nic.br cgi.br | cert.br

# Cibersegurança e privacidade no mundo pós pandemia: desafios, tendências e oportunidades

22º Workshop RNP

16 de agosto de 2021 | Evento *Online*

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT Nacional de Último Recurso

# Serviços Prestados à Comunidade

## Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

## Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

## Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e Político

**Filiações e Parcerias:**

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

HN/P

**Criação:**

**Agosto/1996:** CGI.br publica o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil"[1]

**Junho/1997:** CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://nic.br/pagina/gts/157

## Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

## Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

## Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial, coordenada pelo MCTI
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

https://cert.br/sobre/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

# Segurança e Privacidade: Raiz dos Problemas e Desafios para uma Boa Engenharia de Segurança

**Dra. Cristine Hoepers**
**Gerente Geral**
**cristine@cert.br**

cert.br nic.br cgi.br

# O Que é Privacidade?

***Privacy*** is the ability and/or right to protect your personal information and extends to the ability and/or right to prevent invasions of your personal space (the exact definition of which varies quite sharply from one country to another).

***Confidentiality*** involves an obligation to protect some other person's or organization's secrets if you know them.

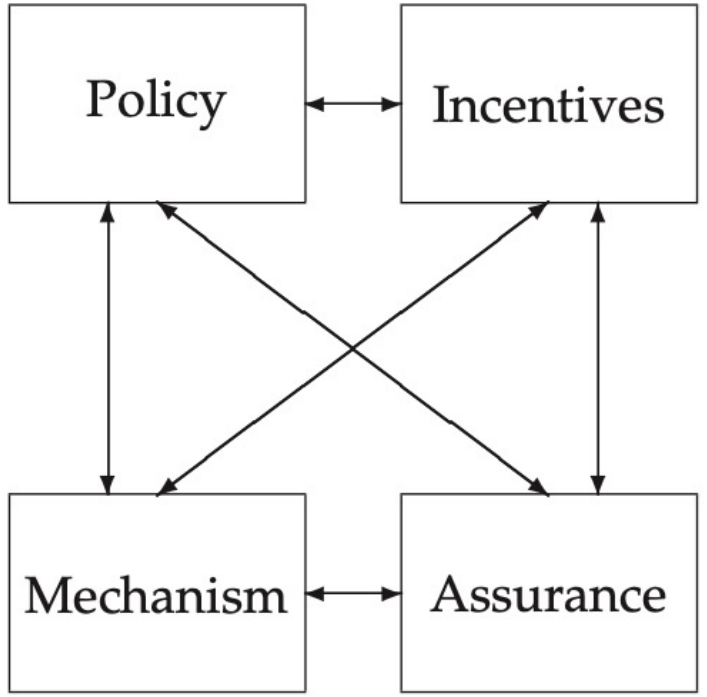
***Secrecy*** is a technical term which refers to the effect of the mechanisms used to limit the number of principals who can access information, such as cryptography or computer access controls.

**Source: Chapter 1: What is Security Engineering?, Security Engineering, 2nd Edition, 2008, Ross Anderson**
**https://www.cl.cam.ac.uk/~rja14/book.html**

# O Que é Engenharia de Segurança?

***Security engineering*** is about building systems to remain dependable in the face of malice, error, or mischance.

***Good security engineering*** requires four things to come together. There's policy: what you're supposed to achieve. There's mechanism: the ciphers, access controls, hardware tamper-resistance and other machinery that you assemble in order to implement the policy. There's assurance: the amount of reliance you can place on each particular mechanism. Finally, there's incentive: the motive that the people guarding and maintaining the system have to do their job properly, and also the motive that the attackers have to try to defeat your policy.




**Source: Chapter 1: What is Security Engineering?, Security Engineering, 2nd Edition, 2008, Ross Anderson**
**https://www.cl.cam.ac.uk/~rja14/book.html**

