

nic.br egi.br

cert.br

IX Fórum Regional – Edição Especial On-line
20 de março de 2020
São Paulo / SP

O Ano é 2020!

Hora de Modernizar a sua Presença na Internet

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

Dr. Klaus Steding-Jessen
Gerente Técnico
jessen@cert.br

cert.br **nic.br** **egi.br**

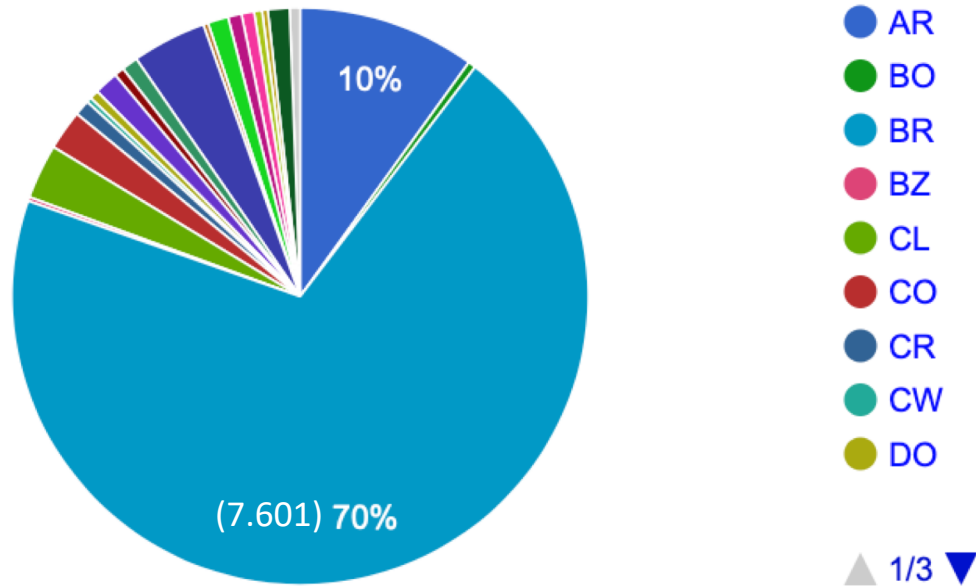
**Antes de falar de segurança:
em qual ecossistema
estamos conectados?**

cert.br nic.br egi.br

Internet no Brasil em Números: Redes Autônomas, Provedores e Interconexão de Tráfego

Alocação de Sistemas Autônomos na América Latina e Caribe

Distribution of ASN per country



Fonte: <https://www.lacnic.net/en/web/lacnic/estadisticas-asignacion>

Dados atualizados em 19 de março de 2020

Provedores de Acesso

- Total de ISPs (estimado): 6.618
- Respondentes: 2.177
- 75% tem 1.000 clientes ou menos

Fonte: <https://www.cetic.br/pesquisa/provedores/>

Interconexão de tráfego

IX.br São Paulo - um dos maiores *Internet eXchanges* do mundo

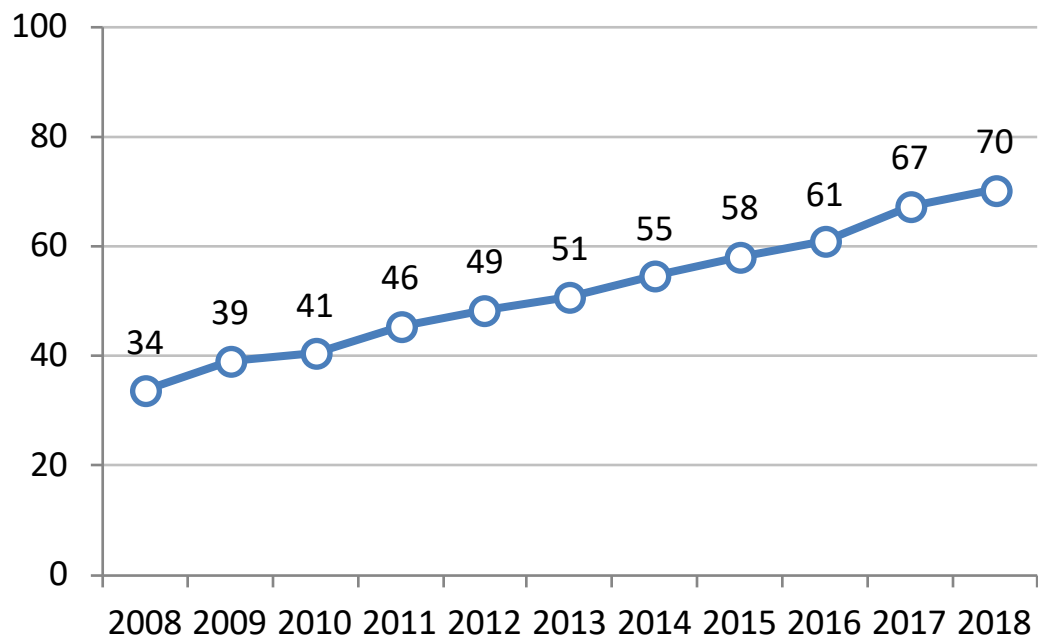
- nº 1 em participantes (1.724)
- nº 3 em pico de tráfego (7.6Tbps) e em média de tráfego (4.78Tbps)

