Segurança em Tecnologia da Informação e Comunicação

2023

Mario Lemes Proença Jr.
DC/UEL

1

Referência do Autor

- **Mario Lemes Proença Jr.**

➢ Universidade Estadual de Londrina
➢ Departamento de Computação
➢ E-mail : proenca@uel.br
➢ Home Page : http://proenca.uel.br
➢ Telefone : 043-3371-4678 (DC/UEL)

2

Objetivos do Curso

Aprender sobre Segurança em Tecnologia de Informação e Comunicação

I) Introdução a Segurança
II) Tipos de Ataques
III) Defesas
IV) Criptografia
V) Protocolos para Segurança

3

I - INTRODUÇÃO

4

Introdução – Redes

- A área de Tecnologia de Informação e Comunicação (TIC) se tornou essencial para o negócio da empresa, deixou de ser coadjuvante e se tornou estratégica.



5

Introdução - Segurança

6

Introdução - Segurança

✓**Por que segurança ?**

www.internetworldstats.com em 04/2023	Mundo	%	Ataques bem sucedidos ?		
população	7.932.791.734		1%	0,10%	0,01%
usuários Internet	5.385.798.406	68%	53.857.984	5.385.798	538.580

www.internetworldstats.com em 03/2021	Mundo	%	Ataques bem sucedidos ?		
população	7.796.615.710		1%	0,10%	0,01%
usuários Internet	4.574.150.134	59%	45.741.501	4.574.150	457.415

7

Introdução a Segurança - Princípios

- **Confidencialidade (*Confidentiality*)**: visa limitar o acesso a informação somente às entidades ou pessoas autorizadas pelo proprietário da informação.
- **Integridade *(Integrity)***: visa garantir que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação.
- **Disponibilidade *(Availability)***: visa garantir que a informação esteja sempre disponível para os usuários autorizados pelo proprietário da informação.

8

Introdução a Segurança - Princípios

- **Autenticação (*Authentication*)**: visa identificar o usuário que está utilizando o recurso.
- **Controle de acesso *(Access Control)***: visa garantir que a pessoa tenha acesso somente a informações que o seu perfil tem acesso.
- **Não repúdio *(non-repudiation)***: visa garantir que a pessoa não possa negar que tenha realizado a ação ou transação.

9

Introdução a Segurança

- **O que proteger ?**
  - Ativos
    - **Dados**
      - **Informação é o dado com valor agregado;**
    - **Pessoas**
    - **Processos**
    - **Tecnologia**
      - **Hardware**
      - **Software**

10

Introdução a Segurança

11

Introdução a Segurança

- ✓ Ameaça: Virus, Worm, cavalo de Tróia, scanning. Elas exploram vulnerabilidades.
- ✓ Vulnerabilidade: Erros em Projetos, Erros em Instalações, falha de hardware ou software.
- ✓ As duas podem ser identificadas, prevenidas e mitigadas.
- ✓ Gerenciamento de Risco deve ser empregado.

12

Introdução a Segurança

- **A Segurança passou a ter importância vital nos negócios atualmente. Cite pelo menos um ou mais exemplos para cada questão relacionado ao que ocorre em sua empresa ou se não existe como você acha que deveria ser?** **(30 m individual)** **(segurança-ex-01)**
  - I. A Informação deve estar disponível para quem ?
  - II. Quais os riscos e ameaças ?
  - III. Qual a política de segurança ?
  - IV. Quais as normas de segurança ?
  - V. Qual o plano de contingência ?
  - VI. Treinamento relacionado a segurança ?

13

Introdução a Segurança

I. A Informação deve estar disponível para quem ?

➢ . . .






14

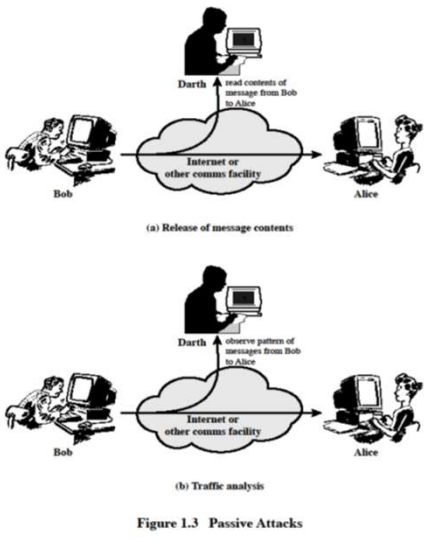
Introdução a Segurança

II. Quais os Riscos e Ameaças

- **Fenômenos físicos**
  - Incêndio, inundação, terremotos, catástrofes, guerras ...
- **Ataques deliberados**
  - Passivos
  - Ativos

15

Introdução a Segurança



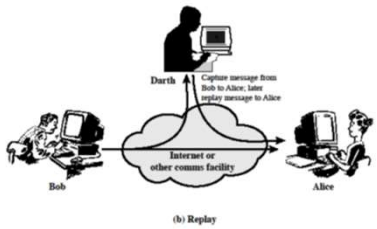
Figuras 1.3 e 1.4 Stallings
Criptogrpahy and network security

Figure 1.3 Passive Attacks

16

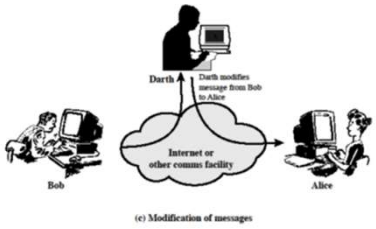
Introdução a Segurança

(a) Masquerade



(b) Replay

Figure 1.4 Active Attacks (page 1 of 2)



(c) Modification of messages

(d) Denial of service

Figure 1.4 Active Attacks (page 2 of 2)

17

Introdução a Segurança

- Atacantes
  - Hackers
  - **Antes queriam notoriedade.**

  - **Hoje querem retorno financeiro.**
    - Ele próprio ou para a organização criminosa que ele pertence.

