

IMD0703 – Segurança de Redes

Histórico e conceitos básicos de segurança.
Revisão da Arquitetura TCP/IP.

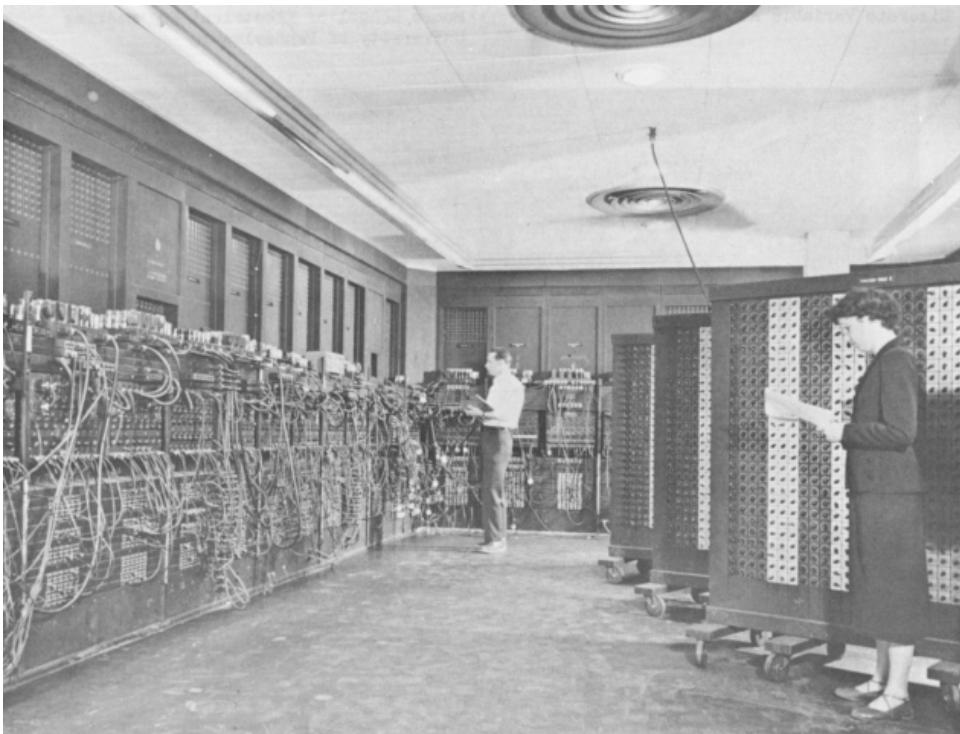




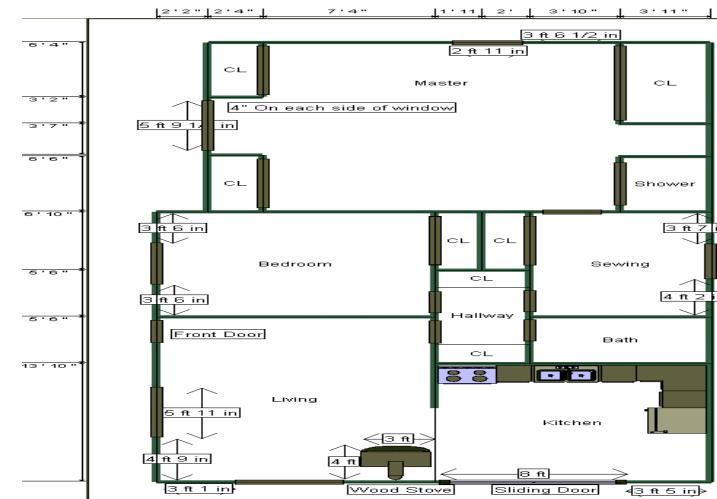
**“A falsa sensação de segurança é muito pior
do que a certeza da insegurança”**

No início...

O Computador



O Perímetro



O Sistema de Segurança



Hoje...

O Computador



O Perímetro



O Sistema de Segurança



E os invasores também mudaram...



Introdução

- Os usuários das redes de computadores mudaram, bem como o uso que os mesmos fazem da rede
 - Alta penetração dos dispositivos de comunicação (*Internet of Things - IoT*)
- A segurança da rede desponta como um sério problema
 - Atualmente nos causa mais problemas ter o computador invadido do que a casa, ou a carteira furtada
- O crescimento comercial assustador da Internet é superado apenas pela preocupação com a segurança deste novo tipo de mídia
- Novas tecnologias, novos ataques, novos mecanismos de defesa... E a guerra segue!
- Entender de segurança de dados e de rede já não é um conhecimento desejável, mas sim indispensável

Introdução

- A segurança em sua forma mais simples se preocupa em garantir que pessoas mal intencionadas (externas, ou internas) não leiam, ou pior ainda, modifiquem dados/mensagens
- É estatisticamente levantado que a maior parte dos problemas de segurança são intencionalmente causados por pessoas que tentam obter algum benefício ou prejudicar alguém
 - Mas não somente! (A “zueira BR”, por exemplo)
- Segundo pesquisas, e constatações feitas pelas próprias empresas especializadas em vender projetos e produtos voltados para o segmento de segurança de informação:
 - “As empresas brasileiras são vulneráveis, frágeis e passíveis de invasões porque a grande maioria dos executivos – não apenas os responsáveis pela área de tecnologia – adotam posturas paternalistas e não profissionais com relação às informações dentro das corporações”

Introdução

- Tipos de Segurança
 - Segurança Física
 - Providenciar mecanismos para restringir o acesso às áreas críticas da organização
 - Segurança Lógica
 - Fornecer mecanismos para garantir:
 - Confidencialidade
 - Integridade
 - Não Repudiação ou Irrefutabilidade
 - Autenticidade