Fonte: <https://www.pch.net/ixp/dir>

Internet no Brasil em Números: Usuários e Dispositivos Utilizados

Usuários de Internet

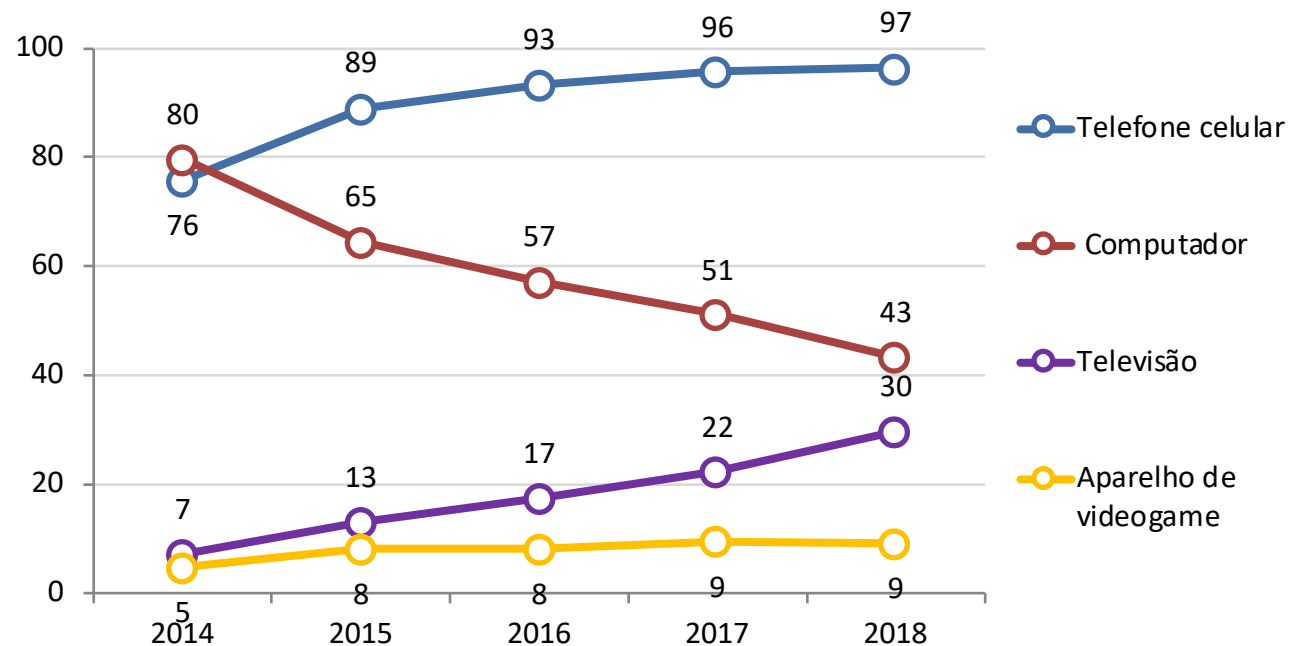
Porcentagem do total da população



126,9 milhões de usuários de Internet
(utilizaram a Internet há menos de 3 meses)

Dispositivo Utilizado para Acesso Individual

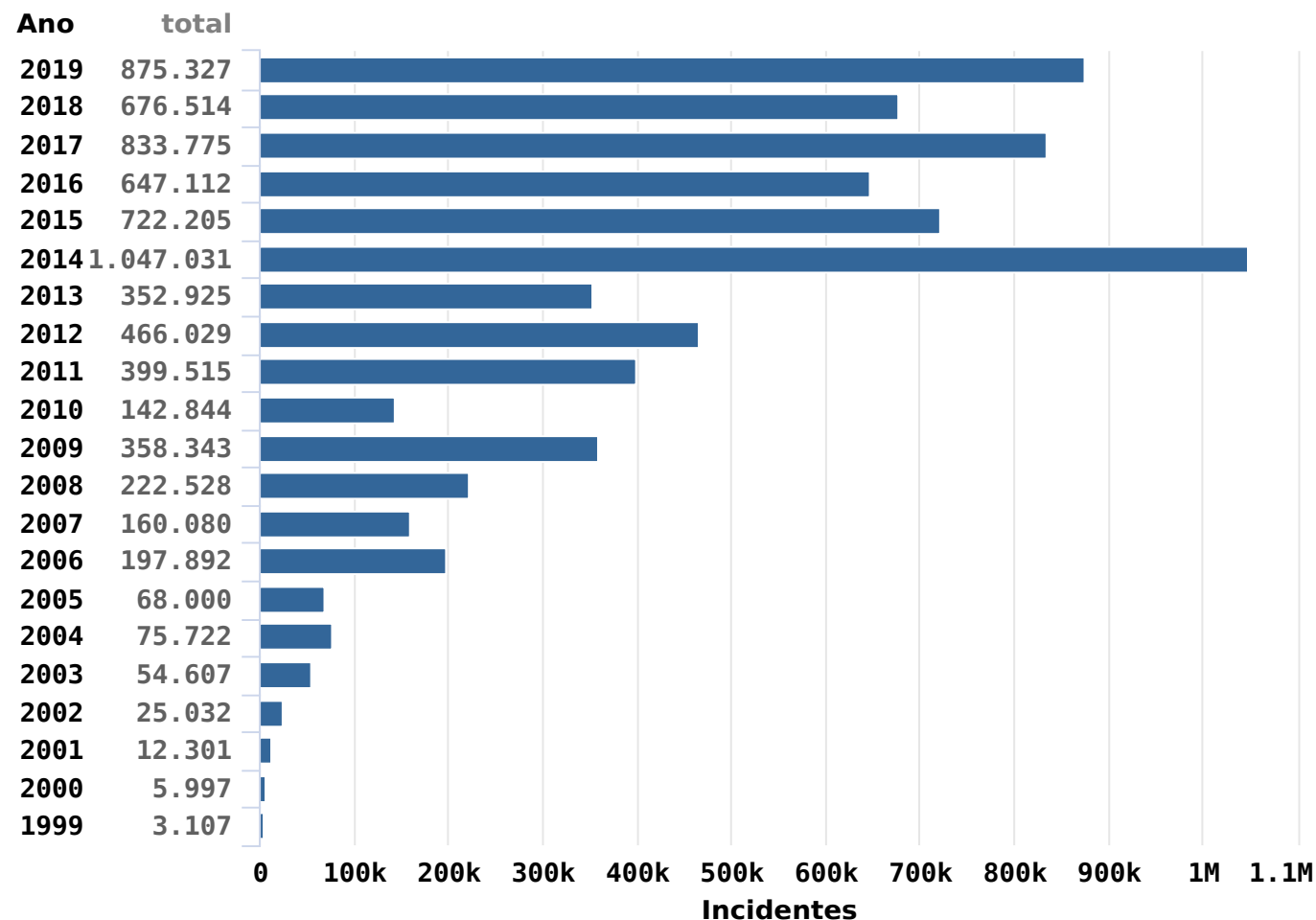
Porcentagem do total de usuários de Internet



Fonte: CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros – TIC Domicílios 2018.
<https://www.cetic.br/pesquisa/domicilios/indicadores>

Incidentes Reportados Voluntariamente para o CERT.br: Dados Totais de 1999 a 2019