# Quais as Causas dos Incidentes?

## Contextos Global e Nacional

cert.br nic.br cgi.br

# You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that

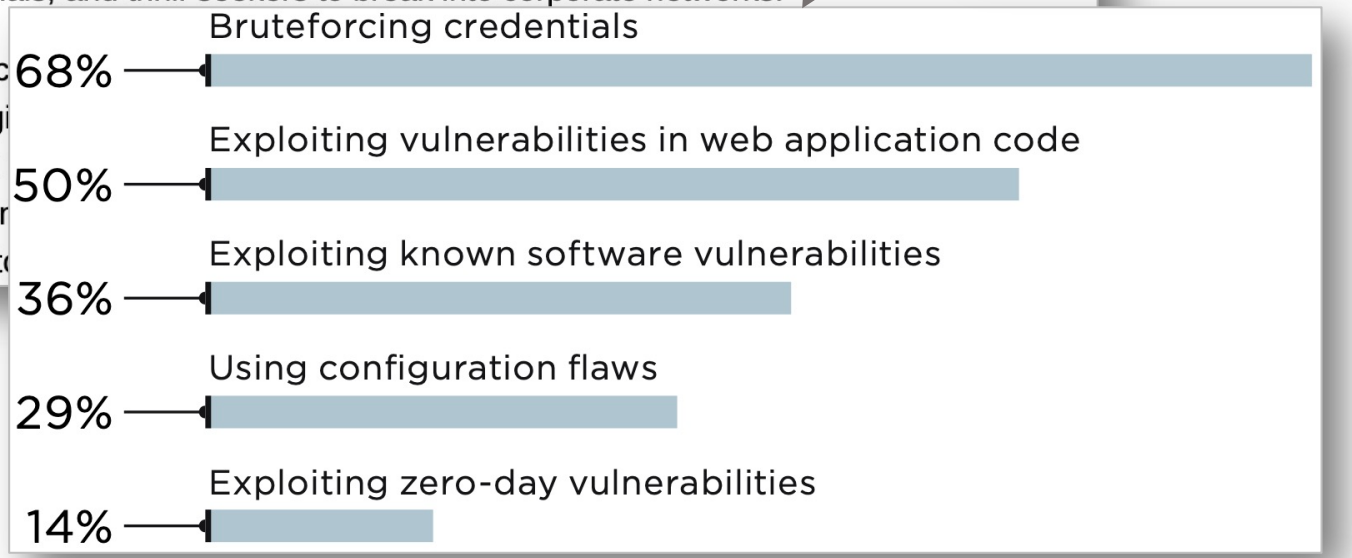
## Three little words: Patches, passwords, policies

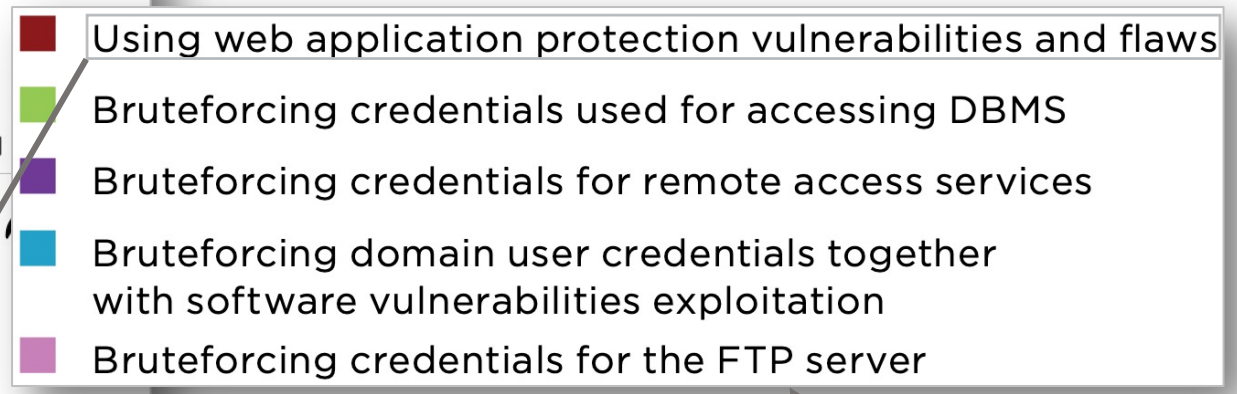
Thu 13 Aug 2020 // 07:06 UTC 31

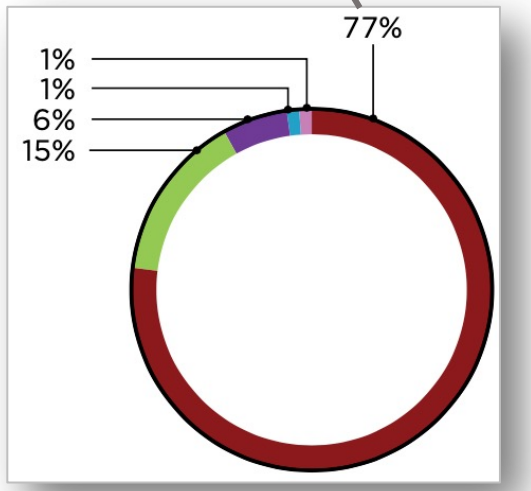
**Shaun Nichols in San Francisco** BIO EMAIL TWITTER

The continued inability of organizations to patch security vulnerabilities in a timely manner, combined with guessable passwords and the spread of automated hacking tools, is making it pretty easy for miscreants, professionals, and thrill-seekers to break into corporate networks.

