CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Democlydes Carvalho
Analista de Incidentes

5º Fórum Brasileiro de CSIRTs
22 de setembro de 2016

5º Fórum Brasileiro de CSIRTs
22 de setembro de 2016

Projeto de Coordenação de Exercício de Teste de Invasão em Órgãos da Administração Pública Federal

CENTRO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA DE REDES DE COMPUTADORES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

http://www.ctir.gov.br

CTIRGov

Democlydes Carvalho
Analista de Incidentes

Objetivo

Apresentar a origem, aspectos estudados e estudo de viabilidade para a composição do Projeto de Coordenação de Exercício de Teste de Invasão em Órgãos da Administração Pública Federal.

Sumário

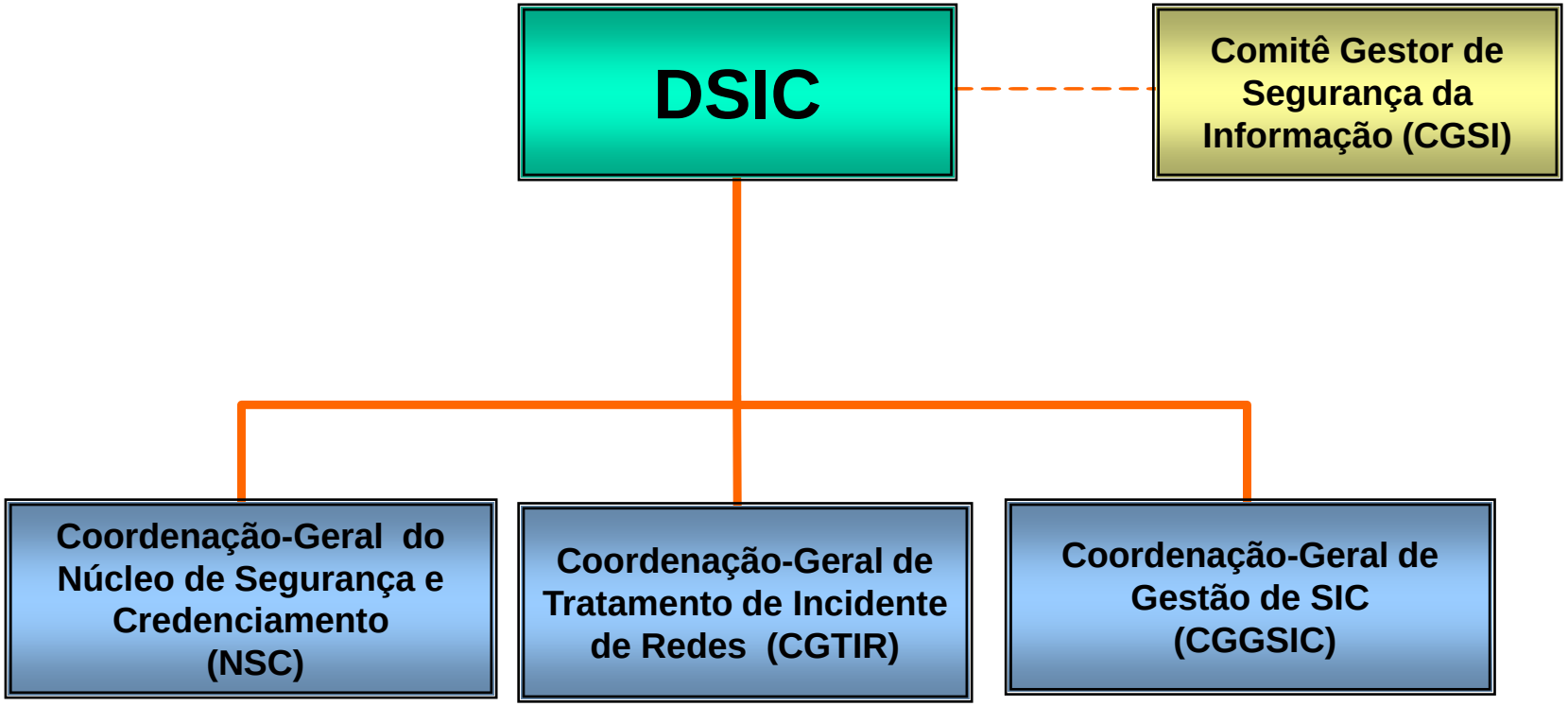
- CTIR GOV
- APF
- TESTES DE INVASÃO
- PROPOSTA DE ESCOPO
- CONCLUSÃO

CTIR GOV

AMBIENTAÇÃO

CTIR GOV
Ambientação

Assessoria Especial da Secretaria Executiva do Conselho de Defesa Nacional



Competência do GSI - PR

Lei 10.683, de 29 de maio de 2003:

Coordenação das atividades de Inteligência Federal e de Segurança da Informação.

