Conectando la investigación y educación europea y latinoamericana

Tratamento de Incidentes de Segurança da Informação

Italo Valcy[1,2], Gildásio Jr[1,2] {italovalcy,jose.gildasio}@ufba.br>

[1]Ponto de Presença da RNP na Bahia (PoP-BA/RNP)
[2]Universidade Federal da Bahia (UFBA)

Supported by European Commission

Agenda

- Estabelecimento de CSIRT
- Fundamentos do Tratamento de Incidentes de Segurança
- Taxonomia
- Principais dificuldades
- Boas práticas de tratamento de incidentes

Definição de CSIRT

- CSIRT: Computer Security Incident Response Team
  - É uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores
- Definição do CERT/CC
  - http://www.cert.org/csirts/csirt_faq.html
- Qual a diferença entre CERT e CSIRT?

Definição de CSIRT

- Siglas e CSIRTs que conhecemos:
  - CERT/CC
  - AusCERT
  - SURFcert
  - CIRCL
  - CERT.BR
  - CAIS/RNP
  - GRA/SERPRO
  - CERT.Bahia
  - ETIR-UFBA

Criando um CSIRT

- Justificando a existência de um CSIRT
  - Aumento no número de incidentes
  - Aumento no número de usuários (e expectativa dos usuários)
  - Aumento da dependência tecnológica
  - *Normatização*
- Necessidade da criação de CSIRTs
  - Ponto chave na manutenção e continuidade do negócio

Normatização

- Conselho de Defesa Nacional (CF, Art. 91)
- Decreto ~~3.505/2000~~ 9.637/18
  - Institui a **Política de Segurança da Informação** nos órgãos e entidades da APF
  - Comitê Gestor de Segurança da Informação (órgão de Estado)
- Lei nº 8.638/2016: Estratégia de Governança Digital
- Lei nº 12.527/2011: Lei de Acesso a Informações
- Decreto 5.482/2005: divulgação de dados da APF pela rede
- Lei nº 13.709/18 e Lei nº 13.853: Lei Geral de Proteção de Dados
- Norma ABNT NBR ISO/IEC 27001, 27002 e 27005
- Decreto 5.772/06: Gabinete de Segurança Institucional da Presidência da República, Departamento de Segurança da Informação

*Ações que objetivam viabilizar e assegurar a **Disponibilidade**, a **Integridade**, a **Confidencialidade** e a **Autenticidade** das Informações.*
D.I.C.A.

Normatização

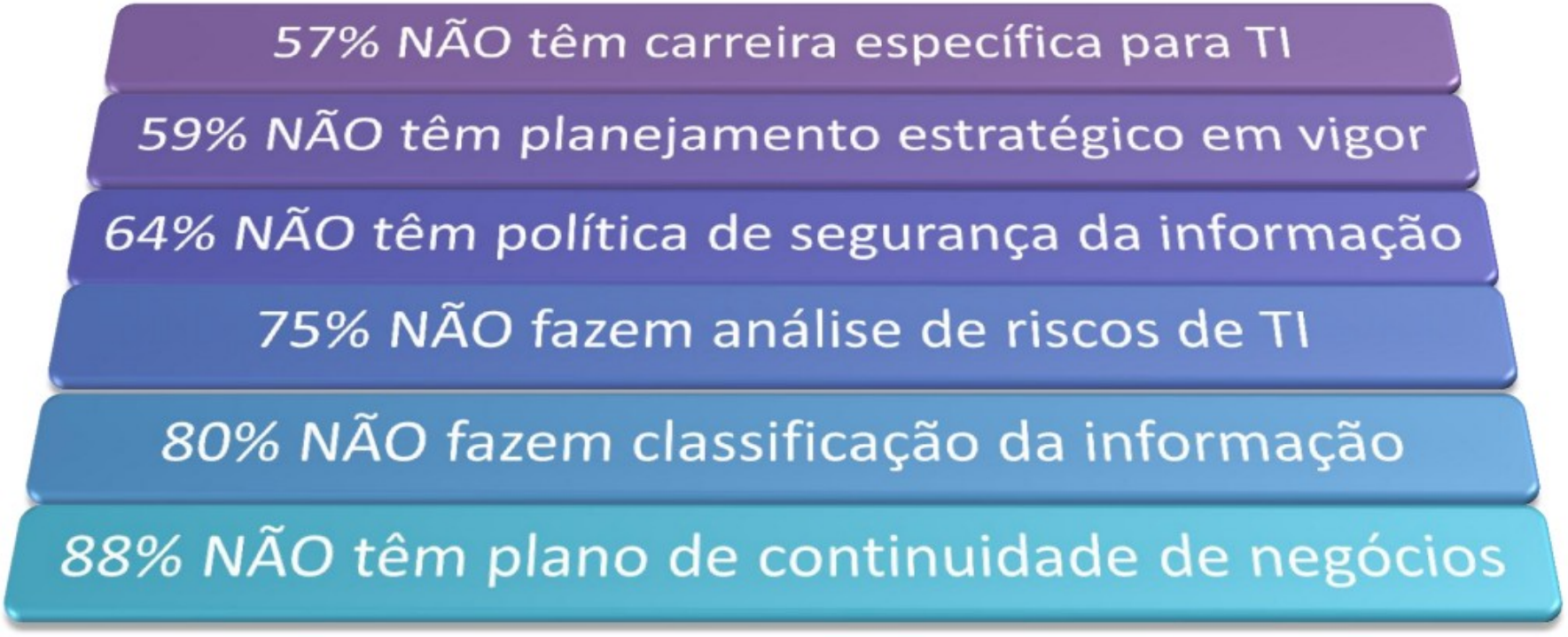
- Legislação de SIC do GSI-PR/DSIC
  - IN 01 GSIPR/DSIC (2008): Disciplina a Gestão de Segurança da Informação e Comunicações na APF
  - NC 01: Atividades de normatização
  - NC 02: Metodologia de Gestão de Segurança da Informação e Comunicação
  - NC 03: Diretrizes para elaboração da PSI
  - NC 05: Disciplina a criação dos ETIRs
  - NC 08: Diretrizes para gerenciamento de Incidentes em Redes Computacionais
  - ...
- Mais informações: http://dsic.planalto.gov.br/

