nic.br cgi.br | cert.br

ITK 2021 DIGITAL – II INNOVATION TECH KNOWLEDGE

07 de outubro 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/

Desafios para Atingir a Segurança e a Proteção de Dados Adequadas

Dra. Cristine Hoepers
Gerente Geral, CERT.br/NIC.br
cristine@cert.br

cert.br nic.br cgi.br

internationalit.com

https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/... | Brasil terá maior exercício de defesa cibernética do hemisfério sul

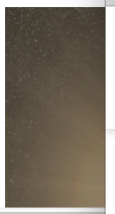
contato@internationalit.com

internationalIT PT HOME SOLUÇÕES SERVIÇOS BLOG CONTATO

International IT · Ago 5 · 3 min para ler

Brasil terá maior exercício de defesa cibernética do hemisfério sul

O Exercício Guardião Cibernético 3.0 é coordenado pelo Comando de Defesa Cibernética (ComDCiber) e faz parte da estratégia nacional de segurança do país. O SENAI, a Cisco e a RustCon vão apoiar o treinamento de cibersegurança para 350 pessoas de 58 organizações públicas e privadas que será realizado pelo Ministério da Defesa.



bcb.gov.br

BANCO CENTRAL DO BRASIL

RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018

Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

O Banco Central do Brasil, na forma do art. 9º da Lei nº 4.595, de 31 de dezembro de 1964, [illegible] de 2015, 7 1965, 7 10.194, 2009,

www.gov.br

Governo Digital

Estratégia Nacional de Segurança Cibernética

Publicado em 11/08/2021 15h13 | Atualizado em 12/08/2021 14h30 Compartilhe:

A **Estratégia Nacional de Segurança Cibernética - E-Ciber** é um conjunto de ações estratégicas do governo federal relacionadas a área de segurança cibernética até 2023. Corresponde ao primeiro módulo da Estratégia Nacional de Segurança da Informação estabelecendo ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto.

> *A E-Ciber orienta a sociedade brasileira sobre as principais ações do governo federal, em termos nacionais e internacionais, na área da*

www.gov.br

Agência Nacional de Telecomunicações

REGULAMENTAÇÃO

Anatel aprova Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações

Normativo entrará em vigor em janeiro de 2021 e prestadoras terão 180 para se adaptarem

Publicado em 17/12/2020 19h17 | Atualizado em 18/12/2020 11h20 Compartilhe:

Optiv Cybersecurity Technology Map

Navigate Cybersecurity at Optiv.com

Navigating the Security Landscape

So much technology. So many vendors. Who does what?

https://www.optiv.com/navigating-security-landscape-guide-technologies-and-providers

olhardigital.com.br

MENU

OLHAR DIGITAL

STJ se restabelece após ransomware; PF investiga cópia de dados

Renato Santino | 13/11/2020 21h45, atualizada em 13/11/2020 21h50

Os estra
Superio
totalme
investig
extensã
arquivos

infomoney.com.br

InfoMoney

O "lado B" da digitalização

Fleury é o mais recente episódio de ransomware; veja como os ataques cibernéticos têm afetado os mercados

Vistos como algumas das maiores ameaças da era atual, sequestros de dados, ou ransomware, viram novo risco a ser monitorado no mercado

ara Riz
2021 08h4

www1.folha.uol.com.br

JBS pagou US$ 11 mi em resposta a ataque ransomware em operações na América do Norte

Empresa cancelou turnos em fábricas nos EUA e Canadá na semana passada, após ser afetada por ciberataque

9.jun.2021 às 21h26

Ouvir o texto A- A+

REUTERS A JBS USA, subsidiária da brasileira JBS nos Estados Unidos, confirmou em comunicado divulgado nesta quarta-feira (9) que pagou o equivalente a US$ 11 milhões (R$ 55,5 milhões) em resposta a um ataque hacker contra suas operações

poder360.com.br

PODER 360 Diretor Fernando Rodrigues

Renner diz não ter pago resgate de dados depois de ataque hacker

A varejista sofreu uma invasão na última 5ª feira (19.ago.2021), mas informou que principais bancos de dados estão preservados

Compartilhe

DC police surveillance cameras were infected with ransomware before inauguration

Malware seized 70 percent of DC police DVRs a week before Trump's inauguration.

SEAN GALLAGHER - 1/30/2017, 5:12 PM

system just one week before Inauguration Day. *The Washington Post* reports that 70 percent of the DVR systems used by the surveillance network were infected with ransomware, rendering them inoperable for four days and crippling the city's ability to monitor public spaces.

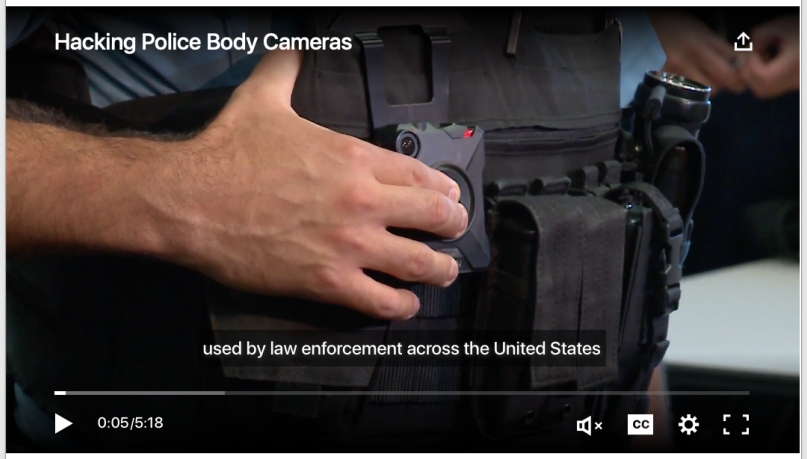
wired.com

WIRED BUSINESS CULTURE GEAR MORE SUBSCRIBE

LILY HAY NEWMAN SECURITY 08.11.2018 03:00 PM

Police Bodycams Can Be Hacked to Doctor Footage

Analysis of five body camera models marketed to police departments details vulnerabilities could let a hacker manipulate footage.

