

Segurança da Informação

Introdução

Sumário

- 1 História
- 2 Definição
- 3 Triáde CID

- 4 Níveis de Impacto
- 5 Considerações
- 6 Bibliografia

História

Creeper (1971)

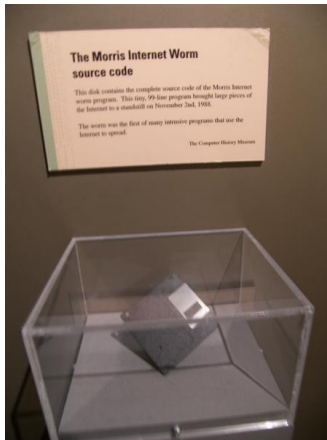
- Considerado o primeiro vírus de computador, exibia a mensagem "Eu sou assustador, pegue-me se for capaz".



I'M THE CREEPER : CATCH ME IF YOU CAN!

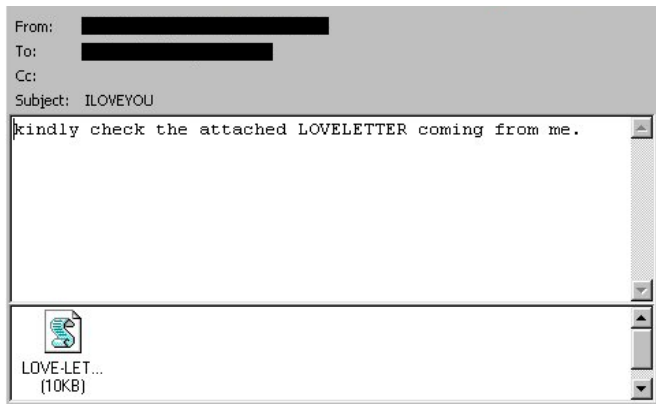
Morris Worm (1971)

- › **Morris Worm** foi o primeiro worm de computador amplamente reconhecido, lançado 1988 por Robert Tappan Morris.
- › O worm para copiar a si mesmo, independentemente do status da infecção no computador.
- › Um computador poderia ser infectado várias vezes.
- › Cada infecção adicional, poderia levar o computador a inutilização.



ILOVEYOU (2000)

- Um dos vírus mais devastadores, espalhou-se por e-mail e causou prejuízos globais massivos estimados em até 10 bilhões de dólares.



Stuxnet (2010)

- *Malware* sofisticado que desativou centrífugas do programa nuclear iraniano, considerado a primeira arma cibernética a atingir sistemas industriais.



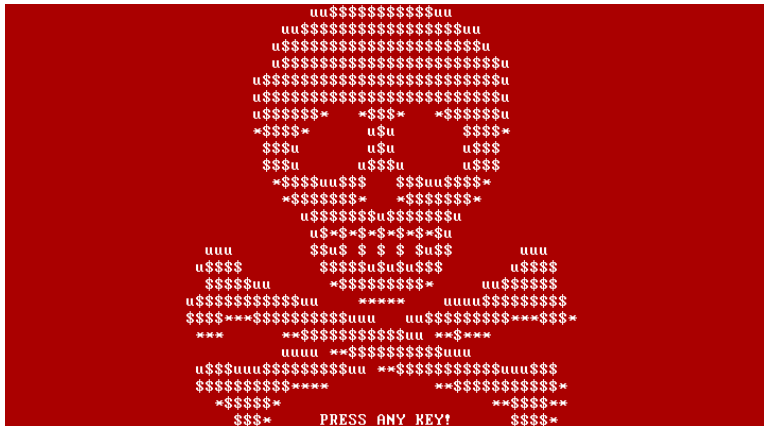
WannaCry (2017)

- *Ransomware* que se espalhou globalmente, infectando mais de 200 mil computadores em 150 países, criptografando arquivos e exigindo resgate em Bitcoin. Explora vulnerabilidade no protocolo SMB do Windows.



NotPetya (2017)

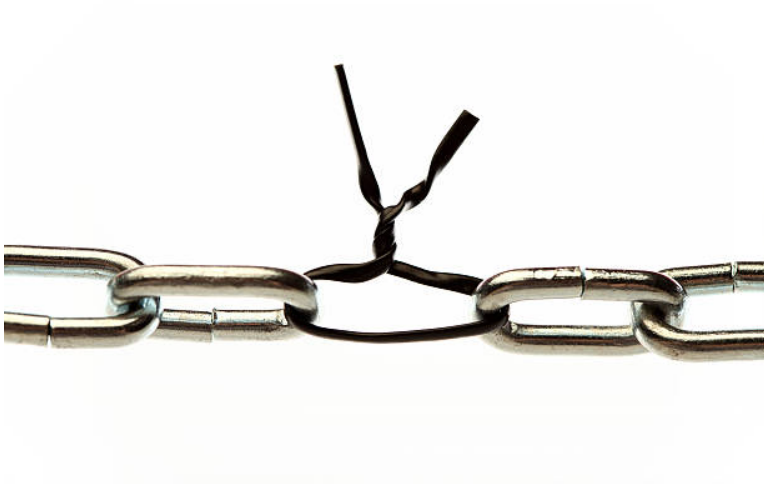
- Malware causador de um dos ataques cibernéticos mais caros da história, atingindo principalmente o setor financeiro via atualização de software comprometida.