Mais informações

- Minicurso sobre Política de Segurança da Informação:
  - https://video.rnp.br/portal/video.action?idItem=21667
- Minicurso sobre Implantação de CSIRT:
  - https://video.rnp.br/portal/video.action?idItem=23468

Acordão 1.603 (TCU, 15/ago/2008)

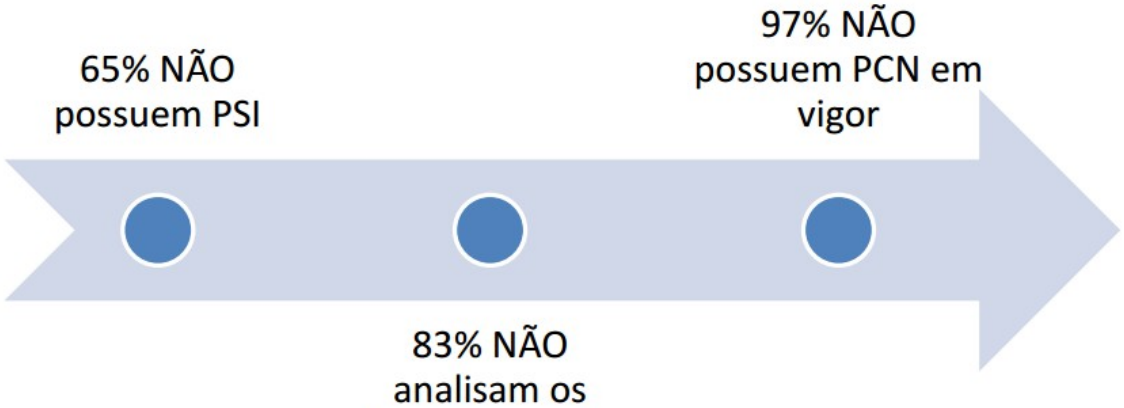
- A situação da segurança da informação (2008)



Fonte: Marcio Braz - Sefti/TCU, 1º Forum RNP

Acordão 2.308 (TCU, 2010)

- 2º levantamento de governança de TI



"nenhum dos indicadores relativos à segurança da informação, (...) apresentou avanço substancial (...) a administração pública permanece exposta aos mesmos riscos, não tem agido para reduzi-los, não consegue estimar suas consequências e continuar a não proteger suas informações críticas adequadamente", Voto Min. Aroldo Cedraz

Acordão 588/2018 (TCU, 2017)

- Levantamento de governança de TI

Critérios de auditoria TCU

- Leis e decretos: Decreto 3.505/2000 (Política de SI para a APF), 4.533/2002 (Salvaguarda de dados), ...
- Normas complementares do GSI/PR
- Normas NBR ISO/IEC 27.001/05, 27.002/05, 31.000 (Gestão de riscos), 15999 (GCN)
- Cobit 4.1 (e posteriores)
- Jurisprudência do TCU