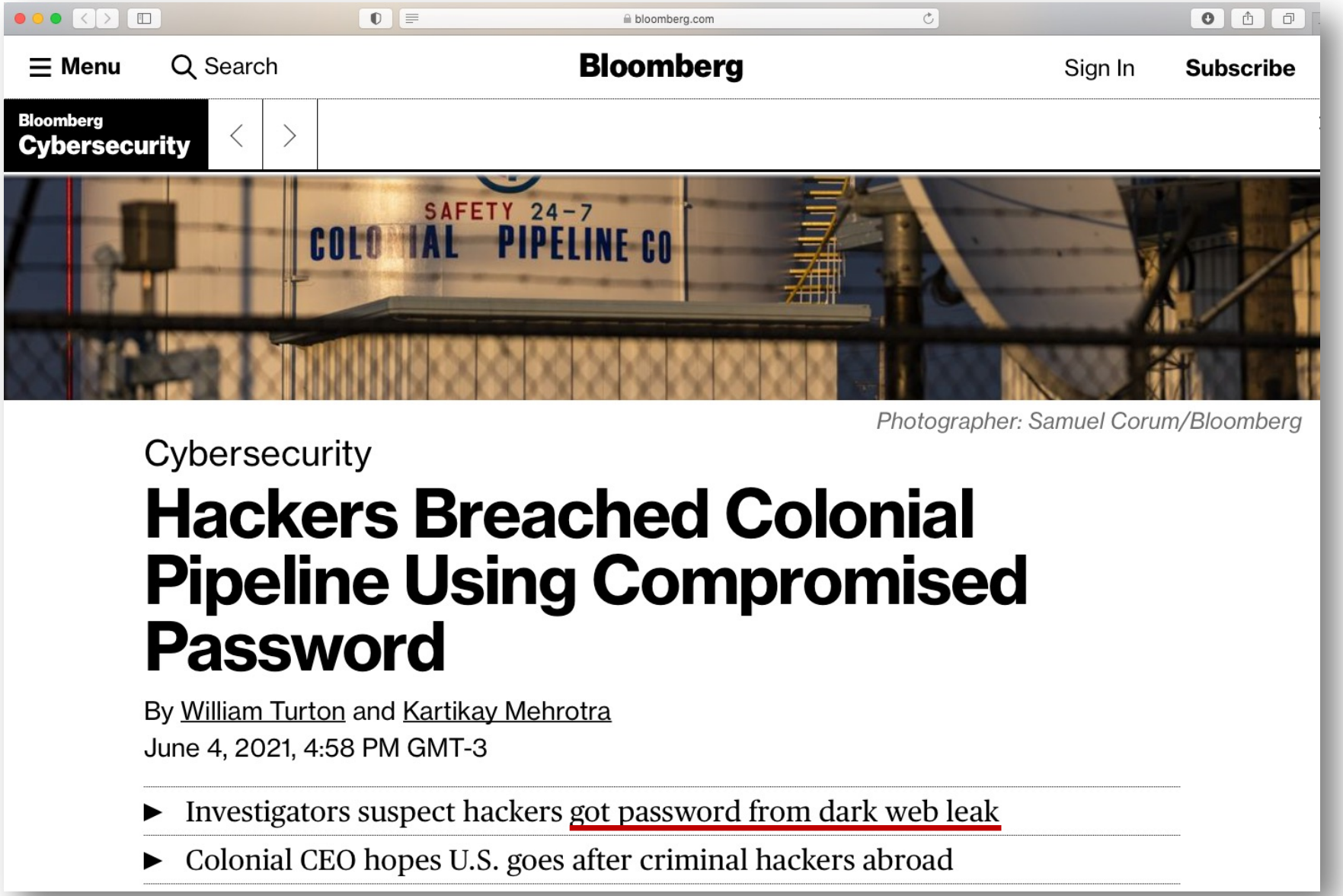


As they proliferate, police body cameras have courted controversy because of the contentious nature of the footage they capture and questions about how accessible those recordings should be.

But when it comes to the devices themselves, the most crucial function they

3 FREE ARTICLES LEFT THIS MONTH | Subscribe

https://arstechnica.com/security/2017/01/dc-police-surveillance-cameras-were-infected-with-ransomware-before-inauguration/
https://www.wired.com/story/police-body-camera-vulnerabilities/



