nic.br cgi.br

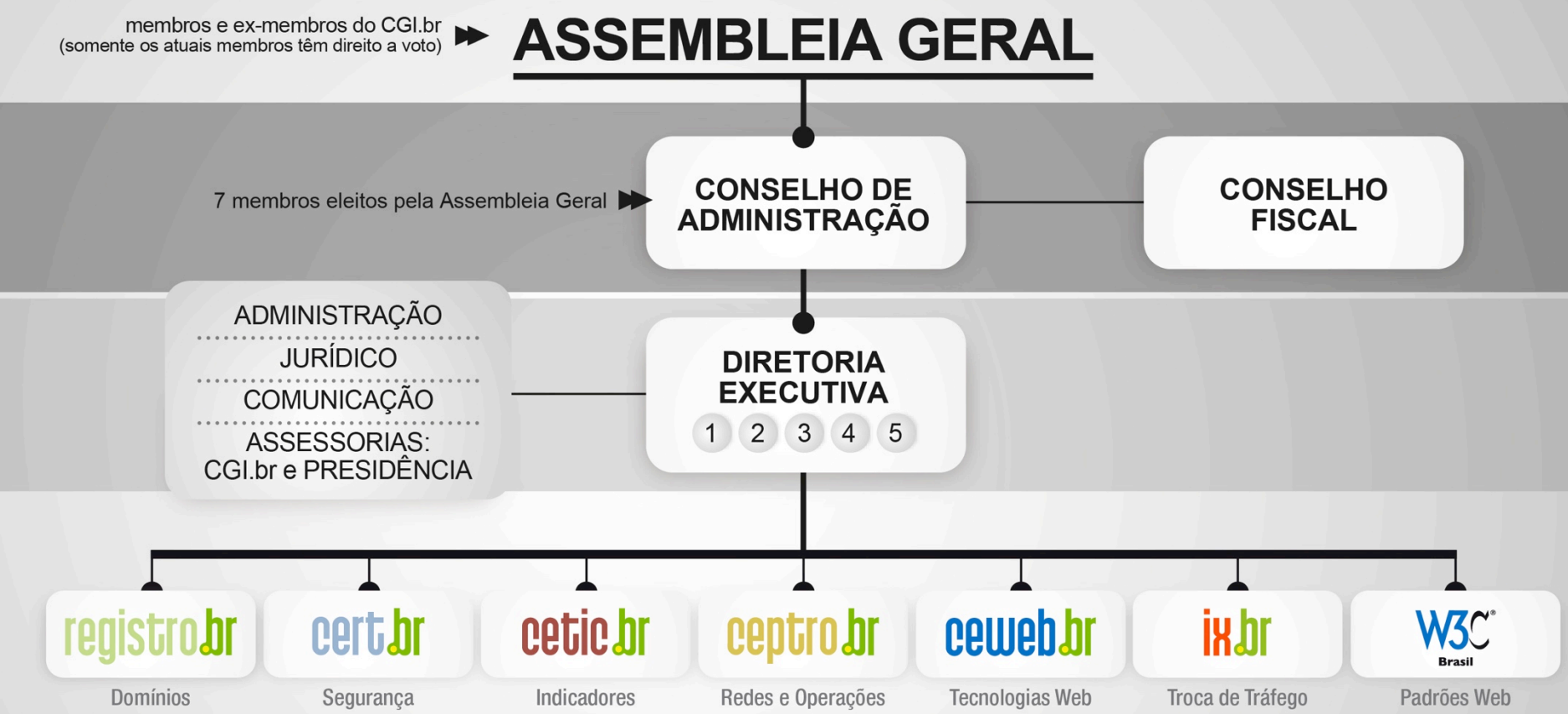
20 anos cert.br

Semana de Segurança da Informação – TRF3
São Paulo / SP
19/06/2018

Segurança na Internet: Tendências e desafios

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

cgi.br

1 2 3 4 5 6 7 8 9 — GOVERNO e 10 11 12 13 14 15 16 17 18 19 20 21 — SOCIEDADE CIVIL

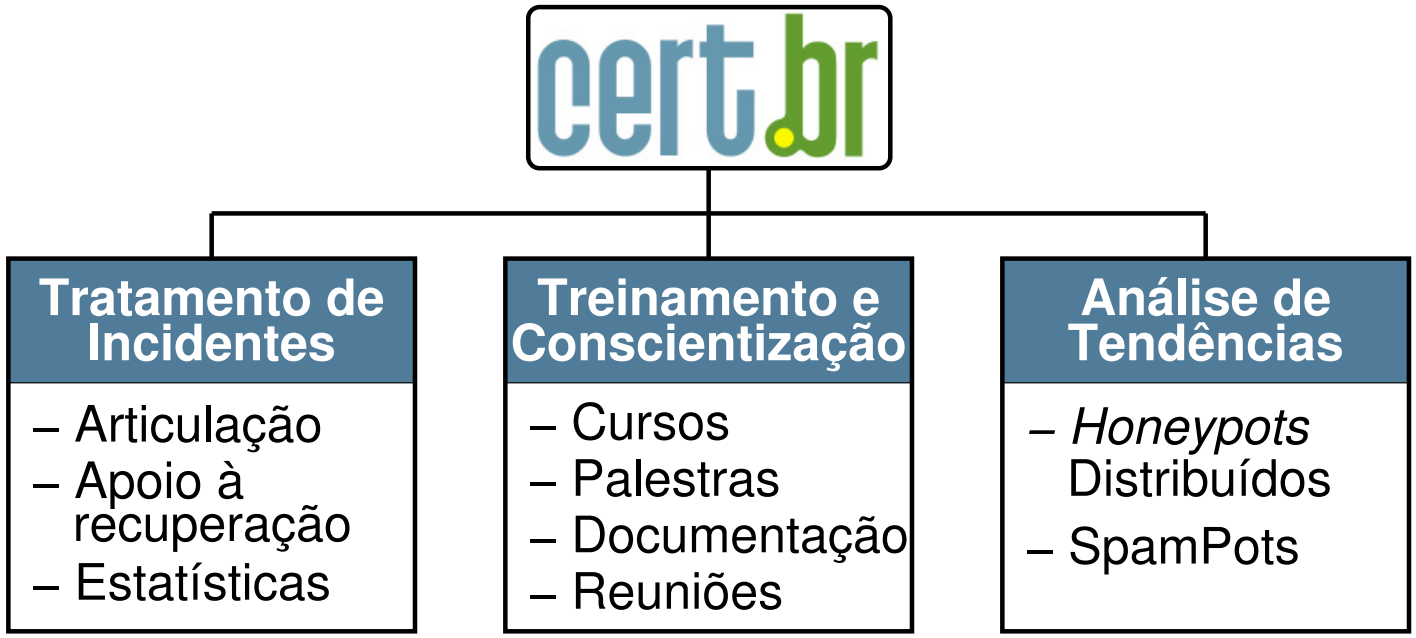
Representantes do Governo:

1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
2 Casa Civil da Presidência da República
3 Ministério das Comunicações
4 Ministério da Defesa
5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 Ministério do Planejamento, Orçamento e Gestão
7 Agência Nacional de Telecomunicações
8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

Representantes da Sociedade Civil:

10 Notório saber em assunto da Internet
11 a 14 Representantes do setor empresarial
- provedores de acesso e conteúdo da Internet
- provedores de infra-estrutura de telecomunicações
- indústria de bens de informática, de bens de telecomunicações e de software
- setor empresarial usuário

15 a 18 Representantes do terceiro setor
19 a 21 Representantes da comunidade científica e tecnológica



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet
PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Agenda

- **Conceitos de Segurança da Informação**
- **Cenário atual de incidentes de segurança**
- **Tendências e desafios**
- **Como melhorar o cenário**

Propriedades da Segurança da Informação

- **Confidencialidade: necessidade de garantir que as informações sejam divulgadas somente àqueles que possuem autorização para vê-las**
  - Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e lê as informações contidas na sua declaração de Imposto de Renda
- **Integridade: necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas**
  - Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal
- **Disponibilidade: necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam**
  - Ex. de quebra: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal

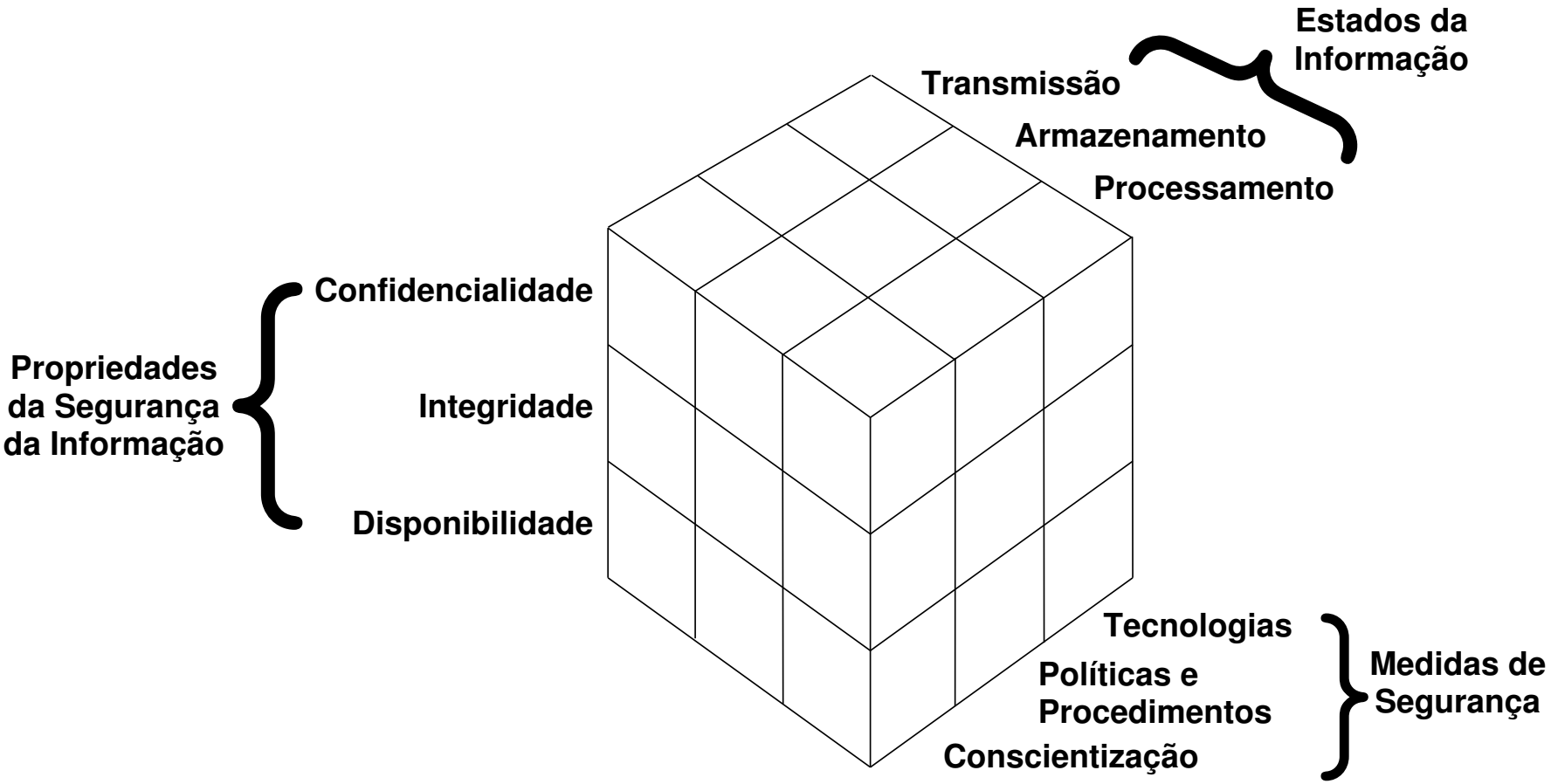
Privacidade vs Confidencialidade

Do ponto de vista de Segurança da Informação:

- **Privacidade: habilidade e/ou direito de proteger suas informações pessoais, extende-se à habilidade e/ou direito de prevenir invasões do seu espaço pessoal**

- **Confidencialidade: envolve a obrigação de proteger os segredos de outras pessoas ou organizações, se você souber deles**

As informações estão em diversos locais e a segurança depende de múltiplos fatores



McCumber Information Security Model

http://www.ibm.com/developerworks/security/library/s-confnotes2/

Riscos

- **Ilusão: achar que não corre riscos**
  - “meus equipamentos não serão localizados”
  - “não tem nada de interessante nos meus equipamentos”
  - “dentro de casa está seguro”

- **Atacantes interessados em quantidade de equipamentos**
  - independente de quais são e de como são

- **Riscos:**
  - sistemas conectados à Internet
  - envolvendo engenharia social

Riscos

- **Uso de engenharia social**
  - exploram fragilidades de usuários
    - códigos maliciosos (*malware*)
      - vírus, trojan, *ransomware*, RAT, etc.
    - aplicativos maliciosos
    - páginas falsas (*phishing*)
    - golpes (antecipação de recursos)

Riscos em Sistemas Conectados à Internet

- indisponibilidade de serviços
- perda de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- **perda de confiança na tecnologia**

Sistemas na Internet

Riscos

Atacantes

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

- defeitos de *software*
- falhas de configuração
- uso inadequado
- projetos sem levar em conta segurança
- fraquezas advindas da complexidade dos sistemas

Importância da Criptografia

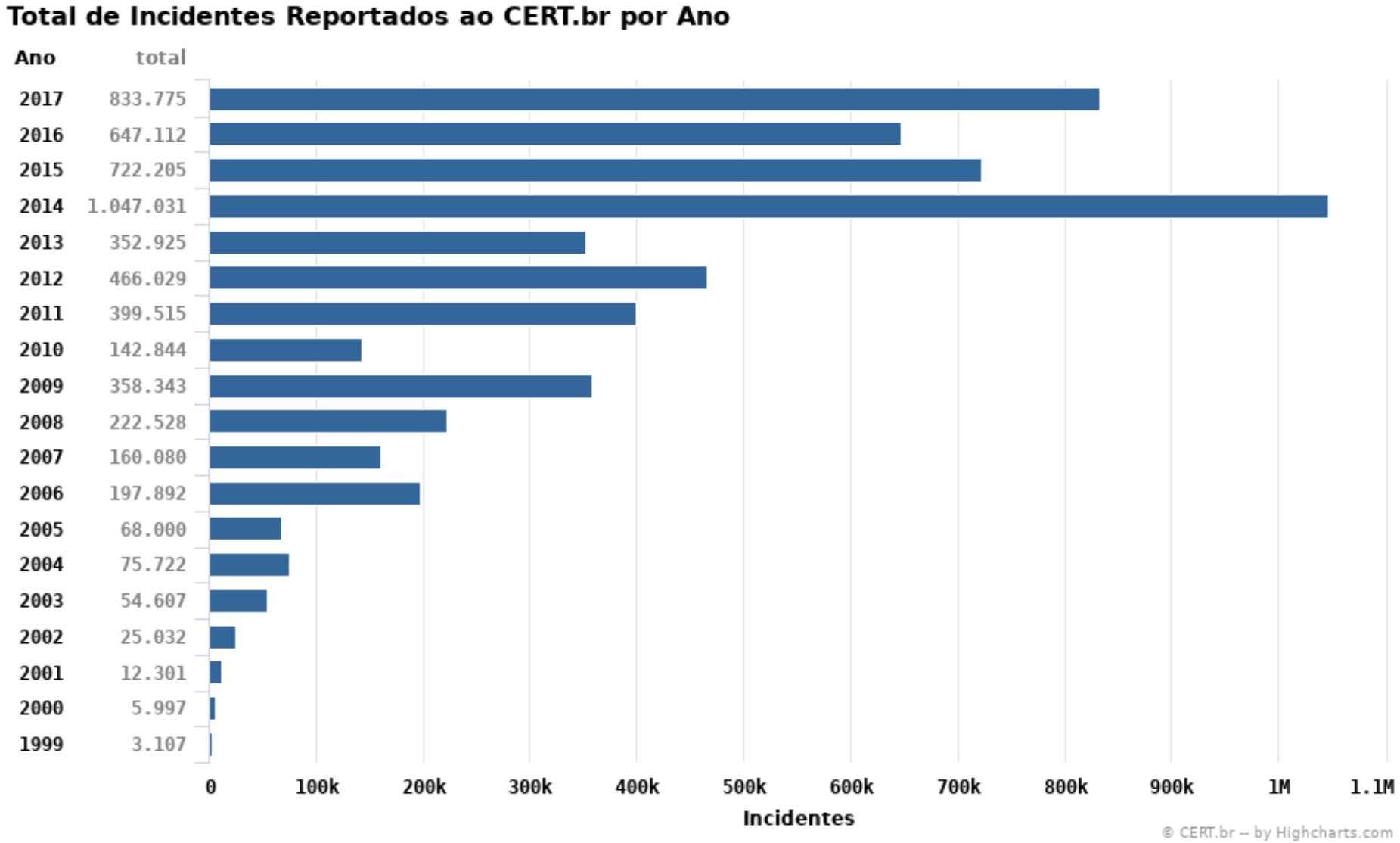
- **Criptografia**
  - ciência e a arte de escrever mensagens em forma cifrada ou em código
  - é um dos principais mecanismos de segurança
  - é a base para o funcionamento de:
    - certificados e assinaturas digitais
    - mecanismos de autenticação
    - conexão segura na Web (HTTPS)
    - conexão segura para outras aplicações na Internet
    - proteção de dados armazenados em disco, em mídias removíveis e dispositivos moveis