DSIC

Decreto 5.772 de 08 de maio de 2006

Decreto 6.931 de 11 de agosto de 2009

Decreto 7.411 de 29 de dezembro de 2010

PLANEJAR E COORDENAR A EXECUÇÃO DAS ATIVIDADES DE SEGURANÇA CIBERNÉTICA E DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NA ADMINISTRAÇÃO PÚBLICA FEDERAL.

Arcabouço Normativo – CTIR Gov

Instrução Normativa GSI Nº 1 , de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. (Publicada no DOU Nº 115, de 18 Jun 2008- Seção 1)

Norma Complementar nº 05/IN01/DSIC/GSIPR , e seu **Anexo**, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1)

Norma Complementar nº 08/IN01/DSIC/GSIPR , Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 1)

Norma Complementar nº 21/IN01/DSIC/GSIPR , Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. (Publicada no DOU Nº 196, de 10 Out 2014 - Seção 1)

Centros de tratamento com responsabilidade nacional

CTIR GOV
Ambientação

Serviços Realizados

Capacitação
- Estágio CDCiber;
- Criação de ETIR´s;
- Colóquios técnicos.

Integração com outros atores:
- SRCC/DPF/MJ
- CERT.br/NIC.br;
- CAIS/RNP;
- CDCiber/MD.

Atuação em Grandes Eventos
- Rio+20;
- Copa das Confederações;
- Jornada Mundial da Juventude;
- Copa do Mundo FIFA 2014;
- Jogos Olímpicos.

Público-Alvo

Comunidade

-Órgãos e entidades da APF (direta e indireta);

-Órgãos Estaduais e Municipais;

Domínios

*.gov.br, *.mil.br, *.jus.br, *.leg.br e *.mp.br

O papel do CTIR Gov

✓ Os órgãos e entidades da APF deverão **comunicar de imediato a ocorrência dos incidentes** de segurança nas redes de computadores ao CTIR Gov, com vistas a permitir que sejam dadas soluções integradas para a APF, bem como a geração de estatísticas (NC n° 05 e 08 - DSIC/GSIPR).

✓ A comunicação de incidentes deverá seguir os "**Padrões para notificação de incidentes de segurança ao CTIR Gov**" (atualizado em agosto/2012).

✓ **Todas as notificações** ou mensagens recebidas pelo CTIR Gov são tratadas adequadamente após o processo de triagem e análise. Em alguns casos torna-se inviável relatar todos os procedimentos realizados aos requisitantes.

✓ O CTIR Gov **não realiza** procedimentos de **investigação criminal**. Eventuais desdobramentos dos incidentes são encaminhados às autoridades policiais competentes.

✓ O CTIR Gov atua como **Centro de Coordenação Nacional**, trabalhando de forma colaborativa e não tem a intenção de concorrer com as ETIR dos órgãos APF e dos Estados.

Mecanismos de Detecção (Tratamento de Incidentes)

- Mecanismo de detecção automatizado (robô de pesquisa).
  - ✓ *Scripts Perl* - Desfigurações, *spamdexing*, erros de código, etc.
  - ✓ *GSS - Google Site Search*
- Monitoramento de postagens em diversas fontes abertas (facebook, twitter, pastebin, pastehtml e outros) por meio de scripts e sites de busca.
- Notificações recebidas de colaboradores: outros CSIRTs, grupos de pesquisa, empresas de segurança e os órgãos da APF e dos Estados.
  - ✓ Projeto *Honeypots* Distribuídos - CERT.br (Blocos IP - APF)
  - ✓ DFL-CERT
  - ✓ *Botnets* Microsoft - *Government Security Program* (GSP)
  - ✓ *ModSecurity* (http://www.modsecurity.org) - Inclusão Remota de Arquivos (RFI) e outros
  - ✓ Parcerias com empresas de segurança
  - ✓ Customização do Request Tracker (RT)

Evolução da abordagem

2016	Melhoria dos processos automatizados visando obter melhor performance, e atualizar a documentação dos processos existentes (em andamento).
2014	Implantação do Data WareHouse de Incidentes integrado ao Sistema automatizado de incidentes.
2012	Aperfeiçoamento dos processos, ampliação do número de serviços oferecidos pelo CTIR Gov à APF e intensificação de trocas de informação com parceiros
2010	Implantação do RT (*Request Tracker*) como ferramenta para suportar o modelo de negócios do CTIR Gov
2008	Criação do “Modelo de melhoria de qualidade baseado em processos para tratamento de incidentes de rede na APF”
2006	Competências da CGTIR publicadas em Portaria Ministerial

Análise e Resposta aos Incidentes

- Para cada tipo de incidente o CTIR Gov possui um procedimento operacional padrão, em constante aperfeiçoamento. Dentre os diversos tipos de incidentes de segurança, destacam-se:
  - Abuso de sítios e páginas falsas;
  - Uso abusivo de servidores de e-mail;
  - Redirecionamento ou hospedagem de artefato ou código malicioso;
  - Ataques de negação de serviço;
  - Uso ou acesso não autorizado a sistemas ou dados;
  - Comprometimento de computadores ou redes;
  - Desrespeito à política de segurança ou o uso inadequado dos recursos de TI;
  - Ataques de engenharia social;
  - Cópia e distribuição não autorizada de material protegido por direitos autorais;
  - Uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes.

