Informação

PROCEDIMENTOS DE SEGURANÇA

Backup de Dados / Aplicação / Maquina Virtual

- O Backup é um dos procedimento básicos de segurança; deve ser realizado e testado periodicamente;
- Recomenda-se que ele seja automático (diariamente, semanalmente e mensalmente);
- Pode ser do tipo Full ou Incremental
- Pode ser baseado em níveis: (i) na maquina do usuário, (ii) no servidor; (iii) disco/fita externa; (iv) site remoto; (v) Nuvem.

Segurança da Informação

PROCEDIMENTOS DE SEGURANÇA

Backup de Dados / Aplicação / Maquina Virtual

- ⚠ Mantido na nuvem ou localmente
- ⚠ Uma nova modalidade seria o “sincronismo de dados” com a nuvem.
- ⚠ Devem fazer parte do backup (i) os dados, (ii) os códigos fontes, (iii) as configurações; recomenda-se também (iv) as aplicações e a imagem das maquinas virtuais
- ⚠ Deve-se elabora um Plano de Backup e um Inventário dos Ativos

Segurança da Informação

PROCEDIMENTOS DE SEGURANÇA

Firewall / Filtros de Conteúdo / Proxy

- O Firewal permite controlar o que pode, quando pode e por quem pode ser acessado.
- Disponível nos Sistemas Operacionais e como um Appliance de Rede
- Alguns podem realizar a análise do conteúdo de pacotes, em busca de:
  - Malwares / Spam / Phishing
  - Conteúdo indevido / impróprios

Segurança da Informação

PROCEDIMENTOS DE SEGURANÇA

Controle sobre o Acesso Móvel

- Deve-se decidir pelo uso ou não de dispositivos móveis dentro da empresa, os quais deverão ser controlados;
- Política de BYOD – Bring Your Own Device
  - Assinatura dos Termo de: (i) Confidencialidade, (ii) Responsabilidade e (iii) Privacidade;

Segurança da Informação

PROCEDIMENTOS DE SEGURANÇA

Política de BYOD – Bring Your Own Device

- Recomenda-se:
  - sw de geolocalização – Roubo ou perda
  - sw de remoção completa dos dados e senhas;
  - sistema de envio de alertas - perda ou roubo;
  - conexão automática com o Wi-Fi da empresa;
  - bloquear a instalação de aplicativos não autorizados;
  - restringir o uso de câmeras;
  - barrar a gravação de áudio;
  - criar logins e senhas fortes
  - usar técnicas de VPN (Virtual Private Network);
  - usar ferramentas de criptografia;

Segurança da Informação

PROCEDIMENTOS DE SEGURANÇA

Soluções de Segurança para E-mail:

- Um dos principais meios de difusão de ameaças:
  - Ataque de Phishing: mensagens falsas
  - Malware
  - Arquivos Infectados
  - Links Maliciosos
  - Roubo e divulgação de dados sensíveis.

Segurança da Informação
PROCEDIMENTOS DE SEGURANÇA

Soluções de Segurança para E-mail:

- No uso de gerenciadores de e-mail:
  - Somente dispositivos autorizados devem acessem o e-mail da empresa;
  - Fornecer proteção ao conteúdo e aos anexos;
  - Usar firewalls para evitar a invasão;
  - Usar filtros contra spam (entrada e saída)

- Deve-se desenvolver e divulgar políticas sobre as boas práticas no uso do e-mail e do gerenciador.

Procedimentos 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 2 - AMEAÇAS A SEGURANÇA

VERSÃO: SETEMBRO DE 2018

Professor: Luís Rodrigo de O. Gonçalves

E-mail: luis.goncalves@ucp.br
Site: http://lrodrigo.sgs.lncc.br