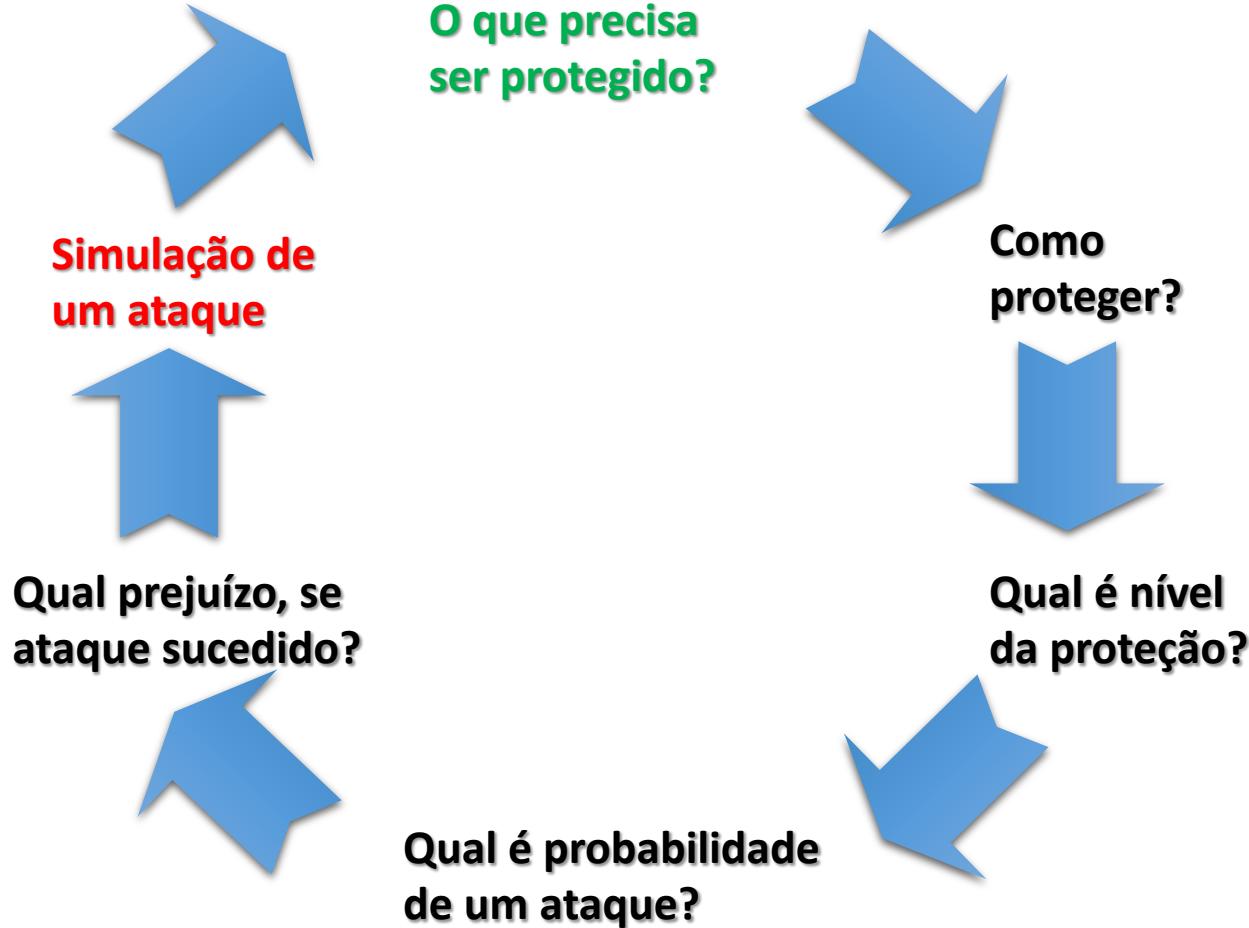
Introdução

- Em Segurança de Redes, os detalhes simples acabam por se mostrar os mais complicados!
- Exemplo 1: Senhas
 - “Por que me deram esta senha tão complicada!?”
 - A escolha da senha pode comprometer ou reforçar a Segurança da Rede
 - O acesso à senha de um usuário não dá acesso apenas aos seus dados particulares, mas a todos os recursos que ele utiliza, como documentos de seu setor, dados dos sistemas administrativos, A REDE, entre outros
 - Programas que “quebram”senhas são comuns hoje em dia

Introdução

- Exemplo 2: Sofisticação dos emails
 - Interpretam diversos tipos de códigos e arquivos
 - Códigos maliciosos se utilizam destes avanços
 - HTML, XML, VBScript, JavaScript
 - Uso de aplicações cliente de e-mail (Outlook, Eudora etc) X utilização de webmail
- Exemplo 3: Farta disponibilidade de ferramentas e literatura hacker
 - Qualquer um pode fazer o download de uma ferramenta ou copiar um script de intrusão
 - Há muita informação sobre falhas/brechas de segurança nos mais diversos dispositivos, sistemas operacionais e linguagens de programação
- Como estes, há muitos outros!

Ciclo de Vida da Segurança



Nosso “Dever de Casa”

- Todo profissional de TI deveria ter uma resposta exata para cada uma destas questões:
 - Quais mecanismos de segurança existem no seu ambiente corporativo?
 - Tais mecanismos são suficientes? Justifique a sua resposta?
 - Quais são as metas para este e o próximo ano no que diz respeito a:
 - Investimentos em Segurança (Tecnologia)
 - Treinamento Pessoal
 - Modificação dos Processos Internos

Ameaças

- Uma ameaça é algum fato que pode ocorrer e acarretar algum perigo a um bem
- As ameaças podem ser intencionais ou não-intencionais
 - Intencionais
 - Furto de informação
 - Vandalismo
 - Utilização de recursos, violando as medidas de segurança
 - Não-intencionais
 - Erros humanos,
 - Falhas em equipamentos,
 - Desastres naturais,
 - Problemas em comunicações

Risco

- Risco intuitivamente é o “perigo ou a possibilidade do perigo” [Aurélio].
- É uma medida da probabilidade da ocorrência de uma ameaça