Criando um CSIRT

Benefícios da existência de um CSIRT

- Possuir mecanismos de resposta a *incidentes de segurança*
  - Necessário definir o conceito de incidente de segurança para a instituição (negócio)
- Manter sua instituição preparada para as ameaças emergentes
- Aumento do grau de segurança ao desenvolver uma cultura de segurança
- Criação de mecanismos que visam à preservação da instituição

Eventos e Incidentes de Segurança

- Segundo [Scarfone et al. 2008] um ***evento*** é qualquer ocorrência observável em um sistema ou na rede
  - Ex: usuário que inicia de uma sessão SMTP, servidor web que recebe requisição HTTP, etc.
- Já um ***evento adverso*** é aquele que tem consequência negativa para a instituição
  - Ex: flooding de pacotes na rede, uso não autorizado de sistemas, etc.
- Consideraremos apenas eventos adversos relacionados à segurança do software dos computadores

Eventos e Incidentes de Segurança

- Segundo [CERT.br 2006] um ***incidente de segurança*** é um evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores
- Alguns exemplos:
  - Negação de Serviço
  - Código Malicioso
  - Acesso não autorizado
  - Uso inapropriado (violação de direitos autorais)

Eventos e Incidentes de Segurança

- Genericamente, [Scarfone et al. 2008] define um ***incidente de segurança*** como violação, ou suspeita de violação, de:
  - política de segurança da informação
  - política de uso aceitável
  - padrão de práticas de segurança de uma instituição
- Mais informações sobre esses documentos:
  - [CERT.br 2006]

Modelos de CSIRTs

- CSIRT centralizado
- CSIRT descentralizado
- CSIRT de crise
- CSIRT de coordenação
- CSIRT misto

Passos para criação do CSIRT

- Definição da área de atuação
- Definição do nome do CSIRT
- Definição de incidente e taxonomia
- Definição de tipo e modelo de CSIRT
- Definição dos serviços do CSIRT

Missão do CSIRT

- A missão do CSIRT deve refletir seu campo de atuação, escopo e representação
  - Constituency
- A missão deve estar alinhada com os objetivos e diretrizes da organização
- Vamos conhecer a missão de alguns CSIRTs

Missão do CSIRT

- Missão do CAIS/RNP

"O CAIS – Centro de Atendimento a Incidentes de Segurança atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes"

http://www.rnp.br/cais/sobre.html

Missão do CSIRT

- Missão do CERT/CC

"The CERT Program is chartered to work with the internet community in detecting and resolving computer security incidents, as well as taking steps to prevent future incidents"

CERT | Software Engineering Institute Carnegie Mellon

http://www.cert.org/meet_cert/meetcertcc.html

Missão do CSIRT

- Missão do CERT.br

"O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. É responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira"

cert.br 15 anos
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

http://www.cert.br/sobre/

Missão do CSIRT

- Missão do AusCERT

"AusCERT is the premier Computer Emergency Response Team (CERT) in Australia and a leading CERT in the Asia/Pacific region. AusCERT operates within a worldwide network of information security experts to provide computer incident prevention, response and mitigation strategies for members and assistance to affected parties in Australia."

AusCERT
Australian Computer Emergency Response Team.

http://www.auscert.org.au/

Serviços do CSIRT

- Existe uma gama de serviços que podem ser oferecidos por um CSIRT
- O CERT/CC divide os serviços em:
  - Reativos
  - Pró-ativos
  - Gerenciais

Serviços do CSIRT

Reativos

- Tratamento de incidentes
- Elaboração de alertas e anúncios
- Análise de artefatos
- Análise Forense

Pró-ativos

- Disseminação de informação
- Monitoramento
- Detecção de intrusão
- Auditoria de segurança
- Análise de vulnerabilidades
- Hardening
- Pentest
- Desenvolvimento de ferramentas de segurança

Qualidade

- Consultoria
- Análise de ricos
- Continuidade do negócio e plano de recuperação de desastres
- Desenvolvimento Seguro
- Educação e treinamento

Leitura recomendada

- Handbook for Computer Security Incident Response Teams

  http://www.cert.org/archive/pdf/csirt-handbook.pdf
- Creating and Managing an Incident Response Team for a Large Company

  http://www.sans.org/reading_room/whitepapers/incident/creating-managing-incident-response-team-large-company_1821
- RFC 2350: Expectations for Computer Security Incident Response

  http://www.ietf.org/rfc/rfc2350.txt

Exercício de Fixação

- Pesquise o Nome, Missão e Serviços de um CSIRT brasileiro, exceto os já apresentados anteriormente