18

Introdução a Segurança

- **Tendências últimos 2 anos**
  - Ataques direcionados a Aplicativos Web
    - Computação ubíqua e onipresente;
    - Phishing
      - Links para download de malwares
  - Ataques direcionados a e-mails;
  - Ataques a redes sociais; Fake News;
  - Ataques a *smartphones* e *gadgets* com wireless, wifi e IP;
  - Aplicações web sofrem
    - Paginas abertas (links abertos), aplicações com furos
    - Servidores configurados de forma errada

19

Introdução a Segurança

- **Tendências últimos 2 anos**
  - Ataques direcionados a APPs de celulares
    - Milhões de APPs
    - Lojas google e Apple não conseguem filtrar todas as novas linhas de códigos que diariamente entram nas atualizações dos APPs
    - Explosão de *malware* em apps de jogos e musicas
    - Evitar links em apps gratuitos
    - ***Ter backup é sempre a melhor e talvez única saída!***

20

Introdução a Segurança

- **Tendências últimos 2 anos**
  - Ransomware
    - Ataque por meio da Web ou e-mail
    - Vulnerabilidades antigas mas não corrigidas
      - Flash, jboss, java, linguagens não atualizadas
    - Navegadores antigos e não atualizados
    - Servidor web desatualizado
    - Pacotes de escritório editor, planilha desatualizados para packs de segurança
    - Sistema operacional não atualizado
    - Software pirata
    - Dados não criptografados
    - Solução fazer backup e testar!!!
    - Nova geração a caminho, controle CPU e outros recursos

21

Introdução a Segurança

- **Tendências últimos 2 anos**
  - Malware para dispositivos IoT
    - Segurança precisa ser reforçada
  - *Ransomware* e *Phishing* direcionados e a temas sazonais
  - Estão utilizando IA, Machine Learning e Deep Learning para ataques de DDoS, phishing de e-mail
  - E-mail e sites redirecionando a paginas comprometidas para coletar informações e/ou realizar ataques
  - As pessoas continuam a ser o elo fraco da corrente

22

Introdução a Segurança

- **Tendências últimos 2 anos**
  - A questão é todas as empresas e computadores podem ser atacados e invadidos.
    - Teste de invasão ou *pen test*; teste de vulnerabilidade !!!
    - A questão principal é se você foi violado ou invadido ...
      - ✓**Qual o dano ?**
      - ✓**Qual o risco ?**
      - ✓**Qual a contramedida ?**

23

Introdução a Segurança

- **Sistemas e Softwares**
  - **A área de desenvolvimento de sistema deve:**
    - Prever testes de vulnerabilidade durante o desenvolvimento do sistema.
    - Fazer correções de vulnerabilidades após o sistema estar em produção.
    - Incluir criptografia nos dados que trafegam pela rede e ficam armazenados.
    - Pensar em segurança nos projetos de software!!!

24

Introdução a Segurança

- **Falta de cuidados em relação a segurança**
  - Pessoas são incautas !
  - Senhas são fracas ! Não são trocadas ! São iguais !
    - **Qual a ultima vez que você trocou sua senha ?**
  - Pessoas ainda acreditam no conto do bilhete !!!
  - Engenharia social com apelos muito fortes !!!
    - **Exemplos e-mails...**
  - Pessoas acreditam no clique e veja minha msg sedutora !!!
  - Muito software pirata !
    - **Quem utiliza software legal ?**

25

Introdução a Segurança

- **Senhas mais utilizadas!!!**

	2022	2021	2020	2019	2018	2017	2016	2015	2014
1	password	123456	123456	123456	123456	123456	123456	123456	123456
2	123456	123456789	123456789	123456789	password	Password	123456789	password	password
3	123456789	12345	picture1	qwerty	123456789	12345678	qwerty	12345678	12345678
4	guest	qwerty	password	password	12345678	qwerty	12345678	qwerty	qwerty
5	qwerty	password	12345678	1234567	12345	12345	111111	12345	abc123
6	12345678	12345678	111111	12345678	111111	123456789	1234567890	123456789	123456789
7	111111	111111	123123	12345	1234567	letmein	1234567	football	111111
8	12345	123123	12345	iloveyou	sunshine	1234567	password	1234	1234567
9	col123456	1234567890	1234567890	111111	qwerty	football	123123	1234567	iloveyou
10	123123	1234567	senha	123123	iloveyou	iloveyou	987654321	baseball	adobe123
11	1234567	qwerty123	1234567	abc123	princess	admin	qwertyuiop	welcome	123123
12	1234	0	qwerty	qwerty123	admin	welcome	mynoob	1234567890	Admin
13	1234567890	1q2w3e	abc123	1q2w3e4r	welcome	monkey	123321	abc123	1234567890
14	0	aa12345678	Million2	admin	666666	login	666666	111111	letmein
15	555555	abc123	000000	qwertyuiop	abc123	abc123	18atcskd2w	1qaz2wsx	photoshop
16	666666	password1	1234	654321	football	starwars	7777777	dragon	1234
17	123321	1234	iloveyou	555555	123123	123123	1q2w3e4r	master	monkey
18	654321	qwertyuiop	aaron431	lovely	monkey	dragon	654321	monkey	shadow
19	7777777	123321	password1	7777777	654321	passw0rd	555555	letmein	sunshine
20	123	password123	qqww1122	welcome	!@#$%^&*	master	3rjs1la7qe	login	12345
21	D1lakiss	1q2w3e4r5t	123	888888	charlie	hello	google	princess	password1
22	777777	iloveyou	omgpop	princess	aa123456	freedom	1q2w3e4r5t	qwertyuiop	princess
23	110110jp	654321	123321	dragon	donald	whatever	123qwe	solo	azerty
24	1111	666666	654321	password1	password1	qazwsx	zxcvbnm	passw0rd	trustno1
25	987654321	987654321	qwer123456	123qwe	qwerty123	trustno1	1q2w3e	starwars	.000000

26

Introdução a Segurança

III. Qual a política de segurança ?

- São princípios básicos para uma organização para segurança.
- Instalações, hardware, software e pessoas !!!

IV. Quais as normas de segurança ?

- Quais os controles aplicáveis a segurança.
- Regras e Procedimentos relacionados aos ativos de TIC.

