Segurança de Rede

Por definição, segurança de rede é todo o sistema de software, hardware e procedimentos que protegem dados, equipamentos e softwares de uma rede.

Política de segurança

- Em sua primeira visita ao laboratório de informática, você deve ter recebido várias recomendações, como:
- Não comer perto do computador;
- Não derramar líquidos no teclado;
- Siga a sequência correta para ligar e desligar os computadores.
- Essas recomendações são chamadas de **Política de Segurança**, que pode ser entendida como um conjunto de diretrizes ou regras que tem como principal objetivo a conscientização dos usuários quanto ao uso dos equipamentos e softwares em um laboratório.
- Essas diretrizes variam de acordo com cada lugar, cabendo ao administrador da rede criar e divulgar a política de segurança a todos os usuários da rede.

Invasão de sistemas

- Hoje, um dos principais focos das empresas é a segurança de seus dados e equipamentos.
- A Internet é a grande ferramenta de comunicação, ao passo que também é o principal veículo para contaminações virtuais como ***vírus, worms e trojans***.
- Estes têm causado muita dor de cabeça em ***administradores de rede*** que controlam a segurança de suas organizações.

Invasão de sistemas

- **Liberdade:** Os usuários de computadores querem **liberdade** para navegar, transmitir ou receber dados em seu computador, de forma rápida e eficiente.

- **Responsabilidade:** Ser um administrador de redes que consiga criar a consciência de proteção para seus usuários é uma tarefa bastante trabalhosa, quando grande parte da **responsabilidade da segurança** das informações está nas mãos de seus usuários.

- **Regras:** Um bom administrador de redes ensina aos seus usuários **regras de boa conduta** para navegação pela Internet. Ele também documenta, realiza atualizações e investe em palestras.

Hacker e/ou Cracker

- **Hacker:**

O termo, por si só, já é polêmico. Muitos profissionais de TI (Tecnologia de Informação) afirmam que não é possível unir as palavras hacker e ética, dada a natureza das atividades desses indivíduos.

Entretanto, por definição, o hacker é um especialista em segurança que possui alto grau de conhecimento em sistemas operacionais e linguagem de programação, procura por falhas nos sistemas através de técnicas diversas e seu objetivo não é causar danos ou roubar informações, mas aprimorar conhecimentos e vencer desafios.

Hacker e/ou Cracker

- **Cracker:**

  São considerados Crackers, os Hackers mal intencionados: que invadem computadores e vão destruindo tudo o que encontram pela frente. Muitos hackers ganham a vida trabalhando na área de segurança e não gostam de ser chamados de crackers.

Risco

- Sexta-feira, meia-noite, uma rua deserta, em um bairro de alto risco. Como descobrir os perigos que se escondem em um beco escuro?
- Com a Internet, os perigos ocorrem da mesma forma tanto para empresas como para usuários comuns, é necessário ter cuidado para não se expor. Vírus, hackers e vulnerabilidades sempre existirão, assim como bactérias, assaltantes e buracos.
- Como na vida real, o maior problema é que, muitas vezes, a busca por proteção na Internet acontece quando o problema ocorre ou quando já é tarde demais. Mais uma vez é essencial ter em mente, quando pensamos em segurança de rede, aquele velho ditado que ouvimos de nossas mães: "É melhor prevenir do que remediar!".

Ameaça Externa

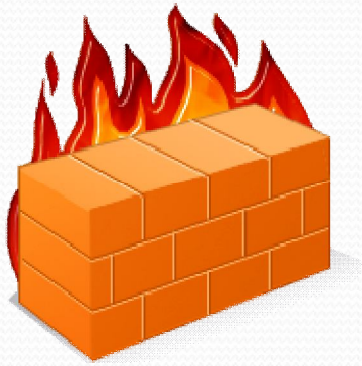
- As ameaças externas compreendem qualquer tipo de ação maléfica efetuada a partir de locais de fora da sua rede e são as ameaças que mais preocupam as instituições ligadas em rede. Quando o site de um banco é invadido ou quando uma rede ou um computador da rede é infectado por um vírus ou até mesmo quando uma mensagem falsa de e-mail é recebida, isso tudo pode ser considerado uma ameaça externa. Os tipos de ameaças externas mais comuns estão listados abaixo:
- Vírus;
- Worms ;
- Cavalos de Tróia;
- Hoax;
- Backdoors ;
- Spywares ;
- Spams.