Resiliência

- **Um sistema 100% seguro é muito difícil de atingir**
- **Novo paradigma: Resiliência**
  - continuar funcionando mesmo na presença de falhas ou ataques
    - definir políticas e estratégias de segurança
    - treinar profissionais para implementar as estratégias e políticas de segurança
    - implantar medidas de segurança que implementem as políticas e estratégias definidas
    - conscientizar os usuários sobre os riscos e sobre as medidas de segurança necessárias
    - formular estratégias para gestão de incidentes de segurança e formalizar grupos de tratamento de incidentes

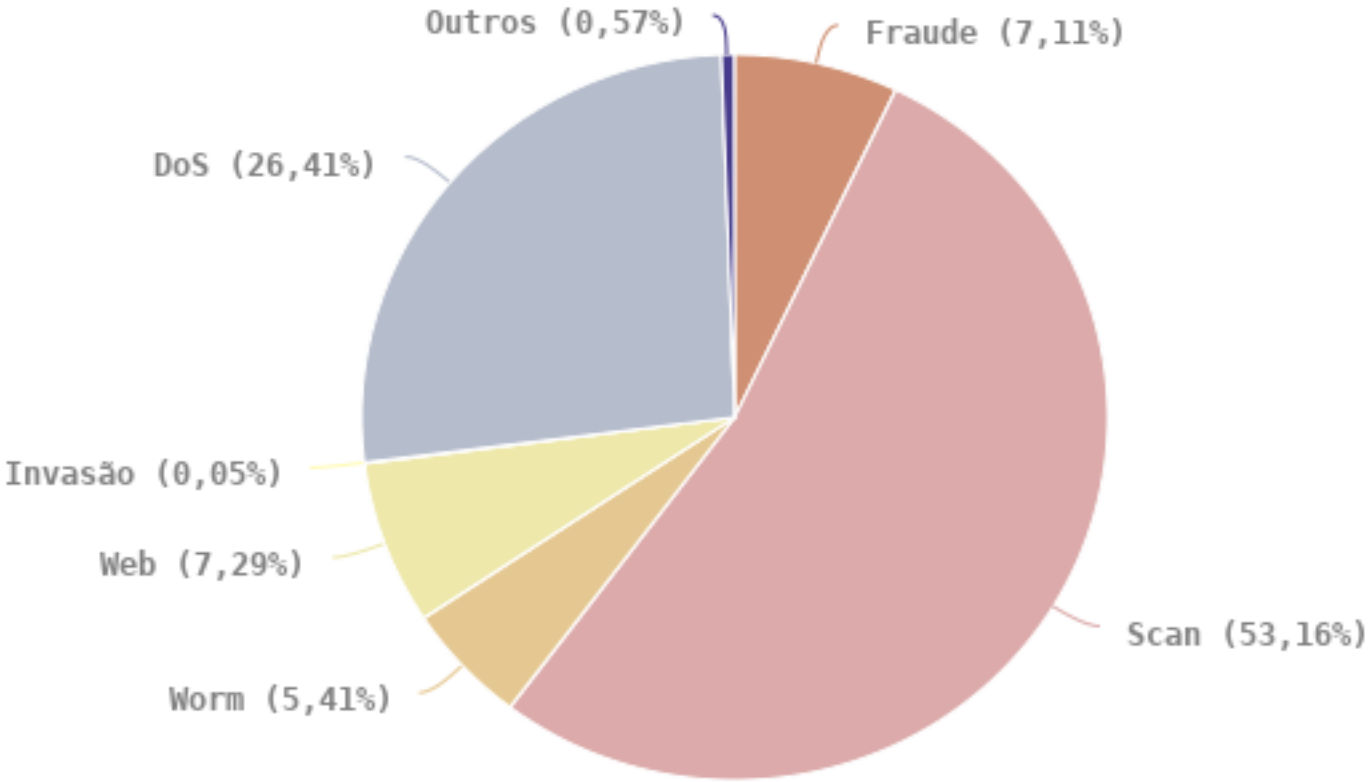
Cenário atual de incidentes de segurança

