Introdução
à
Segurança da Informação

Segurança da Informação

- Segurança... (Aurélio)
  - Estado, qualidade ou condição de seguro.
  - Condição daquele ou daquilo em que se pode confiar;

- Seguro... (Aurélio)
  - Livre de perigo;
  - Livre de risco; protegido, acautelado, garantido;
  - Que não hesita, ou não vacila; firme;
  - Em quem se pode confiar; constante, leal...

Segurança da Informação

- Porque Segurança?
  - ...”enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e falta de novas oportunidades de negócios.”

Segurança da Informação

- A segurança é marcada pela evolução contínua, no qual novos ataques têm como resposta novas formas de proteção... (ciclo)

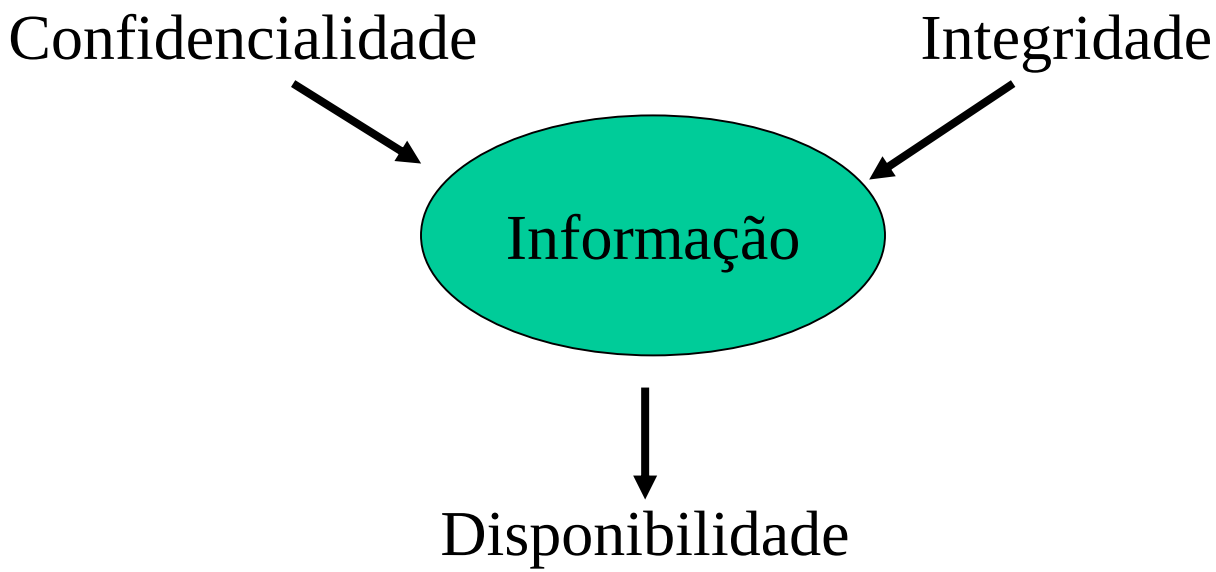
Um típico ambiente de TI

- Considere os recursos envolvidos no desenvolvimento de uma aplicação Web
  - Servidores físicos (hardware).
  - Sistemas operacionais dos servidores.
  - Servidor de aplicação.
  - Servidor HTTP.
  - Aplicação web.
  - Servidor de banco de dados.

Conceitos Básicos

Segurança da Informação

- Um computador é dito seguro se este atende a três requisitos básicos:



Fundamentos de Segurança

- CID:
  - Confidencialidade
  - Integridade
  - Disponibilidade
    - Alguns autores mais recentes incluem também a **Autenticidade** como um pilar! (CIDA)

Segurança da Informação

- **Confidencialidade**:
  - A informação está disponível somente para os devidamente autorizados.
  - Violação da Confidencialidade:
    - alguém obtém acesso não autorizado ao seu computador e lê todas as informacões contidas na sua declaração de Imposto de Renda.

Fundamentos de Segurança

A **Confidencialidade** é um termo diretamente ligado à privacidade de um recurso. Um recurso deve estar acessível apenas para a pessoa ou grupo que foi definido como usuário autorizado para dispor daquele acesso, e nenhum outro. Por exemplo, as notas de um aluno devem ser acessadas somente pelo aluno, pelos professores das disciplinas cursadas por ele e pela equipe de registro acadêmico.

Segurança da Informação

- **Integridade**:
  - A informação não é destruída ou corrompida e o sistema tem um desempenho correto.
  - Violação da integridade:
    - alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal.

Fundamentos de Segurança

O termo **Integridade** possui duas definições: a primeira relacionada com o fato da informação ter valor correto; por exemplo, no resultado da correção de uma prova, a nota obtida foi avaliada por um professor com conhecimento da disciplina, e portanto apto para julgar o conteúdo. A segunda definição está ligada à inviolabilidade da informação, ou seja, a nota não pode ser alterada sem justificativa e por meio controlado. A nota não pode "sumir" ou ser simplesmente alterada.

Segurança da Informação

- **Disponibilidade**:
  - Diz que os serviços/recursos do sistema estão disponíveis sempre que forem necessários.
  - Violação da disponibilidade:
    - O seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

Fundamentos de Segurança

O termo **Disponibilidade** está relacionado ao acesso à informação, que pode ser controlada ou não, e disponível quando necessária. Um ataque de negação de serviço pode, por exemplo, evitar o acesso à informação, afetando a disponibilidade.

Fundamentos de Segurança

É importante notar que a disponibilidade e a integridade podem ser medidas de forma simples, visto que elas são perceptíveis pelos usuários da informação. A confidencialidade, por outro lado, pode ser quebrada sem que se tenha conhecimento do fato, pois a simples visualização de uma informação por um usuário não autorizado não necessariamente altera essa informação. Daí a importância da auditoria, onde são analisados os registros de acesso de determinada informação, com o objetivo de verificar se houve acesso indevido.

Segurança da Informação

- **Alavanca para os negócios**:
  - Muito mais que a disponibilidade, integridade e sigilo das informações ...
  - ... A segurança significa permitir que as organizações busquem seus lucros, os quais são conseguidos por meio de novas oportunidades de negócios, que são resultados da flexibilidade, facilidade e disponibilidades dos recursos de informática.