Fundamentos de Tratamento a Incidentes de Segurança

Motivação

- Aumento do número de incidentes de segurança na Internet
  - Atividades preventivas são importantes, porém **nem todos os incidentes podem ser evitados** [Scarfone et al. 2008]
- Necessidade de estabelecimento de um Processo de Tratamento de Incidentes

Notificações de Incidentes de Segurança

- Principais causas de incidentes:
  - Ataques automatizados feitos por programas maliciosos (e.g. *bot* ou *worm*)
  - Pessoas mal intencionadas, usando ou não ferramentas automatizadas
- Em ambos os casos é importante alertar o responsável pelo sistema, organização ou rede em questão:
  - Notificações de Incidentes de Segurança
- Grande parte das notificações são enviadas pelos CSIRTs (Grupos de Resposta a Incidentes de Segurança)

Notificações de Incidentes de Segurança

- Dados essenciais a serem incluídos em uma notificação:
  - *logs* completos que evidenciem o incidente
  - data, horário e *timezone* (fuso horário) dos logs
  - endereço de origem do ataque, incluindo IP e porta da conexão
  - e-mail de origem
  - envio de informações em formato texto

Notificações de Incidentes de Segurança

- Encontrando o contato do responsável
  - Contato “abuse” no **WHOIS do Register** (ARIN, APNIC, LACNIC, RIPE, AFRINIC)
  - **Cyberabuse WHOIS**
    http://www.fr2.cyberabuse.org/whois/?page=whois_server
  - **Team Cymru WHOIS**
    http://asn.cymru.com/cgi-bin/whois.cgi
  - **Hurricane Electric Internet Service**
    https://bgp.he.net/
  - **Peering DB**
    https://www.peeringdb.com/advanced_search

Notificações de Incidentes de Segurança

- Encontrando o contato do responsável

Recebimento de incidentes

- Recebimento: um CSIRT deve possuir meios de receber notificações de incidentes, por intermédio de **e-mail**, formulários web (?), rede social (?) telefone (?), fax (?), carta (?), etc.

- Não se esqueça do /security no site web e dos endereços de e-mail (abuse, cert, csirt, security, fraud, phishing e spoof) – RFC 2142

Exercício

- Utilizando alguma dos serviços de WHOIS anteriores, verifique se os seguintes contatos estão corretos:
  - 218.234.18.106 abuse@hanaro.com
  - 71.240.222.159 abuse@verizon.net
  - 200.204.153.97 security@telesp.net.br
  - 192.111.229.50 security@rederio.br
  - 200.128.0.21 registro@rnp.br

Tratamento de Incidentes de Segurança

- O tratamento de incidentes de segurança envolve três funções [CERT/CC 2010]:
  - Notificação do incidente
  - Análise do incidente
  - Resposta ao incidente
- O tratamento sistemático e efetivo de incidentes exige a definição de um ***processo de resposta a incidentes de segurança***. Exemplos:
  - Ciclo de vida da resposta a incidentes [Scarfone et. al. 2008]
  - Processo de tratamento de incidentes de segurança da UFRGS [Ceron et. al. 2009]

Tratamento de Incidentes de Segurança

- Ciclo de vida da resposta a incidentes [Scarfone et. al. 2008]:

Tratamento de Incidentes de Segurança

Preparação

- Fase inicial que envolve o estabelecimento de um CSIRT, aquisição de ferramentas, etc.
- Medidas essenciais:
  - Atualização dos SO's e aplicações (anti-vírus, *patches*, etc.);
  - Garantir o registro das atividades dos usuários (logs dos sistemas);
  - Armazenamento seguro dos logs dos sistemas;

Tratamento de Incidentes de Segurança

Detecção e Análise

- Nesta etapa deve-se detectar ou identificar de fato a existência de um incidente.
- Principais atividades:
  - Recebimento e validação da notificação, e extração dos principais dados sobre o Incidente
  - Verificação nas bases de IDS/IPS, anti-vírus ou logs do sistema
  - Consulta na base de conhecimento sobre os incidentes reportados no passado

Tratamento de Incidentes de Segurança

Contenção, Mitigação e Recuperação

- Assim que o incidente é detectado e analisado, deve-se iniciar mecanismos de contenção para evitar que ele se propague ou afete outros recursos da rede
- Inicia-se então o trabalho para mitigação e recuperação dos sistemas afetados.
  - Importante: ***política de backup***