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

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/

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

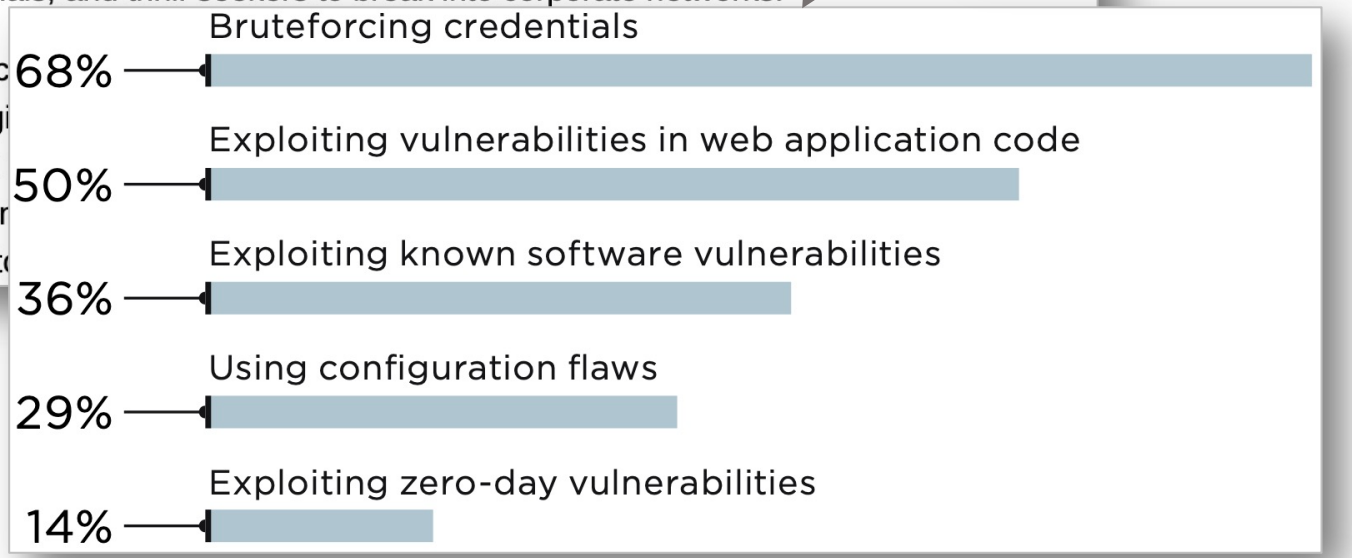
Three little words: Patches, passwords, policies

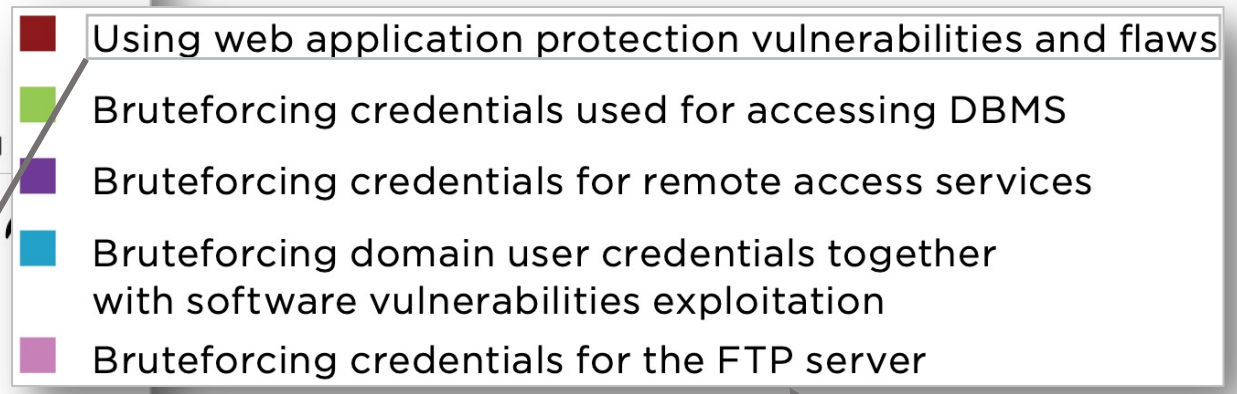
Thu 13 Aug 2020 // 07:06 UTC 31

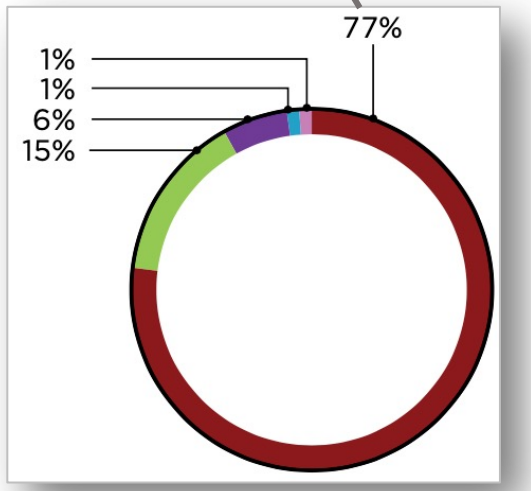
Shaun Nichols in San Francisco BIO EMAIL TWITTER

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

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

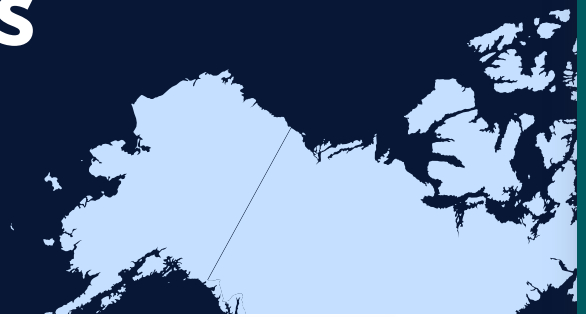
Since a website's source code can be accessed and reviewed by anyone pressing F12 inside their browser, Estadao reporters searched for similar issues in other government sites.