Ameaças

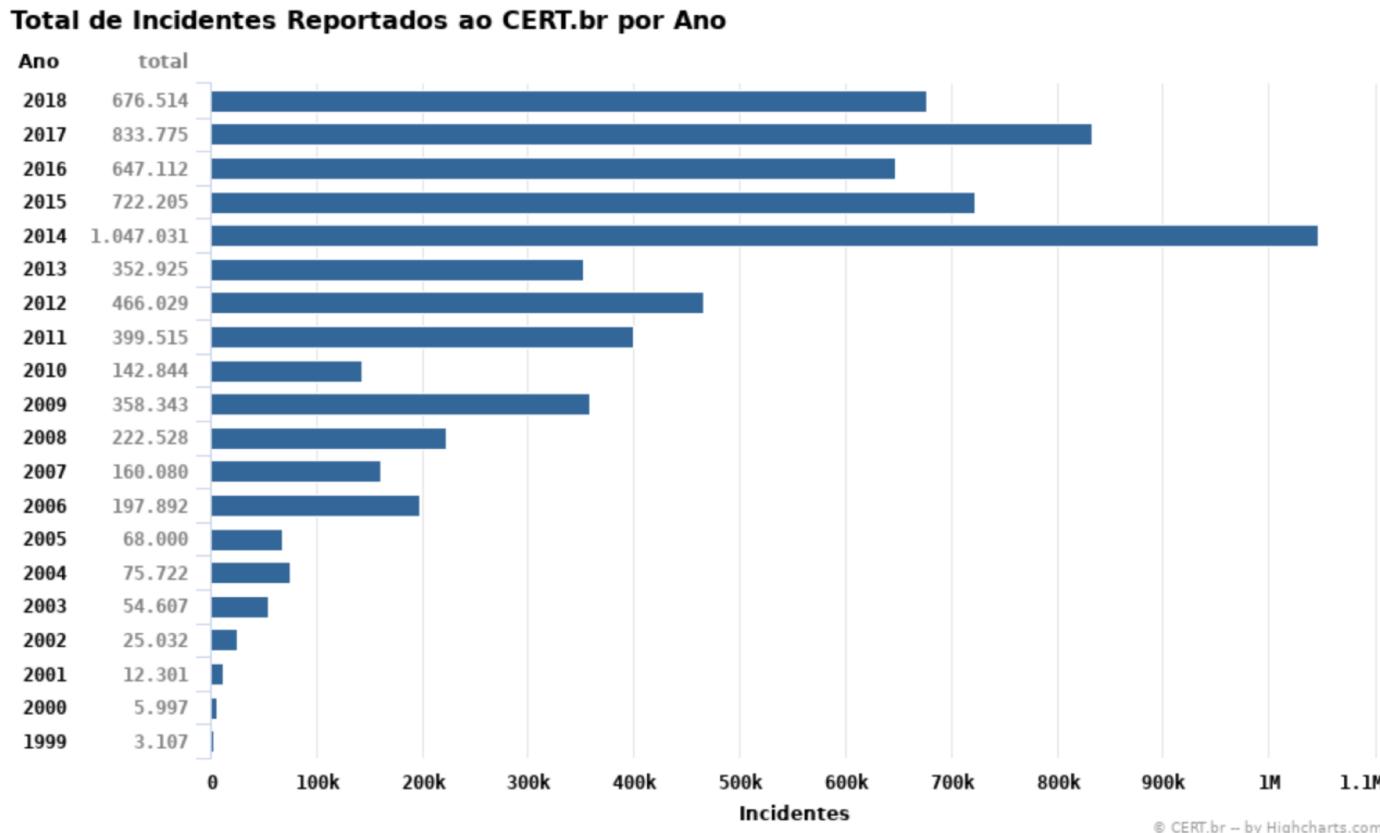
- Ameaças mais comuns às Redes de Computadores
 - Acesso não-autorizado
 - Reconhecimento
 - Recusa de Serviço
 - Manipulação de Dados

Avaliando as ameaças e riscos

- Quais são as ameaças reais ao seu sistema?
 - Quais são os riscos agregados?
- Quais das suas ameaças apresentam riscos imediatos?
 - Para tais riscos existem procedimentos no seu plano de segurança?
 - Existe PCN (Plano de Continuidade do Negócio) no caso de concretização destas ameaças?
- Quais das suas ameaças dificilmente se tornarão riscos imediatos?
 - Qual é a probabilidade do acontecimento?
 - Para tais riscos existem procedimentos no seu plano de segurança?
 - Existe PCN para tais riscos?

Dados Estatísticos

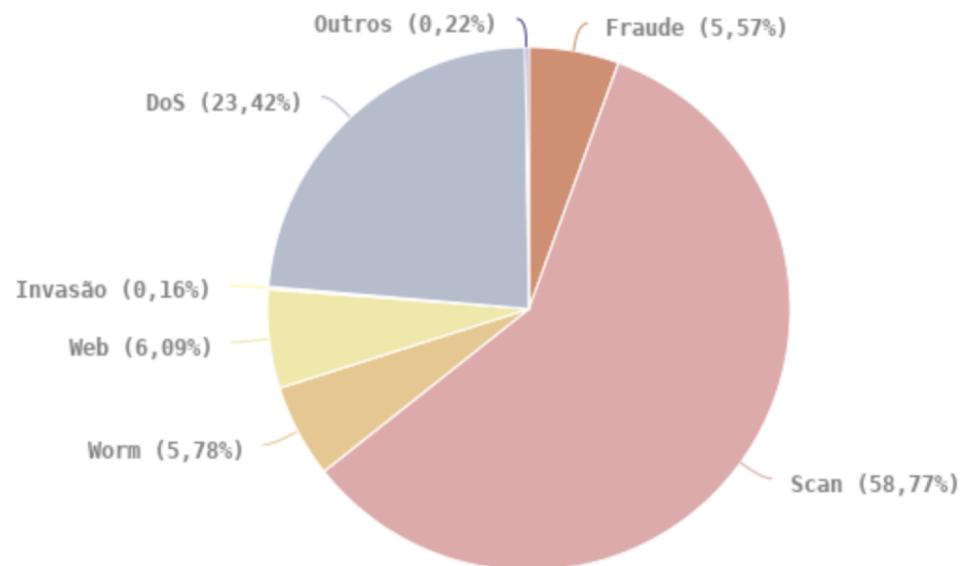
- Incidentes



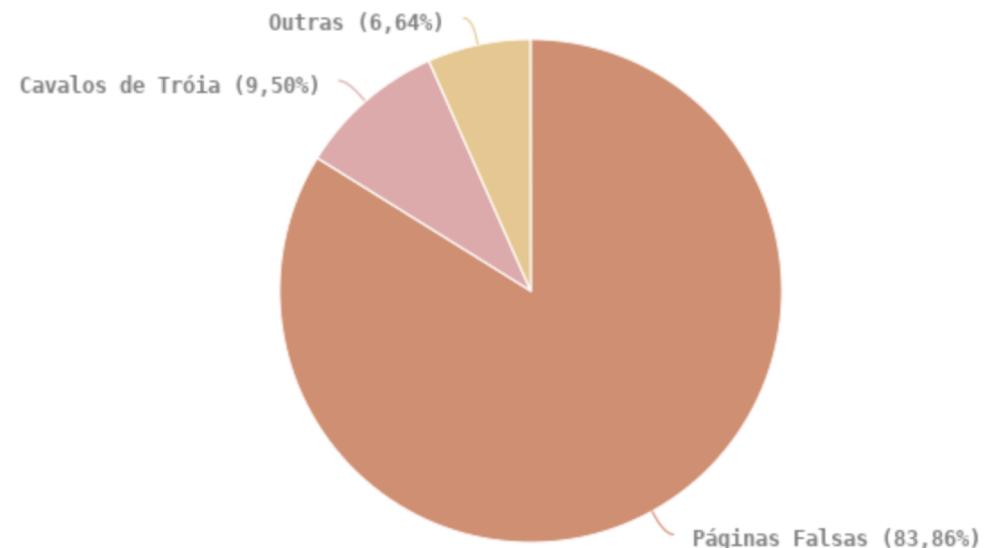
Fonte: CERT. O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil

Dados Estatísticos

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2018
Tipos de ataque



Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2018
Tentativas de fraudes

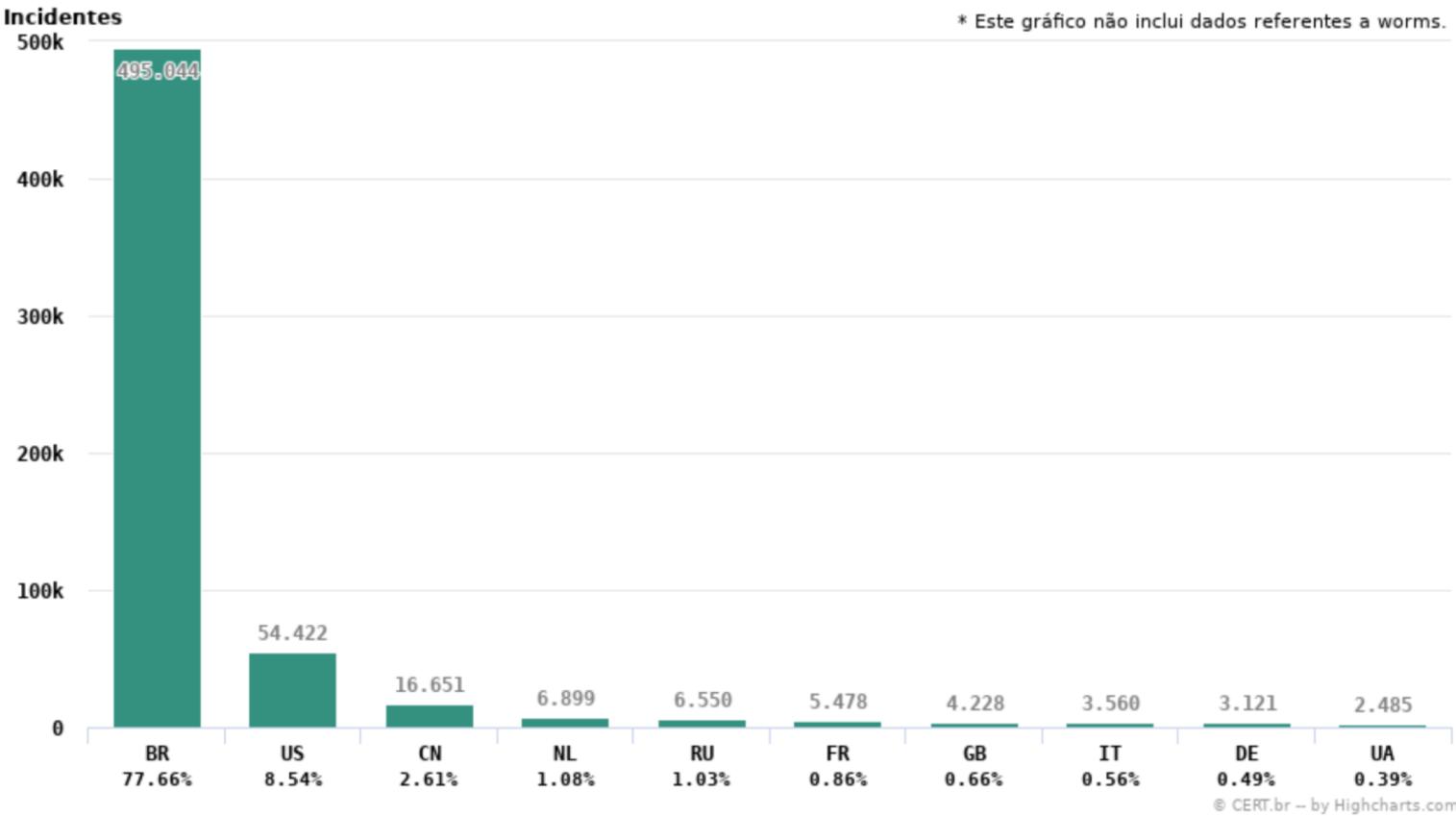


© CERT.br -- by Highcharts.com

Dados Estatísticos

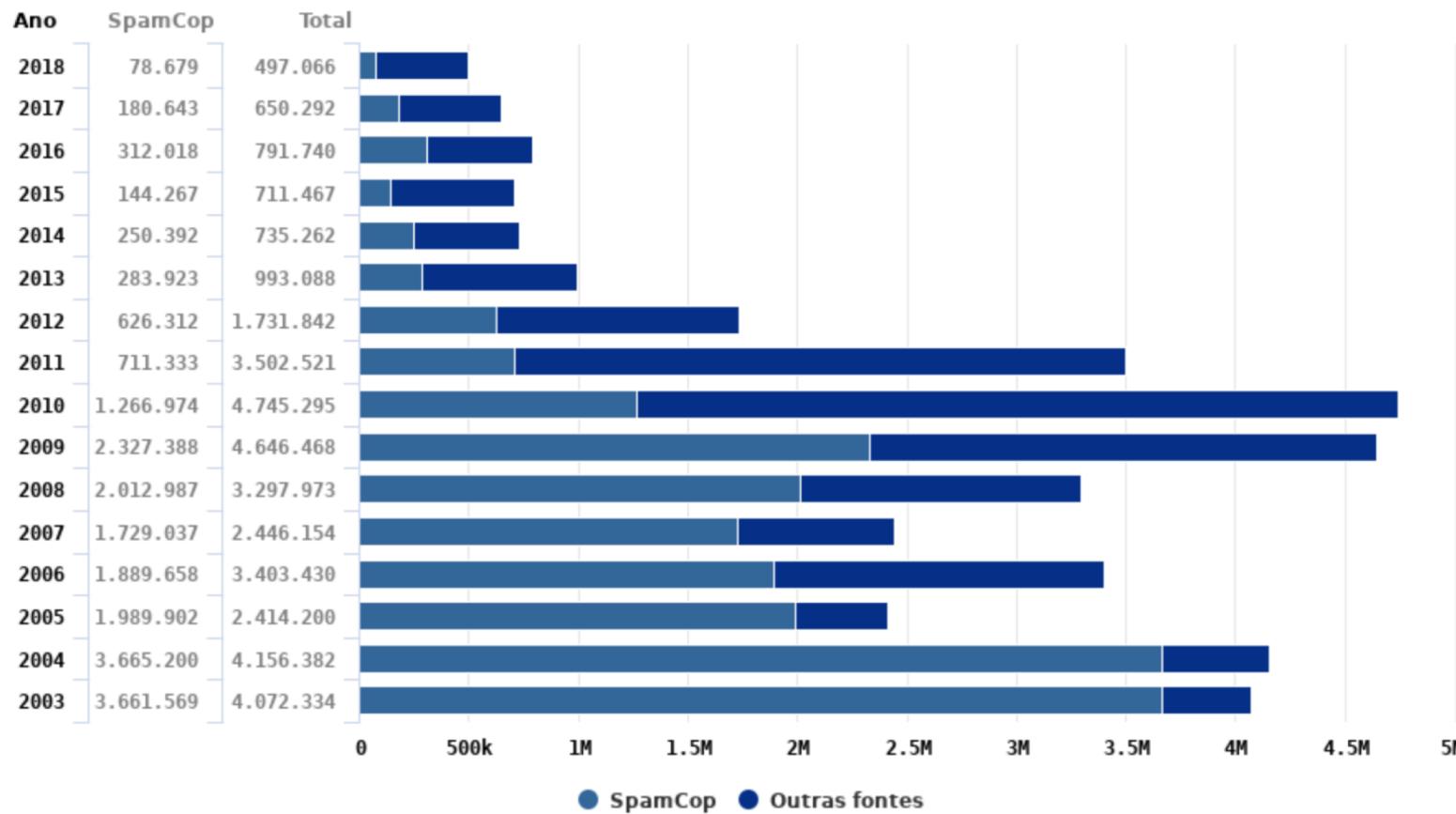
Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2018