Estatísticas CERT.br – 2017

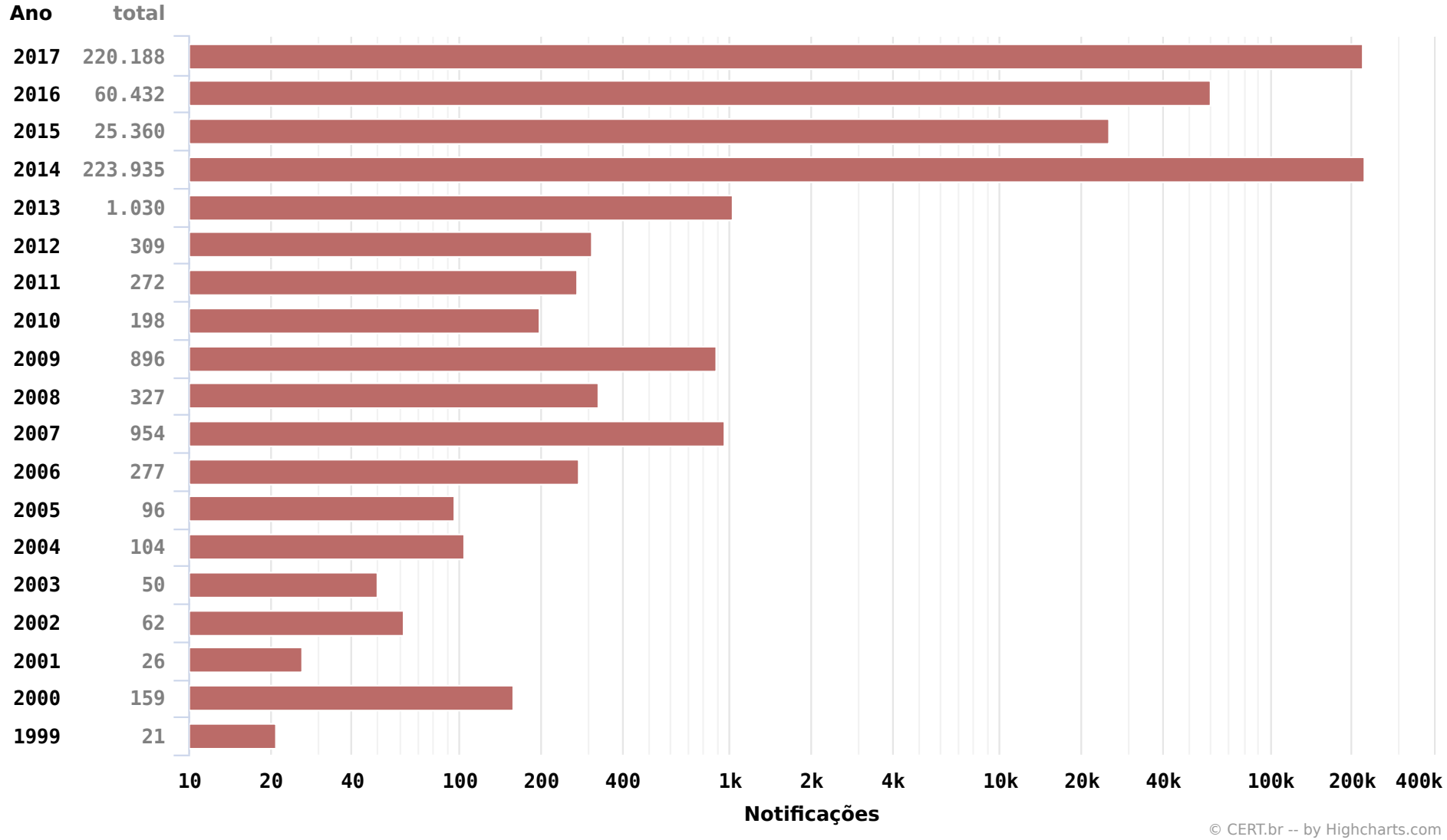


Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2017

Tipos de ataque

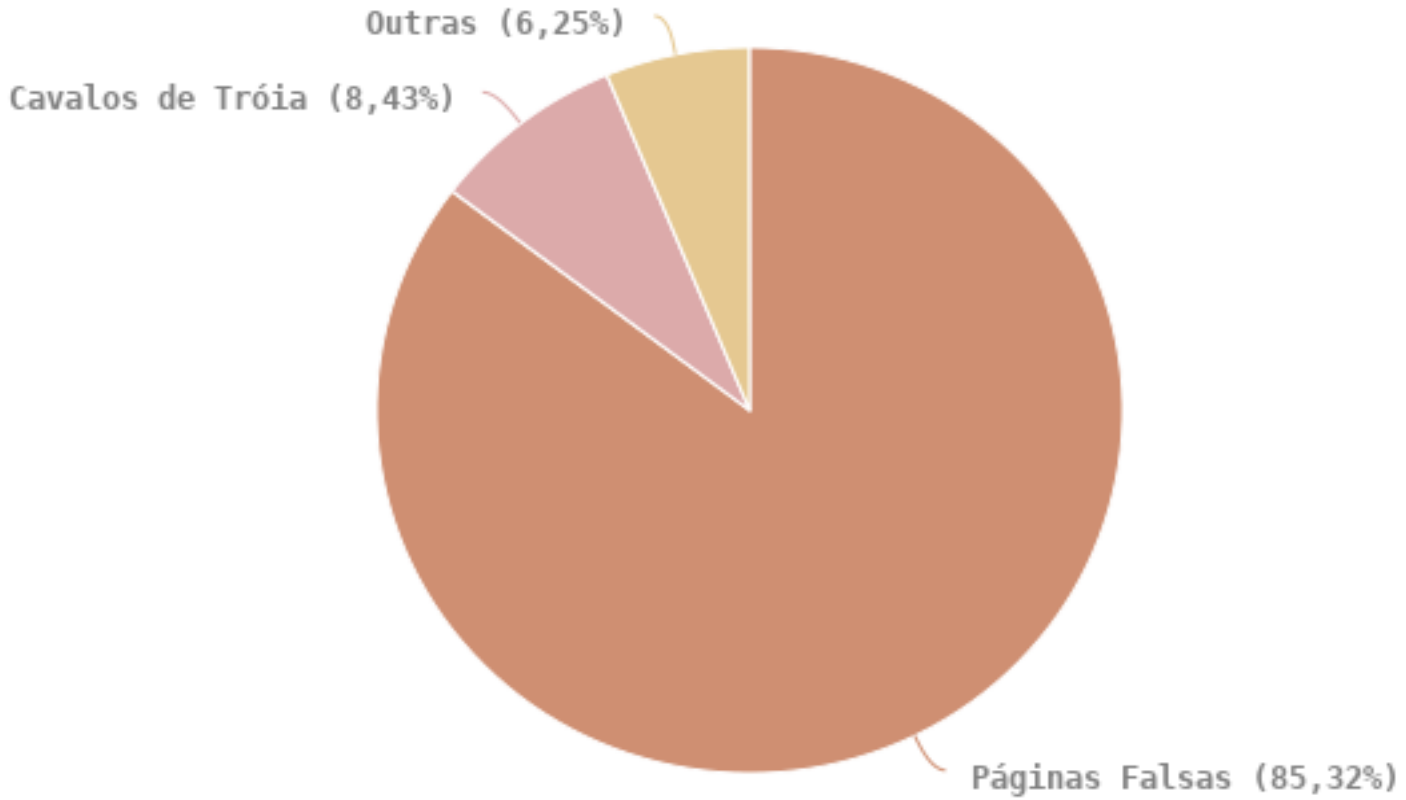


Notificações sobre equipamentos participando em ataques DoS



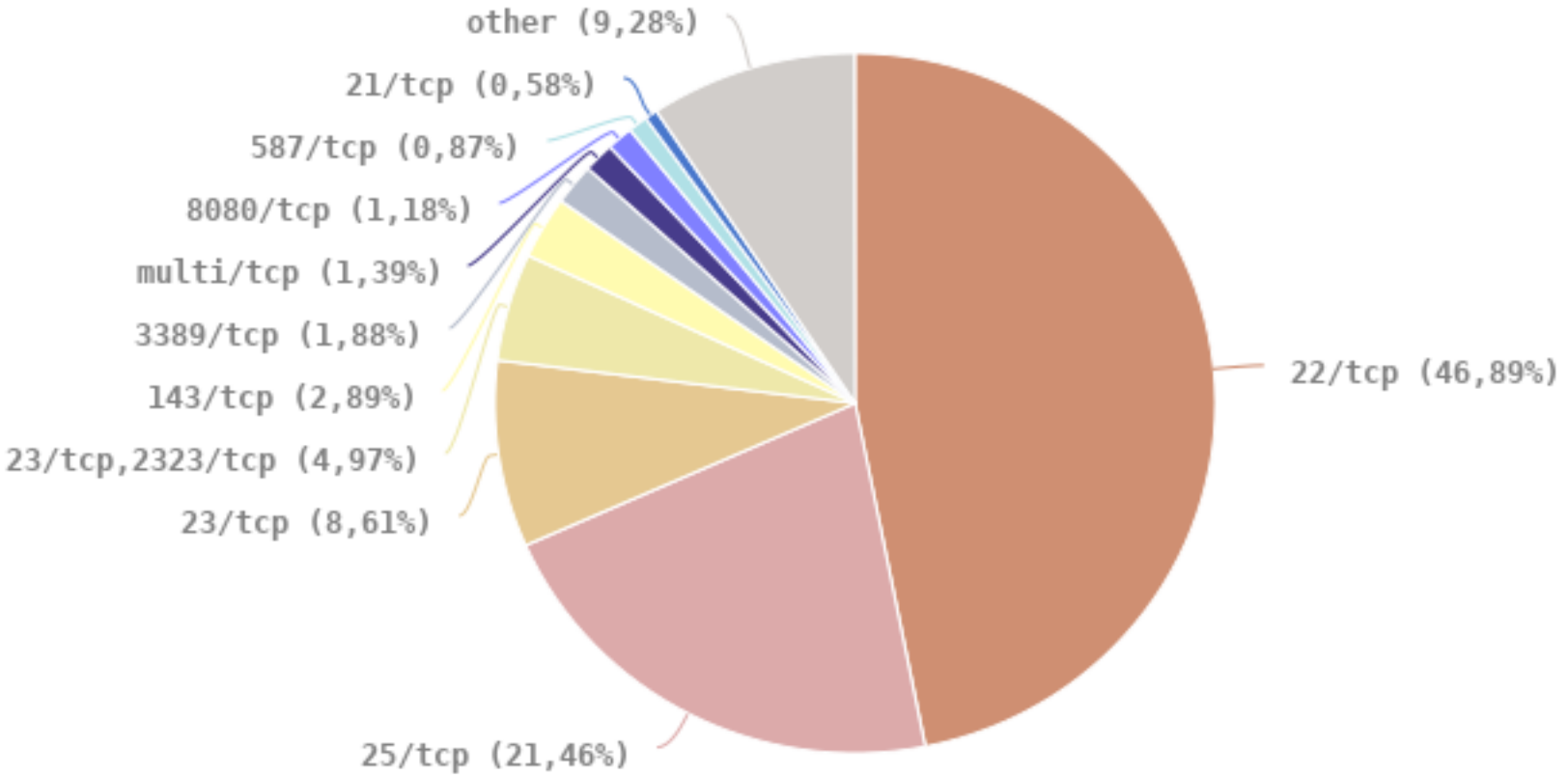
Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2017

Tentativas de fraudes



Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2017

Scans reportados, por porta



* Não inclui scans realizados por worms.

Cenário atual

- **Ataques a usuários finais:**
  - visando serviços de autenticação
  - com foco em grandes corporações
  - levando a grandes vazamento de dados
- **Fruto da mudança de enfoque dos atacantes**
  - é mais fácil e “rentável” atacar um usuário
  - usuários com acesso a muitas e valiosas informações
  - ataques cada vez mais convincentes, explorando
    - engenharia social
    - grande quantidade de informações expostas na Internet
    - a confiança cega que as pessoas têm em contatos conhecidos
- **Credenciais com alto valor no mercado negro**

Malware

- **Novos *malwares* sendo desenvolvidos**
  - difíceis de serem detectados por antivírus
- **RAT e *ransomware* em amplo uso**

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

Ransomware (1/2)

- **Pode infectar:**
  - computadores, equipamentos de rede e dispositivos móveis

- **Infecção ocorre pela execução de arquivo infectado:**
  - recebido:
    - via *links* em *e-mails*, redes sociais e mensagens instantâneas
    - anexado a *e-mails*
  - baixado de *sites* na Internet
  - acessado via arquivos compartilhados ou páginas Web maliciosas (usando navegadores vulneráveis)

Ransomware (2/2)

- **Ações mais comuns**
  - impede o acesso ao equipamento (*Locker ransomware*)
  - impede o acesso aos dados armazenados no equipamento, geralmente usando criptografia (*Crypto ransomware*)
- **Costuma também:**