Total de Incidentes Reportados ao CERT.br por Ano



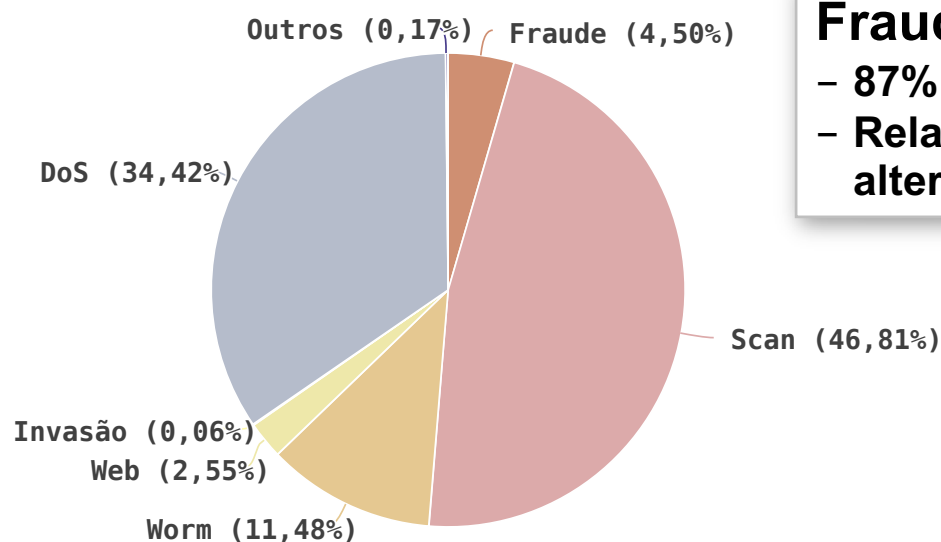
© CERT.br -- by Highcharts.com

Ataques mais comuns no último ano

- DDoS a partir de Internet das coisas
 - Câmeras, *Smartphones*, Roteadores e *Modems* de banda larga/Wi-Fi, TVs
 - Infectados e sendo usados para DDoS e também para:
 - minerar criptomoedas
 - fazer fraudes contra os usuários
- Comprometimento de credenciais
 - Principalmente *e-mails*
 - via ataques de força bruta contra Webmail, POP, IMAP e SMTP
 - via infecção de computadores, celulares e roteadores de banda larga

Fonte: <https://www.cert.br/stats/incidentes/>

Incidentes Reportados para o CERT.br : Detalhes sobre os tipos de incidentes vistos em 2019

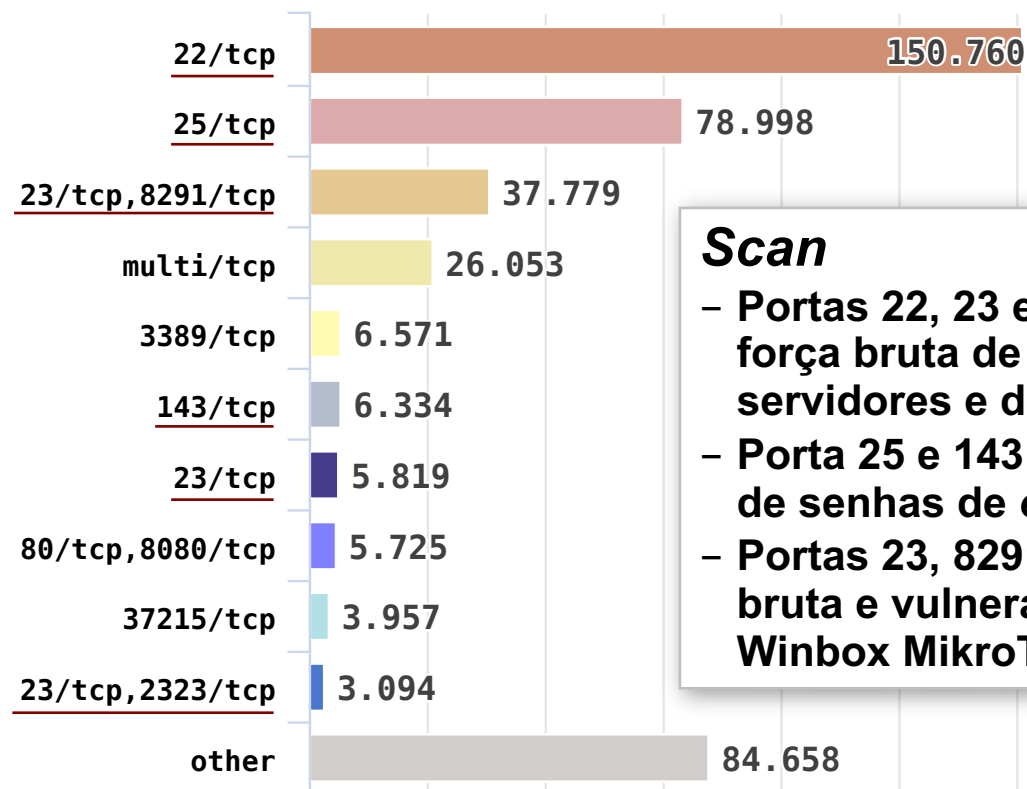


Fraude

- 87% são páginas falsas (*phishing*)
- Relacionadas com invasão de CPEs para alterar o DNS

DDoS

- Aumentou de patamar em 2014
- Maior número em 2019
- 300Gbps é o "normal"
- Tipos mais frequentes
 - . *botnets* IoT
 - . amplificação de tráfego