Tratamento de Incidentes de Segurança

Ações Pós-Incidente

- Esta etapa consiste em avaliar o processo de tratamento de incidentes e verificar a eficácia das soluções adotadas.
- Discutir as *lições aprendidas* com o CSIRT
- Resposta à notificação enviada

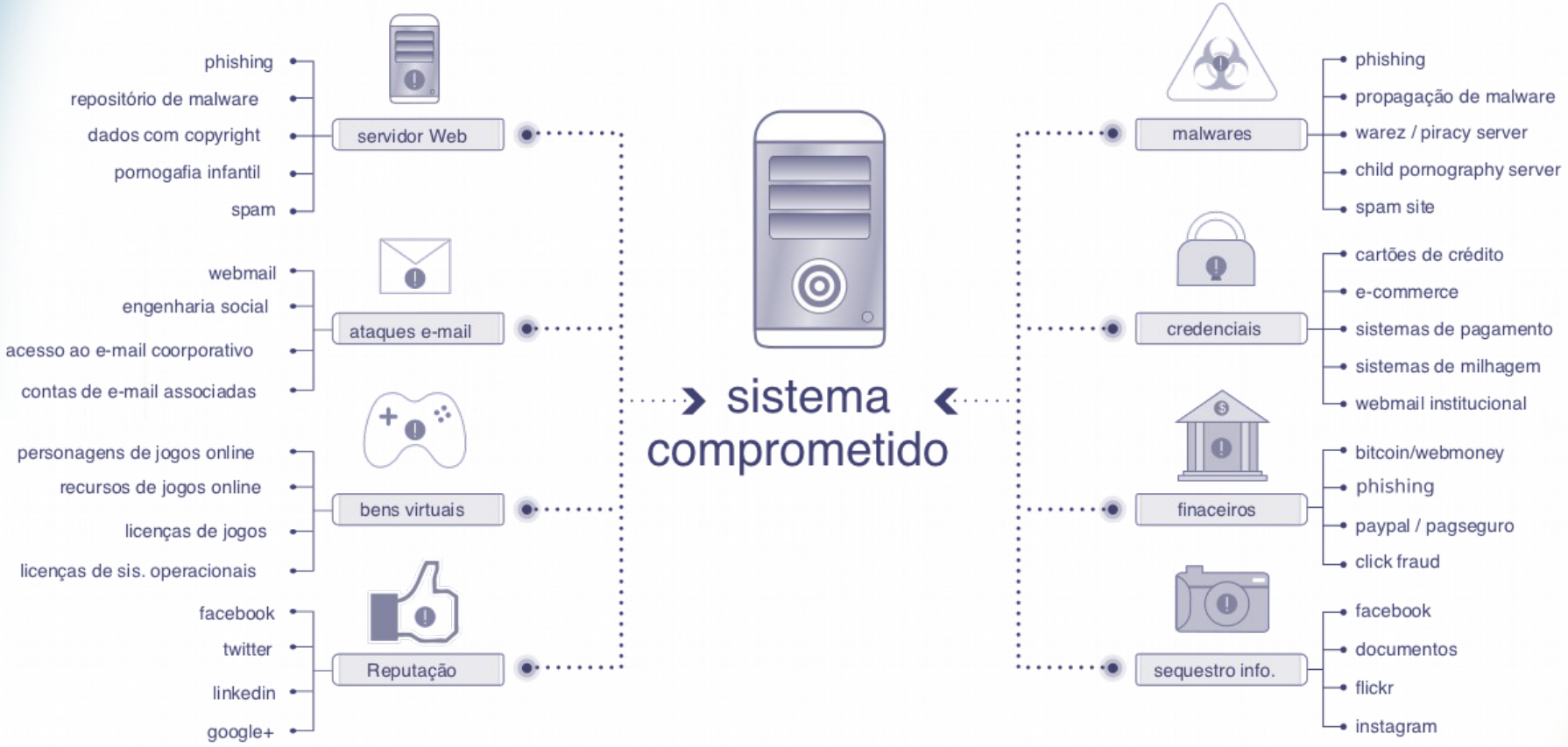
Taxonomia

Taxonomia

Identificar e classificar o tipo e prioridade de um incidente de segurança recebido (triagem), com base em metodologias consolidadas (ex: ENISA) ou características próprias

Determinar quais são os incidentes mais danosos à infraestrutura da instituição.