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/

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.

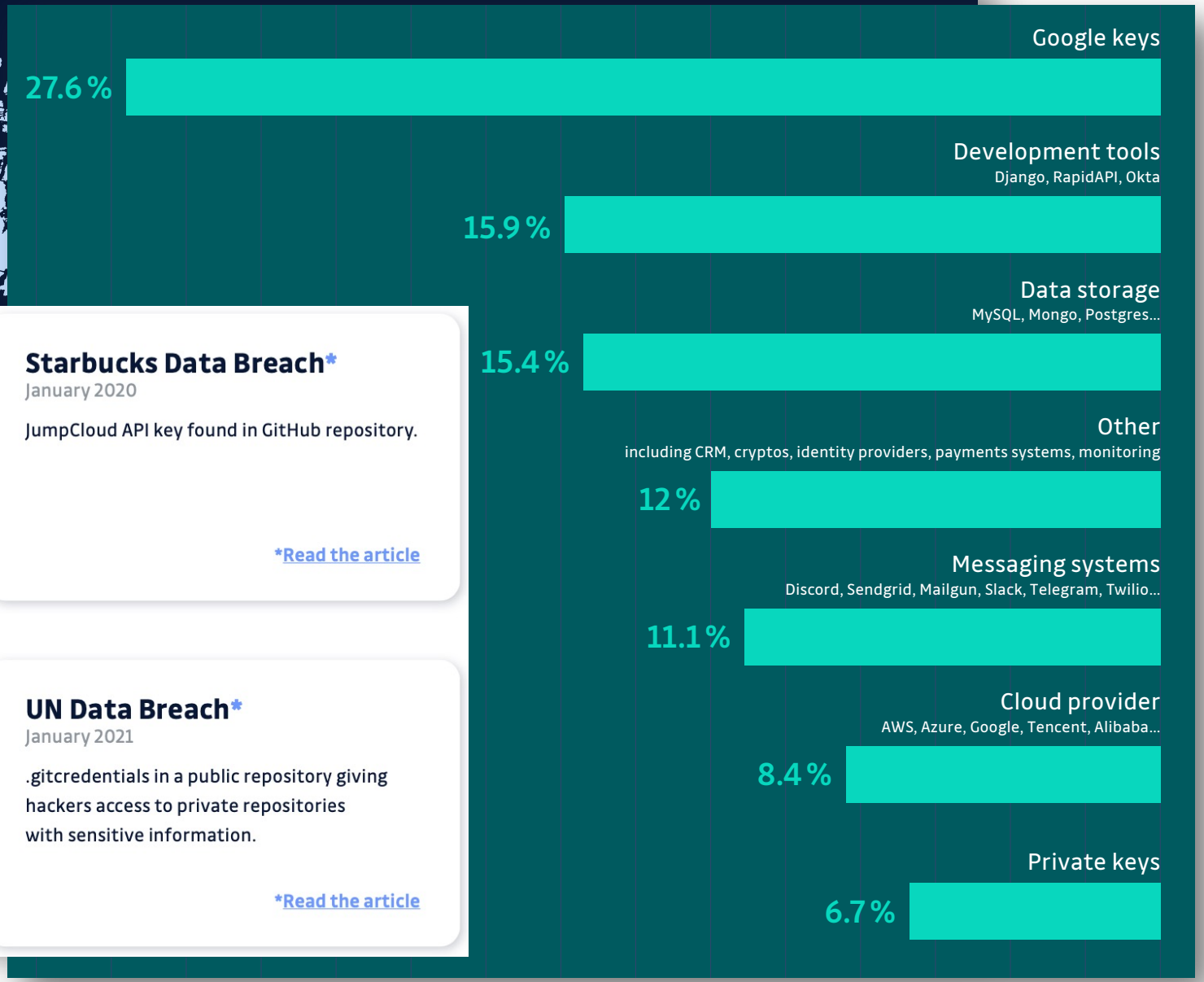
*Read the article

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/

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

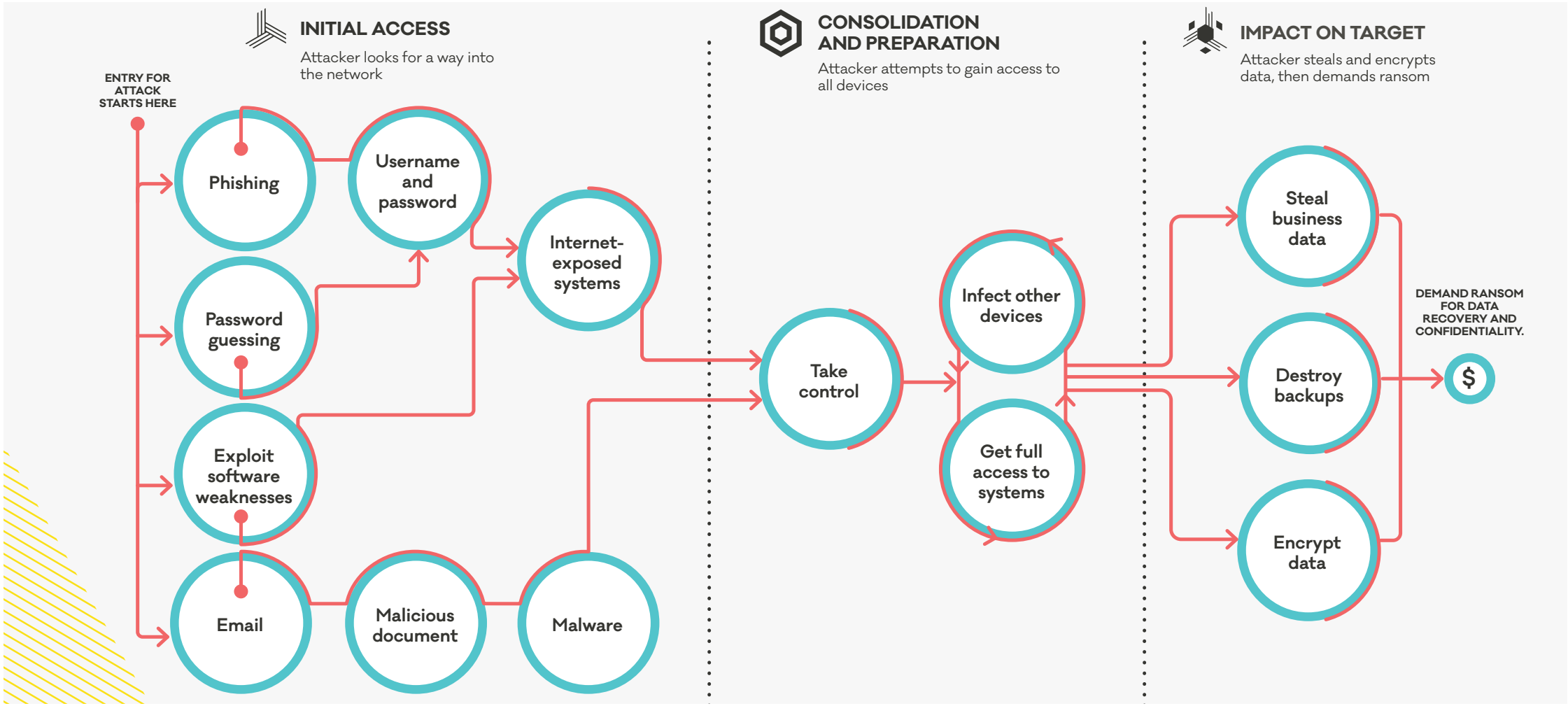
49% of payment apps are vulnerable to encryption key extraction

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

Resumo do diagnóstico da Microsoft sobre causas dos ataques: **CERT NZ How Ransomware Works**



https://www.cert.govt.nz/business/guides/protecting-from-ransomware/
https://docs.microsoft.com/en-us/security/compass/human-operated-ransomware

Precisamos Cuidar do Básico Primeiro:
Causas Mais Comuns de Invasões e Vazamentos de Dados

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

- Acesso indevido via **senhas fracas ou comprometidas/vazadas**