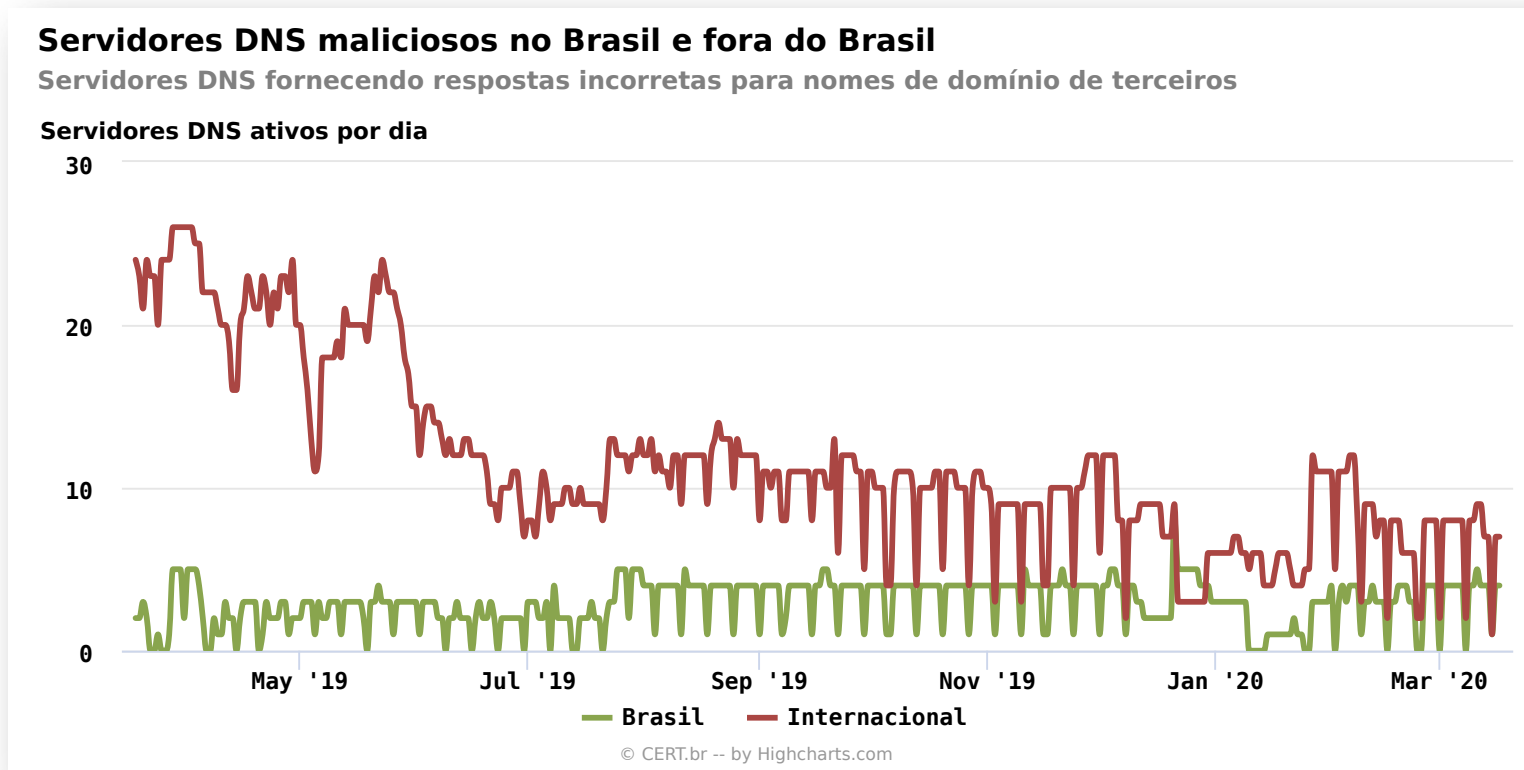
Scan

- Portas 22, 23 e 23, 2323: força bruta de senhas de servidores e de IoT
- Porta 25 e 143: força bruta de senhas de *e-mail*
- Portas 23, 8291: força bruta e vulnerabilidade Winbox MikroTik

Servidores DNS Maliciosos Usados nos CPEs Invadidos: Fornecem Respostas Autoritativas Erradas

Domínios afetados dos seguintes setores:

- Bancos, Serviços de Pagamento, Serviços de *Streaming*, Mobilidade, Redes Sociais, *Webmail*, Comércio Eletrônico, entre outros



Semântica é importante ao reportar incidentes ou pedir takedown!

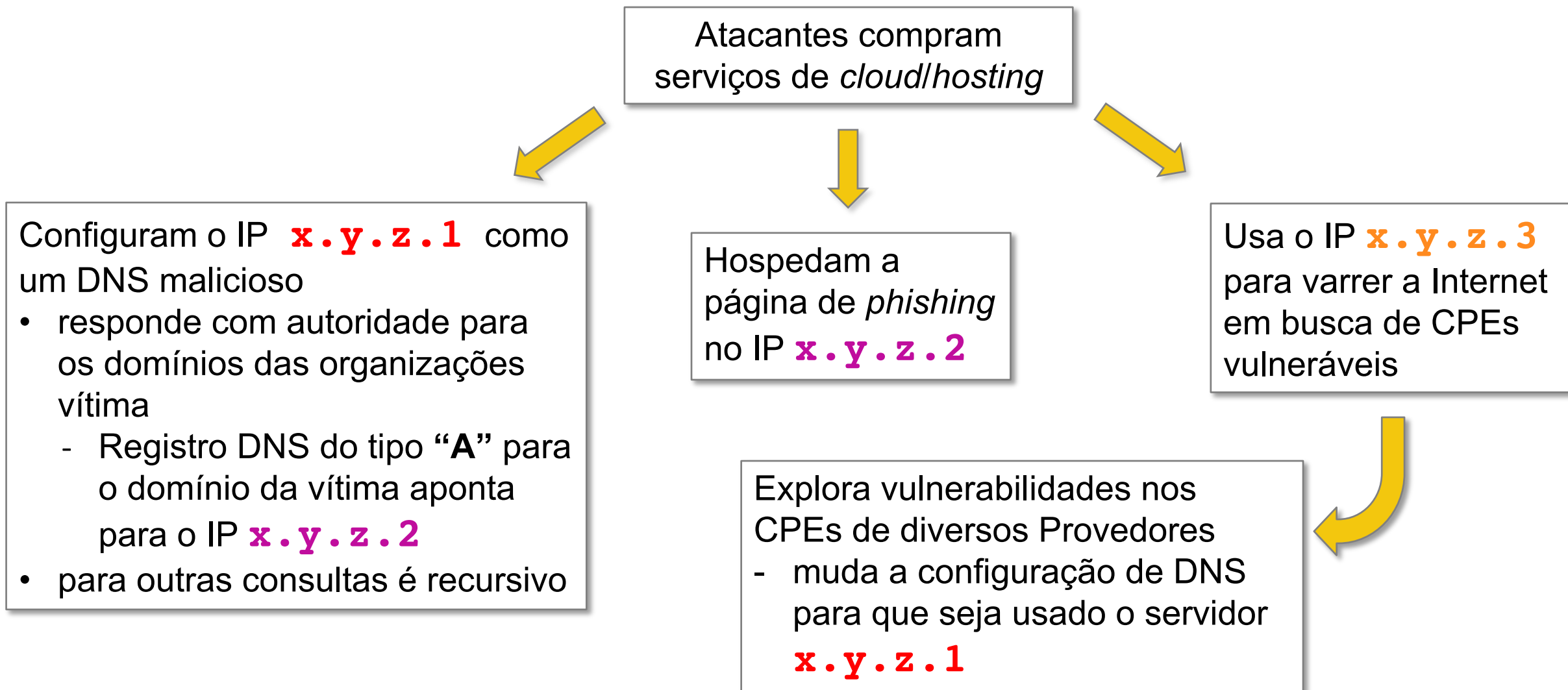
- Isto **não é** um DNS invadido
- Isto **não é** envenenamento (*cache poisoning*)
- Isto **não é** sequestro de domínio (*domain hijacking*)

Isto é um **servidor DNS malicioso** (*rogue*) sendo usado para **sequestro de DNS** (*DNS hijacking*)

- autoritativo para os domínios das vítimas
- recursivo aberto respondendo ao restante das consultas

Fonte: <https://cert.br/stats/dns-malicioso/>

Invasão de Roteadores de Banda Larga (CPEs): Anatomia do Ataque



Invasão de Roteadores de Banda Larga (CPEs): Exemplo de ataque contra o domínio gmail.com

IP **52.211.x.x** é um DNS malicioso

- responde com autoridade para o domínio **gmail.com**
 - Registro DNS do tipo “A” aponta para o IP

35.163.x.x

```
$ dig +short @52.211.x.x gmail.com A
35.163.x.x
```

- para outras consultas é recursivo

Resposta correta:

```
$ dig +short gmail.com A
172.217.29.165
```

A página de *phishing* está no IP **35.163.x.x**

```
$ curl -s -H 'Host: gmail.com' http://35.163.x.x/
<!DOCTYPE html>
<html lang="en">
[...]
<body>
[...]
<a id="link-forgot-passwd" class="need-help"
  href="#/signin/recovery?hl=en"> Esqueceu a senha? </a>
</div>
</div>
<span id="inge" style="display: none" role="alert" class="error-msg">
  Desculpe, Goole não reconhece esse email. <a href="#">Criar
  conta</a> usando esse endereço? </span>
<span id="timeoutError" style="display: none" role="alert"
  class="error-msg"> Algo deu errado. Verifique sua conexão e
  tente novamente.</span>
</form>█
[...]
```

Modernizar a presença na Internet?