27

Introdução a Segurança

V. Qual o plano de contingência ?

- O que fazer em caso de ataque ou incidente ?
  - ?
- Qual o Plano de ação em caso de perda dos ativos de TIC?
  - Hardware
    - **Tem contrato de manutenção 24x7 ou 8x7 ou x ?**
    - **Tem clone ou *spare* ?**
  - Dados e Software
    - **Tem backup 7x7 ou 5x7 ?**
    - **Quantas semanas e meses será a retenção ?**

28

Estatísticas de Segurança

29

Introdução a Segurança

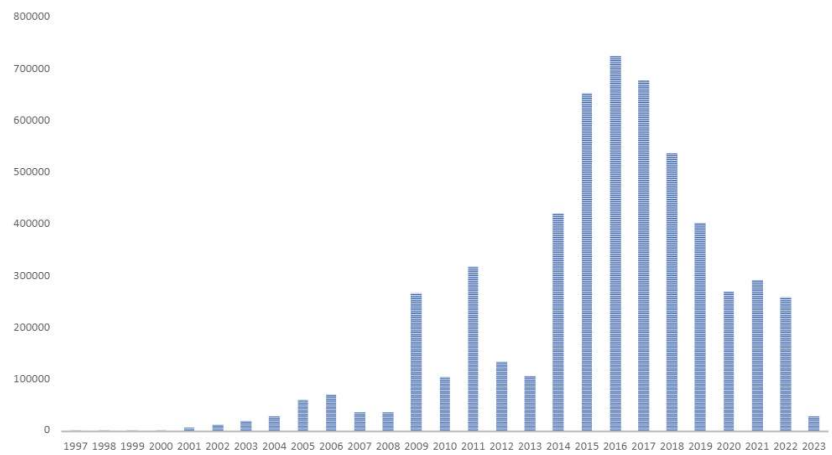
- Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Pesquisa (RNP)
  - ✓ https://www.rnp.br/sistema-rnp/cais

✓Tratamento de Incidentes
✓CSIRTs
✓Catálogo de Fraudes
✓Alertas

30

Introdução a Segurança

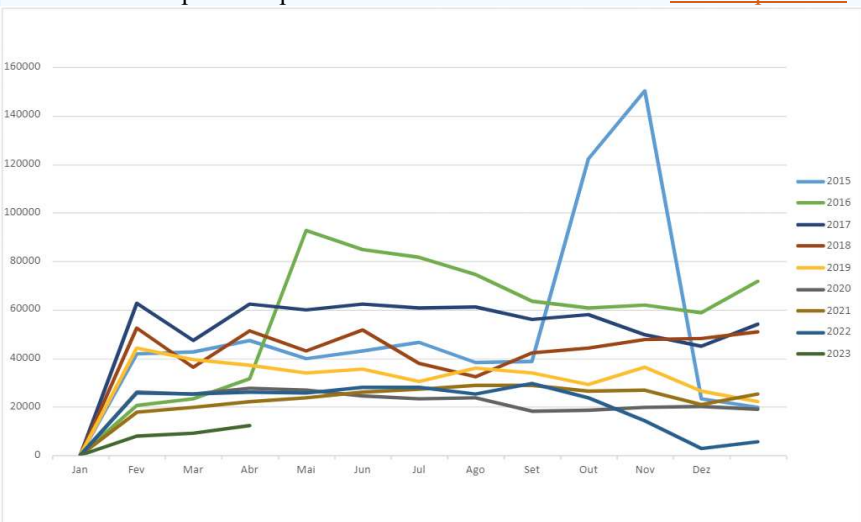
- Incidentes reportados por ano ao CAIS – 1997 a 03/2023 www.rnp.br/cais



31

Introdução a Segurança

- Incidentes reportados por mês ao CAIS – 2015 a 03/2023 www.rnp.br/cais



32

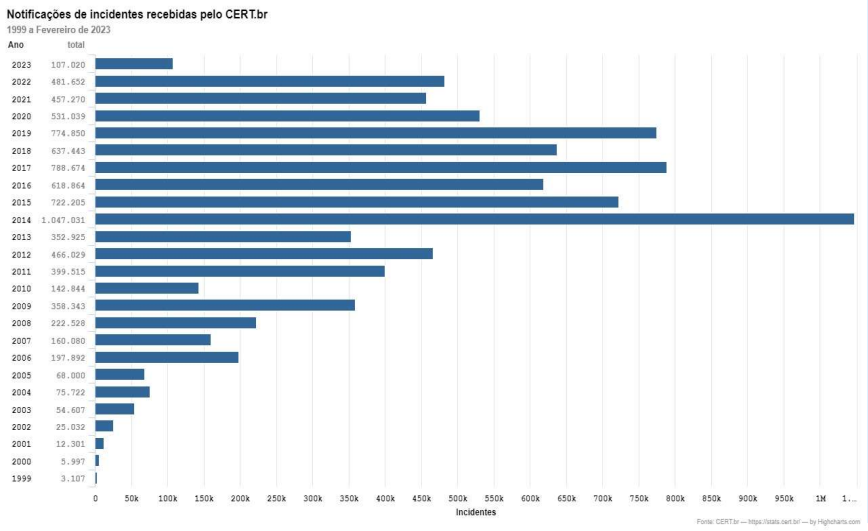
Introdução a Segurança

- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil mantido pelo NIC.br do Comitê Gestor da Internet no Brasil.
  - ✓ www.cert.br

33

Introdução a Segurança

- Incidentes reportados ao CERT.br www.cert.br



34

Introdução a Segurança

- **Totais Mensais e Anual Classificados por Tipo de Ataque reportados ao CERT.br**

	Total	worm	dos	invasão	web	sacn	fraude	Outros
Jan a jun 2020	318.697	55.645	46.164	615	8.811	187.440	18.024	1.998
Jan a dez 2019	875.327	100.477	301.308	527	22.334	409.748	39.419	1.514

