nic.br cgi.br | cert.br

Live “Segurança na Internet: qual é o nosso papel?”

Intra Rede, Ceptro.br/NIC.br

01 de setembro 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

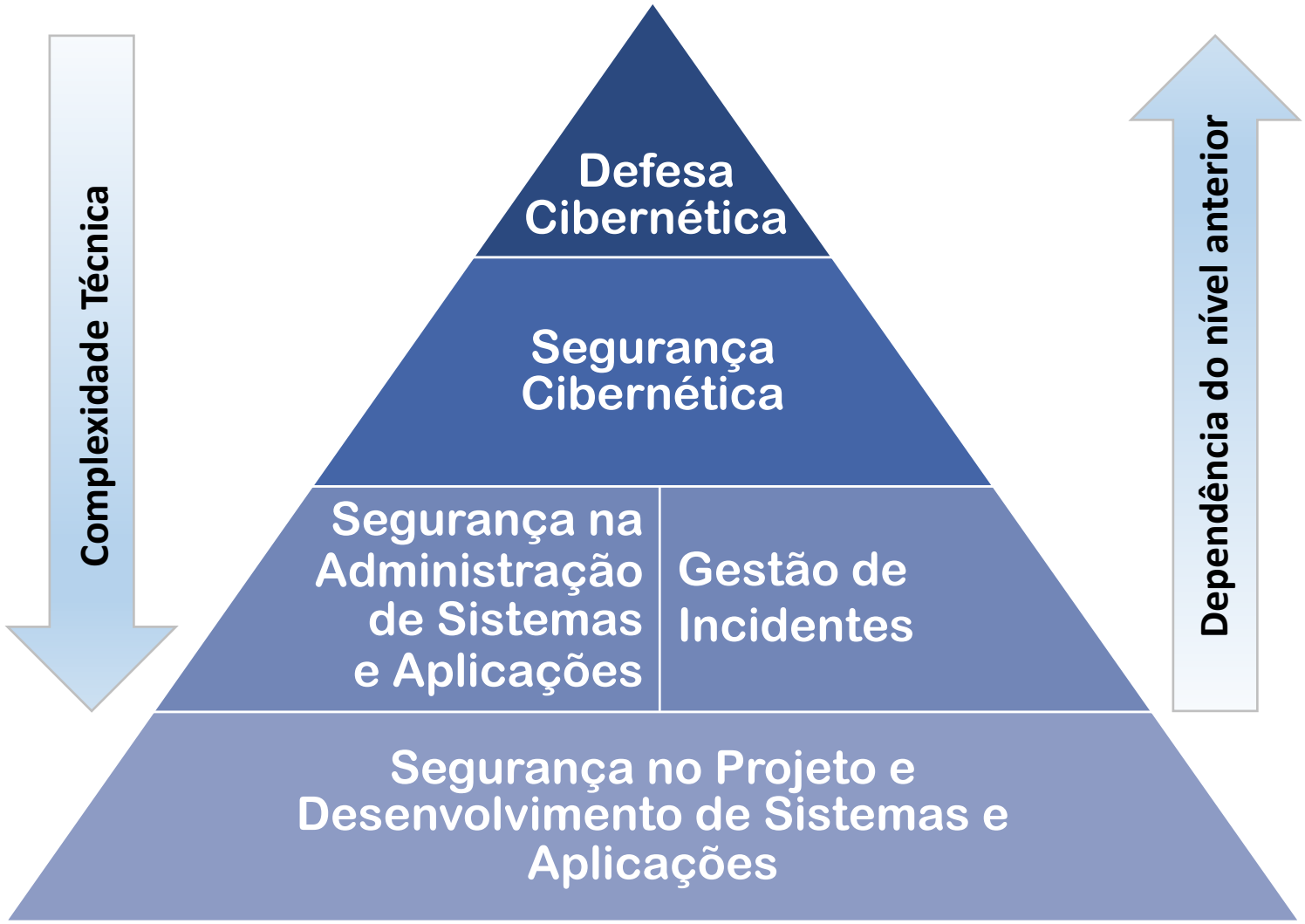
https://cert.br/sobre/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

Segurança na Internet:
Qual é o Papel da Comunidade Técnica?

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

Todos Tem um Papel na Segurança da Internet: **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 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
- 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
IPv6	https://ipv6.br https://test-ipv6.com
RPKI	https://bcp.nic.br/rpki
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
DNSSEC	https://registro.br/tecnologia/dnssec/dnssec-para-provedores/ https://ftp.registro.br/pub/doc/tutorial-dnssec.pdf https://dnsviz.net
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/
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

Os incidentes não são simplesmente reflexo de “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?**

Obrigada

cristine@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br