Top 10 CCs origem de ataques



Dados Estatísticos

Spams Reportados ao CERT.br por Ano



© CERT.br – by Highcharts.com

Vulnerabilidade

- O que quer dizer Vulnerabilidade?
 - Ausência de proteção cobrindo uma ou mais ameaças
- Porque existem tantas Vulnerabilidades?
- Panorama de Vulnerabilidades:
 - Expansão de Ataques Possíveis;
 - Cada sistema possui o seu panorama;
 - Pode ser dividido em:
 - Mundo Físico;
 - Mundo Virtual;
 - Modelo de Confiança;
 - Ciclo de Vida do Sistema.

Mecanismos de defesa

- São muitas as tecnologias disponíveis
 - Anti-spam;
 - Antivírus;
 - Criptografia;
 - Firewall, IDS, IPS;
 - Auditoria;
 - Computação forense;
 - Honeypot e Honeynet;
 - Capturadores de Pacotes
- Dificuldades de integração

Mecanismos de Defesa

- Processos:
 - Normas;
 - Planos e Políticas de Segurança;
 - Treinamentos;
- Como medir a eficiência dos mecanismos de defesa?
- Qual é a relação de redução/aumento de riscos com a adoção de mecanismos de defesa?

Mecanismos de Defesa

- Pontos chave:
 - O uso adequado da tecnologia
 - Configuração correta
 - Atualização periódica
 - Otimização
 - Treinamentos para Usuários
 - **Auditoria**

Atacantes

- São muitos (“lá fora e aqui dentro”) e com diferentes perfis, motivações e habilidades
 - Estudante: Alterar ou enviar e-mail em nome de outros
 - Hacker: Examinar a segurança do Sistema; Roubar informação
 - Empresário: Descobrir o plano de marketing estratégico do competidor
 - Ex-empregado: Vingar-se por ter sido despedido
 - Contador: Desviar dinheiro de uma empresa
 - Corretor: Negar uma solicitação feita a um cliente por e-mail
 - Espiões/Terrorista: Roubar segredos de guerra
 - E muitos outros...

Origem dos Ataques

- Ataques externos:
 - Vulnerabilidade na rede (protocolos, implementações, etc.)
 - Vulnerabilidade nas aplicações (web servers, etc.)
- Causas mais prováveis
 - Falta de proteção ou proteção insuficiente
 - Confiança excessiva
 - Inexistência de auditoria
 - O alvo é de grande interesse
 - Extranet mal programada

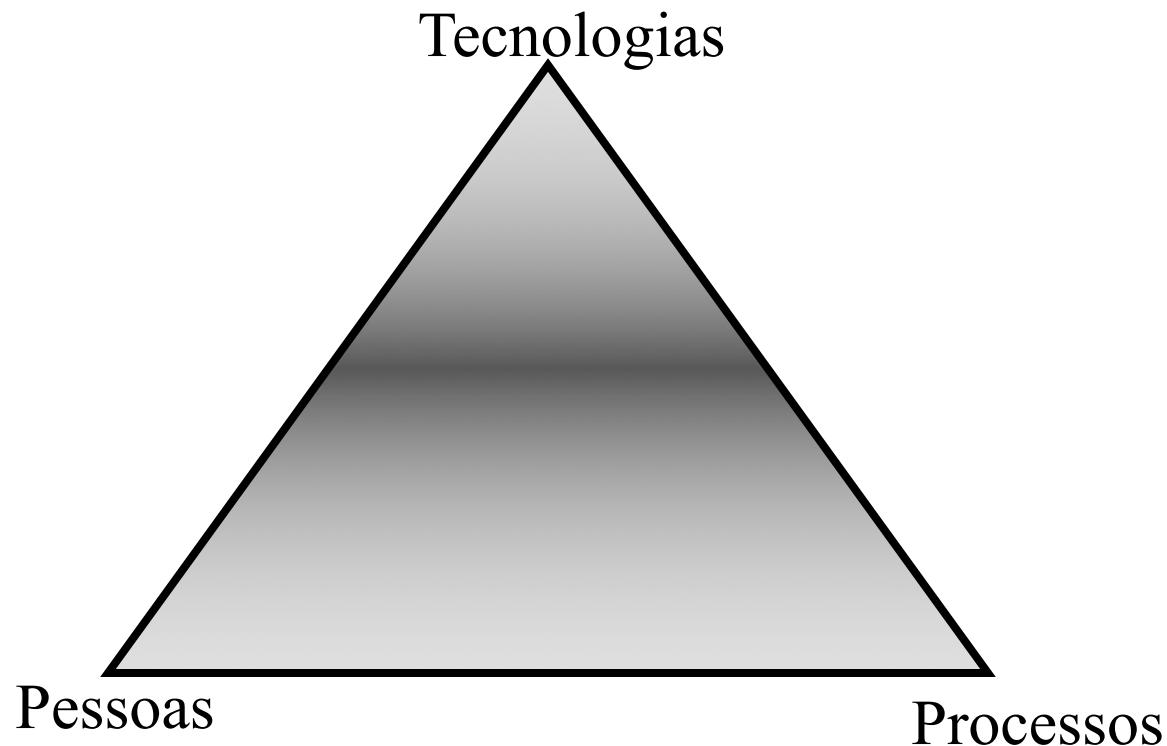
Origem dos Ataques

- Ataques Internos:
 - Acesso não autorizado a dados
 - Sabotagem
 - Engenharia social
 - Infecção por Vírus
- Causas mais prováveis
 - Inexistência de acesso hierárquico
 - Uso de periféricos/dispositivos pessoais
 - Retaliação
 - Intranet mal programada

Necessidade de uma Política de Segurança

- Diretrizes de segurança são responsabilidades dos CIOs, cabendo aos mesmos escreverem e viabilizar sua implementação, sejam elas agradáveis ou não para os funcionários
- Especialistas reconhecem que 100% de segurança é impossível de ser alcançado, todavia é possível alcançar um alto grau de garantia da informação se houver mecanismos de controle diário, 24 horas por dia, sete dias por semana
- Segundo a MODULO (www.modulo.com.br):
 - “Equipamentos só funcionam se tivermos uma política para cuidar das pessoas que lidam com eles”
 - “A equação no caso da informação é tratar do funcionário”