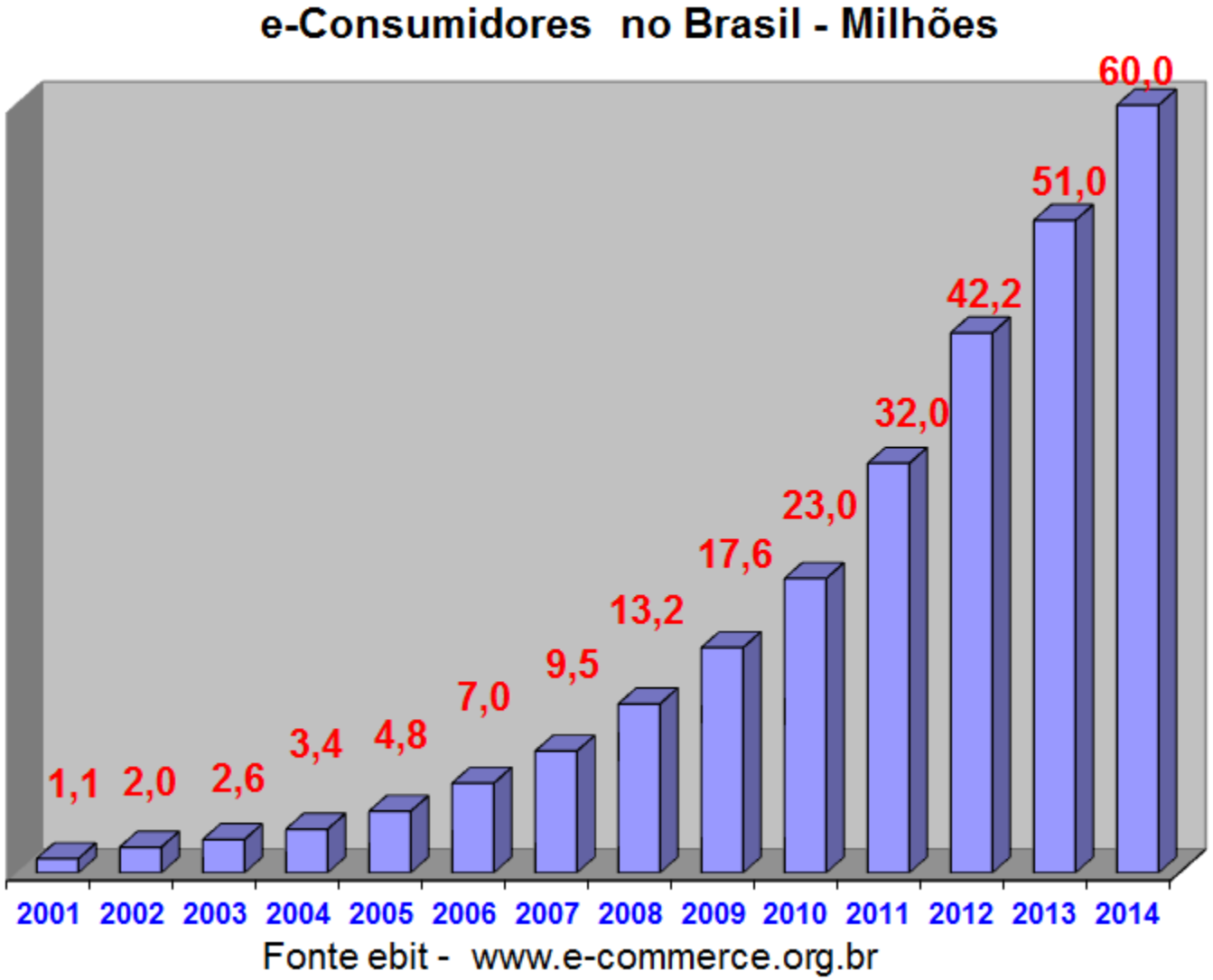
Segurança da Informação

- **Números no Brasil e no Mundo:**

  – **Brasil supera a marca de 80 milhões de internautas no 1º trimestre de 2012.**

*g1.com.br

Segurança da Informação



Segurança da Informação

- Maior evolução, maior preocupação com a segurança;
- Segurança faz parte dos negócios (estratégia da organização);
- Investimentos → principal obstáculo
  - Sempre em segundo plano;
  - Concientização de um elemento essencial para o sucesso do negócio.

Fundamentos de Segurança

Conceitos auxiliares:

- Autenticidade.
- Legalidade.
- Não repúdio.
- Privacidade.

Fundamentos de Segurança

- **Autenticidade**: garantia de que uma informação, produto ou documento foi elaborado ou distribuído pelo autor a quem se atribui.
- **Legalidade**: garantia de que ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica.
- **Não repúdio**: conceito muito utilizado quando tratamos de certificação digital, onde o emissor de uma mensagem não pode negar que a enviou. As tecnologias de certificação digital e assinatura digital são exemplos que propiciam essa condição.
- **Privacidade**: conceito amplo, que expressa a habilidade de um indivíduo em controlar a exposição e a disponibilidade de informações acerca de si. Com o crescimento dos mecanismos de busca, bancos de dados e informações publicadas na internet e redes sociais, esse conceito tem sido muito discutido em fóruns específicos. Um exercício interessante que o aluno pode realizar é buscar o seu próprio nome no site de buscas do Google.

Estratégias de Segurança

- Least Privilege (Menor Privilégio).
- Defense in Depth (Defesa em Profundidade).
- Choke Point (Ponto Único).
- Default Deny & default Permit Stance (Atitude de Bloqueio Padrão e Permissão Padrão).
- Universal Participation (Participação Universal).
- Diversity of Defense (Diversidade de Defesa).
- Inherent Weakness (Fraquezas Inerentes).
- Common configuration(Configuração Comum).
- Common Heritage (Herança Comum).
- Weakest Link (Elo mais Fraco).
- Fail Safe (Falha Segura).
- Simplicity (Simplicidade).

Estratégias de Segurança

- **Least Privilege (Menor Privilégio)**: cada objeto deve ter apenas os privilégios mínimos para executar suas tarefas, e nenhum outro. Apesar de muito importante, é difícil aplicar esse conceito, pois muitas vezes ele envolve uma série de ajustes e um mínimo erro pode fazer com que o recurso pare de funcionar. Como exemplo, podemos citar um servidor web. Executar o processo do servidor como o usuário administrador provavelmente fornecerá uma série de privilégios desnecessários a ele. Nesse caso, convém criar um usuário específico (ex: httpd) e definir as permissões mínimas para que o serviço funcione. Por exemplo: permissão de leitura na pasta onde ficam as páginas HTML e permissão de leitura e gravação na pasta onde ficam os registros de acesso.

Estratégias de Segurança

- **Defense In Depth (Defesa em Profundidade)**: não depender de um único mecanismo de segurança, independente do quão forte ele possa parecer. Não existe nenhum mecanismo 100% seguro, então qualquer mecanismo pode ser subvertido. Colocar defesas redundantes pode ser uma boa estratégia, pois um atacante, ao passar por suas defesas mais externas, ainda terá outras camadas de defesa para ultrapassar antes de comprometer o sistema como um todo.

Estratégias de Segurança

- **Choke Point (Ponto Único)**: canal estreito por onde os atacantes são forçados a passar, que pode ser monitorado e controlado. Exemplos: praça de pedágio em uma estrada, caixa de supermercado. Esse é o princípio utilizado pelos firewalls.

Estratégias de Segurança

- **Default Deny e Default Permit Stance (Atitude de Bloqueio Padrão e Permissão Padrão)**: atitude geral em relação à segurança. Na primeira (mais segura), tudo é proibido e o que é permitido deve ser expressamente definido. Na segunda, tudo é permitido e o que é proibido deve ser definido. Em sistemas seguros, deve-se buscar sempre a primeira atitude (Default Deny), apesar de nem sempre ser possível. Para o caso do acesso à internet por um nave - gador, seria viável bloquear toda a internet e liberar apenas o que é permitido?