APF

APF

Responsabilidades

- ✓ “.gov.br” – Ministério do Planejamento
- ✓ “.mil.br” – Ministério da Defesa
- ✓ “.jus.br” – Conselho Nacional de Justiça
- ✓ “.leg.br” – Instituto Legislativo Brasileiro
- ✓ “.mp.br” – Conselho Nacional do Ministério Público

APF

Domínios/Subdomínios da APF

gov.br	jus.br	leg.br	mil.br	mp.br
ipen.br			eb.br	
cdtn.br			cebw.org	
foroiberam.org			cabw.org	
			rbjid.com	
			esg.br	

- Coleta de dados sobre os domínios do governo realizada em outubro de 2009 já identificava um total de 18.796 sítios sob o .gov.br, a partir de URLs percorridas.

APF

Órgãos

Administração direta do Poder Executivo

Presidência da república:

- Gabinete Pessoal
- Casa Militar (CM)
- Advocacia-Geral da União (AGU)
- Casa Civil (CC)
- Controladoria-Geral da União (CGU)
- Banco Central (BC)
- Núcleo de Assuntos Estratégicos,
- Secretaria da Micro e Pequena Empresa (SMPE)
- Secretaria de Assuntos Estratégicos (SAE)
- Secretaria de Aviação Civil (SAC)
- Secretaria de Comunicação Social (SeCom)
- Secretaria de Direitos Humanos (SDH)
- Secretaria de Políticas para as Mulheres (SPM)
- Secretaria de Portos (SEP)
- Secretaria de Relações Institucionais,
- Secretaria-Geral da Presidência (SG)
- Secretaria de Políticas de Promoção da Igualdade Racial (SEPPIR)

Ministérios

Desafios e Fatores Agravantes

Crescente conectividade abrem brechas na segurança das redes da APF.

Equipamentos com grande longevidade, ultrapassados e desatualizados, apresentando vulnerabilidades

A natureza crítica dificulta atualizações, identificações e correções de vulnerabilidades, uma vez que a interrupção do funcionamento de equipamentos afeta vários setores importantes da sociedade.

APF

Evolução dos Incidentes (confirmados)

- **2012** 7862
- **2013** 8393
- **2014** 9587
- **2015** 9480
- **2016** 5237 (primeiro semestre)

Influências

- Momento político (Governo, Eventos, Campanhas...).
- Rápido crescimento das Redes dos Órgãos.
- Baixa formação e emprego de gestores.
- Qualidade de mão de obra / Evolução e disseminação das ações de ataque.
- Maturidade / Reação às notificações / Falta da cultura de segurança.
- Falta de modelo de Política de Segurança
- Transição no CTIR Gov.

TESTES DE INVASÃO

TESTES DE INVASÃO

Orientação Normativa

- ESTRATÉGIA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES E DE SEGURANÇA CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL (2015 – 2018);

- Metas da Estratégia:
  - **2016**, a criação de Grupo de Trabalho objetivando a modelagem e o planejamento de exercícios de ataques cibernéticos às redes da APF; e
  - **2017**, o encaminhamento do resultado do Grupo de Trabalho de modelagem e planejamento de exercícios de ataques cibernéticos às redes da APF ao órgão central (GSI/PR).

Categorias de Avaliações

Toda organização utiliza diferentes tipos de **avaliações de segurança** para avaliar o **nível de segurança** de seus sistemas.

As categorias de avaliações são: **análise de vulnerabilidades**, **auditoria de segurança** e **teste de invasão**.

Cada tipo de avaliação requer habilidades profissionais diferentes.

TESTES DE INVASÃO

Conceitos

- ***Penetration testing (pentest)* - teste de penetração.**
  - Simulação de ataques reais para avaliar os riscos associados e as potenciais falhas de segurança nos sistemas corporativos.
  - Testes metodológicos com o objetivo de expor as possíveis vulnerabilidades em redes e sistemas operacionais
  - Pode ser estendida para websites, redes sem fio, banco de dados, aplicativos e programas.