35

Introdução a Segurança

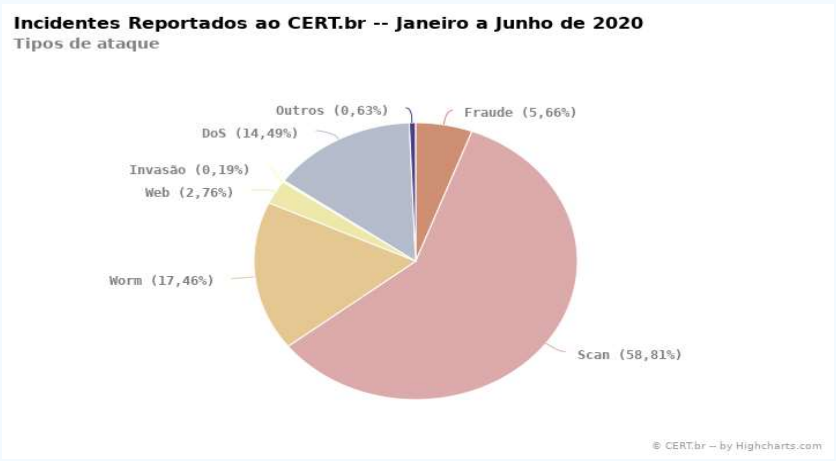
Legenda CERT.br, Tipo de Ataque reportados

- ✓ **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- ✓ **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.
- ✓ **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.

36

Introdução a Segurança

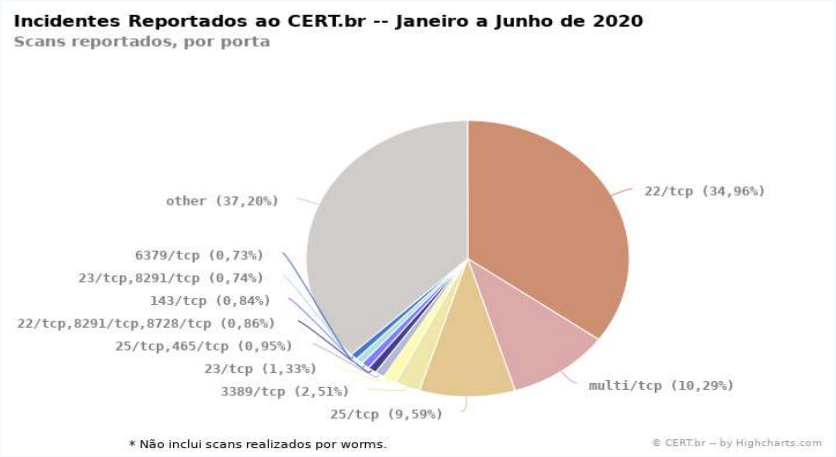
- Totais Mensais e Anual Classificados por Tipo de Ataque reportados ao CERT.br jan a jun / 2020



37

Introdução a Segurança

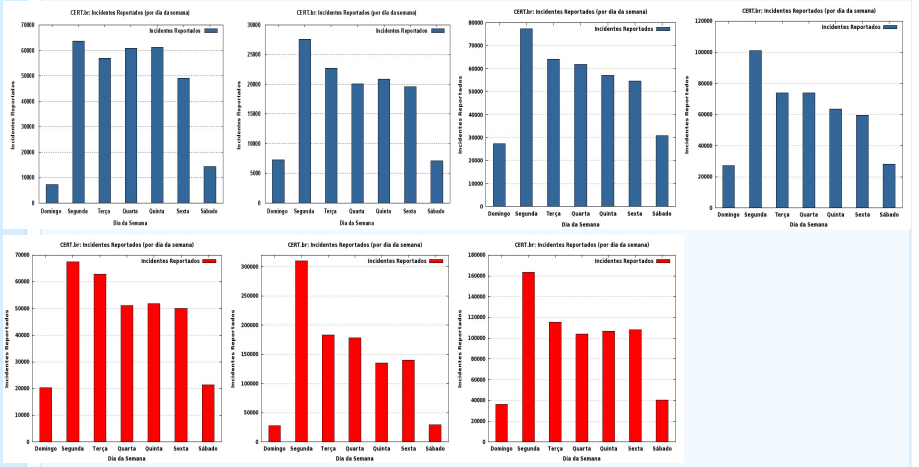
- Totais Mensais e Anual Scans por porta reportados ao CERT.br jan a jun 2020



38

Introdução a Segurança

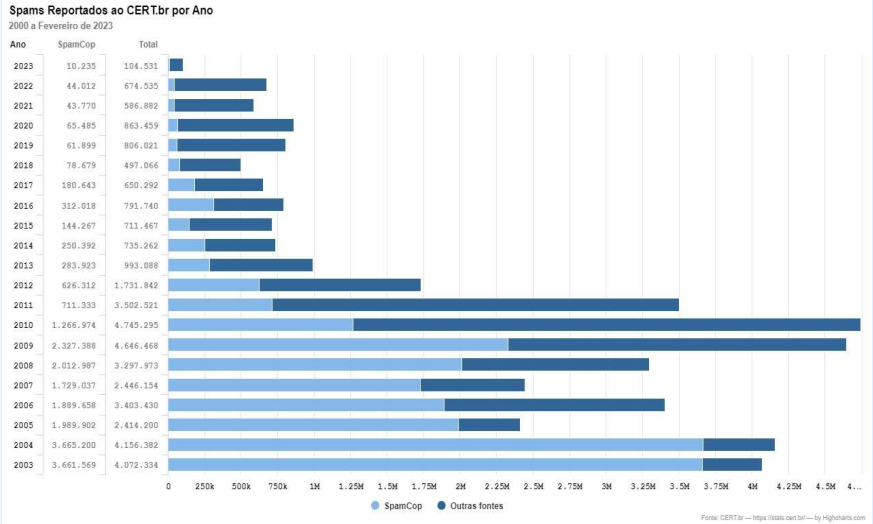
•Totais Mensais e Anual Classificados por Tipo de Ataque reportados ao CERT.br jan/dez/2009/2010/2011/2012/2013/2014/2015