O que isso tem a ver com a minha empresa? E com segurança?

cert.br nic.br egi.br

	Padrões	Vantagens da Adoção
Autenticação com Múltiplos Fatores	Tokens <ul style="list-style-type: none"> • em <i>hardware</i> (FIDO2/U2F) • em <i>software</i> (HOTP/TOTP) 	Impede sucesso de força bruta de senhas Reduz impacto do comprometimento de credenciais
Criptografia forte	HTTPS mandatório e HSTS Versões atuais de TLS <i>Forward Secrecy</i>	Garantia das transações e da proteção de dados Reduz a chance de quebra da criptografia Impede quebra de cripto de tráfego antigo capturado
Segurança de DNS	DNSSEC	Proteção contra envenenamento de <i>cache</i> Habilitar o uso de outras tecnologias como o DANE
Segurança de <i>e-mail</i>	STARTTLS <ul style="list-style-type: none"> • idealmente c/ DANE DMARC, DKIM e SPF	Proteção contra <i>sniffing</i> (“espionagem”) Aumento da reputação da mensagem legítima (ajuda a prevenir <i>phishing</i> da sua marca)
Protocolo IP	IPv6 é o atual IPv4 é legado – e já acabou <ul style="list-style-type: none"> • novas redes só terão IPv6 	Mais estabilidade <ul style="list-style-type: none"> • Não depender de CGN ou tradução v6 → v4 • Redes móveis tendem a ter IPv6 nativo no futuro Facilita o processo investigativo e de tratamento de incidentes
Segurança de roteamento	RPKI	Certificação de recursos Validação de origem no BGP

Como Testar e Onde Procurar Referências

cert.br nic.br egi.br

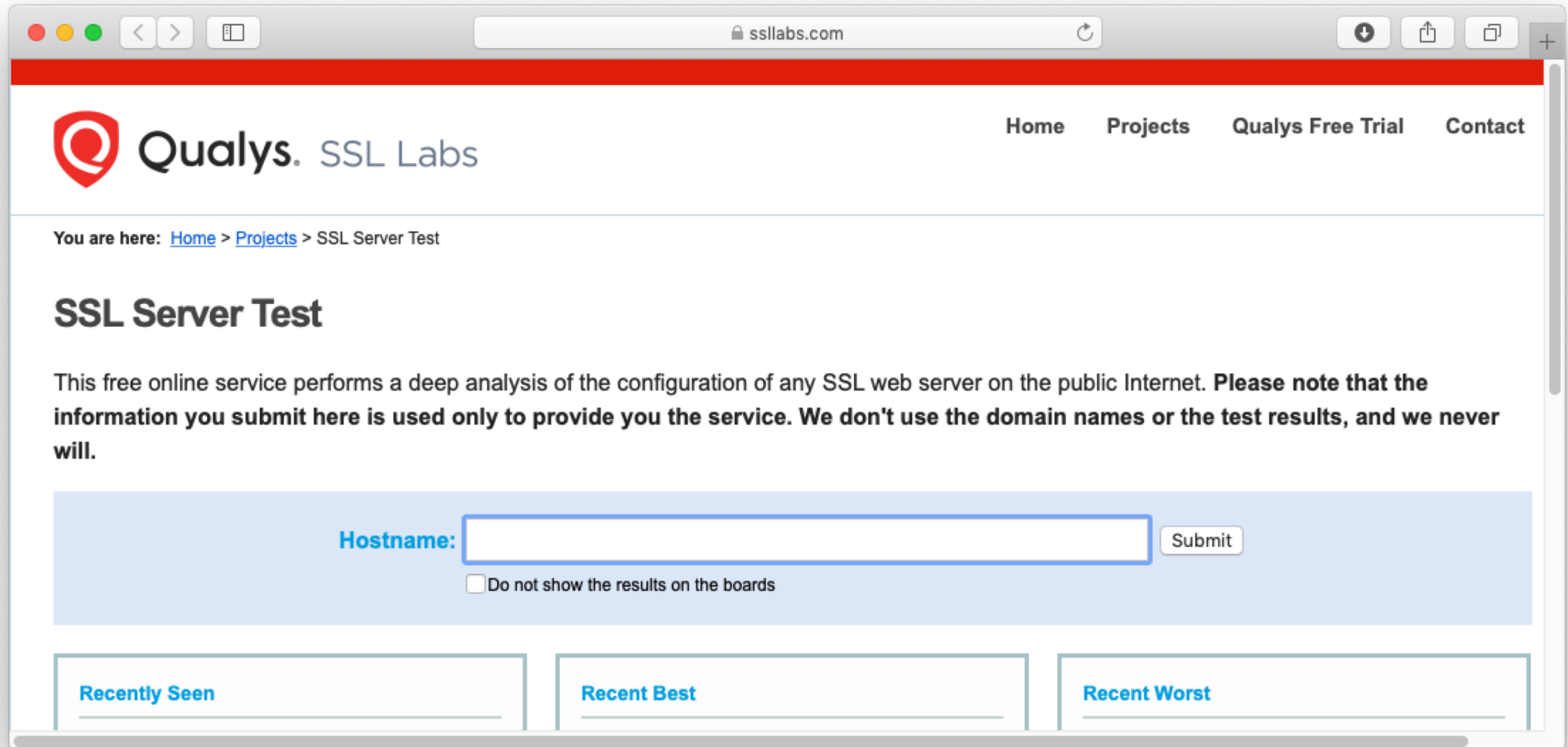
Is your Internet up to date? <https://internet.nl>

The screenshot shows a web browser window with the URL internet.nl. The page features the Internet.nl logo with the tagline "IS YOUR INTERNET UP TO DATE?". Navigation links include Home, News, Knowledge base, Hall of Fame, and About Internet.nl. A teal banner reads: "Modern Internet Standards provide for more reliability and further growth of the Internet. Are you using them?". Below this are three test sections:

- Test your website** (with a padlock icon): "Modern address? Signed domain? Secure connection? Security options?" with a link to "about the test". Input field: "Your domain name: www.example.nl". Button: "Start test".
- Test your email** (with an envelope icon): "Modern address? Signed domain? Anti-phishing? Secure connection?" with a link to "about the test". Input field: "Your email address: @ example.nl". Button: "Start test".
- Test your connection** (with a signal icon): "Modern addresses reachable? Domain signatures validated?" with a link to "about the test". Button: "Start test".