  - apagar arquivos de *backup*
  - buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também
  - cifrar arquivos na nuvem
- **Extorsão é o principal objetivo dos atacantes**
  - pagamento feito geralmente via *bitcoins*
  - não há garantias de que o acesso será restabelecido
  - instigam medo e pânico na vítima

Phishing (1/2)

- **Tenta induzir o usuário a fornecer credenciais, dados financeiros ou executar ações**
- **Ponto de entrada para diversos outros golpes**

https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/
http://www.eweek.com/security/rsa-s-securid-breach-started-with-phishing-email
https://www.helpnetsecurity.com/2017/09/13/phishers-linkedin-hijacked-accounts/
http://politica.estadao.com.br/noticias/geral,hackers-atacam-sistema-de-e-mails-e-de-leitura-de-documentos-do-itamaraty,1172332

Phishing (2/2)

- **Alguns tipos:**
  - enviados de forma massificada
  - em cascata:
    - uso de conta forjada/genérica para envio de *e-mails* aos funcionários
    - uso de conta invadida para envio de *e-mails* a funcionários específicos
      - responder conversas em andamento, incluindo *links*
      - usuários acreditam em contatos conhecidos
        - mesmo com conteúdo "estranho"
  - *spear phishing* - direcionados a grupos específicos
  - *whaling* - direcionados a alvos chave das organizações
  - *watering hole attacks* - direcionados a *sites* acessados pelos verdadeiros alvos
  - *SMiShing* - direcionados a usuários de dispositivos móveis

EMPRESAS ALEMÃS PERDEM MILHÕES DE EUROS EM “FRAUDE DO CEO”

JUL 10, 2017 ROBERTO CHU AMEAÇAS DIGITAIS NO COMMENTS YET

Empresas alemãs perderam milhões de euros para o crime organizado em um golpe apelidado de "fraude do CEO" que usa falsos memorandos de altos executivos para convencer funcionários de contabilidade à transferir fundos, disse nesta segunda-feira a agência federal de segurança cibernética da Alemanha (BSI).