This is acc
Technologi
and found
its red tear
available t




https://www.theregister.com/2020/08/13/pentest_networks_fail/
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pentests-2020-eng.pdf

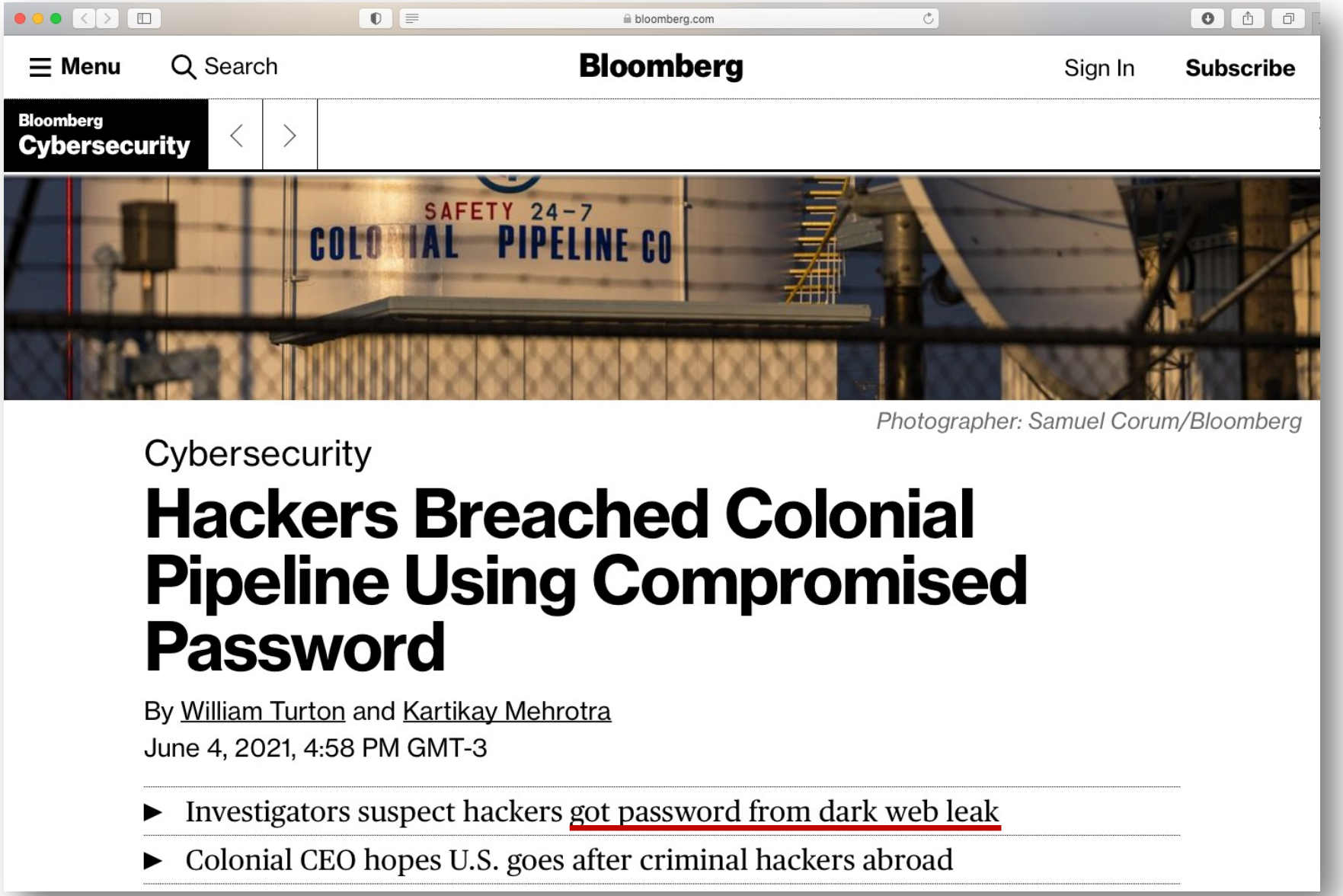
Cybersecurity
INSIDERS

# Insider Threat Awareness Month Reminds Us That the Biggest Threats Can Arise from Within

Posted By **cyberinsiders**

Insider Threat Awareness Month offers a great opportunity to make organizations realize that today's modern cyberattack is no longer carried out by a dark cyber-assassin with sophisticated hacking techniques. The reality is that they no longer hack in at all, they log in using weak, stolen, or otherwise compromised passwords. And a shocking amount of the time, it is actually an insider doing the "hacking."

https://www.cybersecurity-insiders.com/insider-threat-awareness-month-reminds-us-that-the-biggest-threats-can-arise-from-within/




https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

## Top 10 Most Exploited Vulnerabilities 2016–2019

U.S. Government reporting has identified the top 10 most exploited vulnerabilities by state, nonstate, and unattributed cyber actors from 2016 to 2019 as follows: CVE-2017-11882, CVE-2017-0199, CVE-2017-5638, CVE-2012-0158, CVE-2019-0604, CVE-2017-0143, CVE-2018-4878, CVE-2017-8759, CVE-2015-1641, and CVE-2018-7600.

## Alert (AA20-133A)

### Top 10 Routinely Exploited Vulnerabilities

Original release date: May 12, 2020

Print Tweet Send Share

### Summary

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the broader U.S. Government are providing this technical guidance to advise IT security professionals at public and private sector organizations to place an increased priority on patching the most commonly known vulnerabilities exploited by sophisticated foreign cyber actors.