SSL Server Test

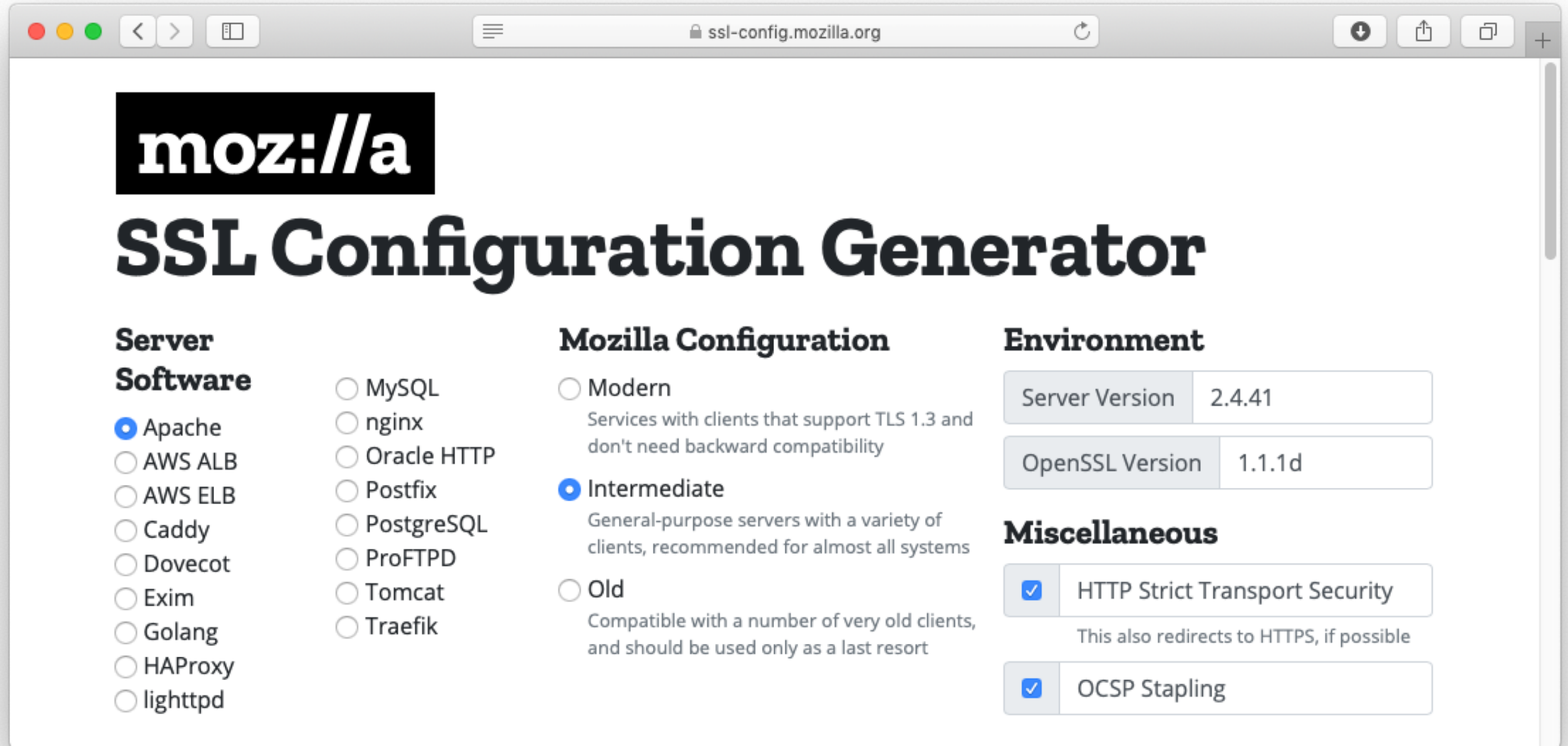
<https://www.ssllabs.com/sslltest/>



The screenshot shows a web browser window with the address bar displaying "ssllabs.com". The page header features the Qualys SSL Labs logo on the left and navigation links for "Home", "Projects", "Qualys Free Trial", and "Contact" on the right. Below the header, a breadcrumb trail reads "You are here: [Home](#) > [Projects](#) > SSL Server Test". The main heading is "SSL Server Test". A paragraph of text explains the service: "This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will." Below this text is a light blue form area containing a "Hostname:" label, a text input field, and a "Submit" button. A checkbox labeled "Do not show the results on the boards" is positioned below the input field. At the bottom of the page, there are three columns with the headings "Recently Seen", "Recent Best", and "Recent Worst".

SSL Configuration Generator

<https://ssl-config.mozilla.org/>



The screenshot shows a browser window with the URL `ssl-config.mozilla.org`. The page features the Mozilla logo and the title "SSL Configuration Generator". It is divided into three main sections: "Server Software", "Mozilla Configuration", and "Environment".

Server Software

- Apache
- AWS ALB
- AWS ELB
- Caddy
- Dovecot
- Exim
- Golang
- HAProxy
- lighttpd
- MySQL
- nginx
- Oracle HTTP
- Postfix
- PostgreSQL
- ProFTPD
- Tomcat
- Traefik

Mozilla Configuration

- Modern
Services with clients that support TLS 1.3 and don't need backward compatibility
- Intermediate
General-purpose servers with a variety of clients, recommended for almost all systems
- Old
Compatible with a number of very old clients, and should be used only as a last resort

Environment

Server Version: 2.4.41

OpenSSL Version: 1.1.1d

Miscellaneous

- HTTP Strict Transport Security
This also redirects to HTTPS, if possible
- OCSP Stapling

RPKI TEST – A RIPE Labs experiment



<https://sg-pub.ripe.net/jasper/rpki-web-test/>

 **RPKI TEST** 


a RIPE Labs **experiment** in collaboration with Job Snijders/NTT



```
testing valid ROA...[passed]
testing invalid ROA (5sec)...[passed]
AS [redacted] drops RPKI invalid BGP routes from prefix
[redacted].0.0/20 as witnessed by your public IP
[redacted]
```

 **RPKI TEST** 

a RIPE Labs **experiment** in collaboration with Job Snijders/NTT



```
testing valid ROA...[passed]
testing invalid ROA (5sec)...[failed]
AS [redacted] accepts RPKI invalid BGP routes from
prefix [redacted].32.0/19 as witnessed by your
public IP [redacted]
```