39

Introdução a Segurança

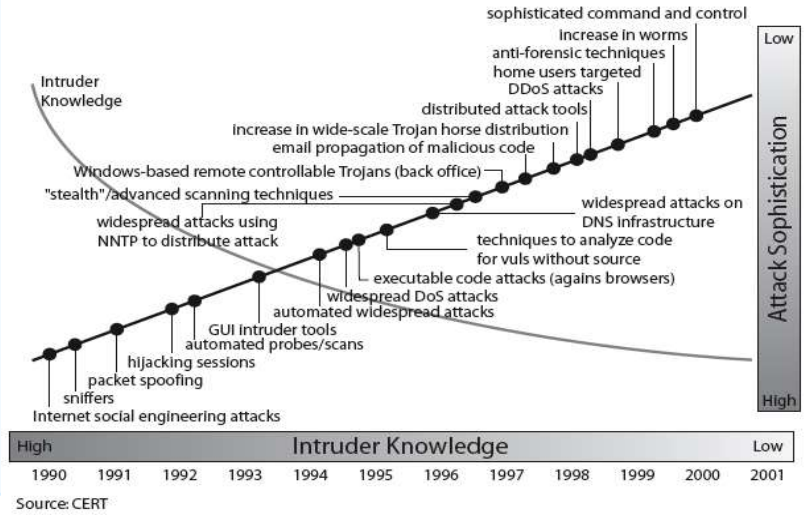
• Total Anual de SPAM reportados ao CERT.br 2003 a 2023



40

Introdução a Segurança

- Os ataques se tornaram mais sofisticados e o conhecimento necessário para tanto diminuiu. (stallings cripto 4d.)



41

Introdução a Segurança

- *United States Computer Emergency Readiness Team*

http://www.kb.cert.org/vuls

- **US-CERT publishes information about a wide variety of vulnerabilities. Vulnerabilities that meet a certain severity threshold are described in US-CERT Technical Alerts. It is difficult, however, to measure the severity of a vulnerability in a way that is appropriate for all users. For example, a severe vulnerability in a rarely used application might not qualify for publication as a technical alert but might be very important to a system administrator who runs the vulnerable application. US-CERT Vulnerability Notes provide a way to publish information about these less-severe vulnerabilities.**
- **You can customize database queries to obtain specific information, such as keyword, vendor, year**
  - ✓https://www.kb.cert.org/vuls/search/

42

Introdução a Segurança

- **Relatório de ameaças da McAfee**
  - ✓ **MCAFEE LABS THREATS REPORT 11/2020**
  - ✓ **https://www.mcafee.com/enterprise/en-us/lp/threats-reports/nov-2020.html**

43

Introdução a Segurança

- **Relatório de ameaças da Panda *Security* em 2009/2021**
  - *Relatório Anual de 2009*
  - *Relatório Anual de 2010*
  - Relatório de Abril a Junho de 2011
  - *Relatório Anual de 2011*
  - *Relatório Anual de 2014 2015 2016*
  - *Relatório Anual de 2017 2018*
- *Panda Security launches its Threat Insights Report 2020*
  - *https://www.pandasecurity.com/en/mediacenter/panda-security/threat-insights-report-2020/*

44

Introdução a Segurança

- **News**
  - *Google contrata Hacker que invadiu Google+*
  - **Hacker afirma: Facebook sabe tudo o que você faz na web, mesmo após log out**

45

Introdução a Segurança

- **News**
  - **Google Security Blog**
  - **Safe Browsing - Protecting Web Users for 5 Years and Counting, 19/06/2012/google**
    - **Google identifica aproximadamente 10 k sites maliciosos por dia !!!**
    - **Hoje Safe Browsing Google Transparency Report**

46

Introdução a Segurança

- **News**
  - **Malware bate recorde em 2011, 26 milhões de exemplares**
  - **O número de ameaças lançadas diariamente aumentou de 63.000 para 73.000 !!!**
  - **Em 2014 os números aumentaram.**
  - **Em 2016 Kaspersky Lab: 323,000 New Malware Samples Found Each Day**

47

Introdução a Segurança

- **Informações sobre uso de HTTPS by Google**
  - **Nos produtos Google**
  - **Uso de HTTPS reportado pelo Google**

48

II - Ataques

49

Ataques

- Ataques
  - **Passivos**
    - Escutas
    - Monitoramentos
  - **Ativos**
    - Disfarçar, passar pelo outro
    - Capturar e depois liberar
    - Capturar mensagem legitima e alterar
    - *Denial of service* ou negação de serviço

50

Ataques

- **Ataque de Força Bruta**
  - Consiste em tentar todas as combinações possíveis para quebrar uma criptografia;
  - Busca exaustiva de todas as combinações para encontrar a chave para decifrar o **código** ou uma **senha**;
    - Como esta sua senha ?

51

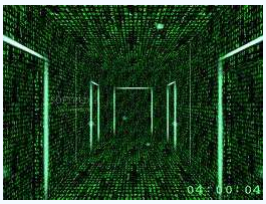
Ataques

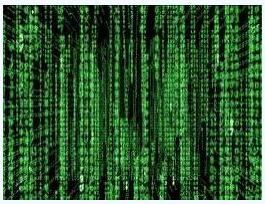
- **Ataque a senhas fracas**
  - Consiste em tentar todas as combinações possíveis e previsíveis para encontrar senhas de mamões;
    - Como esta sua senha ?
      - **Senhas fracas**: Datas aniversario, telefone, nomes parentes e de cachorros, papaia ...
      - **Lugares fáceis**: embaixo do teclado, mouse pad, embaixo do telefone, embaixo da mesa, monitor, na 1ª gaveta ... ☺

52

Ataques

- **Ataque de Criptoanálise**
  - Consiste em tentar decifrar o texto contando com informações privilegiadas sobre o algoritmo utilizado para cifrar o texto;
  - O objetivo é reduzir as operações para quebra da criptografia.