## s Exploited in 2020

10 vulnerabilities from 2016 to 2019 listed above, the U.S. orted that the following vulnerabilities are being routinely cated foreign cyber actors in 2020:

- Malicious cyber actors are increasingly targeting unpatched Virtual Private Network vulnerabilities.
  - An arbitrary code execution vulnerability in Citrix VPN appliances, known as CVE-2019-19781, has been detected in exploits in the wild.
  - An arbitrary file reading vulnerability in Pulse Secure VPN servers, known as CVE-2019-11510, continues to be an attractive target for malicious actors.
- March 2020 brought an abrupt shift to work-from-home that necessitated, for many organizations, rapid deployment of cloud collaboration services, such as Microsoft Office 365 (O365). Malicious cyber actors are targeting

https://us-cert.cisa.gov/ncas/alerts/aa20-133a

# Alert (AA21-209A)

More Alerts

## Top Routinely Exploited Vulnerabilities

Original release date: July 28, 2021 | Last revised: August 04, 2021

Print Tweet Send Share

## Summary

This Joint Cybersecurity
(CISA), the Australian Cy
(NCSC), and the U.S. Fec

This advisory provides c
(CVEs)—routinely exploi

*Table 1:Top Routinely Exploited CVEs in 2020*

| Vendor | CVE | Type |
|---|---|---|
| Citrix | CVE-2019-19781 | arbitrary code execution |
| Pulse | CVE 2019-11510 | arbitrary file reading |
| Fortinet | CVE 2018-13379 | path traversal |
| F5- Big IP | CVE 2020-5902 | remote code execution (RCE) |
| MobileIron | CVE 2020-15505 | RCE |
| Microsoft | CVE-2017-11882 | RCE |
| Atlassian | CVE-2019-11580 | RCE |
| Drupal | CVE-2018-7600 | RCE |
| Telerik | CVE 2019-18935 | RCE |
| Microsoft | CVE-2019-0604 | RCE |
| Microsoft | CVE-2020-0787 | elevation of privilege |
| Netlogon | CVE-2020-1472 | elevation of privilege |

https://us-cert.cisa.gov/ncas/alerts/aa21-209a

# Intertrust Releases 2021 Report on Mobile Finance App Security

*Report of over 150 mobile finance apps reveals a high level of security vulnerabilities across both iOS and Android, highlighting the importance of in-app security*

June 02, 2021 12:00 PM Eastern Daylight Time

SAN FRANCISCO--(BUSINESS WIRE)--Intertrust, the pioneer in digital rights management (DRM) technology and leading provider of application security solutions, today released its 2021 State of Mobile Finance App Security Report. The report reveals that 77% of financial apps have at le

"Poor financial app security puts bot financial organizations and their customers at risk, especially given th rise in cyberattacks over the course the pandemic. This report shines a li on the ongoing threats and helps finance app vendors understand the importance of building in security mechanisms from day one"

Tweet this

One or more security flaws were found in every app tested

84% of Android apps and 70% of iOS apps have at least one critical or high severity vulnerability

81% of finance apps leak data

49% of payment apps are vulnerable to encryption key extraction

Banking apps contain more vulnerabilities than any other type of finance app

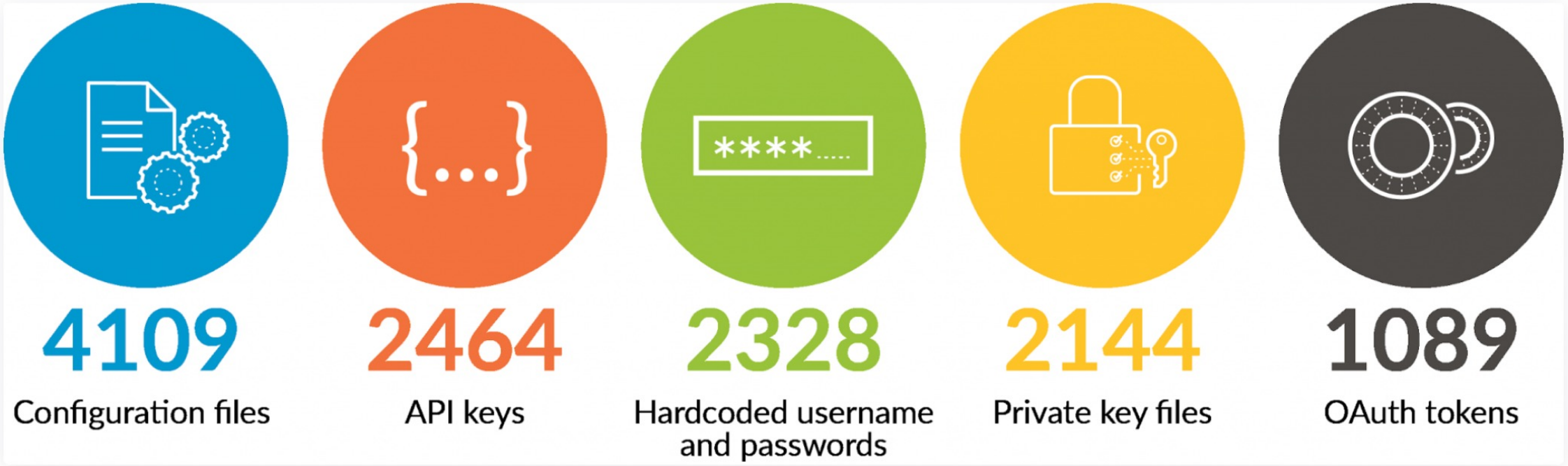
Cryptographic issues pose one of the most pervasive and serious threats, with 88% of analyzed apps failing one or more cryptographic tests. This means the encryption used in these financial apps can be easily broken by cybercriminals, potentially exposing confidential payment and customer data and putting the application code at risk for analysis and tampering.