Padrões	Referências
Tokens em <i>hardware</i> (FIDO2/U2F)	https://fidoalliance.org/specifications/
Tokens em <i>software</i> (HOTP/TOTP)	https://tools.ietf.org/html/rfc4226 https://tools.ietf.org/html/rfc6238
HTTPS mandatório e HSTS Versões atuais de TLS <i>Forward Secrecy</i>	https://www.ssllabs.com/ssltest/ https://ssl-config.mozilla.org https://observatory.mozilla.org
DNSSEC	https://registro.br/tecnologia/dnssec/dnssec-para-provedores/ ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf https://dnsviz.net
STARTTLS [idealmente c/ DANE] DMARC, DKIM e SPF	https://starttls-everywhere.org https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-secure-the-connections-of-mail-servers https://meca.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 https://sg-pub.ripe.net/jasper/rpki-web-test/

Outras Referências de Interesse para Uma Internet Melhor

cert.br nic.br egi.br

Precisamos um Ecossistema mais Saudável: Programa por uma Internet mais Segura

Objetivo principal:

- Reduzir o número de sistemas que possam ser abusados para gerar ataques DDoS

Incentivo à adoção de boas práticas:

- *Hardening*
- Segurança de roteamento (MANRS)
- *Anti-spoofing* (BCP 38)
- Reduzir serviços abertos que permitam amplificação

Iniciativa conjunta:

- ISOC, NIC.br, SindiTelebrasil, Abranet, Abrint, Abinee

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



Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

Requisitos mínimos de segurança

- Aplicáveis a IoT em geral

Trabalho desenvolvido no LAC-AAWG – Latin American and Caribbean Anti-Abuse Working Group

- Editora: Lucimara, Chair LAC-AAWG / CERT.br

Publicação conjunta

- **M³AAWG** - *Messaging, Malware and Mobile Anti-Abuse Working Group*
- **LACNOG** - *Latin American and Caribbean Network Operators Group*

Disponível em

- Português, Inglês, Japonês e Koreano

www.m3aawg.org/CPESecurityBP-Portuguese

www.lacnog.net/docs/lac-bcop-1

www.m3aawg.org/CPESecurityBP

LACNOG-M³AAWG 공동 작성
(가입자 대내장치) 최소 보안 요구사항에 대한
Best Current Operational Practices
LAC-BCOP-1

Documento conjunto LACNOG-M³AAWG:
Melhores Práticas Operacionais Atuais
sobre Requisitos Mínimos de Segurança para
Aquisição de Equipamentos para Conexão de Assinante (CPE)
LAC-BCOP-1
Maio 2019

Este documento está disponível no site do LACNOG em www.lacnog.net/docs/lac-bcop-1
Este documento está disponível no site do M³AAWG em www.m3aawg.org/CPESecurityBP-Portuguese
A versão original em Inglês está disponível no site do M³AAWG em www.m3aawg.org/CPESecurityBP

Este é um documento conjunto de Melhores Práticas Operacionais Atuais (*Best Current Operational Practices*, BCOP) desenvolvido pelo LACNOG (Grupo de Operadores de Redes da América Latina e o Caribe) e pelo M³AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group). É o produto das versões originais do LACNOG por seus grupos de trabalho LAC-AAWGs (Grupo de Trabalho Antiabuso da América Latina e o Caribe) e Grupo de Trabalho BCOP, em cooperação com membros do M³AAWG, Assessores Técnicos Sêniores e o Comitê Técnico do M³AAWG.

Índice

Sumário Executivo	2
1. Terminologia	2
2. Requisitos Gerais (<i>General Requirements – GR</i>)	3
3. Requisitos de Segurança de Software (<i>Software Security Requirements – SSR</i>)	4
4. Requisitos de Atualização e Gerenciamento (<i>Update and Management Requirements – MR</i>)	4
5. Requisitos Funcionais (<i>Functional Requirements – FR</i>)	5
6. Requisitos de Configuração Inicial (<i>Initial Configuration Requirements – IR</i>)	7
7. Requisitos do Fornecedor (<i>Vendor Requirements – VR</i>)	8
8. Lista de Acrônimos	8
9. Agradecimentos	9
10. Referências Informativas	9
Anexo 1 – Tabela de Requisitos	11

LACNOG
Grupo de Operadores de Redes da América Latina e o Caribe
Departamento de Montevideo, República Oriental do Uruguai
www.lacnog.net

M³AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302
San Francisco, California 94109 U.S.A. – www.m3aawg.org

LACNOG-M³AAWG Joint Best Current Operational Practices
Minimum Security Requirements
Premises Equipment (CPE) Acquisition
LAC-BCOP-1
May 2019

Available on the LACNOG website at www.lacnog.net/docs/lac-bcop-1
Available on the M³AAWG website at www.m3aawg.org/CPESecurityBP

Best Current Operational Practices (BCOP) document developed by LACNOG¹ (Network Operators Group) and M³AAWG² (Messaging, Malware and Mobile Anti-Abuse Working Group). It is the product of LACNOG's original drafts by its working groups: Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG) and BCOP Working Group. M³AAWG members, Senior Technical Advisors and the M³AAWG

Network Operators Group (LACNOG), <http://www.lacnog.net/>
Anti-Abuse Working Group (M³AAWG), <http://www.m3aawg.org/>
Latin American and Caribbean Anti-Abuse Working Group (LAC-AAWG), <http://www.lacnog.net/lac-aawg/>
Best Current Operational Practices (BCOP), <http://www.lacnog.net/wg-bcop/>

M³AAWG
Messaging, Malware and Mobile Anti-Abuse Working Group
781 Beach Street, Suite 302
San Francisco, California 94109 U.S.A. – www.m3aawg.org

Conscientização: Portal InternetSegura.br



The screenshot shows a web browser window with the URL `internetsegura.br`. The page header includes the `nic.br` logo, the `INTERNET SEGURA BR` logo, and navigation links for `Sobre`, `Outras iniciativas`, and `Como Pedir Ajuda`. The main content area features the headline: **Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!**

Below the headline, there are six categories of target audiences, each with an illustration and a label:

- para Crianças**: Illustration of two children, a boy and a girl.
- para Adolescentes**: Illustration of two young adults, a man and a woman.
- para Pais e Educadores**: Illustration of a woman and a man, both holding briefcases.
- para 60+**: Illustration of an elderly couple.
- para Técnicos**: Illustration of a man in a yellow shirt and blue pants, standing next to a server rack.
- para Interesse Geral**: Illustration of a diverse group of people of various ages and ethnicities.

Conscientização: Materiais sob Licença Creative Commons

Segurança na INTERNET

Faça sua parte e todos teremos uma Internet mais segura!