A agência BSI disse que as autoridades que investigam a nova fraude receberam uma lista de 5 mil alvos potenciais, e notificaram as empresas envolvidas.

Organizações criminosas estão usando informações que conseguem em redes sociais, sites corporativos, sites de empregos e até ligações para as companhias para falsificar as informações de contato de altos executivos.

A BSI disse que a Polícia Federal Criminal alemã estimou que o golpe já custou milhões de euros a empresas nos últimos meses.

A fraude visa funcionários dos departamentos de contabilidade e auditoria de uma companhia que foi autorizada a transferir dinheiro, muitas vezes usando pressão de tempo e avisos sobre um suposto "projeto secreto" para manipulá-los à realizar os falsos pagamentos.

http://www.e-guardian.com.br/ameacas/empresas-alemas-perdem-milhoes-de-euros-em-fraude-do-ceo

Tendências e desafios

Tendências e desafios (1/2)

- **Ataques cada vez mais:**
  - potentes
  - fáceis de serem realizados
  - acessíveis e baratos (para quem ataca)

- **Grande uso de engenharia social**
  - usuários sendo usados para propagação

- **Usuários não são especialistas**
  - cada vez maior o número de dispositivos vulneráveis e que precisam de manutenção

Tendências e desafios (2/2)

- **Sistemas cada vez mais complexos**
  - segurança não é parte dos requisitos
  - falta de profissionais capacitados para desenvolver com requisitos de segurança
  - pressão econômica para lançar, mesmo com problemas

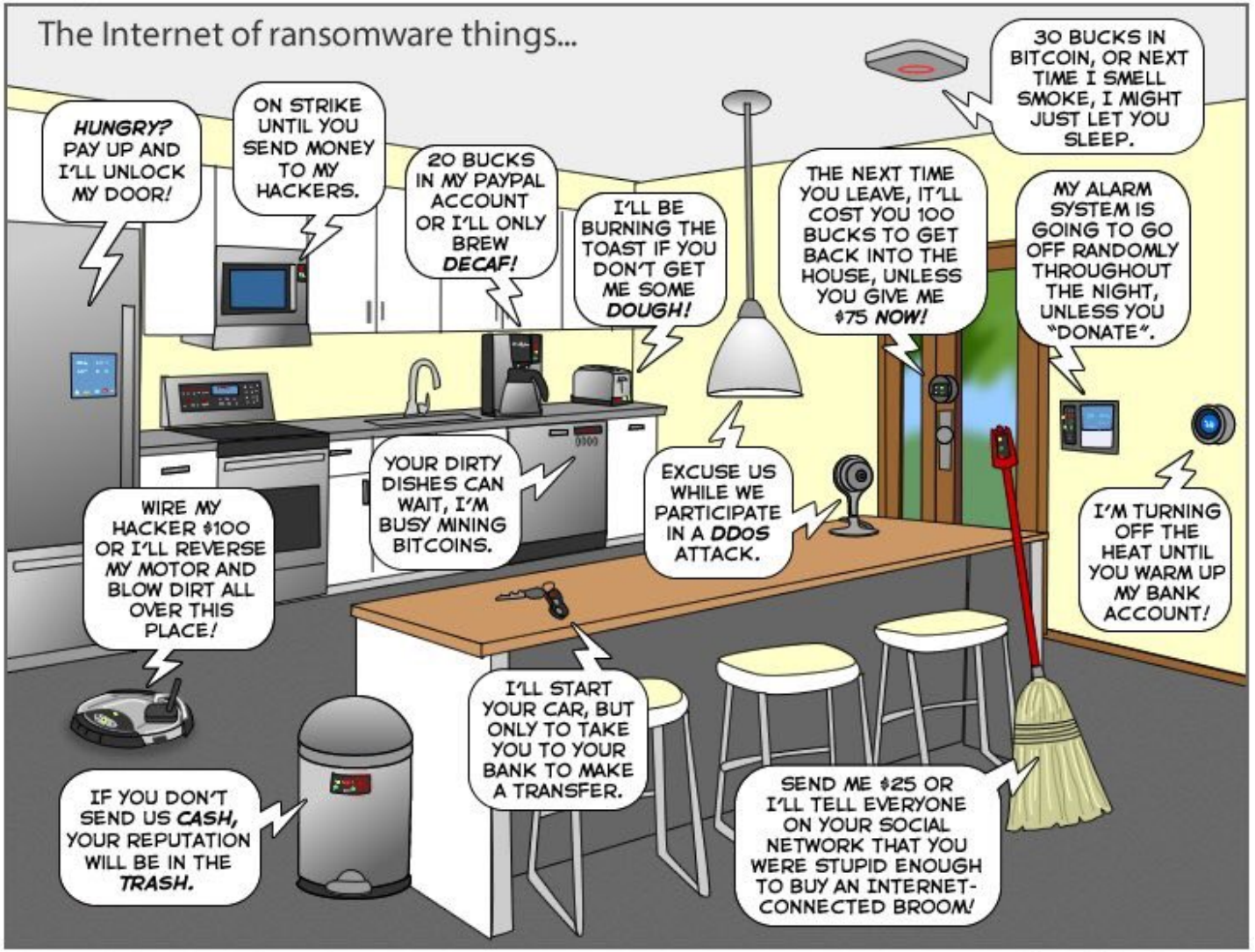
- **IoT**
  - cada vez mais equipamentos/sistemas conectados
  - falta de cuidados de segurança
    - no projeto, implementação e adoção
  - dificuldade de atualização de sistemas