https://www.businesswire.com/news/home/20210602005213/en/Intertrust-Releases-2021-Report-on-Mobile-Finance-App-Security

# Não são só usuários que comprometem senhas:
# **Desenvolvedores expõe senhas e chaves no 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:




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

# SolarWinds – Ataque atribuído à Russia pelos EUA
# **Possível vetor do comprometimento: senha no GitHub**

SolarWinds FTP credentials were leaking on GitHub in November 2019 Featured

3 Shares | Share | Tweet 3

By Sam Varghese

**More details are emerging about poor security at SolarWinds, following the compromise of its Orion network management software that was then used to effect attacks on many companies in a number of regions around the globe.**

A researcher from India had advised SolarWinds in November 2019 that he had found a public GitHub repository which was leaking the company's FTP credentials.

bounty hunter, said in a tweet: "Was
raging SolarWinds. Hmmm, how that
d was *****123 Rolling on the floor

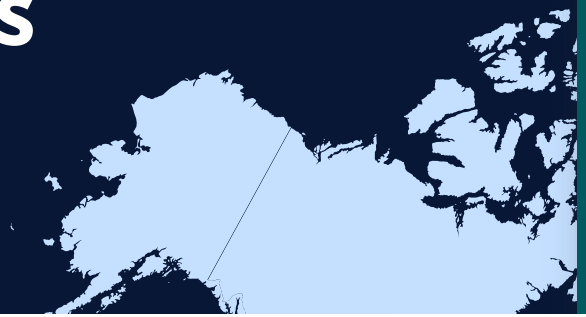
Downloads Url: http://downloads.solarwinds.com
FTP Url: ftp://solarwinds.upload.akamai.com
Username:
Password:
POC: http://downloads.solarwinds.com/test.txt

I was able to upload a test POC.
Via this any hacker could upload malicious exe and update it with release SolarWinds product.

https://www.itwire.com/security/solarwinds-ftp-credentials-were-leaking-on-github-in-november-2019.html
https://threatpost.com/solarwinds-default-password-access-sales/162327/

TOP 10

# Where leaks come from



| | |
|---|---|
| 01 | India |
| 02 | Brazil |
| 03 | United States |
| 04 | Nigeria |
| 05 | France |
| 06 | Russia |
| 07 | UK |
| 08 | Canada |
| 09 | Bangladesh |
| 10 | Indonesia |

## Uber Data Breach*

May 2014

Hackers discovered credentials in a personal public repository on GitHub that granted access to a database containing private information of thousands of Uber drivers.

*Read the article

## Starbucks Data Breach*

January 2020

JumpCloud API key found in GitHub repository.

*Read the article

## Equifax Data Breach*

April 2020

Leaked secrets in personal GitHub account granted access to sensitive data for Equifax customers.