Estratégias de Segurança

- **Universal Participation (Participação Universal)**: todos devem participar do processo de segurança. Uma única pessoa que não participa do processo pode comprometer todo o sistema. É importante lembrar que a segurança envolve pessoas, e que elas devem estar envolvidas, motivadas e participando do processo.

Estratégias de Segurança

- **Diversity of Defense (Diversidade de Defesa)**: utilizar diferentes sistemas e formas de defesa, de modo que uma vulnerabilidade em um sistema pode não estar presente em outros. Um certo cuidado deve ser tomado para não recair em um dos problemas listados a seguir.
  - **Inherent Weaknesses (Fraquezas Inerentes)**: sistemas de um mesmo tipo podem sofrer da mesma fraqueza inerente a esse tipo de sistema. Exemplos: falha de conceito ou falha de um protocolo com implementação comum.
  - **Common Configuration (Configuração Comum)**: sistemas diferentes configurados por uma mesma pessoa ou grupo podem sofrer de problemas semelhantes de configuração.
  - **Common Heritage (Herança Comum)**: sistemas de fabricantes diferentes podem usar componentes comuns e consequentemente terem as mesmas falhas.

Estratégias de Segurança

- **Fail Safe (Falha Segura)**: os sistemas, em caso de falha, devem sempre fazê-lo de modo a inibir qualquer tipo de acesso. O prejuízo da falta de acesso é preferível ao acesso liberado de forma irrestrita em caso de falha.

Estratégias de Segurança

- **Simplicity (Simplicidade)**: manter o ambiente simples. A complexidade esconde potenciais problemas de segurança. Interfaces gráficas, gerenciadores centralizados e sistemas com configurações simples são alguns exemplos desse princípio. Porém, deve-se tomar cuidado com o excesso de simplicidade. Um simples botão na ferramenta com os dizeres "torne meu sistema seguro" pode não ser adequado. Os sistemas devem ter um mínimo de parametrização, pois cada ambiente possui suas peculiaridades.

Incidentes de Segurança

De acordo com o Cert.br, um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. Em geral, toda situação na qual uma entidade de informação corre riscos pode ser considerada um incidente de segurança. No entanto, cada organização deve definir o que, em relação aos seus sistemas, para ela pode vir a ser um incidente de segurança. Em alguns casos, organizações podem classificar como incidentes de segurança qualquer ato que possa não estar em conformidade com a política de segurança adotada pela instituição.

Tratamento e Resposta de Incidentes

Todo incidente ocorrido na organização deve ser tratado de acordo com uma metodologia definida previamente. Assim, para atender ao processo de resposta a incidentes de segurança a organização deve elaborar uma metodologia visando gerenciar consequências de uma quebra de segurança. Seu principal objetivo é minimizar o impacto causado por um incidente e possibilitar o restabelecimento dos serviços no mais curto espaço de tempo possível.

Computer Security Incident Report Team (CSIRT)

Segundo o Cert.br, um CSIRT, ou Grupo de Resposta a Incidentes de Segurança, é uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores. Normalmente, um grupo de resposta a incidentes pode ser um grupo dentro da própria instituição trabalhando exclusivamente para a resposta a incidentes dos serviços prestados pela empresa ou pode trabalhar na forma de comunidade, auxiliando várias instituições e produzindo estatísticas e relatórios que beneficiam todo um grupo ou mesmo um país (Cert.br 2007).

Tratamento de Incidentes

Ciclo de vida de um incidente

- Estágio 1 – Preparação dos Processos.
- Estágio 2 – Gerenciamento de riscos.
- Estágio 3 – Triagem.
- Estágio 4 – Resposta a incidentes.

Ciclo de Vida de Incidentes

Estágio 1 – Preparação dos processos

O início do ciclo de vida de um incidente começa antes do próprio incidente. É necessária a elaboração de processos e procedimentos para a correta ação empregada contra ameaças e vulnerabilidades possíveis à organização. É importante que todos os processos empregados sejam testados e aperfeiçoados. Esses processos têm por finalidade o correto emprego dos recursos para a resposta a incidentes.

Ciclo de Vida de Incidentes

Estágio 2 – Gerenciamento de riscos

Por meio de ações corretivas e preventivas de ameaças existentes, pois estas são um fator intrínseco dentro de uma organização. O gerenciamento de riscos é muito importante e deve ser um processo contínuo dentro de uma organização, desenvolvendo medidas de segurança e calculando seu impacto para cada uma das etapas de um ciclo de incidentes.

Ciclo de Vida de Incidentes

Estágio 3 – Triagem

O método de recepção de todo e qualquer indício de incidente é de suma importância, pois é com uma correta triagem da informação que se inicia todo o processo de catalogação e resposta ao incidente. Os grupos de resposta a incidentes comumente informam apenas um meio de contato ou "hotline", seja para um grupo de resposta de âmbito nacional, privado ou mesmo dentro da organização. Essa triagem é importante para a aplicação correta do controle de segurança da informação impactado pelo incidente. Normalmente, esse controle também é atribuído a um gerente de incidente, profissional especializado no problema que estará à frente do incidente até a sua resolução.

Ciclo de Vida de Incidentes

Estágio 4 – Resposta a incidentes

Quando um incidente já passou pela triagem, ele é submetido ao plano de resposta a incidentes da organização. Nesse ponto, atividades anômalas são facilmente detectadas e a adoção de medidas apropriadas pode rapidamente identificar sistemas afetados, dimensionando o montante do prejuízo.

Trabalho dos CSIRTs

Prevenção:

- Auditoria de segurança.
- Treinamento e orientação a usuários.
- Disseminação de informação relacionada à segurança.
- Monitoração de novas tecnologias.

Trabalho dos CSIRTs

Resposta:

- Tratamento de incidentes.
- Tratamento de vulnerabilidades.
- Qualidade de serviços de segurança.
- Consultoria em segurança.
- Análise de riscos.
- Planejamento e recuperação de desastres.

Trabalho dos CSIRTs

Prevenção

Caracterizam-se como serviços proativos os serviços onde o grupo procura se antecipar aos problemas de maneira a preveni-los, gerando uma base de conhecimento para futura pesquisa. Dentre as principais atividades de prevenção destacam-se a auditoria de segurança e o treinamento e orientação a usuários.

Trabalho dos CSIRTs

Auditoria de segurança

A auditoria de segurança dentro de uma empresa visa submeter seus ativos a uma análise de segurança com base nos requisitos definidos pela organização ou por normas internacionais. Também pode implicar na revisão das práticas organizacionais da empresa bem como testes em toda a sua infraestrutura. Nos dois últimos módulos deste treinamento, será abordado o processo de *hardening* para servidores Linux e Windows. Uma vez aprovado um processo de *hardening*, este pode ser utilizado para auditar a segurança de um ambiente, já que nesse documento encontra-se a configuração mínima recomendada para um ativo.

Trabalho dos CSIRTs

Treinamento e orientação a usuários

Uma das funções de um CSIRT também é a promoção de palestras e workshops sobre segurança dentro de uma organização. Essas palestras têm o intuito de informar aos usuários as políticas de seguranças vigentes e como se proteger de vários ataques, principalmente de engenharia reversa.