Ameaça Interna

- Podemos considerar como uma invasão interna quando usuários inexperientes, por falta de informação ou por ingenuidade, realizam ações inadequadas, como por exemplo, anotar informações secretas em locais inseguros ou abrir arquivos anexados de e-mails sem as devidas precauções.
- Um outro exemplo de ameaça interna que costuma causar grandes estragos é aquela feita por funcionários insatisfeitos e subornáveis de grandes empresas. Estes atuam divulgando informações secretas ou facilitando a entrada de invasores na rede da empresa.

Barrando a Invasão

- Atualmente, as corporações investem em consultorias de segurança, dispositivos e softwares, como: Firewalls, antivírus, entre outros. Esses recursos auxiliam e protegem as redes de computadores dessas corporações contra as ameaças cibernéticas. A proteção da informação nunca foi tão estudada e necessária como nesse tempo em que vivemos



Riscos...

Quais são as maiores ameaças?

Vírus!!!

- Os vírus atuam sempre infectando outras células, eles nada fazem quando estão isolados.
- Já sabemos também que os vírus de computador trabalham de maneira idêntica aos vírus biológicos. Portanto, podemos definir um vírus de computador como sendo um programa de informática capaz de se multiplicar mediante a contaminação de outros programas ou arquivos.

- Os vírus de computadores podem produzir desde efeitos simplesmente importunos até altamente destrutivos. Além disso, esses "pesadelos virtuais" geralmente têm datas agendadas para atuarem, como por exemplo: **Sexta-feira 13**, **dia dos namorados**, **dia das bruxas**, etc. É muito importante ficar atento a essas datas!

Importante!!!

- Os vírus, geralmente, estão anexados a arquivos executáveis (.exe, .com, .bat) que ao serem abertos ou executados, instalam o vírus no computador.

- **Anexos executáveis:**
- Deve-se estar atento aos anexos executáveis: não os execute se não souber realmente o que faz o arquivo. Se ele foi enviado por e-mail, o cuidado deve ser rigoroso.

- É importante conhecer a procedência e, se preciso for, tentar falar com quem lhe enviou o anexo antes de abri-lo. Pois, algumas vezes, os vírus são enviados utilizando um endereço de e-mail como destinatário sem que o dono desse e-mail esteja ao menos sabendo.

- É preciso passar sempre o antivírus em qualquer arquivo novo que é utilizado no computador, principalmente os recebidos por e-mail ou gravados em disquetes de outras pessoas. O antivírus ainda é a melhor ferramenta tanto para evitar como para sanar problemas com vírus em seu computador. Mantenha-o sempre atualizado e execute-o frequentemente.

Tipos de vírus existentes:

- **Vírus de boot:** Ataca a trilha zero do disco rígido, responsável pela inicialização do sistema operacional. Uma vez infectado esse registro, na próxima vez que ocorrer o ***boot*** do sistema, o vírus entrará em ação.

- **Vírus de arquivos ou de programas:** Atacam os programas, copiando o seu código no código fonte do programa alvo. A partir daí, sempre que o programa infectado for executado, o vírus ficará ativo, infectando outros programas.

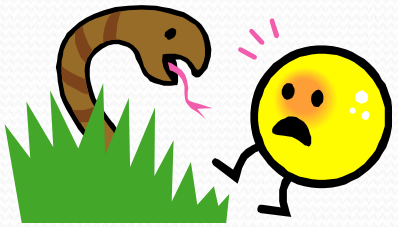
- **Vírus multipartite:** Agregam funções dos vírus de boot e dos vírus de arquivo. Isso significa que eles atacam tanto os setores de boot como os programas do computador.

- **Vírus de macro:** Programas como o Word e Excel possibilitam que o usuário crie pequenas seqüências de comandos para que esses sejam executados automaticamente, visando facilitar e agilizar as tarefas mais freqüentes dos usuários. Essa automação é chamada de macro. Entretanto, alguns vírus são feitos adicionando código malicioso a esses macros e os anexando a inocentes documentos. Os principais alvos são exatamente os editores de texto e as planilhas de cálculo, principais geradores de macros.

- **Vírus retroativo:** Vírus que tem como alvo os programas de antivírus, buscando causar danos a eles e atrapalhando, assim, a segurança do seu computador.

Worm

- Vamos relembrar das aulas de biologia? Você sabe a diferença entre um vírus e um verme?
- Os vermes têm um comportamento diferenciado ao dos vírus, pois, conseguem parasitar diretamente o ser humano, sem a necessidade de infectar células para se reproduzirem.
- Da mesma forma como os vermes, os programas parasitas - conhecidos como **Worms** - realizam cópias de si mesmos, sem infectar outros arquivos.