53

Ataques

- **Ataque de "Homem do Meio"**
  - Ataque chamado ***Man-in-the-middle***;
  - Consiste em um usuário mal intencionado que se infiltra na comunicação entre duas entidades, captura os pacotes enviados decifra e retransmite para eles sem que os mesmos percebam. De posse dos pacotes capturados o atacante pode decifrá-los;

54

Ataques

- **Ataque de *Replay***
  - Ataque do tipo Man in the Middle onde os dados que estão sendo transmitidos de A para B são interceptados para posterior retransmissão;
  - Contra medidas
    - Session token
    - Timestamping
    - nonce (number used once) + Message authentication Code (MAC)

55

Ataques

- **Ataque de *denial of dervice* (DoS attack) ou *distributed denial of service* (DDoS attack)**
  - Ataque chamado ***Negação de serviço***;
  - Consiste em realizar maciças solicitações validas a um determinado provedor de serviço de tal forma que o mesmo fique impedido de atender aos usuários normais;
  - Alvos mais comuns são servidores web e de e-mail;
  - Normalmente realizada por computadores zumbis;
  - Sintoma
    - Perda de performance;
    - Serviço não disponível;

56

Ataques

- **Ataque de *denial of dervice* (DoS attack) ou *distributed denial of service* (DDoS attack)**
  - Ataque pode executar
    - Consumo de recursos computacional como disco, largura de banda ou tempo de processador;
    - Alteração da tabelas de roteamento;
    - Cancelamento de sessões TCP;
    - Desligamento de componentes físicos de rede;

57

Ataques

- ***Malware***
  - *Malicious software*, pode ser:
    - Vírus, worms, trojan ou cavalos de tróia, spywares;
  - Tem o objetivo se infiltrar no computador de uma vitima com o objetivo de adquirir informações pessoais;
  - Se divide em duas categorias: 1ª que precisam de um programa hospedeiro e 2ª que são independentes;

58

Ataques

- ***Phishing***
  - Consiste em adquirir informações pessoais de forma enganosa utilizando engenharia social por meio de *e-mails* ou páginas Web falsas;
  - Um estelionatario envia e-mails falsos forjando a identidade de pessoa conhecida ou mesmo popular que seria considerada confiável !!!

59

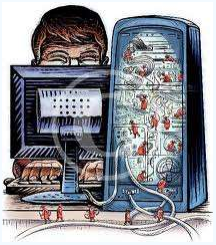
Ataques

- ***Phishing*** **(Safe Browsing - Protecting Web Users for 5 Years and Counting, 19/06/2012/google)**
  - **https://transparencyreport.google.com/safe-browsing/overview**

60

Ataques

- ***Spyware***
  - Consiste em um programa automático que tem o objetivo de recolher informações e costumes sobre o usuário, sem autorização e conhecimento do mesmo, transmitindo o resultado para uma entidade externa.


Ataques

- ***Vírus***
  - É um programa do tipo *malware* que infecta o computador com objetivos espúrios e tenta fazer copias de si em outros programas ou mesmo computadores;
  - A contaminação se da por meio da execução de um programa ou arquivo infectado que venha por meio de um e-mail, pendrive, hd externo;

Ataques

- ***Worms***
  - É um programa que tem a capacidade de se propagar automaticamente pelas redes, enviando copias de sim mesmo para outros computadores;
  - Em alguns casos alterando seu código, ou seja sofrendo mutação.

63

Ataques

- ***Vírus***
  - *Vários reports*
    - *https://www.microsoft.com/en-us/wdsi/threats*
    - ✓ *https://www.mcafee.com/enterprise/en-us/threat-center.html*

64

Ataques

- ***SCAM***
  - Fraude ou golpe com finalidade de se obter vantagens financeiras;

65

Ataques

- ***Trojan ou Cavalo de Tróia***
  - *Software* do tipo *malware* infiltrado no computador da vitima com o objetivo de dominar o sistema para que o mesmo seja manipulado pelo atacante.
  - *Sofware* aparentemente normal e útil que em um determinado momento realiza uma função maléfica para prejudicar a vítima.

66

Ataques

- ***Backdoor***
  - São portas ou pontos de entrada deixadas propositalmente em um software que permite ao atacante se infiltrar no computador da vitima com o objetivo de dominar o sistema para que o mesmo seja manipulado pelo atacante.
  - São ameaças reais de programadores inescrupulosos.

- **Bomba lógica**
  - Um código embutido em um software propositadamente por um programador para prejudicar uma empresa ou organização;

67

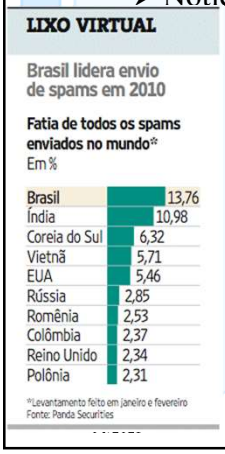
Ataques

- ***SPAM***
  - Consiste no envio de mensagem não solicitada;
    - Boato ou *hoaxes*;
    - Correntes;
    - Propagandas;
    - Golpes ou SCAN;
    - *Phishing*;
    - *Trojans*;

68

Ataques

- ***SPAM***
  - Infelizmente o Brasil ocupa lugar de destaque no ranking mundial de SPAM;
  - Notícias sobre SPAM



- **Brasil é o terceiro país em ranking mundial de spam de 2010**

http://computerworld.uol.com.br/seguranca/2010/07/14/brasil-e-o-terceiro-pais-em-ranking-mundial-de-spam-de-2010/

- **Brazil, India and Korea top the first 2010 ranking of spam sources segundo** Panda Security

http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=10111

- **Relatório da Symantec sobre SPAM *Phishing* 10/2010**
  - » **clique**

69

Ataques

- **Ataque de *Scanning***
  - Consiste na varredura de endereços com o objetivo de encontrar portas abertas para invadir os computadores;

70

Ataques

- **Ataque de DNS *Spoofing***
  - Consiste em falsificar respostas do DNS direcionando a vitima a domínios e sites diferentes do requerido;
  - A vítima acessando a site ou domínio do atacante fica totalmente vulnerável a ataques de *sniffer* e falsificação de solicitação de senhas e cadastros etc...