Trabalho dos CSIRTs

Disseminação de informação relacionada à segurança

A disseminação de informação é primordial para o sucesso de um grupo de resposta a incidentes. Essa disseminação pode ocorrer tanto dentro da organização, através de documentos e boletins internos, como com a confecção de artigos para distribuição para outros órgãos externos à empresa.

Trabalho dos CSIRTs

Monitoração de novas tecnologias

Um Grupo de Resposta a Incidentes monitora novos desenvolvimentos técnicos de ataques para ajudar a identificar novas tendências de futuras ameaças. Esse serviço envolve a leitura de fóruns e listas de discussão, sites e revistas especializadas.

Trabalho dos CSIRTs

Resposta

Os serviços reativos englobam atividades que são realizadas após algum evento ou requisição dentro da organização. Baseiam-se em análises de logs e produção de relatórios em função de alguma detecção de atividade maliciosa. Dentre as principais atividades de resposta a incidentes, podemos destacar as seguintes.

Trabalho dos CSIRTs

Tratamento de incidentes

Segundo Chuvakin e Peikari, autores do livro *Security Warrior*, uma reposta a incidente é um processo de identificação, contenção, erradicação e recuperação de um incidente de computador, realizado pelo time de segurança responsável.

O tratamento de incidentes é a principal atividade de um time de resposta a incidentes. São os incidentes que vão gerar todo o processo de identificação, classificação e tomada de decisão sobre quais procedimentos tomar para sanar o problema, quantas vezes o problema foi constatado dentro de um período, qual o impacto causado pelo incidente e se este obteve ou não sucesso.

Trabalho dos CSIRTs

Tratamento de vulnerabilidades

O tratamento de vulnerabilidades visa submeter os sistemas a uma auditoria a fim de saber quais suas fraquezas e como preveni-las através de mitigação de alguns serviços.

Essa metodologia está diretamente ligada à criação do plano de continuidade de negócios dentro de uma organização, pois, através das avaliações feitas, é possível fazer uma análise de risco e impacto para as vulnerabilidades encontradas.

Trabalho dos CSIRTs

Qualidade de serviços de segurança

A qualidade dos serviços de segurança proporciona aumento na experiência adquirida na prestação de serviços proativos e reativos descritos acima. Esses serviços são concebidos para incorporar os feedbacks e as lições aprendidas com base no conhecimento adquirido por responder a incidentes, vulnerabilidades e ataques.

Parte de um processo de gestão da qualidade da segurança pode melhorar a segurança a longo prazo, gerando base dados de incidentes e suas propostas para solução.

Trabalho dos CSIRTs

Consultoria em segurança

Um CSIRT pode ser utilizado para fornecer aconselhamento sobre as melhores práticas de segurança, principalmente dentro de um ambiente militar. Esse serviço pode ser utilizado na preparação de recomendações ou identificando requisitos para a aquisição, instalação ou obtenção de novos sistemas, dispositivos de rede, aplicações de software ou criação de processos. Esse serviço inclui proporcionar orientação e ajuda no desenvolvimento organizacional ou no círculo de políticas de segurança. Ele pode também envolver o aconselhamento às normas legais legislativas ou de outros órgãos governamentais.

Trabalho dos CSIRTs

Análise de riscos

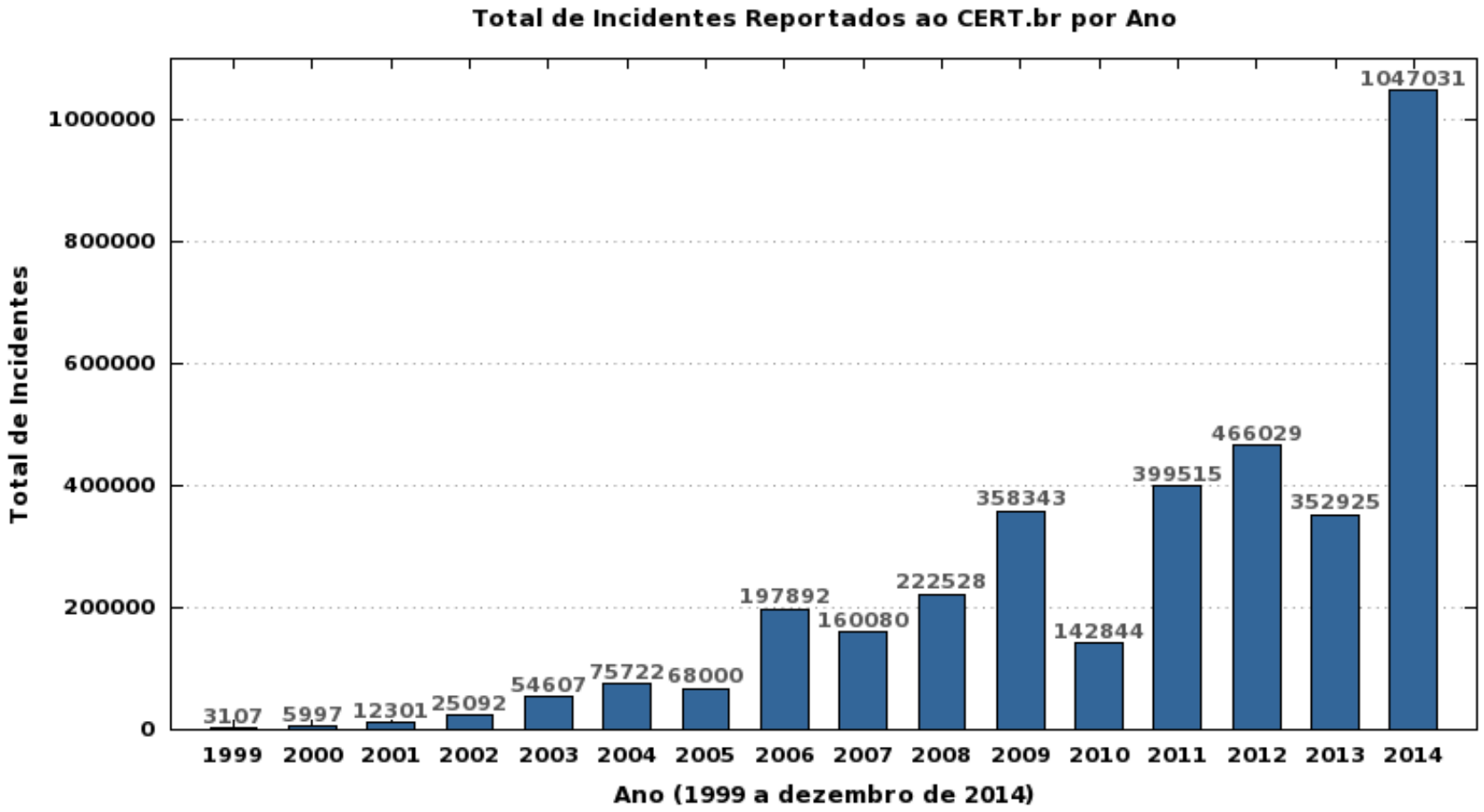
Um Grupo de Resposta a Incidentes pode ser capaz de acrescentar valor à análise de risco e avaliações. Isso pode melhorar a capacidade da organização para avaliar ameaças reais, fornecer avaliações qualitativas e quantitativas dos riscos para os ativos da organização e avaliar estratégias para melhor defesa.

