nic.br cgi.br | cert.br

Reunião Técnica da Coordenação-Geral de Normatização
Autoridade Nacional de Proteção de Dados – ANPD
15 de março de 2021 – *On-line*

Contribuição para Tomada de Subsídios nº 2/2021 da ANPD

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

Conceitos:
Risco vs. Dano no Contexto de Dados Pessoais

Risco:

É a possibilidade de sofrer dano ou perda.

- há sempre a presença da incerteza
- precisa ter uma condição de risco
  - ameaça + vulnerabilidade
- há um impacto (consequência) se o risco for realizado

Exemplos são a possibilidade de:

- perdas financeiras
  - ex: dados de cartões de crédito foram furtados
- perda de privacidade
  - ex: vulnerabilidades em um banco de dados com dados pessoais sensíveis (médicos)
- furto de identidade
  - ex: *login* e senha foram expostos

Dano:

É a realização do risco, em que o dano deixa de ser uma possibilidade e foi confirmado

- não há mais incerteza
- é possível comprovar o dano

Exemplos são a confirmação de:

- perdas financeiras
  - ex: dados de cartões de crédito foram usados para compras por golpistas
- perda de privacidade
  - ex: dados médicos foram acessados e divulgados amplamente na Internet
- furto de identidade
  - ex: *login* e senha foram furtados e o atacante acessou a conta

Relevância e Grau de Risco:
Possíveis Critérios para Avaliação

Tecnicamente a classificação e a priorização de um incidente levam em conta

- Categoria
  - *malware*, invasão, negação de serviço, etc
- Envolvidos
  - pessoas, organizações, tipos de dados, etc
- Escopo
  - num. de dispositivos, criticidade do ativo, etc
- Impacto na informação
  - confidencialidade, integridade, disponibilidade?
- Consequências (na ordem de relevância para os que envolvem dados pessoais)
  - risco de morte ou dano físico
  - preconceito
  - furto de identidade / prejuízos financeiros
  - reputação / constrangimento
  - perda de acesso a sistemas

Adicionalmente para dados pessoais

- Nível de exposição dos dados
  - ex1: furto de dados em claro vs. dados cifrados
  - ex2: dados foram divulgados publicamente vs. estão apenas em fóruns privados ou não divulgados
- Complexidade técnica para fazer uso dos dados
  - ex: **vazar *hash* da senha** (exige conhecimento sobre uso de *software* de quebra de criptografia e, potencialmente, não seriam afetados sistemas bem implementados ou usuários com senhas fortes) **vs. vazar senha em texto claro** (qualquer atacante pode abusar dos dados e todos os usuários são afetados igualmente)

Notificação vs. Comunicação de Incidentes

Notificar um Incidente

- Termo técnico utilizado nas áreas de Gestão de Riscos e Gestão de Incidentes
- Informal
- CSIRTs recebem notificações
- Pode ser apenas suspeita
  - rumor infundado
  - falso positivo
  - tentativa sem sucesso
- Precisa confirmar se realmente ocorreu um incidente
  - a confirmação do incidente ocorre apenas após a análise

Comunicar um Incidente Relevante à ANPD

Artigo 48: "*O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.*"

- Incidentes confirmados pelos agentes de tratamento
  - que passaram por um processo de triagem, análise e resposta feita por equipe especializada
  - que satisfizeram critérios de relevância definidos pela ANPD
- Acompanhados de relatórios incluindo
  - categoria de incidente, tipo de dados afetados, escopo e consequências do incidente
- Não é possível avaliar risco de eventos não confirmados ou sob suspeita
  - suspeitas não devem gerar comunicação ao titular, sob pena de gerar fadiga de alertas

Referências

– FIRST Computer Security Incident Response Team (CSIRT) Services Framework
https://www.first.org/standards/frameworks/csirts/
– Defining Incident Management Processes for CSIRTs: A Work in Progress, SEI/CMU
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153
– Computer Security Incident Handling Guide, NIST Special Publication 800-61 Revision 2
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
– Reference Incident Classification Taxonomy
https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
– CSIRT Case Classification (Example for Enterprise CSIRT)
https://www.first.org/resources/guides/csirt_case_classification.html

Sobre o CERT.br

cert.br nic.br cgi.br

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:

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
- 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/

Obrigada

cristine@cert.br

Notificações para: cert@cert.br @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br