Ataque de Ransomware ao STJ (2020)

- Em novembro de 2020, o Superior Tribunal de Justiça sofreu um ataque de ransomware que criptografou todo seu acervo de processos, suspendeu sessões de julgamento e exigiu resgate, mas o backup permitiu a restauração dos dados.

Definição



Reflexões:

- Segurança é uma corrente; é tão segura quanto o elo mais fraco (SCHNEIER, 2001).
- Segurança é um processo, não um produto (SCHNEIER, 2001).

Cybersecurity é um conjunto de ferramentas, políticas, conceitos e salvaguardas de segurança, diretrizes, abordagens de gerenciamento de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser usados para proteger o ambiente cibernético, a organização e os recursos do usuário.

(ITU, 2009)

Segurança de Computadores: a proteção oferecida para um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema de informação.

(NIST, 1995)

Triáde CID

É possível destacar três objetivos fundamentais da segurança de computadores. Sendo eles:

- Confidencialidade;
- Integridade;
- Disponibilidade.

Esses três conceitos formam o que é frequentemente denominado **tríade CID**

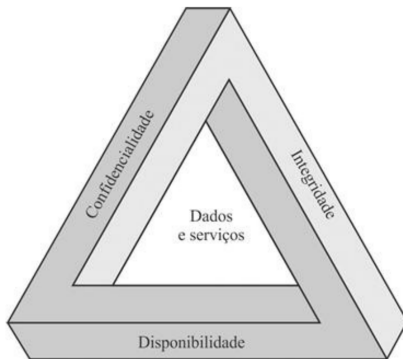


Figura 1: Tríade de requisitos de segurança (STALLINGS; BROWN, 2015).

*Preservar restrições autorizadas ao acesso e revelação de informações, incluindo meios para proteger a privacidade pessoal e as informações proprietárias. **Uma perda de confidencialidade consiste na revelação não autorizada de informações.***

(National Institute of Standards and Technology, 2004)

› Confidencialidade

- ›› **Confidencialidade de dados:** Garante que informações privadas ou confidenciais não fiquem disponíveis nem sejam reveladas a indivíduos não autorizados.
- ›› **Privacidade:** Garante que os indivíduos controlem ou influenciem quais informações sobre eles podem ser coletadas, armazenadas e para quem podem ser reveladas.

Formas de oferecer confidencialidade:

- › Criptografia;
- › Controle e níveis de acesso;
- › Segurança Física;
- › Anonimização de Dados.

*Defender contra a modificação ou destruição imprópria de informações, garantindo a **irretratabilidade** (ou não repúdio) e a **autenticidade** das informações. **Uma perda de integridade consiste na modificação ou destruição não autorizada de informações.***

(National Institute of Standards and Technology, 2004)

- › Utilização de funções hash (ex.: SHA-256) para verificar alterações em dados.
- › Assinaturas digitais para garantir que o conteúdo não foi modificado.
- › Certificados digitais.
- › Controles de acesso adequados para evitar alterações não autorizadas.
- › Mecanismos de versionamento e log de eventos.
- › *Backups* regulares para restaurar informações originais em caso de corrupção.

Embora a utilização da tríade CID para definir objetivos de segurança seja bem estabelecida, algumas pessoas na área da segurança acreditam serem necessários conceitos adicionais.

- A propriedade de ser genuína e poder ser verificada e confiável; confiança na validade de uma transmissão, de uma mensagem ou do originador de uma mensagem.
- Isso significa verificar que os usuários são quem dizem ser e que cada dado que chega ao sistema veio de uma fonte confiável.

- O objetivo de segurança que leva à exigência de que as ações de uma entidade sejam rastreadas e atribuídas unicamente àquela entidade.
- Os sistemas devem manter registros de suas atividades para permitir análise forense posterior, de modo a rastrear violações de segurança ou auxiliar em disputas sobre uma transação.

Assegurar que o acesso e o uso das informações seja confiável e realizado no tempo adequado. Uma perda de disponibilidade consiste na interrupção do acesso ou da utilização de informações ou de um sistema de informação.

citeFIPSPUB199

- › Implementação de redundância em servidores, links e dispositivos de rede.
- › Uso de balanceamento de carga para distribuir requisições.
- › Políticas de [backup] e recuperação de desastres.
- › Proteção contra ataques de negação de serviço (DoS/DDoS).

Níveis de Impacto

Definição de três níveis de impacto (National Institute of Standards and Technology, 2004) quando existe quebra de segurança, isto é, **fragilidade em um dos requisitos da tríade CID**.