Trabalho dos CSIRTs

Planejamento e recuperação de desastres

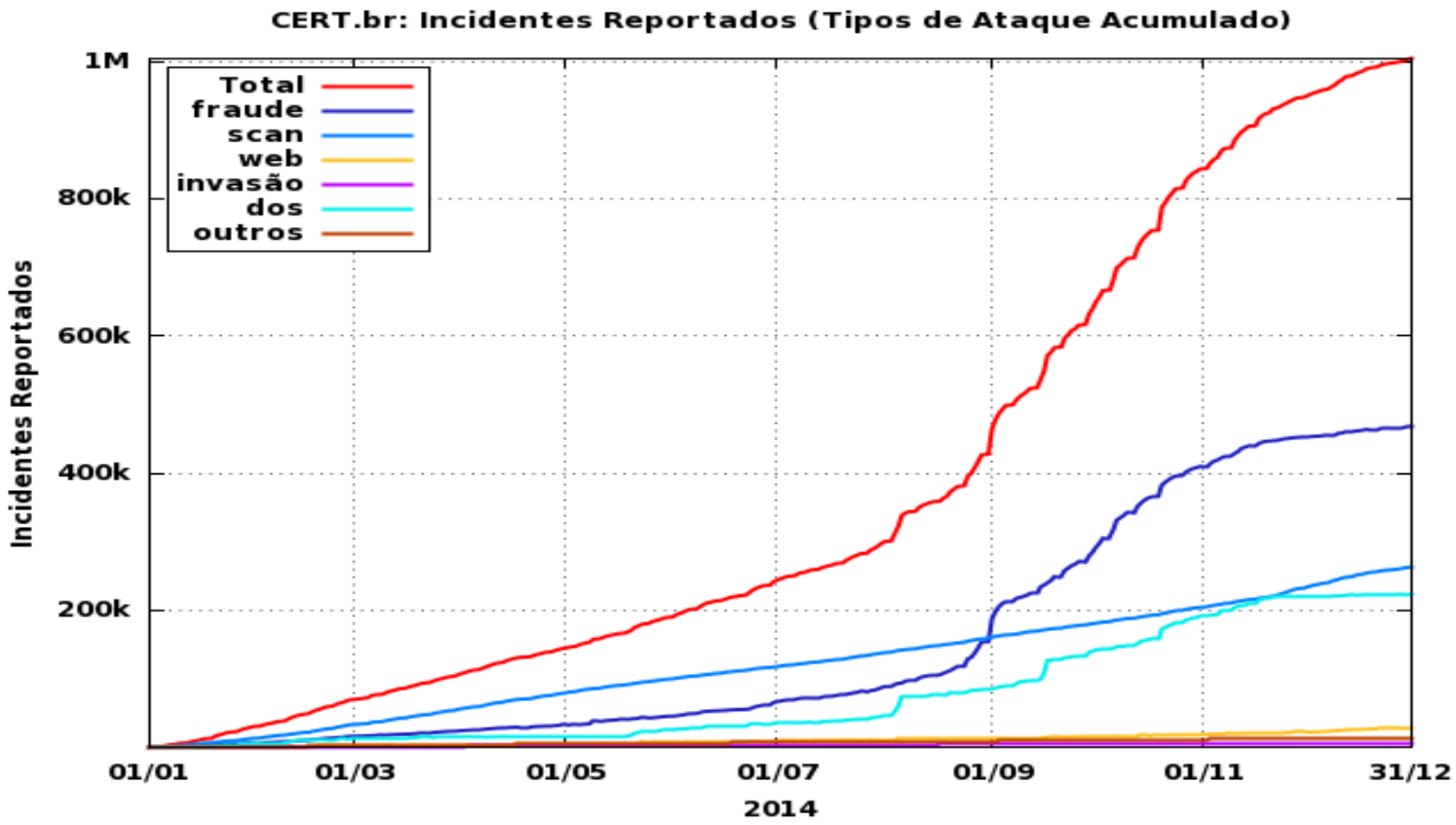
Com base em ocorrências anteriores e futuras previsões de tendências emergentes de incidentes de segurança, pode-se afirmar que quanto mais os sistemas de informação evoluem, mais aumenta a chance de acontecer um incidente. Por isso, o planejamento deve considerar os esforços e experiências passadas de um CSIRT.

Segurança da Informação



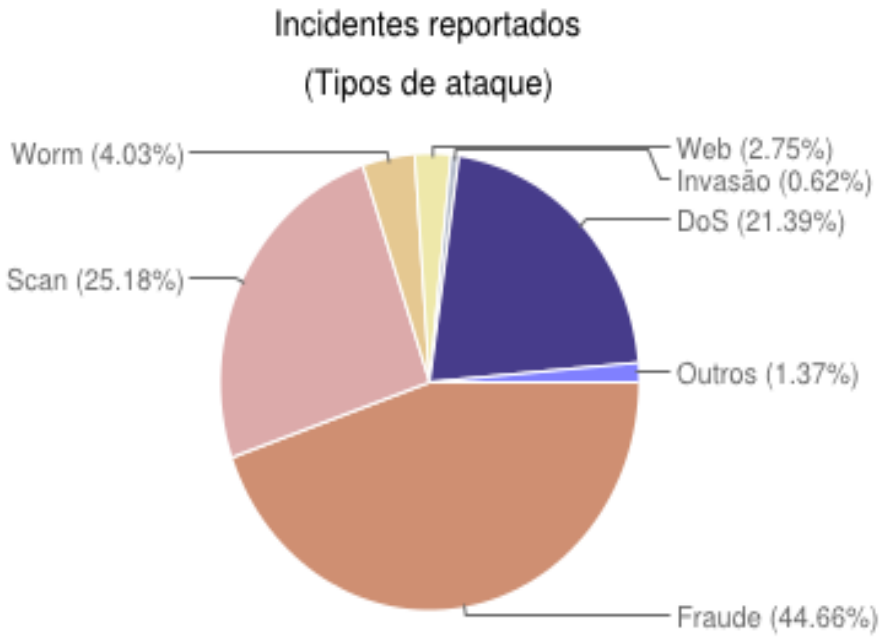
Segurança da Informação

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2014



Segurança da Informação

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2014



Segurança da Informação

Este gráfico não inclui os dados referentes a worms.