Já há muito tempo que segurança na Internet não é um assunto somente de interesse de um público especializado. Com a iniciativa InternetSegura.br, o NIC.br produz e disponibiliza gratuitamente uma série de materiais, em diversos formatos, que orientam diferentes públicos sobre o uso seguro da Internet. www.internetsegura.br

Catálogo de materiais e iniciativas do NIC.br

para Crianças

Guia Internet Segura

Apresenta conceitos de segurança na Internet de forma lúdica, com atividades para colorir, palavras cruzadas, desafios criados, dicas, complete a frase, caça-palavras, entre outros.



Formato impresso, colorido e permite inclusão de logo de parceiros de impressão

Desafios

Contém tanto os desafios do guia Internet Segura como materiais adicionais, atualizados periodicamente. internetsegura.br/desafios



para Adolescentes

Encarte #FikDik

Encarte do guia #Internet com Responsa - Cuidados e Responsabilidades no Uso da Internet, que apresenta os principais cuidados, riscos e consequências do uso inadequado da Internet de forma resumida.



para Pais e Educadores

Guia Internet Segura para seus filhos

Informações para pais e responsáveis sobre como proteger os filhos, seja zelando pela privacidade das crianças, ou utilizando tecnologias de controle parental.



Guia #Internet com Responsa - Cuidados e responsabilidades no uso da Internet

Orienta pais, responsáveis e educadores de adolescentes em temas sensíveis, como exposição excessiva na Internet, liberdade de expressão e danos à imagem e reputação, cyberbullying, danos e riscos da prática de nude, selfie, entre outros. Acompanha o encarte #FikDik



Guia #Internet com Responsa na sua Sala de Aula

Explica os desafios do uso da Internet a partir da exposição excessiva, dos direitos e possíveis danos à imagem dos professores e alunos, e dos limites da liberdade de expressão.



Slides: Fascículos da Cartilha de Segurança para Internet

Slides para a divulgação de boas práticas sobre o uso seguro da Internet. Há versões de apoio para professores, com notas explicativas. Disponíveis em formatos PowerPoint (.ppt), Libre-Office (.odp), PDF sem notas explicativas e PDF com notas explicativas. cartilha.cert.br/downloads



VEJA TAMBÉM

Curso de Formação de Professores Multiplicadores para o Uso Consciente e Responsável da Internet: cursointernetcomresponsa.nic.br

TIC Kids Online Brasil

Indicadores com mapeamento de possíveis riscos e oportunidades on-line a partir dos usos que crianças e adolescentes de 9 a 17 anos fazem da Internet. Contém dados distintos para "crianças e adolescentes" e "pais e responsáveis". ctic.br/pesquisa/kids-online

TIC Educação

A pesquisa entrevistou alunos, professores, coordenadores pedagógicos e diretores para mapear o acesso, o uso e a apropriação das tecnologias de informação e comunicação (TIC) em escolas públicas e privadas de educação básica. ctic.br/pesquisa/educacao

Para quem tem 60 anos ou mais

#Internet com Responsa 60+: Cuidados e responsabilidades no uso da Internet

Apresenta cuidados específicos para essa faixa etária, pois esse ambiente repleto de informações e oportunidades também oferece alguns riscos para quem ingressou no uso das novas tecnologias recentemente.



para Técnicos

Portal BCP e Programa Por uma Internet Mais Segura

Reúne um conjunto de boas práticas operacionais para Sistemas Autônomos (ASs) conectados à Internet. São destacadas algumas práticas que, embora extremamente importantes, ainda não são adotadas amplamente pelos ASs brasileiros. O portal também disponibiliza conteúdos e iniciativas direcionadas à comunidade de operadores de redes e serviços que formam a Internet por meio do Programa por uma Internet Mais Segura. bcp.nic.br



VEJA TAMBÉM

Curso de Boas Práticas Operacionais para Sistemas Autônomos - Presencial: bcp.nic.br/curso-bcop

Curso "Fundamentals of Incident Handling": cert.br/cursos/fih/

Curso "Advanced Topics in Incident Handling": cert.br/cursos/atih/

Interesse geral

Cartilha de Segurança para Internet

Documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. Apresenta o significado de diversos termos e conceitos utilizados na Internet, aborda os riscos de uso desta tecnologia e fornece uma série de dicas e cuidados a serem tomados pelos usuários. Também disponível em cartilha.cert.br e em espanhol em cartilha.cert.br



Fascículos da Cartilha de Segurança para Internet

Aborda tópicos específicos contidos na Cartilha de Segurança para Internet e complementa conteúdos que não estavam disponíveis à época da última edição da Cartilha, como Boatos, cuidados atualizados para Redes Sociais e Códigos Maliciosos. Também disponíveis em cartilha.cert.br/fasciculos e em espanhol em cartilha.cert.br/fasciculos



Guia #Internet com Responsa Vai às Compras

Detalha os cuidados necessários para realizar compras na Internet de forma responsável, além de enfatizar a importância de exercer direitos previstos no Código de Defesa do Consumidor.



Portal Antispam.br

Fonte de referência imparcial e embasada tecnicamente sobre o spam. Contém desde informações para administradores de redes e usuários finais, incluindo vídeos que abordam de forma simples e divertida os perigos aos quais os usuários estão expostos, explicam o que é spam e dão dicas de como navegar com mais segurança na rede. antispam.br



VEJA TAMBÉM

Materiais de referência:

Caderno CGL.br "Combate ao spam na Internet no Brasil"

Histórico e reflexões sobre o combate ao spam e a gerência da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil. cgi.br/publicacao/combate-ao-spam-na-internet-no-brasil

DISTRIBUIÇÃO DOS MATERIAIS

O NIC.br tem o compromisso de atender todos os interessados em seus materiais, da forma mais racional possível. Para que o máximo de interessados sejam atendidos, sem desperdício, limitamos o envio de materiais a lotes de 100 unidades. Caso sua instituição tenha interesse em distribuir uma quantidade maior, teremos o prazer em disponibilizar o conteúdo para que a impressão, com seu logotipo, seja realizada de acordo com sua capacidade.

SEJA UM PARCEIRO PARA A IMPRESSÃO DOS MATERIAIS!

Escreva para info@nic.br solicitando a inclusão do seu logotipo e especifique quais materiais você gostaria de imprimir.

LICENCIAMENTO

O objetivo primordial da produção dos nossos materiais é o compartilhamento de conteúdo, portanto a maioria destes está disponível gratuitamente para download e uso sob licenças Creative Commons. Sua instituição pode utilizá-los livremente, sem necessidade de autorização prévia, desde que a fonte seja mencionada, o uso do material não seja comercial (venda do material) e que o conteúdo não seja alterado. Para usos específicos fora do escopo da licença, escreva para info@nic.br.

Confira todas as nossas publicações e atividades em nic.br.

nic.br cgi.br

Obrigado

@ cristine@cert.br

@ jessen@cert.br

@ notificações para: cert@cert.br

@ @certbr

<https://cert.br>

20 de março de 2020

nic.br cgi.br

www.nic.br | www.cgi.br