- **Baixo:** Pode-se esperar que a perda cause efeito adverso limitado sobre operações organizacionais, ativos organizacionais ou indivíduos. Exemplos de efeito adverso limitado incluem:
 - 1 Degradação na capacidade de completar uma tarefa até um ponto e por uma duração tal que a organização consegue executar suas funções primárias, mas a efetividade das funções sofre redução perceptível;
 - 2 Dano desprezível a ativos organizacionais;
 - 3 Perdas financeiras insignificantes;
 - 4 Dano reduzido a indivíduos.

- **Moderado:** Pode-se esperar que a perda cause efeito adverso sério sobre operações organizacionais, ativos organizacionais ou indivíduos. Exemplos de efeito adverso sério incluem:
- 1 Degradação significativa na capacidade de completar uma tarefa até um ponto e por uma duração tal que a organização consegue executar suas funções primárias, mas a efetividade das funções sofre significativa redução;
 - 2 Dano significativo a ativos organizacionais;
 - 3 Perda financeira significativa;
 - 4 Dano significativo a indivíduos, não envolvendo perda de vida ou ferimentos sérios que ameacem a vida.

- **Alto:** Pode-se esperar que a perda cause efeito adverso grave ou catastrófico sobre operações organizacionais, ativos organizacionais ou indivíduos. Exemplos de efeito adverso grave ou catastrófico incluem:
- 1 Grave degradação ou perda de capacidade de completar uma tarefa até um ponto e por uma duração tal que a organização não consegue executar uma ou mais de suas funções primárias;
 - 2 Grande dano a ativos organizacionais;
 - 3 Grande perda financeira;
 - 4 Dano grave ou catastrófico a indivíduos, envolvendo perda de vida ou ferimentos sérios que ameacem a vida.

Considerações

1.

Segurança de computadores é essencialmente uma batalha de capacidade entre um perpetrador que tenta encontrar brechas e o projetista ou administrador que tenta fechá-las. A grande vantagem que o atacante tem é que só precisa descobrir uma única fraqueza, ao passo que o projetista tem de encontrar e eliminar todas as fraquezas para conseguir segurança perfeita.

2.

Há uma tendência natural da parte de usuários e gerentes de sistemas de perceberem pouco benefício em fazer investimento em segurança até ocorrer uma falha de segurança.

3.

Segurança requer monitoramento regular, até constante, e isso é difícil no ambiente de curto prazo e sobrecarregado de hoje.

4.

Segurança ainda é muito frequentemente mero acessório a ser incorporado a um sistema depois de concluído o projeto, em vez de ser parte integral do processo de construir o projeto.

5.

Muitos usuários e até mesmo administradores de segurança consideram que segurança forte atrapalha a operação eficiente e amigável ao usuário de um sistema de informação ou a utilização da informação.



Capítulo 1 (SCHNEIER, 2001)



Capítulo 1 (Brown, 2013)

Bibliografia

BRASIL. **Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).**

[S. l.: s. n.], 2014.

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).** [S. l.: s. n.], 2018.

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais.

BROWN, L. L. **Segurança de Computadores - Princípios e Práticas.** 1. ed. São Paulo: GEN LTC, 2013.

FOROUZAN, Behrouz; MOSHARRAF, Firouz. **Redes de Computadores: Uma abordagem Top-Down.** São Paulo: McGraw Hill, 2014.

 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **NBR ISO/IEC 27000, 27001 e 27002**. Genebra, 2022. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação.

 SCHNEIER, Bruce. **Secrets and Lies: Digital Security in a Networked World**. 15th Anniversary Edition. Indianapolis, IN: Wiley, 2015. p. 448.

 UNION, European. **General Data Protection Regulation (Regulation EU 2016/679)**. [S. l.: s. n.], 2016. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Regulation on the protection of natural persons with regard to the processing of personal data.

BISHOP, Matt. **Computer Security: Art and Science**. 2. ed. Boston, MA: Addison-Wesley, 2018.

DIAS, Claudia. **Segurança e Auditoria da Tecnologia da Informação**. São Paulo: Axcel Books, 2000.

HINTZBERGEN, J. *et al.* **Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002**. 1. ed. Rio de Janeiro: Brasport, 2018.

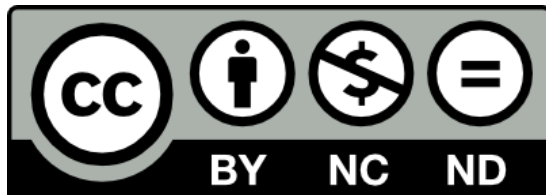
MCCLURE, Stuart. **Hackers Expostos: Segredos e Soluções Para a Segurança de Redes**. 7. ed. Porto Alegre: Bookman, 2013.

SCHNEIER, Bruce. **Segurança.com**. 1. ed. São Paulo: Campus, 2001.



ZWICKY, Elizabeth D. **Construindo Firewalls para a Internet**. 2. ed. Rio de Janeiro: Editora Campus, 2000.

Estes slides estão protegidos por uma licença Creative Commons



Este modelo foi adaptado de Maxime Chupin.

Segurança da Informação

Introdução