Tripé da Segurança



Política de Segurança

- Conforme definição da norma ABNT NBR ISO/IEC 27002:2005
 - “A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.”
- A Política de Segurança é o instrumento utilizado para a definição das normas a serem utilizadas na organização, práticas a serem exercidas/aplicadas aos ativos (funcionários, clientes, prestadores de serviços, fornecedores, informação, hardware, software) da empresa
 - É uma declaração formal das regras pelas quais as pessoas a quem é dado acesso ao ativo tecnológico e informação de uma organização devem obedecer

Política de Segurança

- O desenvolvimento de uma política de segurança deve ser uma atividade interdepartamental
- As áreas afetadas devem participar do processo envolvendo-se e comprometendo-se com as metas propostas além de:
 - Entender o que é necessário
 - Saber por o que são responsáveis
 - O que é possível com o processo
- Quem deve ser envolvido na definição da Política de Segurança?
 - Administrador(es) da rede
 - Responsáveis pela gestão da organização
 - Representantes dos utilizadores afetados pela Política de Segurança
 - Conselheiro legal

Política de Segurança

- Implementar uma política de segurança em uma organização implica em implementar controles de segurança do tipo:
 - Físicos
 - Lógicos
 - Organizacionais
 - Pessoais
 - Operacionais
 - De desenvolvimento de aplicações
 - Das estações de trabalho
 - Dos servidores
 - De proteção na transmissão de dados

Política de Segurança

- Controles físicos referem-se à:
 - Restrição de acesso indevido de pessoas a áreas críticas da empresa (ex: Sala de Servidores)
 - Restrições de uso de equipamentos ou sistemas por funcionários mal treinados
- Controles lógicos referem-se à:
 - Prevenção e fortalecimento de proteção seletiva de recursos
 - Problemas/prevenção causados por vírus, e acesso de invasores
 - Fornecer/retirar autorização de acesso
 - Fornecer relatórios informando que recursos estão protegidos, e que usuários tem acesso a esses recursos
 - Maneira fácil e compreensível de administrar essas capacidades

Política de Segurança

- Controles organizacionais referem-se à:
 - Responsabilizar cada usuário por lista de deveres
 - Especificar em cada lista o que, quando, e como deve ser feito
 - Esclarecer as consequências do não cumprimento da lista
- Controles pessoais referem-se à:
 - Criação de motivação/treinamento sobre segurança
 - Bloqueio dos arquivos pessoais do empregado quando da sua demissão
 - Troca de senha quando da demissão do funcionário
 - Inclusão de tópicos de segurança computacional no manual dos empregados
 - Cobrar aspectos de segurança na avaliação o funcionário

Política de Segurança

- Controles operacionais referem-se à:
 - Acompanhar e registrar cada problema, sua causa e sua solução
 - Planejar estruturas de arquivos e de diretórios
 - Prever/fornecer proteção de energia ao parque computacional e de conectividade (hubs, switches, routers, etc.)
 - Garantir a confiabilidade e a integridade dos dados avaliando o aspecto custo da rede
- Controle do desenvolvimento de aplicações referem-se à:
 - No caso das empresas não-desenvolvedoras de aplicações:
 - Adquirir software necessário e documentação necessária
 - No caso de empresas desenvolvedoras de aplicações:
 - Verificar a existência/eliminar bugs em softwares
 - Dar apoio de software em outros locais da organização
 - Manter / atualizar documentação

Política de Segurança

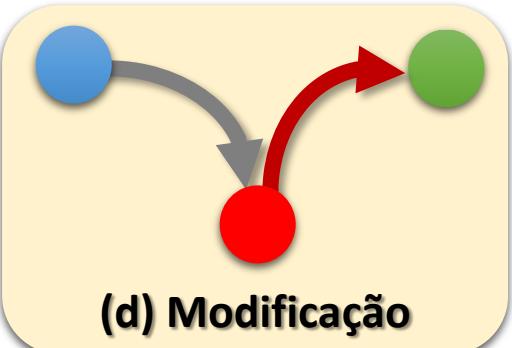
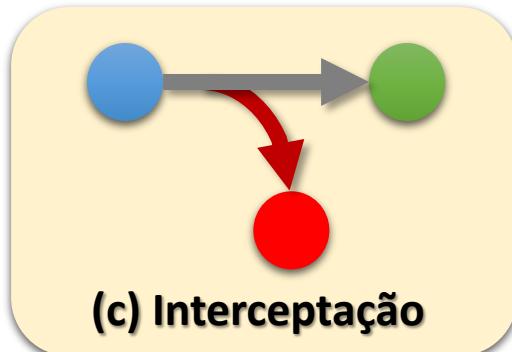
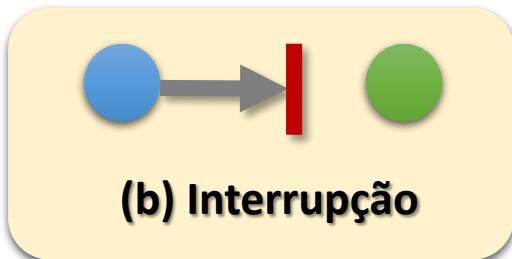
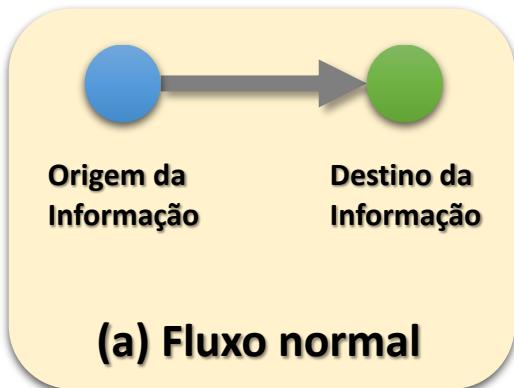
- Controle das estações de trabalho referem-se à:
 - Proteger os computadores contra roubo de placas, e acessos ao interior do gabinete (uso de travas);
 - Controlar instalação de programas de captura de senha;
 - Controlar acesso às estações.
- Controles do servidor referem-se à:
 - Prover proteção diversa (contra incêndios, umidade, temperatura, acesso)
 - Mantê-lo em ambiente fechado
- Controles de proteção à transmissão de dados referem-se à:
 - Uso de criptografia;
 - Filtros/proxy/firewall nas fronteiras da rede
 - Uso de fibras ópticas ou cabos pneumáticos que emitem alarmes quando despressurizados por “grampos”

Importante...