  - Senhas expostas no Github/Pastebin pelos próprios donos/desenvolvedores dos sistemas
  - Força bruta de senhas em serviços protegidos só com conta e senha. Exemplos:
    - *e-mails* e serviços em nuvem
    - acesso remoto (VPN, SSH, RDP, Winbox, etc)
    - gestão remota de ativos de rede e servidores
- Exploração de **vulnerabilidades antigas** para invasão e/ou movimentação lateral
  - falta de aplicação de correções
  - erros de configuração
  - falta/falha de processos

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

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

Todos Tem um Papel na Segurança:
Ecossistema é Complexo e Interdependente

Quase tudo é *software* e está conectado à Internet

Ataques são constantes

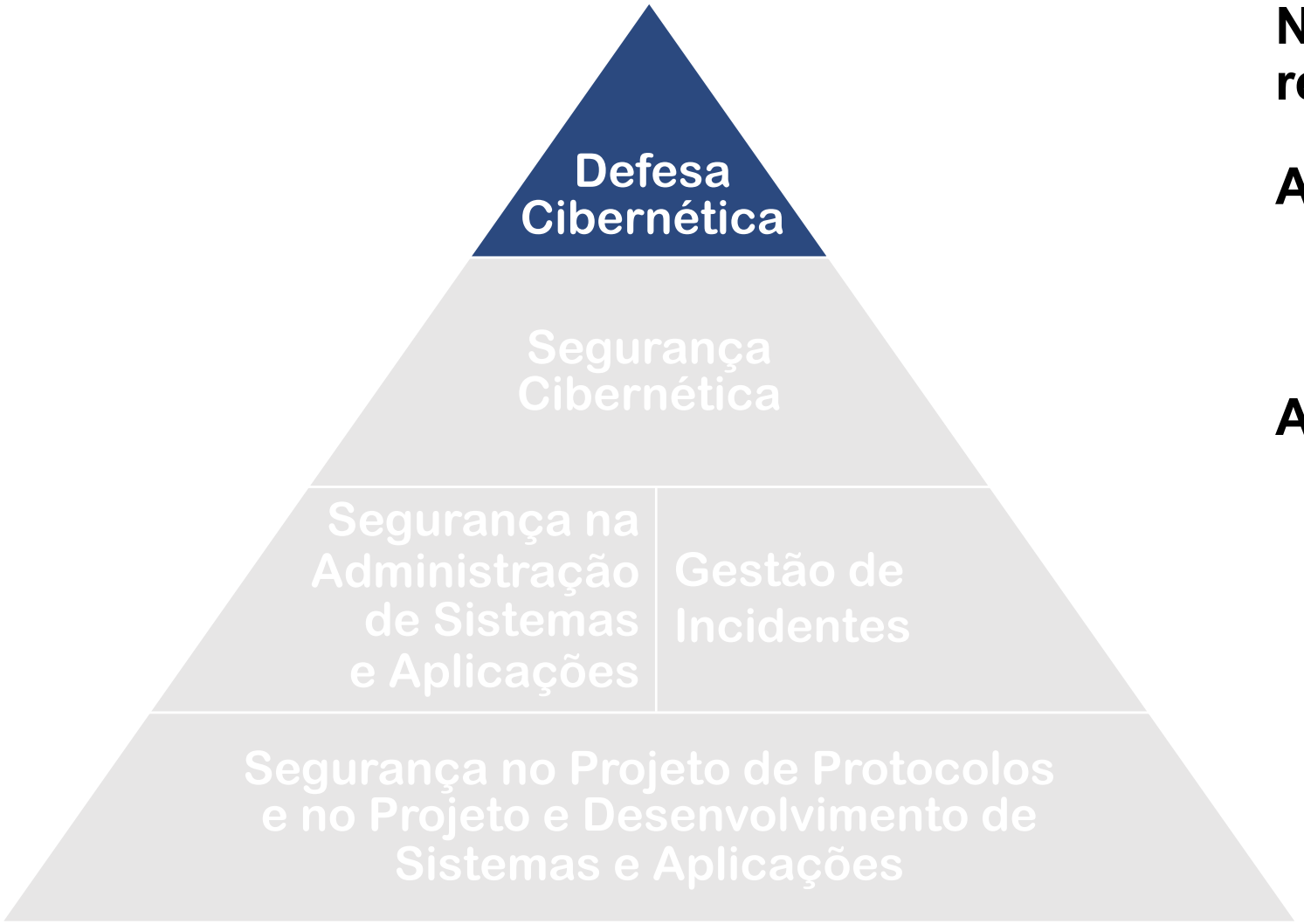
- Motivações diversas
- Volume crescente
  - ferramentas facilitam a perpetração por atacantes não especializados