Legenda:

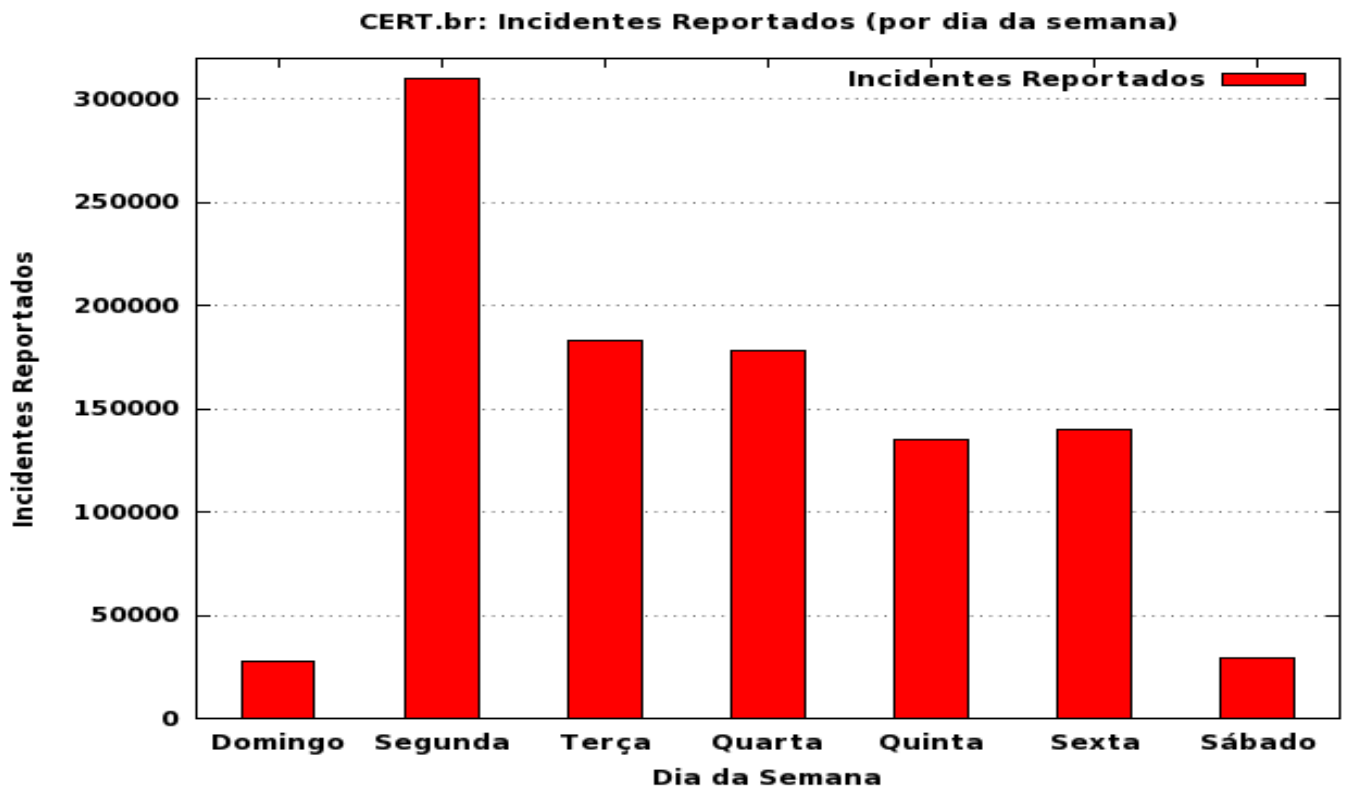
- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

Obs.: Vale lembrar que **não se deve confundir scan com scam**. Scams (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

$Date: 2015/03/30 14:08:53 $

Segurança da Informação

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2014



Segurança da Informação

- **Preocupação com segurança:**
  - Como preocupar com segurança se não conhece os riscos???
  - Se não conhece os riscos... Para que a proteção???
  - 32% das empresas (BR) → não sabem informar se já sofreram algum incidente de segurança.

Segurança da Informação

- **Mitos mais comuns:**
  - ‘isso nunca acontecerá conosco’;
  - ‘nunca fomos atacados, não precisamos de mais segurança’;
  - ‘já estamos seguros com o firewall’;
  - ‘não dá para gastar com segurança agora, deixa assim mesmo’;
  - ‘vamos deixar funcionando e depois resolveremos os problemas de segurança’;
  - ...

Segurança da Informação

- **Prejuízos causados pelos principais vírus:**

Ano	Vírus	Prejuízos (em milhões de U$)
1999	Melissa	1.200
2000	I Love You	8.750
2001	Nimda	635
2001	Code Red (variações)	2.620
2001	Sircam	1.150
2002	Klez	9

Segurança da Informação

- **Uso dos computadores domésticos:**
  - Transações financeiras (bancárias ou mesmo compra de produtos e serviços);
  - Comunicação (e-mails)
  - Armazenamento de dados (pessoais ou comerciais)

Segurança da Informação

Por que devo me preocupar com a segurança do meu computador?

- você, provavelmente, não gostaria que:
  - suas senhas e números de cartões de crédito fossem furtados e utilizados por terceiros;
  - sua conta de acesso a Internet fosse utilizada por alguém não autorizado;
  - seus dados pessoais, ou até mesmo comerciais, fossem alterados, destruídos ou visualizados por terceiros;
  - seu computador deixasse de funcionar, por ter sido comprometido e arquivos essenciais do sistema terem sido apagados, etc.

Segurança da Informação

- **Por que alguém iria querer invadir meu computador??????**
- Motivos:
  - alguma atividade ilícita, para esconder a real identidade e localização do invasor;
  - utilizar seu computador para lançar ataques contra outros computadores;
  - utilizar seu disco rígido como repositório de dados;
  - destruir informações (vandalismo);
  - disseminar mensagens alarmantes e falsas;
  - ler e enviar e-mails em seu nome;
  - propagar vírus de computador;
  - furtar números de cartões de crédito e senhas bancárias;
  - furtar a senha da conta de seu provedor;
  - **....?!?!?!?!?!?**

Engenharia Social

Segurança da Informação

- **Engenharia Social:**
  - O termo é utilizado para descrever um método de ataque, onde alguém faz 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 da Informação

- **Engenharia Social:**

- Exemplo 1: você recebe uma mensagem e-mail, onde o remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de Internet Banking está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso a conta bancária e enviá-la para o atacante.

Segurança da Informação

- **Engenharia Social:**

- Exemplo 2: você recebe uma mensagem de e-mail, dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um site da Internet, para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.

Segurança da Informação

- **Engenharia Social:**

- Exemplo 3: algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a Internet está apresentando algum problema e, então, pede sua senha para corrigi-lo. Caso você entregue sua senha, este suposto técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso a Internet e, portanto, relacionando tais atividades ao seu nome.

Segurança da Informação

- **Engenharia Social:**

- Estes casos mostram ataques típicos de engenharia social, pois os discursos apresentados nos exemplos procuram induzir o usuário a realizar alguma tarefa e o sucesso do ataque depende única e exclusivamente da decisão do usuário em fornecer informações sensíveis ou executar programas.

Vulnerabilidade

Segurança da Informação

- **Vulnerabilidade:**
  - Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Segurança da Informação

- **Vulnerabilidade:**
  - Existem casos onde um software ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota.

Segurança da Informação

- **Vulnerabilidade:**
  - Novas tecnologias trazem consigo novas vulnerabilidades;
  - Novas vulnerabilidades surgem diariamente → novos ataques serão sempre criados

SENHAS

Segurança da Informação

- **Senhas:**

  – Autenticar o usuário: o processo de verificação da identidade do usuário, assegurando que este é realmente quem diz ser.

  – Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você.
    - ler e enviar e-mails em seu nome;
    - obter informações sensíveis dos dados armazenados em seu computador, tais como números de cartões de crédito;
    - esconder sua real identidade e então desferir ataques contra computadores de terceiros;

* Nos tempos de mainframe (Segurança) → USUÁRIO/SENHA

Segurança da Informação

Portanto, a senha merece consideracão especial, afinal ela é de sua inteira responsabilidade.

Segurança da Informação

- **Senhas:**
  - **Não usar:**
    - Nomes;
    - Sobrenomes;
    - números de documentos;
    - placas de carros;
    - números de telefones e;
    - Datas.
  - Esses dados podem ser facilmente obtidos.

Segurança da Informação

- **Elaboração de senhas:**
  - Uma boa senha não deve ser curta (pelo menos oito caracteres entre letras, números e símbolos);
  - Deve ser simples de digitar e fácil de lembrar;
  - Utilizar letras maiúsculas, minúsculas, números, sinais de pontuação;
  - Evitar repetições de letras (paralelepípedo).

Segurança da Informação

- **Elaboração de senhas:**
  - Quanto mais “bagunçada” melhor (mais difícil de descobrir)
  - Uma regra realmente prática e que gera boas senhas difíceis de serem descobertas é utilizar uma frase qualquer e pegar a primeira, segunda ou a última letra de cada palavra.
  - Se tiver dificuldades para memorizar uma senha forte, é preferível anotá-la e guardá-la em local seguro, do que optar pelo uso de senhas fracas.

Segurança da Informação

- **Quantas senhas diferentes devo usar?**
  - Procure identificar o número de locais onde você necessita utilizar uma senha. Este número deve ser equivalente a quantidade de senhas distintas a serem mantidas por você.
  - Utilizar senhas diferentes, uma para cada local, é extremamente importante, pois pode atenuar os prejuízos causados, caso alguém descubra uma de suas senhas.

Segurança da Informação

- **Troca de senhas:**
  - Regularmente (2 ou 3 meses) → confidencialidade.
  - A primeira senha deve ser trocada com a maior urgência possível.

Segurança da Informação

- **Cuidados com as senhas:**
  - Certifique-se de não estar sendo observado ao digitar a sua senha;
  - Não forneça sua senha em hipótese alguma;
  - Não utilize computadores de terceiros (por exemplo, em LAN houses, cybercafes, stands de eventos, etc) em operações que necessitem utilizar suas senhas;
  - Certifique-se que seu provedor disponibiliza serviços criptografados, principalmente para aqueles que envolvam o fornecimento de uma senha.

Segurança da Informação

- **Como descobrir senha:**
  - Observar o processo de digitação da sua senha;
  - Utilizar algum método de persuasão, para tentar convencê-lo a entregar sua senha;
  - Capturar sua senha enquanto ela trafega pela rede.

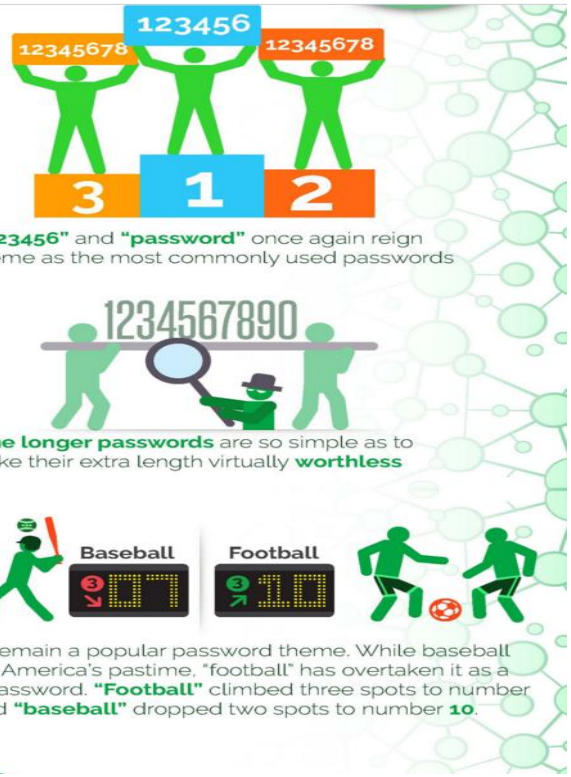
Segurança da Informação

- **Senha de Administrador:**
  - Elaborar uma boa senha para o usuário Administrator (ou root)
  - Utilizar o usuário Administrator (ou root) somente quando for estritamente necessário;
  - Criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador.

Segurança da Informação

As senhas mais utilizadas em 2014 - SplashData

RANK	PASSWORD	CHANGE FROM 2014
1	123456	Unchanged
2	password	Unchanged
3	12345678	1 ↗
4	qwerty	1 ↗
5	12345	2 ↘
6	123456789	Unchanged
7	football	3 ↗
8	1234	1 ↘
9	1234567	2 ↗
10	baseball	2 ↘
11	welcome	NEW
12	1234567890	NEW
13	abc123	1 ↗
14	111111	1 ↗
15	1qaz2wsx	NEW
16	dragon	7 ↘
17	master	2 ↗
18	monkey	6 ↘
19	letmein	6 ↘
20	login	NEW



Códigos Maliciosos (Malware)

Segurança da Informação

- **Código malicioso ou Malware (Malicious Software – Software malicioso):**

  - é um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador.
  - Alguns exemplos de malware são:
    - vírus;
    - worms e bots;
    - backdoors;
    - cavalos de tróia;
    - keyloggers e outros programas spyware;
    - rootkits.

Segurança da Informação

- **Negacão de Serviço (Denial of Service)**
  - Nos ataques de negação de serviço (DoS – Denial of Service) o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à Internet.
- Exemplos deste tipo de ataque são:
  - gerar uma grande 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 a suas caixas de correio no servidor de e-mail ou ao servidor Web.

Segurança da Informação

- **DDoS (Distributed Denial of Service)**
  - constitui um ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.
  - Normalmente estes ataques procuram ocupar toda a banda disponível para o acesso a um computador ou rede, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede.

Segurança da Informação

- **Prevenções:**
  - E-mail: conteúdo/engenharia social;
    - Desligar opções:
      - abrir ou executar anexos;
      - Execução de JavaScript e de programa Java;
      - Se possível, o modo de visualização de e-mails HTML.
  - Essas opções podem evitar propagação automática de vírus e cavalos de tróia, entre outros.