**Se existe alguma política de segurança e as pessoas
da organização não sabem, não serve para nada!!!**

Ataques



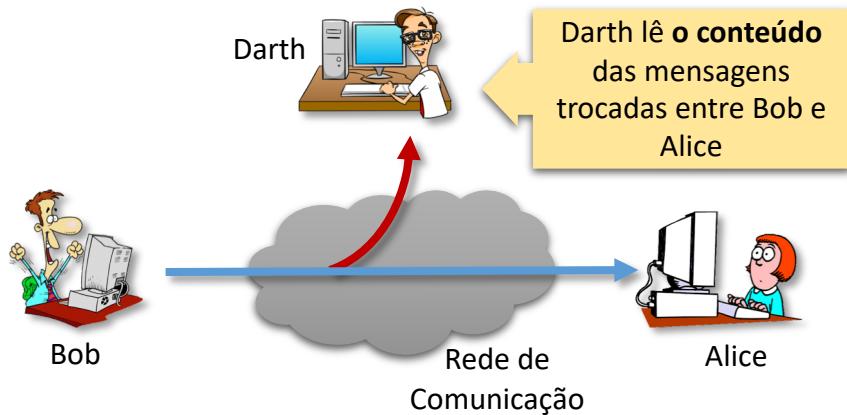
Ataques

- Interrupção
 - Recursos do sistema são destruídos ou tornados inacessíveis (DoS, DDoS);
 - Este é um ataque à disponibilidade
- Interceptação
 - Acesso não autorizado à informações;
 - Este é um ataque à confidencialidade
- Modificação
 - Alteração de informações de forma não autorizada;
 - Este é um ataque à integridade
- Fabricação
 - Dados são fabricados de forma ilegal, na tentativa destes serem vistos como dados autênticos;
 - Este é um ataque à confidencialidade

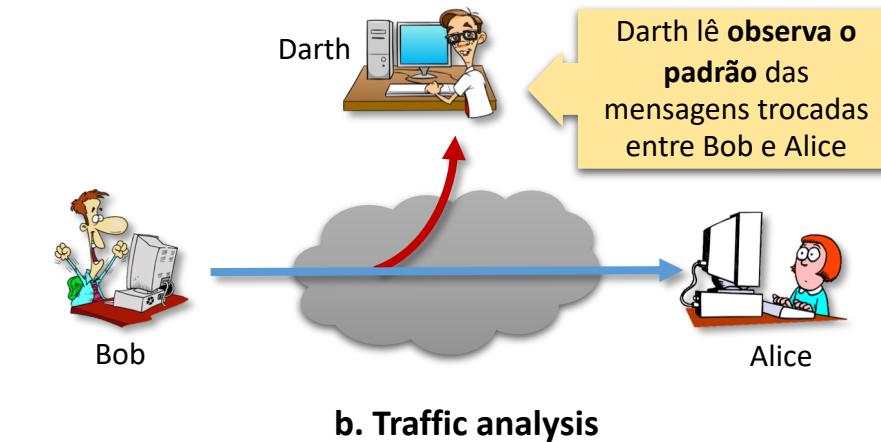
Ataques

- Ataques podem ser passivos ou ativos
- Ataques passivos:
 - Não alteram os sistemas ou as informações
 - Difíceis de serem detectados
 - Exemplo: *Packet sniffing*
- Ataques ativos:
 - Alteram os sistemas ou as informações
 - Mais fáceis (???) de serem detectados
 - Exemplos: *Spoofing*, modificação, *DoS*

Ataques Passivos

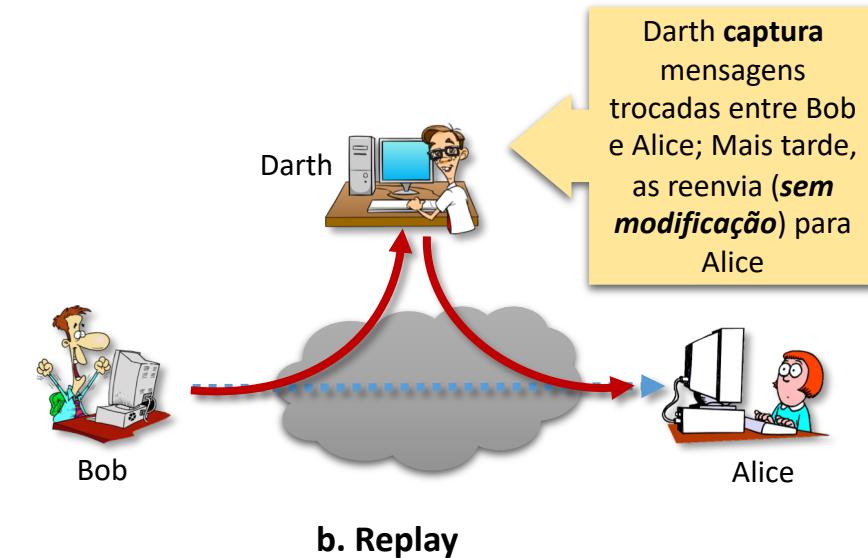
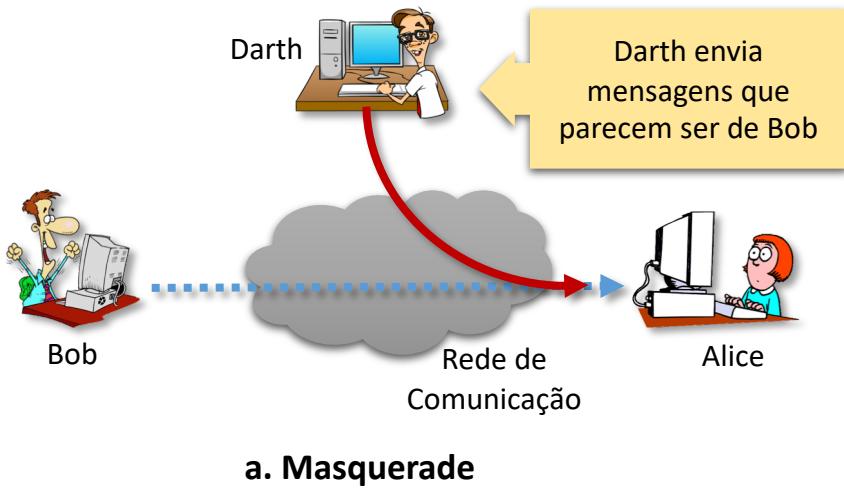