71

Ataques

- ***Bot e Botnets***
  - Um *bot* é um tipo de *malware* que permite o atacante a ter controle sobre o computador afetado;
  - Os *bots* normalmente são utilizados para compor uma rede de *bots* chamadas de *botnets;*
  - Os computadores infectados também são chamados de computadores *zumbis*;
  - As *botnets* são compostas de centenas até milhares de computadores;

72

Ataques

- ***Bot e Botnets***
  - Tipos de ataques realizados pelas *botnets*
    - DDOS;
    - SPAM
    - *Keylogging*
    - *Sniffing*
    - Objetivo é o lucro !!!

73

Ataques

- ***Bot e Botnets***

74

Ataques

- ***Engenharia Social***
  - **Atualmente um dos mais temíveis ataques, que não se pode evitar por meio de firewall, senhas fortes ou mesmo dispositivo tecnológico !!!**
  - ***Vitima:*** 
  - Defcon 2011, hacker provaram que os funcionários caem facilmente em ataques ardilosos por telefone.
  - **Funcionários precisam de treinamento !!!**
  - **Funcionários são uma das maiores vulnerabilidades !!!**

75

Ataques

- **Algo mais ?**

✓ Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution

✓ (14/set/2010) https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2010/ms10-062

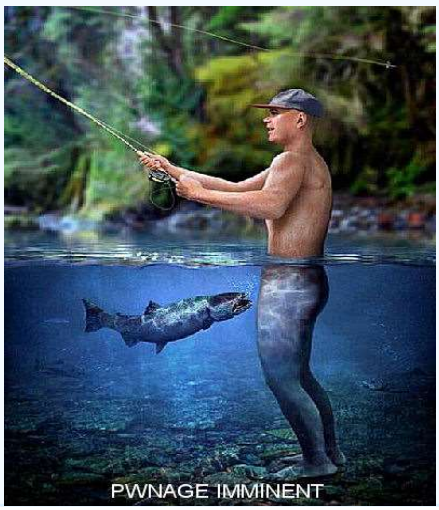
✓ **Microsoft Security Response Center**

- ✓ https://www.microsoft.com/en-us/msrc?rtc=1
- ✓ https://msrc.microsoft.com/update-guide

76

Ataques

- **Algo mais ?**



77

Ataques

- **Objetivo a ser alcançado ? Não ser dominado !!!**

78

III - Defesas

79

Defesas - Processos

- **É fundamental que as organizações tenham bem definidas:**
  - Políticas
    - Exemplos
  - Normas e regras para os serviços
    - Exemplos
  - Treinamentos
    - Segurança !!! Você tem ?
  - Auditorias visando avaliar as políticas e normas de segurança.
    - Sua empresa faz ?

80

Defesas - Processos

- **É fundamental que os usuários:**
  1. Sejam céticos quanto a tudo em TIC;
  2. Façam backup regularmente;
     - ➢Guarde os backups em lugares separados do original;
     - ➢Tenha mais de uma copia;
  3. Tenha softwares legais;
  4. Mantenha os softwares atualizados;
  5. Não responda a e-mails sem sentido !!!
  6. Monitore quem compartilha seu computador;
  7. Utilize somente computadores confiáveis;
  8. Utilize antivírus, anti spyware e firewall;
  9. Troque as Senhas ! ! !
  10. Tenha cuidado !!!

81

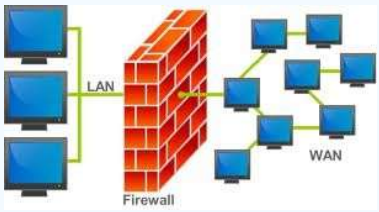
Defesas - Tecnologias

- Firewall
- IDS
- Antivírus
- Anti-spam
- **Criptografia**
- **Protocolos de Segurança**
- Honeypots
- Sniffer

82

Defesas - Firewall

- **Firewall**
  - Se constitui em uma porta onde todo o trafego da rede deve passar;
  - É empregado um conjunto de regras para o trafego que entra e o que sai, *inbound* e *outbound*;
  - Somente o trafego autorizado deverá passar pelas regras vigentes no firewall;



83

Defesas - Firewall

- **Firewall**
  - Firewall proporciona
    - Controle de serviços: possibilita o controle em quais serviços pode ou não ser acessados;
    - Controle de direção do trafego: possibilita determinar qual direção solicitações de serviços irão seguir;
    - Controle de usuário: possibilita controle a acesso de serviços por usuário;

84

Defesas - Firewall

- **Firewall**
  - Firewall protege contra ataques internos que são muitos !!!
  - Não pode proteger contra ataques que o contornam !!!
  - Exemplos
    - Versões para uso nas em *datacenter* (*enterprise systems*)
    - Versões para uso domestico (*home user*)
    - Iptables nativo no linux

85

Defesas - Firewall

- **Firewall -** Exemplos sistemas proprietários !!!
  - ✓ **Cisco**
  - ✓ **Check Point VPN-1**
  - ✓ **Fortinet**
  - ✓ **Palo Alto Networks**
  - ✓ **Barracuda**
  - ✓ **IBM**
  - ✓ **Panda**
  - ✓ **Mcafee**
  - ✓ **Sophos**
  - ✓ **F-secure**
  - ✓ **Juniper**
  - ✓ **Grisoft**
  - ✓ **Iptables nativo no linux e livre.**

86

Defesas - Firewall

- **Firewall**
  - Exemplos Iptables nativo no linux e livre.

- **# videoconferencia com o Cern**
- **# ----------#**

- **$IPTABLES -A FORWARD -p tcp -m multiport -s 172.10.0.0/16 -d vidyoportal.cern.ch --dport 443,17992,17990,80 -j ACCEPT**
- **$IPTABLES -A FORWARD -p tcp -m multiport -d 172.10.0.0/16 -s vidyoportal.cern.ch --sport 443,17992,17990,80 -j ACCEPT**

- **$IPTABLES -A FORWARD -p udp -m multiport -s 172.10.0.0/16 -d vidyoportal.cern.ch --dport 50000:65535 -j ACCEPT**
- **$IPTABLES -A FORWARD -p udp -m multiport -d 172.10.0.0/16 –s vidyoportal.cern.ch --sport 50000:65535 -j ACCEPT**

87

Defesas - Firewall

- **Firewall**
  - Exemplos Iptables nativo no linux e nat ip valido invalido.