Taxonomia


phishing
repositório de malware
dados com copyright
pornogafia infantil
spam
servidor Web
webmail
engenharia social
acesso ao e-mail coorporativo
contas de e-mail associadas
ataques e-mail
personagens de jogos online
recursos de jogos online
licenças de jogos
licenças de sis. operacionais
bens virtuais
facebook
twitter
linkedin
google+
Reputação
sistema comprometido
malwares
phishing
propagação de malware
warez / piracy server
child pornography server
spam site
credenciais
cartões de crédito
e-commerce
sistemas de pagamento
sistemas de milhagem
webmail institucional
finaceiros
bitcoin/webmoney
phishing
paypal / pagseguro
click fraud
sequestro info.
facebook
documentos
flickr
instagram

Taxonomia

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES	DESCRIPTION
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content
	Harmful Speech	Discreditation or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals)
	Child/Sexual/Violence/ ...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.
Intrusions	Privileged account compromise	A successful compromise of a system or application (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.
	Unprivileged account compromise	

https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Taxonomia

Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) – or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
	DDoS	
	Sabotage	
	Outage (no malice)	
Information Content Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	Masquerading as another entity in order to persuade the user to reveal a private credential.
Vulnerable	Open for abuse	Open resolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.
Test	Meant for testing	Meant for testing

https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Taxonomia

Categoria	Descrição
copyright	Violação de Direitos Autorais
dos	Negação de Serviço
intrusao	Tentativa de intrusão ou intrusão de sistema ou rede
malware	Código Malicioso
phishing	Fraudes Eletrônicas
spam	Envio de SPAM
varredura	Varredura de redes ou sistemas
vulnerabilidade	Vulnerabilidade em rede ou sistema
web-defacement	Desfiguração de página web
vazamento	Vazamento de informações sensíveis
outros	Outros tipos de incidente

Fonte: Plano de Tratamento de Incidentes UFBA

Taxonomia

Criticidade = Impacto x Urgência

- Impacto: consequências negativas para a organização; como o incidente afeta os processos de negócio
  - Ex: incidente implica em perda de prazos legais
- Urgência: tempo aceitável para tratamento do incidente ou tendência de agravamento
  - Ex: precisa ser reestabelecido assim que possível

Matriz de criticidade e SLA

IMPACTO	URGÊNCIA		
	BAIXA	MÉDIA	ALTA
ALTO	3	2	1
MÉDIO	4	3	2
BAIXO	5	4	3

Prioridade	**Tempo Máximo para Solução (TMS)**
1	Em até 2hs
2	Em até 4hs
3	Em até 8hs
4	Em até 12hs
5	Em até 24hs ou em data posterior específica ou programada