Organizações precisam

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

Melhora do cenário depende de cada ator fazer sua parte

A Defesa Cibernética é um Nicho Especializado mas a Eficácia Dependerá das Ações de Todos os Atores



Nenhum grupo ou estrutura resolverá o problema sozinho

A segurança se faz nas "pontas"

- depende de *software* seguro
- depende de redes resilientes

As "pontas" não conseguem

- coletar inteligência sobre ataques vindos de outras nações
- dedicar recursos para estudar vetores de ataques de baixa probabilidade mas altíssimo impacto

Efetividade das Soluções e Ferramentas de Segurança Depende da Base Sólida

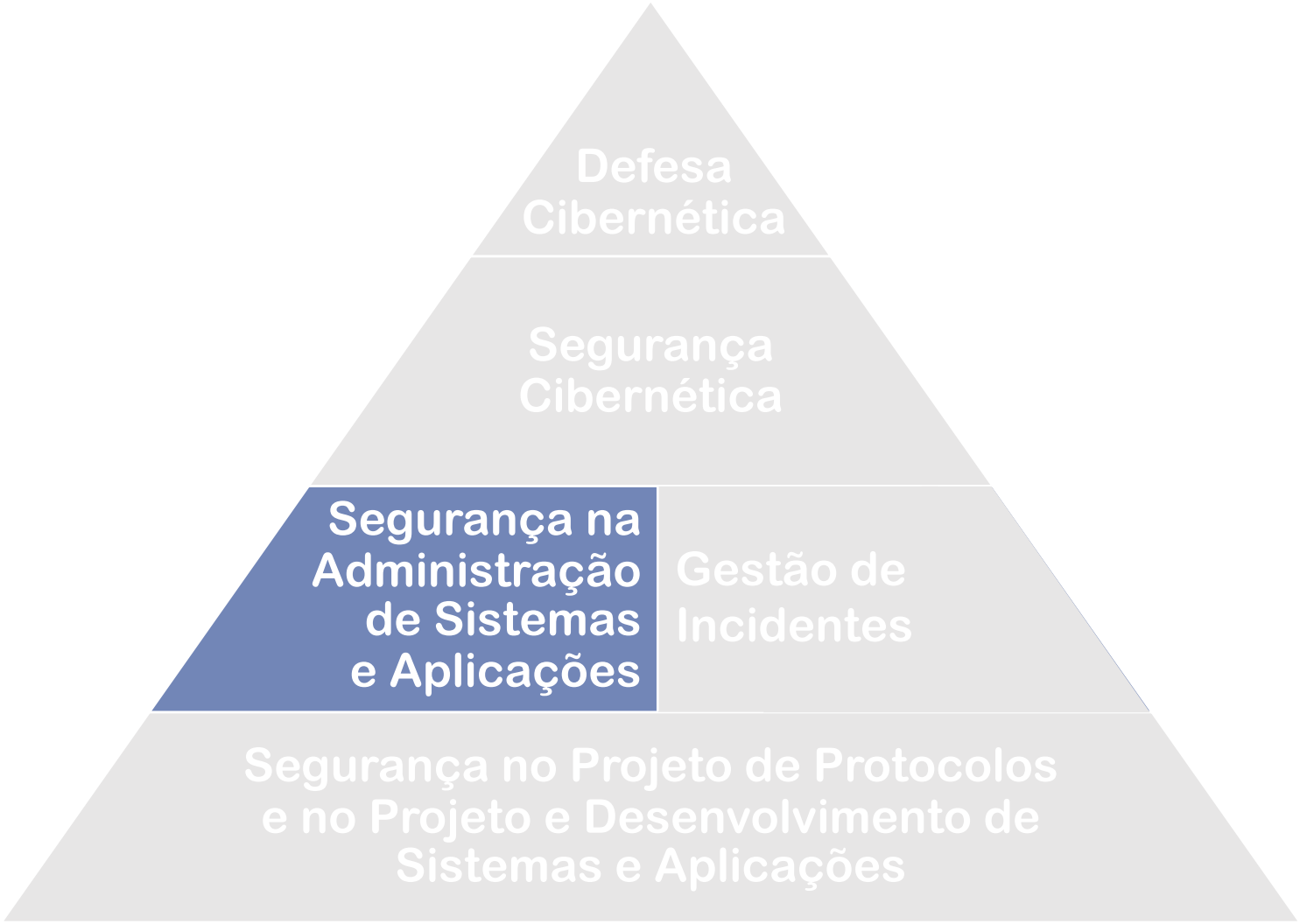