a. Release of contents message

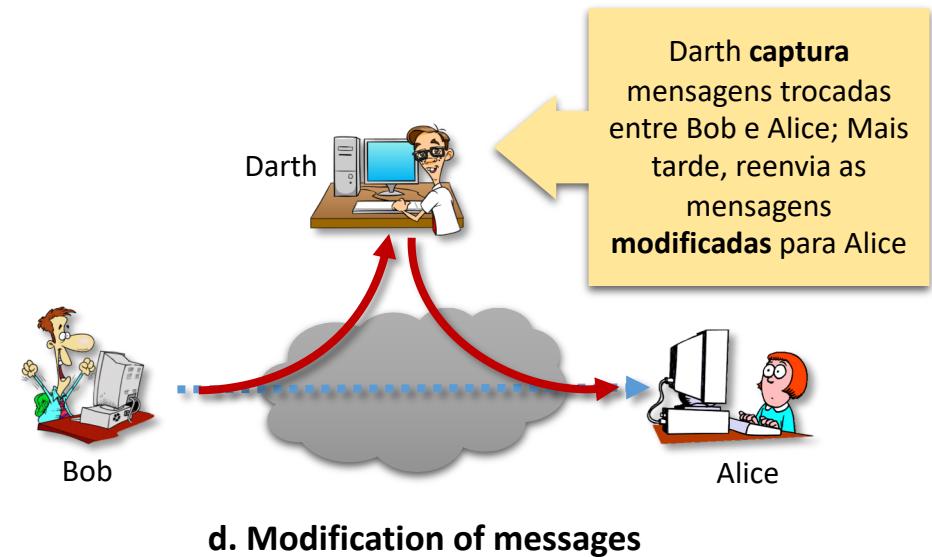
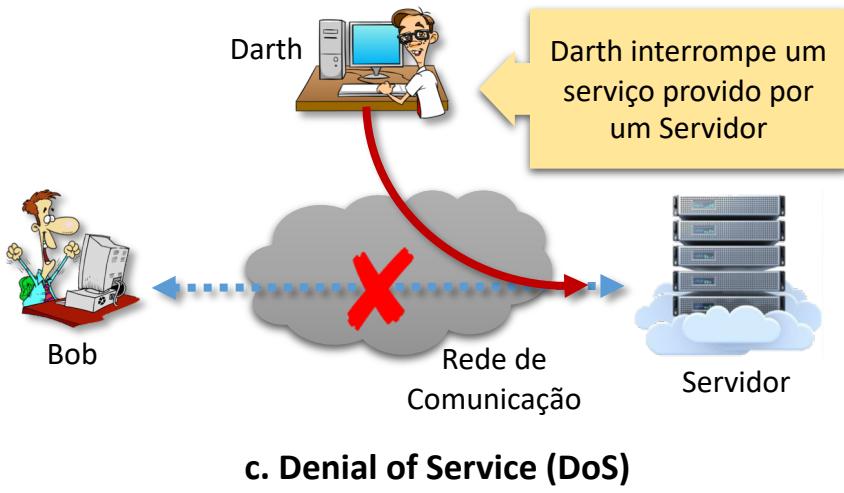


b. Traffic analysis

Ataques Ativos (1)



Ataques Ativos (2)



Serviços de Segurança

- Autenticação (*Authentication*)
 - A garantia que a entidade envolvida na comunicação é verdadeiramente quem diz ser
- Controle de Acesso (*Access Control*)
 - A prevenção contra uso não autorizado de um recurso e envolve garantir:
 - QUEM pode acessar o recurso
 - Sob QUAIS CONDIÇÕES o acesso pode ocorrer
 - O QUE aqueles que possuem acesso ao recurso podem fazer
- Confidencialidade dos Dados (*Data Confidentiality*)
 - A proteção dos dados contra a revelação não autorizada

Serviços de Segurança

- Integridade dos Dados (*Data Integrity*)
 - A garantia de que um dado recebido está exatamente da mesma forma como foi enviado por uma entidade autorizada
 - Necessário garantir que os dados não sofreram alterações, inserções, remoções ou replay
- Não repúdio (*Non-Repudiation*)
 - Fornece proteção contra a negação por uma das entidades envolvidas na comunicação de ter participado em toda/parte da comunicação
- Auditoria
 - Fornece informações relevantes sobre o sistema
- Disponibilidade
 - Garante que o recurso estará disponível para utilização

Serviços x Mecanismos de Segurança

Serviço	Cifragem	Assinatura Digital	Controle de Acesso	Integridade dos Dados	Autenticação	Controle do Roteamento	Notarização
Autenticação de entidades pares	✓	✓	✗	✗	✓	✗	✗
Autenticação da origem dos dados	✓	✓	✗	✗	✗	✗	✗
Controle de Acesso	✗	✗	✓	✗	✗	✗	✗
Confidencialidade	✓	✗	✗	✗	✗	✓	✗
Confidencialidade no fluxo de tráfego	✓	✗	✗	✗	✗	✓	✗
Integridade dos dados	✓	✓	✗	✓	✗	✗	✗
Não repúdio	✗	✓	✗	✓	✗	✗	✓
Disponibilidade	✗	✗	✗	✓	✓	✗	✗

Por que ainda temos problemas com segurança?

- Fragilidade da Tecnologia
 - TCP/ IP
 - Sistema Operacional
 - Equipamentos de Rede
- Fragilidade de Configuração
- Fragilidade da Política de Segurança
 - Falta de uma política escrita

Questionamentos

- Questões a serem discutidas
 1. Por que a segurança é tão importante em todas as organizações?
 2. Por que a segurança é um dos habilitadores de negócios em um ambiente cooperativo?
 3. Quais são os maiores riscos que rondam as organizações?
 4. Qual é a importância e a necessidade da educação dos usuários?
 5. Qual é a importância e a necessidade de uma política de segurança?
 6. Quais são as fronteiras entre as organizações no ambiente cooperativo?

Desmistificando o Hacker

Desmistificando o Hacker

- Genios ?

```
#include <stdio.h>
int main(void)
{
    int count;
    for(count=1;count<=500;count++)
        printf("I will not throw paper airplanes in class.");
    return 0;
}
```

MONDO 2013

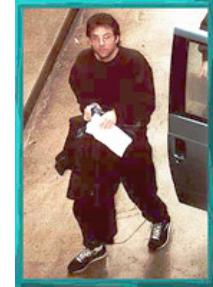


Nerds, bandidos, experientes, jovens... ?



Conhecendo o inimigo...

- O Gênio Problemático
 - Possui um profundo conhecimento sobre sistemas de computador
 - Capacidade para encontrar vulnerabilidades obscuras em SO's, apps e protocolos e explora-las
 - Extremamente habilidoso em evitar contramedidas
 - Adapta-se dinamicamente a novos ambientes
- O Idiota
 - Pequeno (ou nenhum) verdadeiro conhecimento sobre sistemas de computador
 - Faz downloads cegos e roda códigos escritos por algum Gênio Problemático
 - Conta a todo mundo o que fez
 - Pode ser detido apenas chamando a sua mãe
- **Quem você acha que causa mais danos?**



Mitnick



Simpson

Alguma Questão?