Principais dificuldades

Principais Dificuldades

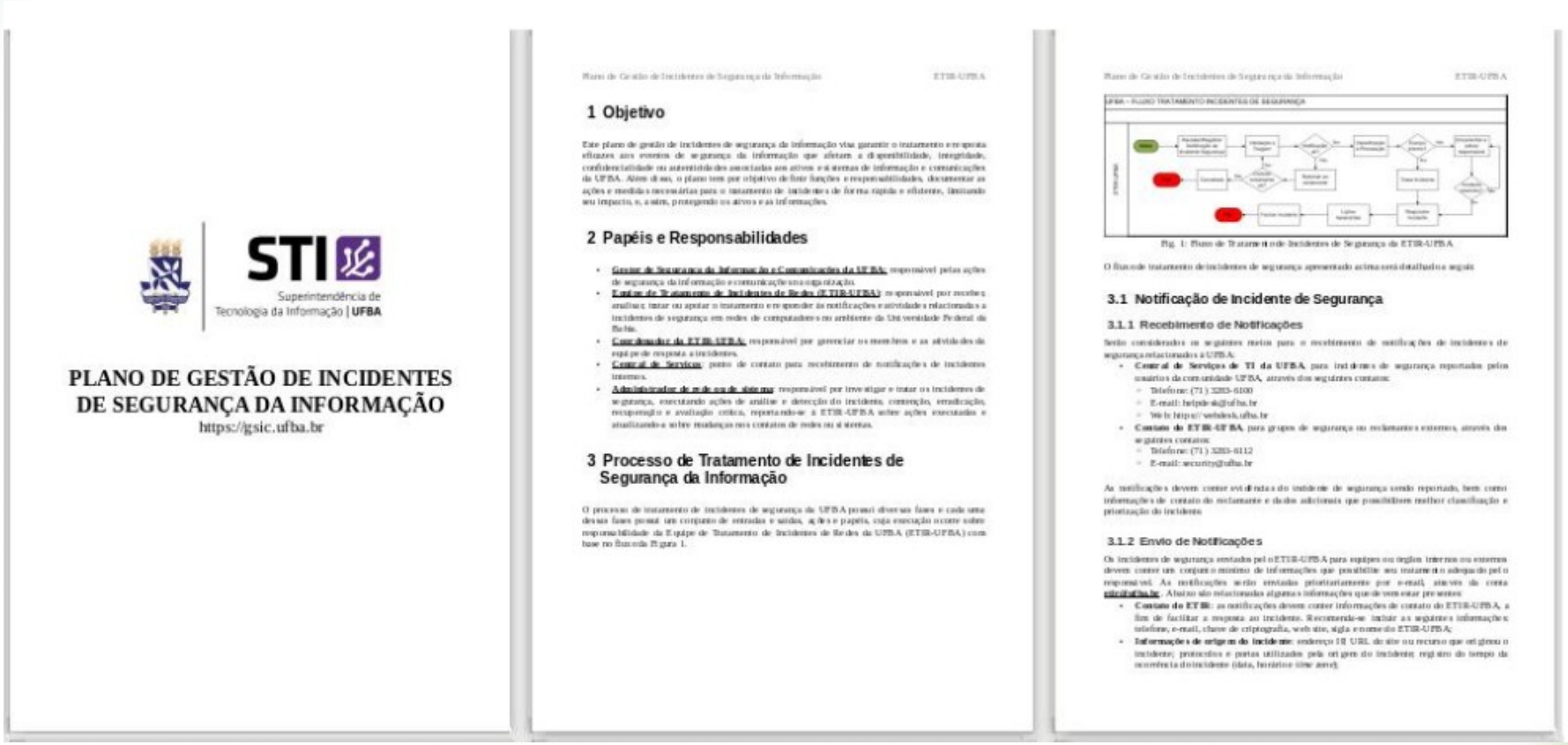
- Cada uma daquelas fases requer ações específicas de mitigação ou controle.
- Para incidentes que são gerados por uma instituição, alguns fatores podem dificultar seu tratamento, exemplo:
  - Tradução de Endereços de Rede (NAT)
  - Configuração dinâmica de rede nos hosts (DHCP)
  - Análise dos registros do sistema (logs)
  - Quantidade de notificações *versus* atribuições do CSIRT
  - ...

Boas práticas

Plano de Tratamento de Incidentes de Segurança

- Documento que descreve de maneira formal e geral o processo de tratamento de incidentes da organização
  - Papéis e Responsabilidades
  - Referências legais e normativas
  - Fluxo de tratamento de incidentes
  - SLAs e Procedimento de escalonamento
  - PDCA

Plano de Tratamento de Incidentes de Segurança



STI
Superintendência de Tecnologia da Informação | UFBA

PLANO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

https://gsic.ufba.br

Plano de Gestão de Incidentes de Segurança da Informação ETIR-UFBA

1 Objetivo

Este plano de gestão de incidentes de segurança da informação visa garantir o tratamento e resposta eficazes aos eventos de segurança da informação que afetam a disponibilidade, integridade, confidencialidade ou autenticidade dos ativos de informação e comunicações da UFBA. Além disso, o plano tem por objetivo definir funções e responsabilidades, documentar as ações e medidas necessárias para o tratamento de incidentes de forma rápida e eficiente, limitando seu impacto, e, assim, protegendo os ativos e as informações.

2 Papéis e Responsabilidades

- Gestor de Segurança da Informação e Comunicações da UFBA: responsável pelas ações de segurança da informação e comunicações na organização.
- Equipe de Tratamento de Incidentes de Redes (ETIR-UFBA): responsável por receber, analisar, tratar ou apoiar o tratamento e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no ambiente da Universidade Federal da Bahia.
- Coordenador da ETIR-UFBA: responsável por gerenciar os membros e as atividades da equipe de resposta a incidentes.
- Central de Serviços: ponto de contato para recebimento de notificações de incidentes internos.
- Administrador de rede ou de sistema: responsável por investigar e tratar os incidentes de segurança, executando ações de análise e detecção do incidente, contenção, erradicação, recuperação e avaliação crítica, reportando-se à ETIR-UFBA sobre ações executadas e atualizando-a sobre mudanças nos contatos de redes ou sistemas.

3 Processo de Tratamento de Incidentes de Segurança da Informação

O processo de tratamento de incidentes de segurança da UFBA possui diversas fases e cada uma delas fases possui um conjunto de entradas e saídas, ações e papéis, cuja execução ocorre sobre responsabilidade da Equipe de Tratamento de Incidentes de Redes da UFBA (ETIR-UFBA) com base no fluxo da Figura 1.