Segurança depende de

- Sistemas menos vulneráveis
- Ambiente bem projetado para permitir uso adequado das ferramentas
- Cooperação de todos os atores: gestores, usuários e outros profissionais de tecnologia da informação

Impossível segurança 100%

- Proteger o que é mais crítico
- Conscientizar e educar
  - usuários
  - profissionais

A Implantação das Tecnologias Precisa Focar em Boas Práticas de Segurança



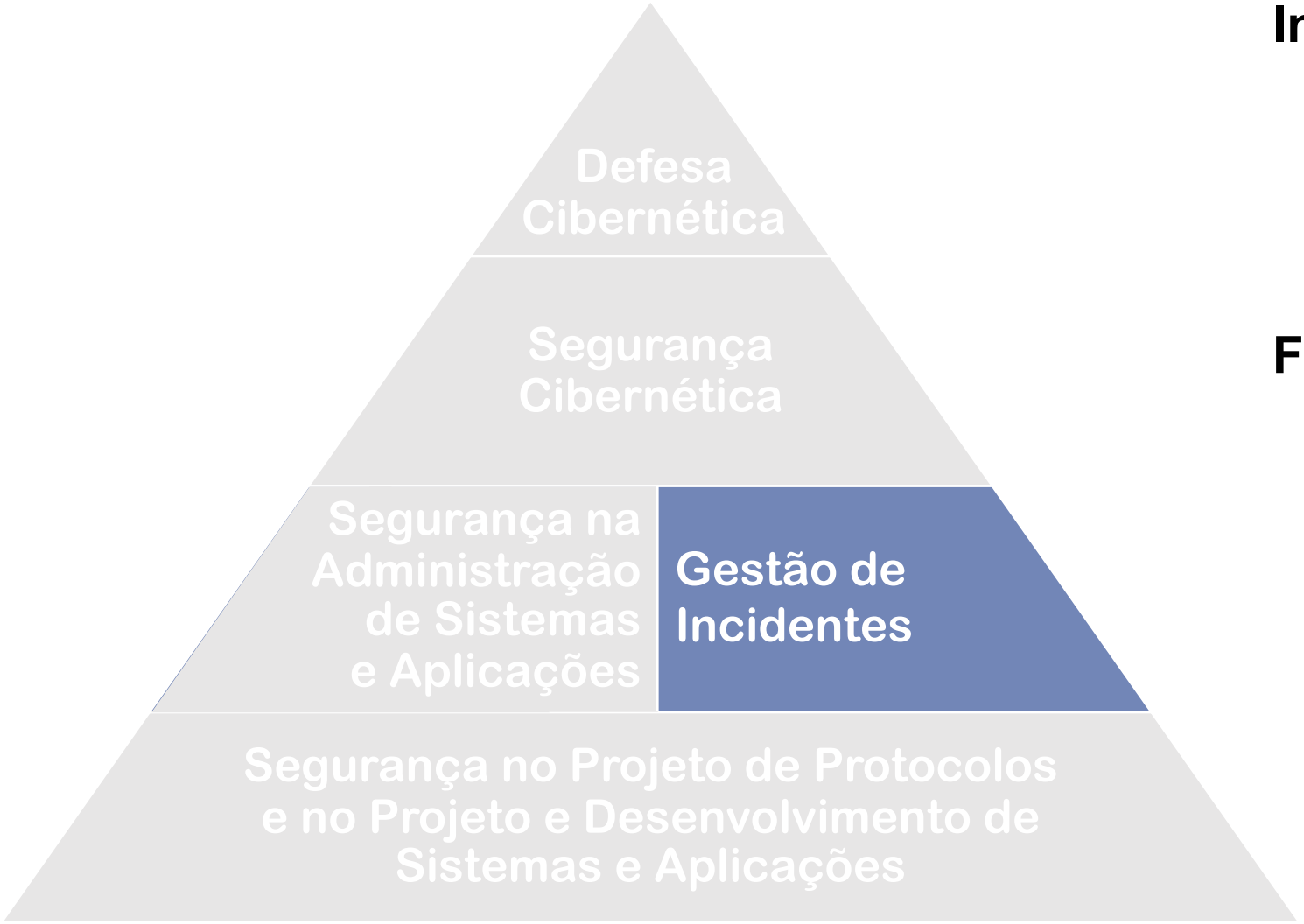
Desafios

- Sistemas com muitos problemas
  - vulnerabilidades
  - sem instrumentação para permitir configurações mais seguras
- Poucos profissionais com sólidos conhecimentos de Internet
- Complexidade dos ambientes