Segurança da Informação

- **Prevenções:**
  - E-mail:
    - Manter sempre atualizado o programa leitor;
    - Não clicar em links (se deseja digite-o no browser);
    - Desconfiar sempre de anexos;
    - Download diretamente de site de interesse;

Segurança da Informação

- **Prevenções:**
  - Navegador (Browsers):
    - Manter sempre atualizado;
    - Desativar a execução de programas Java e JavaScript;
    - ActiveX apenas de sites conhecidos e confiáveis;
    - Bloquear pop-up windows;
    - Transações somente em máquina conhecida e em site com conexões seguras (nunca através de link, sempre digitando o endereço direto no browser);

Segurança da Informação

- **Prevenções:**
  - Tenha um antivírus que:
    - Identifique e elimine a maior quantidade possível de vírus;
    - Analisar os arquivos que são obtivos pela internet;
    - Verificar continuamente as unidades de armazenamentos (HD, CDs, DVDs, pen drives etc.
    - Pesquisas em e-mails recebidos e enviados;
    - Mídia de inicialização;
    - Atualização diária de assinaturas de vírus e malwares;

Ameaças

Segurança da Informação

Ameaças

- Para que seja possível proteger os sistemas computacionais de ataques e invasões, precisa-se conhecer quem são as pessoas que possuem conhecimento para comprometer a segurança dos mesmos e quais as tecnologias disponíveis que podem ser utilizadas por elas para atingir seus objetivos.

Segurança da Informação

Os riscos que rondam as organizações

- Hacker:
  - Termo genérico para identificar quem realiza o ataque em um sistema computacional;
  - Por definição original, são aqueles que utilizam seus conhecimentos para invadir sistemas, não com o intuito de causar danos às vítimas;

Segurança da Informação - Ameaças

- Psicólogo canadense Marc Rogers, chegou ao seguinte perfil de um hacker:
  - Indivíduo obsessivo, de classe média, de cor branca, do sexo masculino, entre 12 e 28 anos, com pouca habilidade social e possível história de abuso físico e/ou social.

Segurança da Informação - Ameaças

- Classificação dos diversos tipos de hackers:
  - Script Kiddies → iniciantes;
  - Crackers → Conhecimento avançado em informática
  - Carders → compras pela internet com cartões roubados
  - Cyberpunks → mais velhos, mas ainda anti-sociais;
  - Insiders → empregados insatisfeitos;
  - Coders → os que escrevem sobre suas "proezas"
  - White hat → profissionais contratados;
  - Black hat → crackers;
  - Gray hat → hackers que vivem no limite entre o white hat e o black hat.
  - Phreackers → hackers da telefonia

Segurança da Informação - Ameaças

- Script Kiddies:
  - Conhecidos também com Newbies;
  - Geralmente são inexperientes e novatos;
  - Conseguem ferramentas prontas na internet e utilizam sem entender o que estão fazendo;
  - Ameaça mais comumente enfrentada pelas empresas (maioria);

*incentiva o investimento em segurança nas empresas.

Segurança da Informação - Ameaças

- Crackers:
  - Possuem conhecimento avançado em informática
  - São capazes de quebrar proteções de sistemas e softwares
  - Roubam informações importantes
  - destroem os sistemas invadidos
  - São os responsáveis pela maioria dos crimes virtuais de destaque em jornais e revistas (devido as grandes perdas financeiras para a empresa invadida)

Segurança da Informação - Ameaças

- Cyberpunks:
  - São os hackers dos tempos românticos;
  - Dedicam às invasões por puro divertimento e desafio;
  - Extremo conhecimento e são obcecados pela privacidade de seus dados (criptografia);
  - Geralmente são os que encontram vulnerabilidades;
  - Prestam um favor às organizações, publicando-as.

Segurança da Informação - Ameaças

- Insiders:
  - São os maiores responsáveis pelos incidentes mais graves;
  - Funcionários e ex-funcionários da própria empresa (as maiores ameças);
  - Conhecimento dos processos da empresa;
  - Acesso a documentos importantes;
  - Acesso válido (login);
  - Práticas como engenharia social e suborno são características.

Segurança da Informação - Ameaças

- Insiders (Cont...):
  - O conhecimento é a base da economia e constitui um dos grandes fatores de vantagem competitiva (capital intelectual);
  - Casos de roubos de projetos → GE, Kodak, Gilette e ...
  - Geralmente são funcionários descontentes com o seu trabalho;
  - Podem ser facilmente manipulados pelo concorrente.

Segurança da Informação - Ameaças

- Insiders (Cont...):
  - É considerado uma nova modalidade de crime organizado → máfias e cartéis de drogas.
  - Organizações especializadas em espionagem industrial;
  - Incentivo do governo em alguns países (França, Japão e Israel);
  - Trabalho facilitado de espionagem → hotéis, grampos telefônicos e câmeras escondidas.

Segurança da Informação - Ameaças

- Insiders (Cont...):
  - Timothy Allen Lloyd → condenado a 41 meses de prisão pelo crime de instalar bomba lógica (1996-2002)
  - Outros grandes riscos:
    - Funcionários terceirizados
    - Pessoal de segurança e limpeza

Segurança da Informação - Ameaças

- Funcionários confiáveis:
  - Cientista nuclear americano foi acusado de ter vendido segredos da tecnologia de armas nucleares para a China.
  - Funcionário (Colorado USA) utilizou a internet para transferir um software avaliado em US$1.000.000 para um concorrente na China.

Segurança da Informação - Ameaças

- Funcionários subornados ou enganados:
  - Espião alemão seduz funcionária para conseguir informações confidenciais dessa empresa, o que incluía métodos de pesquisa DNA e informações dos projetos da companhia.

Segurança da Informação - Ameaças

- Funcionários antigos:
  - José Ignácio Lopez e mais sete outros funcionários deixaram a GM para se transferir para VW. Levaram 10 mil documentos privativos da GM.

Segurança da Informação - Ameaças

- Funcionários insatisfeitos:
  - Administrador de sistemas insatisfeito com o salário implantou uma bomba lógica em mil dos 1.500 equipamentos da organização;
  - Instalação: 22/02/2002;
  - Ativação: 04/03/2002;
  - Esperava lucro com a compra de ações.

Segurança da Informação - Ameaças

- Coders:
  - São hackers que resolveram compartilhar seus conhecimentos;
  - Publicação de livros;
  - Proferindo palestras e seminários sobre suas proezas (Kevin Mitnick);

Segurança da Informação - Ameaças

- White Hat:
  - São conhecidos como “hackers do bem”, “hackers éticos”, samurais;
  - Utilizam seus conhecimentos para descobrir vulnerabilidades nos sistemas e aplicar as correções necessárias;
  - Trabalho profissional e legal dentro das organizações.

Segurança da Informação - Ameaças

- Black hat:
  - Utilizam seus conhecimentos para invadir sistemas e roubar informações secretas das organizações;
  - Geralmente tentam vender as informações roubadas para as próprias vítimas (chantagem).

Segurança da Informação - Ameaças

- Gray hat:
  - São black hats que fazem o papel de white hats, a fim de trabalhar na área de segurança.
  - Falta conhecimentos profundos sobre segurança.

Segurança da Informação - Ameaças

- Phreackers:
  - São os hackers da telefonia, responsáveis pro fraudes telefônicas:
    - Alteração de contas
    - Ataques às centrais telefônicas
    - Realização de ligações gratuitas
    - Atualmente o maior alvo desses hackers é a telefonia celular.

Segurança da Informação - Ameaças

- Filme:

Hackers Criminosos e Anjos