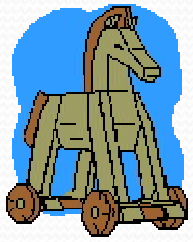


Worms são mais perigoso que um vírus comum?

- Os **Worms** podem ser considerados mais perigosos que os próprios vírus, devido a sua forma de transmissão, que os tornam mais difíceis de se evitar.
- Assim como os vírus, os worms podem infectar a máquina do usuário através da execução de um programa malicioso.
- Por isso, também é recomendado ter um antivírus atualizado e executá-lo freqüentemente. Além disso, é importante tomar cuidado com os sites em que navegamos e os links em que clicamos.

Cavalo de Tróia

- São programas que aparentam ser aplicativos normais, porém eles escondem códigos maliciosos.
- De forma escondida, executam funções não comandadas pelo usuário, como por exemplo, enviar informações pessoais ou abrirem ***portas de comunicação*** dos computadores e, até mesmo, permitir que seu computador seja controlado remotamente.
- Os Trojans não conseguem se auto-reproduzir, mas podem ser altamente destrutivos.



Portas de comunicação

- Portas de comunicação são ligações para conexões do seu computador para uma rede externa a ele (conexão de saída) ou de uma rede externa para ele (conexão de entrada). Só existe comunicação entre dois computadores, quando houver conexões de entrada e saída estabelecidas entre esses dois computadores através de uma determinada porta de origem e outra porta de destino.
- É importante saber que só existe uma porta aberta em um computador, se a mesma estiver executando um serviço, que pode ser um programa ou uma aplicação, sob aquela porta. Para se fechar qualquer porta de um computador, basta fechar o serviço que está sendo executado sob a porta.

Hoax

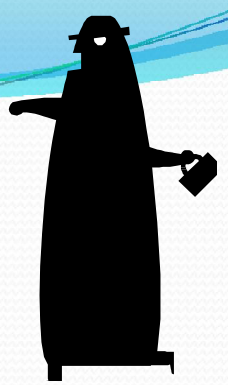
- É uma palavra da língua inglesa que, em português, significa **pregar uma peça** ou **passar um trote**, que é a principal característica do hoax.
- Em informática eles são páginas web ou e-mails que trazem informações falsas sobre um determinado assunto.

- Alguns dele[illegible]m histórias e pedem para serem repassados, outros solicitam que você execute alguns comandos em seu computador para se proteger quando, na verdade, esses comandos o levam a danificar o seu computador; e existem, ainda, os que requisitam senhas bancárias, entre outras informações sigilosas.

Backdoors

- Os **Backdoors** são programas maliciosos que abrem *portas de comunicação* no computador infectado. O seu objetivo é fazer com que um computador fique vulnerável para que outro computador possa acessá-lo via Internet. Na maioria das vezes, eles são instalados por *Cavalos de Tróia.*

Spywares



- Os spywares são programas espiões, que observam o dia-a-dia do usuário para capturar informações sobre seu perfil, como preferências, gostos e costumes, para enviá-las ao servidor que o instalou.
- Essas informações são úteis para os sites enviarem propagandas de seu gosto, e esse é o motivo pelo qual, durante a navegação na Internet, repentinamente nos é mostrado um anúncio de propaganda.

Spams

- Originalmente, SPAM foi o nome dado a uma marca de presunto picante (SPiced hAM, em inglês, de onde surgiu a sigla).
- Porém, na Internet, o significado de Spam pode ser definido como mensagens de conteúdo inútil, ou melhor, mensagens que o usuário não espera receber e que, geralmente, trazem somente propagandas não requisitadas por ele.
- Atualmente, os spams são enquadrados na ilegalidade, sendo o seu propagador sujeito a penas jurídicas.

Como se prevenir?

O que podemos fazer?

O que devemos fazer?

O que instalar ?

Cuidados com Senhas

- Você já observou como utilizamos senhas para quase tudo? Caixas eletrônicos, em cofres de bancos, sites e e-mails. Como seria possível nos identificar se não houvesse uma senha.
- As senhas são uma forma de garantir a segurança e a privacidade, além de identificá-lo aos sistemas.

Pacotes de correção ou atualização

- A atuação de hackers e crackers na busca por falhas de segurança de sistemas operacionais e softwares, faz com que vulnerabilidades nos programas sejam descobertas com muita velocidade. Por isso, pacotes de correções ou atualizações são cada vez mais comuns nos dias de hoje.