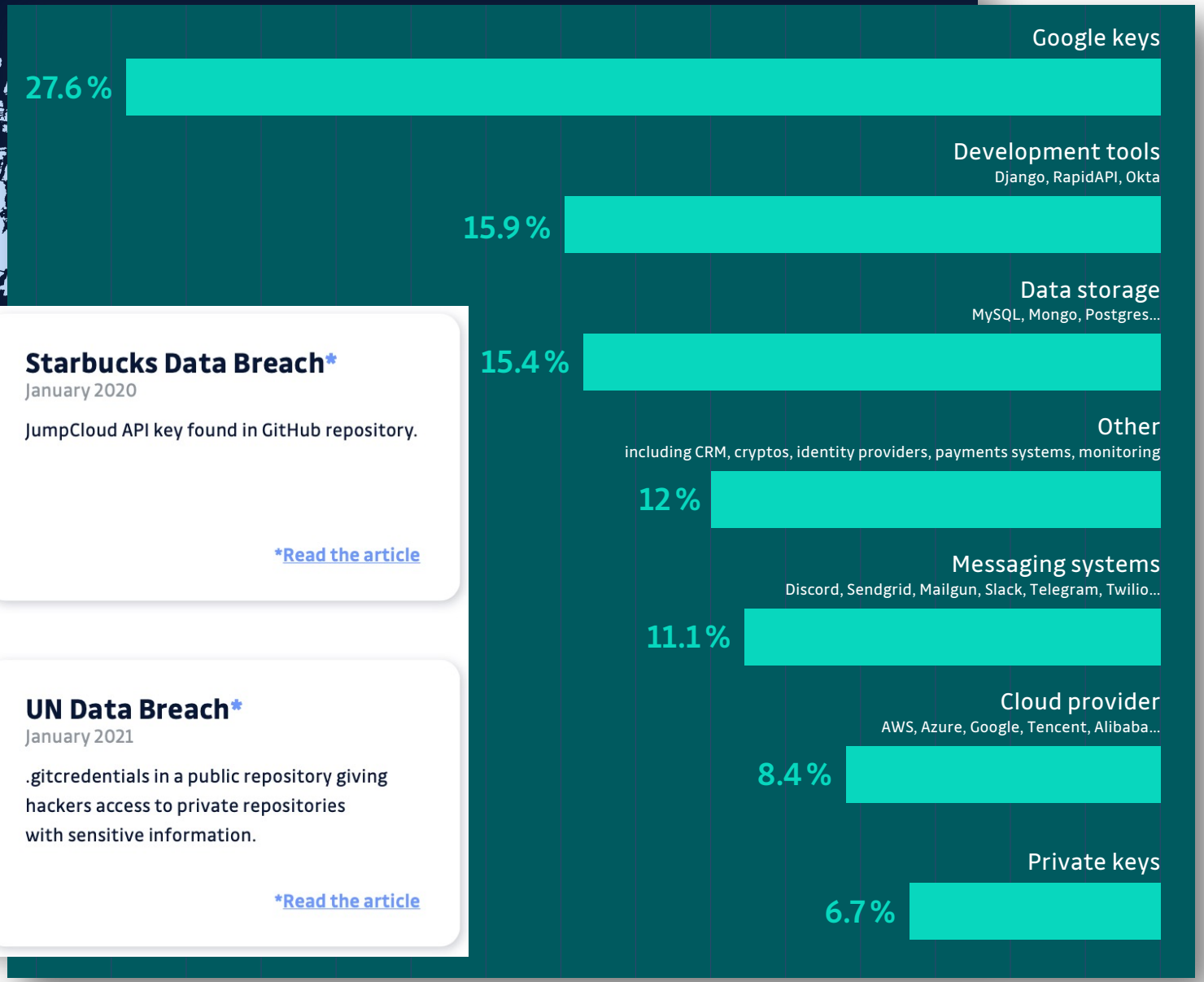
*Read the article

## UN Data Breach*

January 2021

.gitcredentials in a public repository giving hackers access to private repositories with sensitive information.

*Read the article




**State of Secrets Sprawl on GitHub - 2021: https://blog.gitguardian.com/state-of-secrets-sprawl-2021/**

The personal and health information of more than 16 million Brazilian COVID-19 patients has been leaked online after a hospital employee uploaded a spreadsheet with usernames, passwords, and access keys to sensitive government systems on GitHub this month.

## Personal data of 16 million Brazilian COVID-19 patients exposed online

affected by the leak are Brazil President Jair Bolsonaro, ers, and 17 provincial governors.

By Catalin Cimpanu for Zero Day | November 26, 2020 -- 21:22 GMT (13:22 PST) | Topic: Coronavirus: Business and technology in a pandemic

## Data of 243 million Brazilians exposed online via website source code

The password to access a highly sensitive Minist database was stored inside a government site's s code.

By Catalin Cimpanu for Zero Day | December 3, 2020 -- 14:17 GMT ( Topic: Security

Since a website's source code can be accessed and reviewed by anyone pressing F12 inside their browser, Estadao reporters searched for similar issues in other government sites.

Reporters said the site's source code contained a username and password stored in Base64, an encoding format that can be easily decoded to obtain the initial username and password, with little to no effort.

https://www.zdnet.com/article/personal-data-of-16-million-brazilian-covid-19-patients-exposed-online/
https://www.zdnet.com/article/data-of-243-million-brazilians-exposed-online-via-website-source-code/

# Resumo sobre os Incidentes Observados pelo CERT.br: **Causas Mais Comuns de Invasões e Vazamentos de Dados**

**Ataques mais reportados e mais observados em sensores:**

- Força bruta de senhas em serviços protegidos só com conta e senha. Exemplos:
  - *e-mails* e serviços em nuvem
  - acesso remoto e gestão remota de ativos de rede e servidores
- Comprometimento via exploração de vulnerabilidades conhecidas
  - 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
- todos os serviços tivessem 2FA / MFA
- houvesse mais atenção a erros e configurações

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/

Você teria um conselho para as empresas para reduzir o número de incidentes?

