Grupo de Resposta a Incidentes de Segurança

Segurança Básica

Segurança de sistemas

Garantia de...

Disponibilidade

Confidencialidade

Integridade

Segurança de sistemas

Disponibilidade:

A disponibilidade diz que os serviços/recursos do sistema estão disponíveis sempre que forem necessários

Confidencialidade:

A confidencialidade diz que a informação só está disponível para aqueles devidamente autorizados

Segurança de sistemas

Integridade:

A integridade diz que a informação não é destruída ou corrompida e o sistema tem um desempenho correto

Problemas e soluções!

Problemas !

Segurança de sistemas

Vírus:

Pequenos programas capazes de replicar-se inserindo seu código dentro de outros arquivos.

Segurança de sistemas

Worms:

Tem a maioria das características de um vírus, mas não precisam infectar outros arquivos para sua disseminação.

Segurança de sistemas

Cavalos-de-Tróia:

Programa que promete ser útil e, na verdade, provoca estragos intencionais.

Segurança de sistemas

Keyloggers:

Programas que capturam teclas digitadas e enviam relatórios aos invasores (inclusive senhas!). Alguns keyloggers são tão avançados que possuem recursos de captura das telas e mouse do micro.

Segurança de sistemas

Bombas-lógicas:

Também chamadas de *slag code*, são instruções adicionadas a uma aplicação que ficam inativas por um período de tempo pré-determinado, ou até que um evento ocorra, ativando as instruções.

Segurança de sistemas

Backdoors:

Meio de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão.

Segurança de sistemas

Injeção de código:

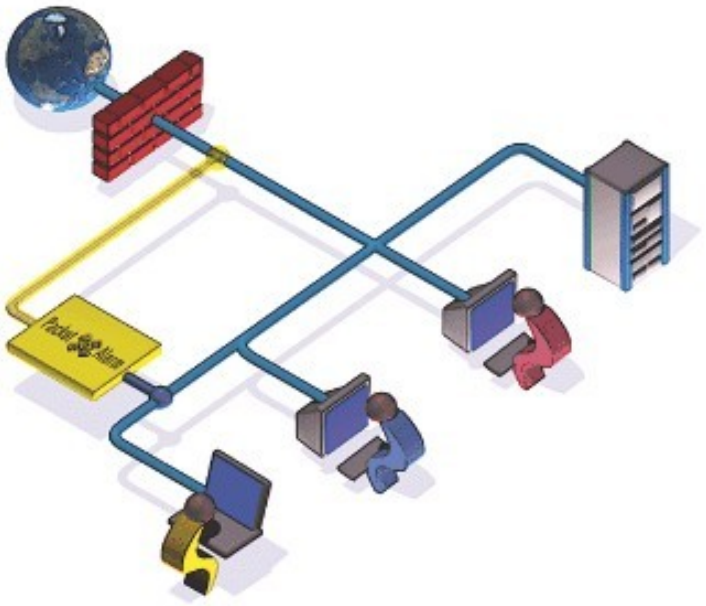
- Mal-tratamento das entradas dos usuários para formulários ou banco de dados

Cross-site Scripting
SQL Injection
Script Injection

Segurança de sistemas

“Sniffing”:

- Escuta de pacotes que alcancem uma interface de rede.



Segurança de sistemas

“Spoofing”:

- Uma máquina se faz passar por outra para ter a confiabilidade que a primeira (original) teria.

Segurança de sistemas

Engenharia Social:

- Método de ataque onde faz-se uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não-autorizado a computadores ou informações.

Segurança de sistemas

Ataques por força bruta:

Método para quebrar esquemas de autenticação através da tentativa combinatória, aleatória ou de inúmeros usuários e chaves pré-definidos.

Negação de Serviço (DoS):

Utilização de um computador para tirar de operação um serviço ou computador conectado à Internet.

Exemplos:

- **Gerar uma sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo;**
- **Gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível, de modo que qualquer computador desta rede fique indisponível;**
- **Tirar serviços importantes de um provedor do ar, impossibilitando o acesso dos usuários às suas caixas de correio no servidor de *e-mail* ou ao servidor *Web*.**

Segurança de sistemas

Pichação (Defacement):

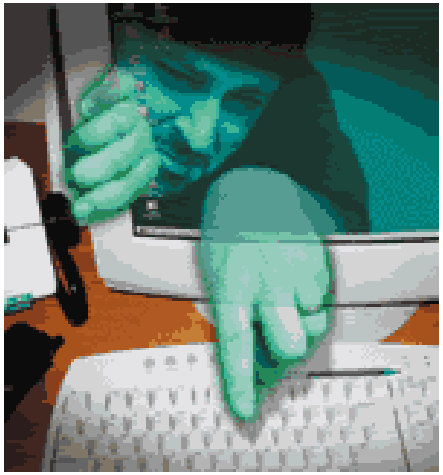
-Substituição ou alteração não autorizada de um web site. O mais conhecido arquivo de defacements é o http://www.zone-h.org , que monitora não só defacements, mas também invasões web em qualquer nível.

Segurança de sistemas

Roubo (Físico e Digital):

- Cópia de documentos de acesso restrito.

- De nada serve ter um sistema eletronicamente seguro, se qualquer pessoa consegue acesso físico aos dados.



Segurança de sistemas

Uso indevido de recursos:

Não existe uma definição exata do que possa ser considerado um uso abusivo da rede. Internamente às empresas e instituições, situações que caracterizam o uso abusivo da rede estão definidas na política de uso aceitável.

Soluções!

Segurança de sistemas

Algumas medidas de segurança a serem tomadas :

- Utilizar senhas seguras , alternando-a entre caracteres, símbolos e números.

Exemplo: #Amdsst01

- Utilzar criptografia na troca de informações na rede.

Segurança de sistemas

- Instalar e manter atualizados um bom programa antivírus e suas assinaturas.

- Instalar e Manter atualizado um bom anti-spyware.

- Utilizar um firewall pessoal de alta confiabilidade e alta proteção .

Segurança de sistemas

- Desabilitar no seu programa leitor de e-mails a auto-execução de arquivos anexados às mensagens.

- Não executar ou abrir arquivos recebidos por e-mail ou por outras fontes, mesmo que venham de pessoas conhecidas.

Caso seja necessário abrir o arquivo, certifique-se que ele foi verificado pelo programa antivírus.

Segurança de sistemas

- Manter o seu sistema sempre atualizado , procurando novas versões e paths disponíveis para ele.

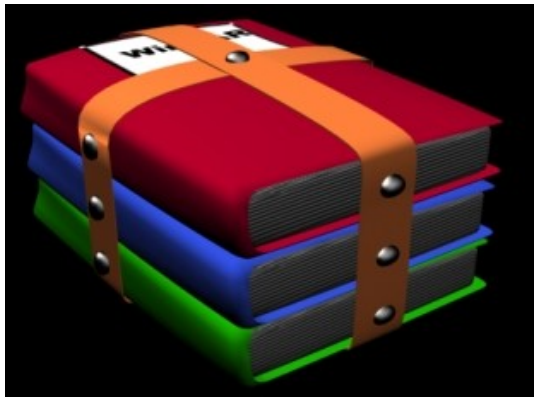
- Fazer Backups de seus documentos.

- Certificar-se que não existam vulnerabilidades em seu computador .

Segurança de sistemas

--Procurar utilizar na elaboração de documentos formatos menos suscetíveis à propagação de vírus, tais como PDF, RTF .

- Procurar não utilizar, no caso de arquivos comprimidos, o formato executável. Utilize o próprio formato compactado, como por exemplo Zip ou Gzip.



Dúvidas?