Necessário Seguir Boas Práticas Globais (como MANRS)

- Aumentam a segurança
- Mantém a interoperabilidade
  - essencial para inovação e desenvolvimento

O Tratamento Ágil e Adequado Reduz Danos e Vítimas



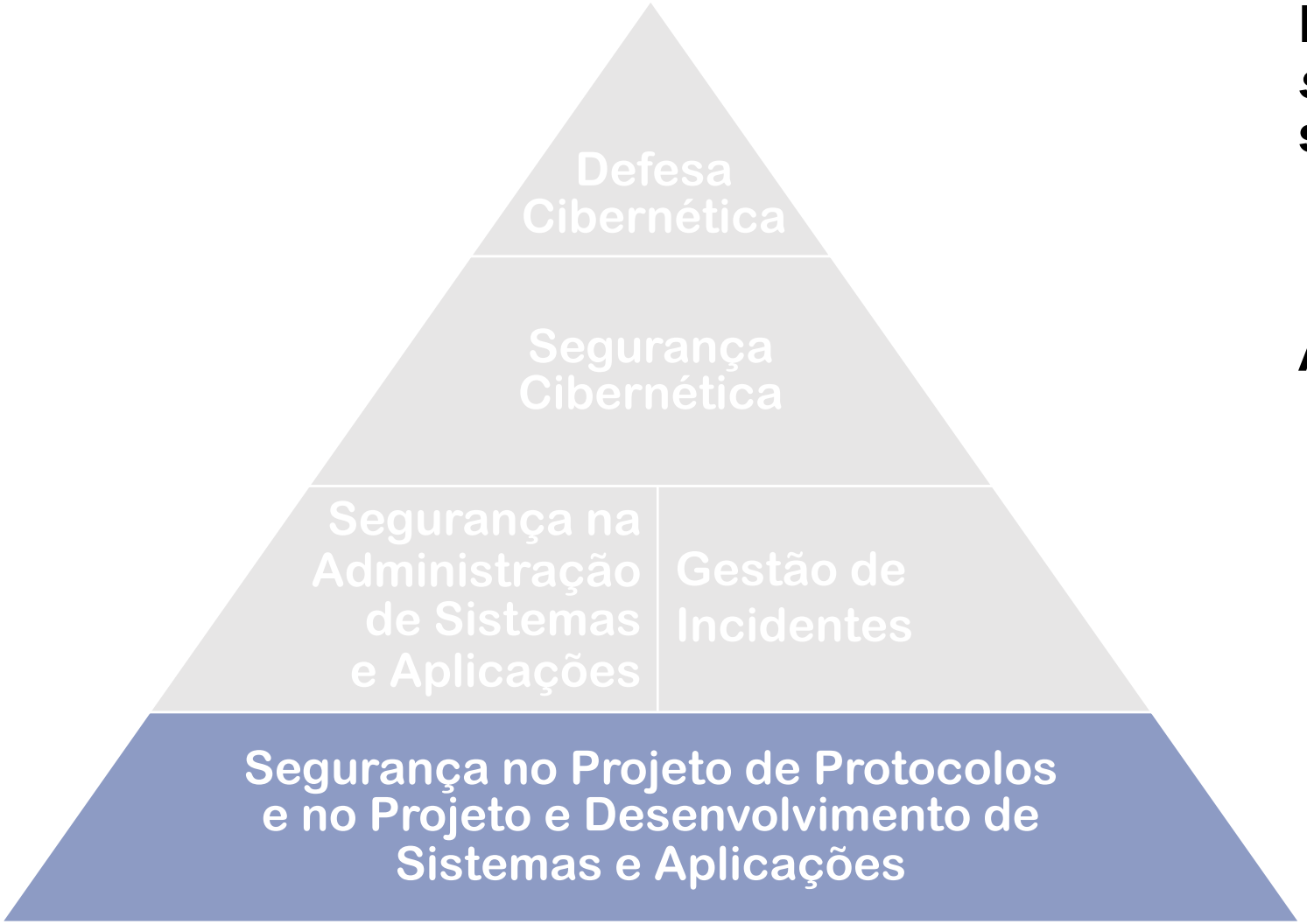
Incidentes ocorrerão

- Ataques novos todos os dias
- Complexidade dos ambientes dificulta proteção e detecção

Foco do CERT.br nos últimos 24 anos

- Aumentar os níveis de segurança e resiliência das redes brasileiras conectadas à Internet
- Fomentar a criação de CSIRTs (Grupos de Tratamento de Incidentes)
- Treinar profissionais na área
- Criar massa crítica para uma comunidade nacional ativa
- Influenciar padrões globais

O Desenvolvimento Precisa Ser Sólido para Reduzir a Superfície de Ataque



Postura dos desenvolvedores de *software* deve considerar segurança

- não se pode pensar “que alguém vai cuidar da segurança depois”

Atores chave para melhora da base

- Professores das áreas de Eng. de *Software* e Programação
- Empresas de *Software* e *Hardware*
  - definir requisitos mínimos de segurança
  - fugir de certificações de *software*
- MEC, Capes, CNPq, MCTIC

Atuação do NIC.br e do Comitê Gestor da Internet no Brasil: **Ajudar Construir um Ecossistema Internet mais Saudável**

Princípios para a Governança e Uso da Internet:

8. Funcionalidade, segurança e estabilidade

A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.

https://principios.cgi.br/

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

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