**"*Multifactor Everything*"**

-- Katie Moussouris (Luta Security, US)
https://youtu.be/4tuC32PlyJk

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

# 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

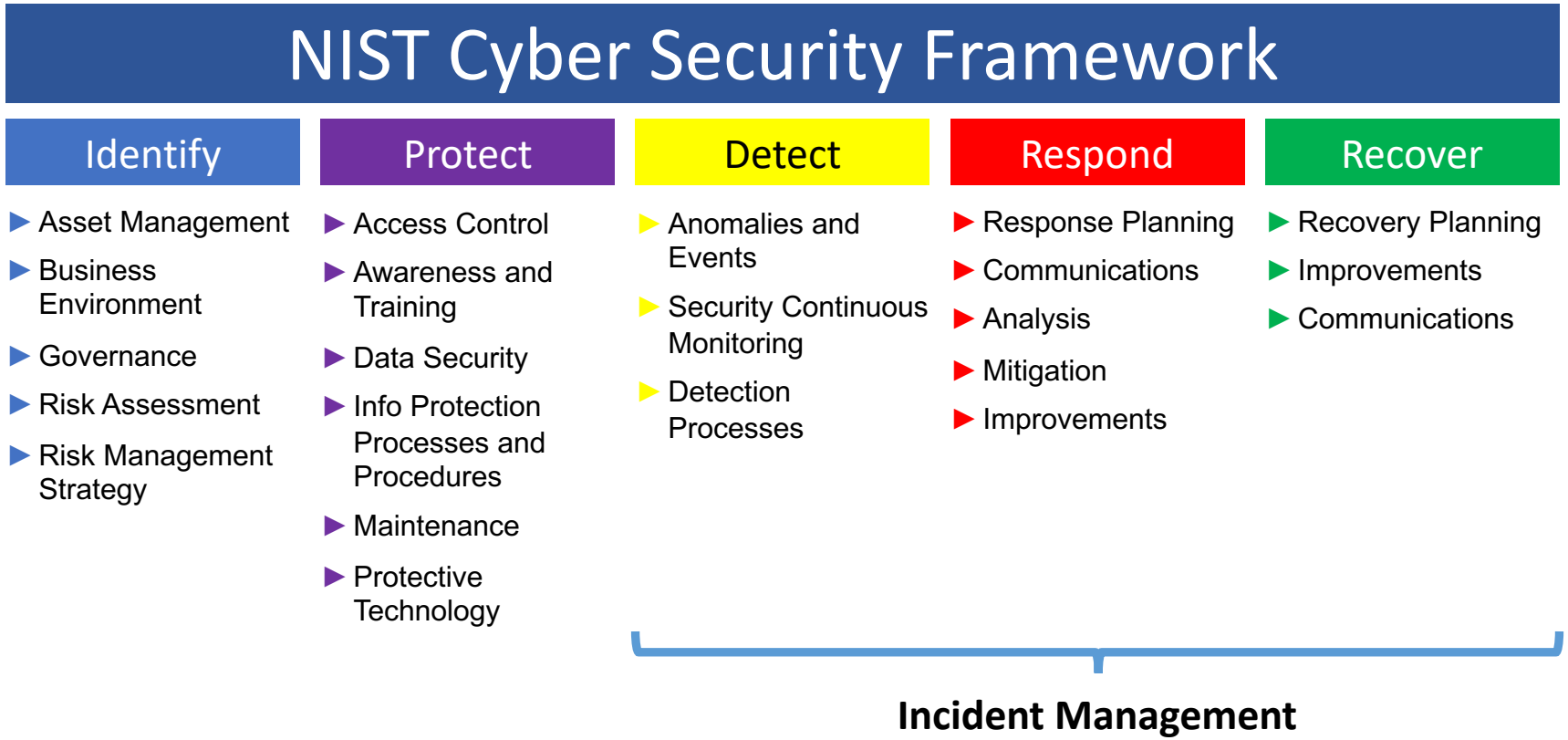
# Ética e Impactos na Sociedade:
# **Sempre Há Consequências Não Previstas**

**Não é porque dá para fazer, que se deve fazer!**

- sempre pense sobre os impactos éticos e de segurança de uma nova tecnologia
- assuma que alguém vai abusar a tecnologia que você está criando