- Os pacotes de correções ou atualizações são disponibilizados, geralmente, nos sites de fabricantes para download gratuito ou nos próprios softwares, na seção de Update.
- Antivírus e sistemas operacionais da família Windows fazem muito uso desse recurso para que seus usuários estejam sempre protegidos.

Antivírus

- Os antivírus protegem e removem vírus, worms e cavalos de tróia de um computador.
- O antivírus é um importante utilitário de segurança e uma medida, tanto preventiva quanto corretiva.
- Todo antivírus tem como princípio básico a verificação de disquetes, CD-ROMs, DVDs, PEN DRIVEs, pastas e arquivos na busca de programas maliciosos.

Atualizando o antivírus

- Durante a verificação da existência de um vírus, o antivírus vasculha os drives (disco rígido e disquete) e compara os dados neles presentes com as informações de um banco de dados dos vírus conhecidos.
- Como nós já aprendemos, todos os dias novos vírus são desenvolvidos. Os fabricantes de antivírus estão constantemente preocupados em aprender a detectá-los e a removê-los, distribuindo suas novas descobertas aos usuários por meio de atualizações das informações cadastradas em banco de dados.

Utilizando vacinas

- No mundo digital também existem vacinas. Porém, ao contrário das vacinas humanas, as vacinas digitais são utilizadas após a infecção do programa, portanto, trata-se de uma medida corretiva!

Anti-Spyware

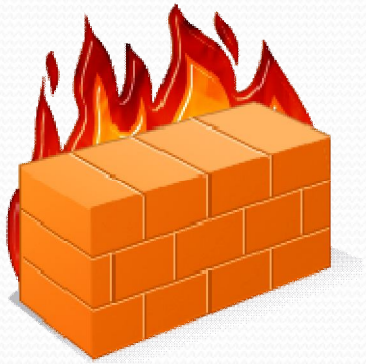
- Uma das formas de conseguirmos nos livrar desses programas é apagando-os manualmente, mas isso exige um trabalho muito grande e um conhecimento exato de sua localização no computador. Foi pensando nisso que programas como o **Spybot** foram desenvolvidos para que você consiga remover os spywares do computador, sem sacrifícios.
- O **Spybot** traz uma vantagem muito interessante e útil ao usuário: a possibilidade de imunizar o sistema contra as ameaças já reconhecidas.

Anti-spam

- Para se livrar desse incômodo, você pode utilizar os próprios servidores de e-mail.
- Eles já possuem serviços de anti-spam: quando um e-mail chega aos servidores, ele é inspecionado, para verificar se caracteriza um Spam conhecido. Com isso, apenas as mensagens com conteúdo interessante são entregues ao usuário.
- Esses e-mails indesejados, na maioria das vezes, são redirecionados para a pasta **Lixo Eletrônico** ou **Lixeira**, para que você possa conferi-los, mais tarde.

Firewall

- O Firewall examina, em tempo real, tudo o que provém da Internet e chega até a sua rede local.
- Para saber o que pode ser liberado ou bloqueado, o firewall utiliza uma lista de regras previamente estabelecidas pelo administrador da rede.
- Com essas regras, o firewall consegue **barrar**, **permitir**, ou **pedir autorização**, quando qualquer ação incomum ou não definida acontecer.



- Muito obrigado...

- Cuidado com a sua segurança...

Firewall

- Firewall em português significa Parede de Fogo. Na área da computação, os firewalls são inseridos entre a rede interna e a rede externa, como por exemplo, entre a rede do laboratório de uma escola e a Internet.
- Essas paredes de fogo são definidas por meio de uma lista de permissões e restrições devidamente configuradas para filtrar o tráfego da rede e impedir que ela seja alvo de ataques e invasões.
- É importante lembrar que os firewalls podem ser softwares instalados em computadores ou em hardwares (equipamentos) conectados à rede.

Artifícios de proteção

- Embora as técnicas de ataque e invasão dessas ameaças estejam se aprimorando cada vez mais, não podemos nos desesperar e deixar de utilizar as facilidades e inovações que o desenvolvimento tecnológico nos permite, como a conexão dos computadores em rede local e a própria Internet.
- Assim como existem as ameaças, existem vários recursos como Firewalls, antivírus, programas de verificação de rede, além de precauções simples como regras para definição de senhas e proteção de arquivos e pastas, que podem ser empregados para nos proteger.