Plano de Gestão de Incidentes de Segurança da Informação ETIR-UFBA

Fig. 1: Fluxo de Tratamento de Incidentes de Segurança da ETIR-UFBA

O fluxo de tratamento de incidentes de segurança apresentado acima será detalhado a seguir.

3.1 Notificação de Incidente de Segurança

3.1.1 Recebimento de Notificações

Serão considerados os seguintes meios para o recebimento de notificações de incidentes de segurança relacionados à UFBA:

- **Central de Serviços de TI da UFBA**, para incidentes de segurança reportados pelos usuários da comunidade UFBA, através dos seguintes contatos:
  - Telefone: (71) 3283-6100
  - E-mail: helpdesk@ufba.br
  - Web: https://webdesk.ufba.br
- **Contato do ETIR-UFBA**, para grupos de segurança ou reclamantes externos, através dos seguintes contatos:
  - Telefone: (71) 3283-6112
  - E-mail: security@ufba.br

As notificações devem conter evidências do incidente de segurança sendo reportado, bem como informações de contato do reclamante e dados adicionais que possibilitem melhor classificação e priorização do incidente.

3.1.2 Envio de Notificações

Os incidentes de segurança enviados pelo ETIR-UFBA para equipes ou órgãos internos ou externos devem conter um conjunto mínimo de informações que possibilite seu tratamento adequado pelo responsável. As notificações serão enviadas preferencialmente por e-mail, através da conta etir@ufba.br. Abaixo são relacionadas algumas informações que devem estar presentes:

- **Contato do ETIR**: as notificações devem conter informações de contato do ETIR-UFBA, a fim de facilitar a resposta ao incidente. Recomenda-se incluir as seguintes informações: telefone, e-mail, chave de criptografia, web site, sigla e nome do ETIR-UFBA;
- **Informações de origem do incidente**: endereço IP, URL do site ou recurso que originou o incidente; protocolos e portas utilizados pela origem do incidente; registro do tempo da ocorrência do incidente (data, horário e time zone);

Boas práticas de tratamento de incidentes

- Ao reportar incidentes, deixar claro as evidências do incidente, Subject deve ser claro e direto
  - Utilizar templates para reportar incidentes
  - E-mail baseado em texto simples
- A fase de preparação é crucial para resposta a incidentes (coleta de logs, monitoramento, contenção)
- Utilizar criptografia na comunicação
- Gestão de ativos (inventário e contatos)

Boas práticas de tratamento de incidentes

- Seguir boas práticas de mercado
  - MANRS (Mutually Agreed Norms for Routing Security)
    - Filtragem
    - Anti-Spoofing
    - Coordenação
    - Validação global
  - Implantação de controles da ISO 27002
  - Gestão de Vulnerabilidades e Risco
  - Gerenciamento de logs centralizado e de qualidade

Boas práticas de tratamento de incidentes

- Princípio da participação universal
  - Treine as equipes que participarão do processo
  - Conscientize seus usuários para reportar incidentes de segurança
  - Disseminação da cultura de segurança para reduzir riscos (ex: ransomware)

Boas práticas de tratamento de incidentes

- Implante ferramentas e tecnologias de apoio
  - Gerenciamento de logs
  - Monitoramento de segurança
  - Contenção de ataques
  - Backup e restauração
  - ...
- Treinamentos técnicos para o CSIRT
  - Análise Forense
  - Offensive security (Ethical hacking, Pentest)
  - Troubleshooting e Hardening de Linux/Windows

Roteiro de Laboratório

- Roteiro de Laboratório 01: práticas de estabelecimento de CSIRT e processo de tratamento de incidentes

Referências

- Scarfone, K., Grance, T., and Masone, K. (2008). Computer Security Incident Handling Guide. NIST Special Publication, 800–61;
- CERT.br (2006). Cartilha de Segurança para Internet. Parte VII: Incidentes de Segurança e Uso Abusivo da Rede;
- CERT/CC (2010). Computer Segurity Incident Response Team FAQ.
- Ceron, J. et. al. (2009). O processo de tratamento de incidentes de segurança da UFRGS. In: IV Workshop de TI das IFES, 2009.
- CAIS (2016). Guia de boas práticas para estabelecimento de CSIRTS na Rede de ensino e pesquisa
- Valcy, I. e Alexandro, Y. (2017). Estabelecimento de CSIRTs e Processo de tratamento de Incidentes de Segurança em instituições acadêmicas brasileiras: estudo de caso da parceria CAIS/RNP e UFBA. TICAL