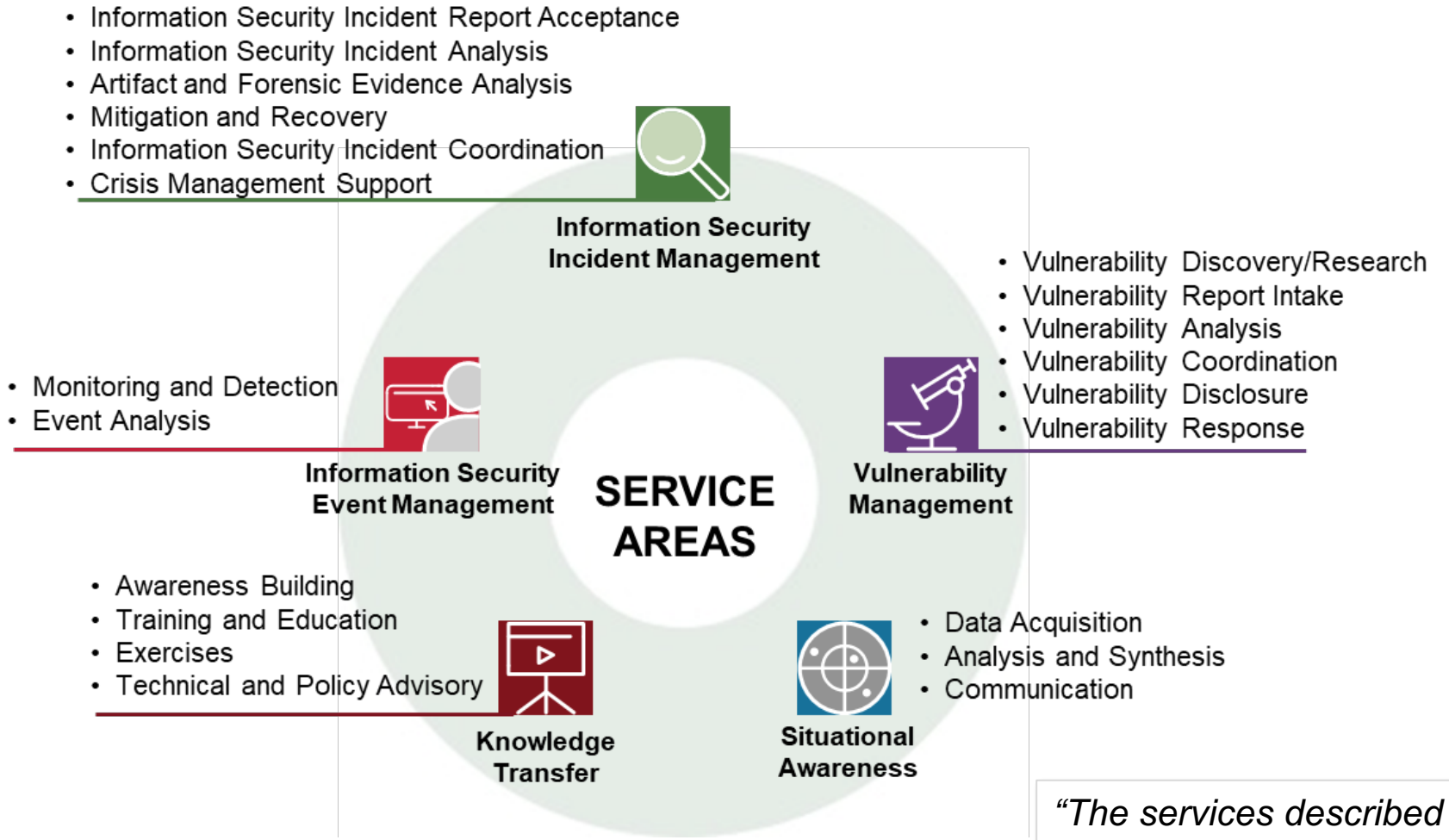
Sempre se pergunte: **O que poderia dar errado?**

# Depois do Básico, Importante Cobrir os Outros 20%:
# **Há diversos *frameworks* para organizar as ações**




**Original em Inglês e tradução para o Português disponíveis em:**
https://www.nist.gov/cyberframework/framework
https://www.uschamber.com/sites/default/files/intl_nist_framework_portugese_finalfull_web.pdf

# Gestão de Incidentes é Parte da Maturidade:
# **CSIRTs Atuam Além da Gestão de Incidentes**




***Computer Security Incident Response Team (CSIRT) Services Framework*:**
https://www.first.org/standards/frameworks/csirts/

*"The services described are those potential services a CSIRT could provide. No CSIRT is expected to provide all described services."*

# Todos Tem um Papel na Segurança e Proteção de Dados: **Ecossistema é Complexo e Interdependente**


**Quase tudo é *software* e está conectado à Internet**

**Ataques são constantes**

- Motivações diversas
- Volume crescente
  - ferramentas facilitam a perpetração por atacantes não especializados

**Organizações precisam**

- Operar mesmo sob ataque
- Estar preparadas para lidar com estes ataques

**Melhora do cenário depende de cada ator fazer sua parte**

# Precisamos um Ecossistema mais Saudável:
# **Faça a sua parte!**

PROGRAMA INTERNET +SEGURA


https://bcp.nic.br/i+seg

# Conscientização de Todos é Essencial:
# **Portal InternetSegura.br – materiais gratuitos**

# Cartilha de Segurança para Internet:
# **Fascículos e Slides para Palestras e Treinamento**

**Conteúdo disponível *online* gratuitamente sob Licença *Creative Commons***

- **Fascículos** que cobrem assuntos específicos relacionados com segurança na Internet
- ***Slides*** sobre cada um dos temas, que podem ser utilizados, por exemplo, para dar aulas ou palestras de conscientização
  - Dica do dia no *site*, via *Twitter* e RSS
  - Impressões em pequena escala enviadas a escolas e centros de inclusão digital
  - Possível gerar versões personalizadas com logo da instituição

    Exemplos de parceiros de impressão e distribuição:

    Itaipu, Eletronuclear, ELO, Microsoft, Procergs e Metrô SP



https://cartilha.cert.br/

# Obrigada

cristine@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br