- ✓ **$IPTABLES -t nat -A PREROUTING -p tcp -m multiport -d 189.90.66.140 --dport 22,80,443,5433,8005,9001 -j DNAT --to 10.90.66.15**
- ✓ **$IPTABLES -A FORWARD -p tcp -m multiport -d 10.90.66.15/32 --dport 22,80,443,5433,8005,9001 -j ACCEPT**
- ✓ **$IPTABLES -A FORWARD -p tcp -m multiport -s 10.90.66.15/32 --sport 22,80,443,5433,8005,9001 -j ACCEPT**

88

Defesas - IDS

- **Sistemas de Detecção de Intrusão**
  - Também chamados de IDS (*Intrusion Detect Systems*)
  - É uma ferramenta para segurança que trabalha com base na detecção de padrões;
  - Também conhecido como 2ª linha de defesa
    - O intruso já esta dentro !!!

89

Defesas - IDS

- **Sistemas de Detecção de Intrusão**
  - O intruso pode ser
    - Alguém de fora disfarçado
    - Alguém de dentro infrator
  - Normalmente o intruso irá buscar por alguma vulnerabilidade.

90

Defesas - IDS

- **Sistemas de Detecção de Intrusão**
  - Normalmente o intruso irá buscar a senha de um usuário para uma vez efetuado *login* na rede possa garimpar mais informações e privilégios para o ataque;
  - Fundamental que o arquivo de senha esta protegido
    - Senhas unidirecionais utilizando função de *hash*;
    - Controle rígido de acesso ao arquivo de senhas;
    - Política de senhas rigorosa, com prazos e tamanhos mínimos;

91

Defesas - IDS

- **Sistemas de Detecção de Intrusão**
  - Arquivo de senhas
    - Senhas padrão devem ser alteradas; (*default*)
      - Ex. roteadores, switches, access point; public private;
    - Senha com 3 ou menos caracteres devem ser proibidas;
    - Senhas com base em dicionário de hacker com palavras conhecidas;
      - Ex. 1234; abcde; jose; maria; utiliza dicionário de palavras comuns...
    - Senha com informações sobre usuários
      - Ex. nome; placa de carro; telefone; aniversario; nome parentes;
    - Política para senhas DEVE ser implementada e mantida!!!

92

Defesas - IDS

- **Sistemas de Detecção de Intrusão**
  - Os IDS trabalham com base na analise de comportamento e desvio de padrão pesquisando por:
    - Anomalia
    - Detecção de padrões, (desvio de padrão)
    - Uso incorreto de privilégios

93

Defesas - IDS

- **Sistemas de Detecção de Intrusão**
- Técnicas para IDS
  - Técnicas baseadas em conhecimento ou padrão conhecidas como *Knowledge-Based*
    - Procura por padrão de ataque ou uma assinatura
    - Tem vantagens nos acertos
    - Desvantagens que necessita atualizações constantes
    - Atacantes modificam padrões constantemente !!

94

Defesas - IDS

- **Sistemas de Detecção de Intrusão**
- Técnicas para IDS
  - ➢ Técnicas baseadas em comportamento conhecidas como *Behavior-Based*
    - ➢ Requer a criação de *baseline*;
      - Perfil de comportamento do usuário e do segmento analisado;
    - ➢ Utiliza algoritmos estatísticos e/ou heurísticas para estabelecer o padrão de comportamento;
    - ➢ Detecta mudanças de padrões na rede*;*

95

Defesas - IDS

- **Sistemas de Detecção de Intrusão**
  - ➢ Problemas são os alarmes falsos:
    - ➢ *Falsos Positivos*
    - ➢ *Falsos Negativos*

96

Defesas - UTM

- **Unified Threat Management (UTM)**
  - ✓ Detecção de Intrusão
  - ✓ Detecção de Vírus
  - ✓ Trojan
  - ✓ Spam
  - ✓ Worms
  - ✓ Spyware
  - ✓ IPS
  - ✓ Filtro URL
  - ✓ Todos os serviços integrados em uma solução
  - ✓ Facilita o gerenciamento (instalação, manutenção, atualização...)
  - ✓ Exemplos de fabricantes: Palo Alto Networks, Cisco, Fortinet, Check Point, SonicWall, Barracuda, Sophos, HPE,

97

Defesas - Honeypot

- ***Honeypot***
  - ➢ São computadores iscas que são colocados propositalmente em posições estratégicas e com problemas e brechas de segurança para registrar ataques a rede;
  - ➢ O objetivo é coletar informações para aprendizado e futuras contramedidas contra os invasores.
  - ➢ São utilizados
    - ➢ Computadores com configurações padrões, instalações básicas
    - ➢ Computadores com aplicações falsas que simulam serviços reais na empresa

98

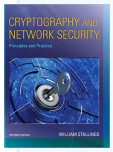
Defesas – Antivírus

- **Antivírus**
- Existe vários anti-vírus disponíveis:
  - *Microsoft Security Essential*
  - F-secure
  - Avast
  - AVG
  - Avira
  - MCAFEE
  - Symantec
  - Panda

99

Bibliografia

- **Computer Security: Principles and Practice, 3rd Edition, 3a ed. William Stallings** ISBN-10: 0133773922 Pearson Prentice Hall Copyright: 2015



- **Cryptography and Network Security: Principles and Practice, 7/E** William **Stallings** ISBN-10: 0134444280, Publisher: Prentice Hall Copyright: 2016

- **Governança Avançada de TI, Na Prática,** Autor: Ricardo Mansur, Editora: Brasport, 2009, ISBN 978-85-7452-404-7.

100

Bibliografia

- **Estratégias de Governança de Tecnologia de Informação**, Alberto Luiz Albertin; Rosa Maria de Moura; editora Elsevier – Campus , 2010 ISBN 978-85-352-3706-1