Novos desafios

- **Internet das Coisas**
  - babás eletrônicas, câmeras
- **Internet dos Brinquedos**

https://www.wired.com/story/dont-gift-internet-connected-toys/
https://techcrunch.com/2017/11/15/call-to-ban-sale-of-iot-toys-with-proven-security-flaws
https://www.cso.com.au/article/614555/germany-bans-q-iot-doll-cayla-illegal-spy-device/

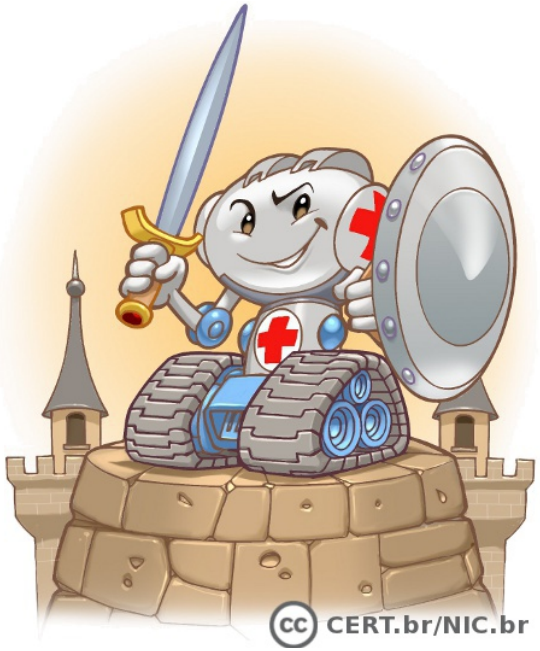
The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

Como melhorar o cenário



Precisamos um ecossistema mais saudável

Nenhum único grupo ou estrutura conseguirá fazer sozinho a segurança

Todos possuem um papel

Precisamos de um ecossistema mais saudável

- **Administradores de redes e sistemas**
  - não emanar “sujeira” de suas redes e adotar boas práticas
  - notificar usuários sobre infecções e indícios de comprometimento
  - fazer *hardening* das máquinas
- **Desenvolvedores**
  - pensar em segurança desde o início
  - pensar nos casos de ABUSO (o ambiente é HOSTIL)
- **Acadêmicos**
  - incluir conceitos de programação segura logo nos primeiros anos
- **Usuários**

Usuários – Primeiro passo

- **Qualquer conta, perfil ou equipamento conectado à Internet pode vir a ser alvo da ação de atacantes**

- **Necessário levar para a Internet os mesmos cuidados e preocupações do dia a dia**
  - atenção com a segurança deve ser um hábito incorporado à rotina
  - independente de local, tecnologia ou meio utilizado

Como se prevenir

- **Aplicar soluções técnicas**
  - ajuda a proteger das ameaças já conhecidas
    - para as quais já existem formas de prevenção
- **Adotar postura preventiva**
  - ajuda a proteger das:
    - ameaças que envolvem engenharia social
    - ameaças ainda não conhecidas
    - ameaças que ainda não possuem solução

Proteger os equipamentos

- **Manter os equipamentos seguros**
  - com a versão mais recente do sistema operacional e dos aplicativos
  - com todas atualizações aplicadas
- **Usar as opções de configuração disponíveis**
- **Usar e manter atualizados mecanismos de segurança**
  - antivírus
  - *antispam*
  - *antiransomware*
  - *firewall* pessoal

Proteger as contas de acesso

- **Ser cuidadoso ao:**
  - elaborar as senhas
  - usar as senhas

- **Evitar o reuso de senhas**

- **Trocar as senhas periodicamente**

- **Usar verificação em duas etapas, sempre que disponível**

Proteger a privacidade e os dados

- **Diminuir a quantidade de dados expostos**

- **Fazer *backups***
  - única garantia efetiva contra *ransomware*
  - devem ser mantidos desconectados

Adotar uma postura preventiva

- **Ser cuidadoso ao abrir arquivos anexos e ao clicar em *links***

- **Não considerar que uma mensagem é confiável com base apenas em seu remetente**
  - remetente pode não ter checado a mensagem
  - pode ter sido enviada de:
    - conta falsa
    - conta invadida

MANTENHA-SE INFORMADO

Cartilha de Segurança para Internet

- Livro (PDF e ePub)
- Conteúdo no *site*
- Fascículos e *slides*
- Dica do dia no *site*, via *Twitter* e RSS

https://cartilha.cert.br/

Publicação cert.br

Cartilha de Segurança para Internet

Fascículo Boatos

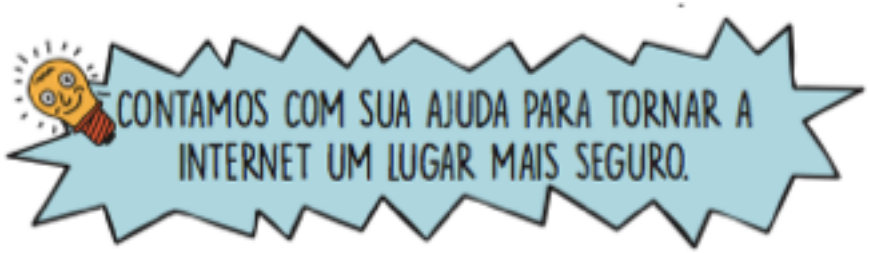
https://cartilha.cert.br/

nic.br

cgi.br

"A Internet é como um espelho da sociedade.
Se você não gosta do que nele vê,
quebrá-lo não é a solução."

Vint Cerf, 2010, fórum em Vilna, Lituânia.



INTERNET SEGURABR

Solicitação de materiais: doc@cert.br

Instituições que desejarem imprimir os materiais podem inserir a marca como "Impresso por:"

Obrigada

www.cert.br

miriam@cert.br

certbr

19 de junho de 2018

nic.br cgi.br

www.nic.br | www.cgi.br