TESTES DE INVASÃO

Motivação - ROI (Return of Investimet) de um teste de invasão

- Mostrar os custos resultantes de um ataque bem sucedido
- Comparar ao custo da própria execução do teste

TESTES DE INVASÃO

Preparação

- Levantamento de detalhes da infraestrutura (dispositivos críticos);
- Assinatura do NDA (do inglês, *Non-Disclosure Agreement*, ou Termo de Confidencialidade);
- Análise de amostragem (esferas de atuação);
- Seleção do formato da simulação; e
- Prazos

Teste de Invasão

Um teste de invasão avalia o **modelo de segurança** da organização como um todo.

Apresentar as consequências de forma mais próxima possível da realidade

- Um profissional que realiza testes de invasão se diferencia de um atacante apenas por seu intento e ausência de atitudes maliciosas.

Tipos de Testes de Invasão

- **Teste Externo**
  - disponibilidade de informações públicas,
  - enumerar os serviços da rede e o comportamento dos dispositivos de segurança analisados.

- **Teste Interno**
  - Pontos de acesso na rede, representando cada segmento físico e lógico.
    - **Black box** = zero conhecimento
    - **Grey box** = conhecimento parcial
    - **White box** = conhecimento total

Escopo de teste

- Definição do Escopo
- Equipes
- Fases
- Técnicas
- Ferramentas

Definição do Escopo

- Determinar o escopo do teste de invasão é essencial para decidir se o teste será um **teste direcionado ou um teste global.**
  - Avaliações globais - descobrir tantas vulnerabilidades quanto possível no sistema/organização avaliado.
  - O teste direcionado - identificar vulnerabilidades em um sistema específico.

- A definição de escopo determinará também:
  - A extensão do teste;
  - O quê será avaliado;
  - A partir de onde será testado;
  - Por quem será avaliado.

Divisão em Equipes

Equipe 01	Equipe 02
• Com o conhecimento e consentimento do setor de TI da organização. • Tem menor custo e é o mais frequentemente utilizado. • O papel primário é pensar sobre como ataques surpresa podem ocorrer.	• Sem o conhecimento do setor de TI da empresa, e com o consentimento da alta gerência. • Pode ser conduzido com ou sem o aviso. (teste anunciado ou não). • Propõe-se a detectar vulnerabilidades da rede e do sistema, e avaliar a segurança pelo ponto de vista do atacante.

Fases do Teste de Invasão

I. Aquisição de informação

II. Varredura

III. Ganhar acesso

IV. Manter acesso

V. Apagar rastros

Técnicas Comuns para Teste de Invasão

- Pesquisa passiva
- Monitoramento de atividades públicas
- Mapeamento de rede e SO’s
- *Spoofing*
- *Sniffing* de rede
- Ataques com *trojan*
- Ataques de força bruta
- Análise de vulnerabilidades
- Análise de cenário

Ferramentas

Fase / Técnica	Ferramentas
Aquisição de Informações	**Maltego -** http://www.paterva.com/web4/index.php/maltego **Binging** - http://www.blueinf.com/tools.html
Scanner de rede e enumeração	**Nmap** - http://www.nmap.org **Netifera** - http://netifera.com **AutoScan** - http://autoscan-network.com
Scanner de Vulnerabilidades	**Nessus** - http://www.nessus.org **NeXpose** - http://community.rapid7.com
Análise de Tráfego	**Wireshark** – http://www.wireshark.org/ **Tcpdump** - http://www.tcpdump.org/

Em busca e analisando: Scanner de Aplicação Web, Exploits, Live CDs, Auditoria de sistemas Windows e Unix, Avaliadores de aplicações...

Controles apontados a serem avaliados por um Teste de intrusão

- Segregação de redes Acesso remoto (filiais e escritórios) e VPN;
- Protocolos de comunicação de Aplicações Web e serviços; e
- Mecanismos de autenticação de usuários.

Documentação

- Criação de Grupo de Trabalho Inter setorial.
- Norma de incentivo (Por meio de cargos com poder de decisão, fundamentado através da assessoria (Secretarias) do GSI).
- Relatório com todos os processos envolvidos, desde a convocação e publicação em boletim.
- Realização de reuniões de ponto de controle.
- Criação do Relatório Gerencial detalhado.

Conclusões

Conclusões

- Os órgãos e entidades da Administração Pública Federal carecem de orientações mais específicas sobre “o que fazer” e “como fazer”, no que se refere à gestão segura de suas informações organizacionais.
- Dados coletados anteriores revelam o panorama da segurança da informação e delineiam a qualidade do tratamento dado pelos órgãos e entidades da APF à segurança da informação, o que pode ser ratificado por um processo simples de Teste de Intrusão.
- Diante da necessidade de garantir e incrementar a segurança da informação e comunicações e a fim de colaborar para a diminuição das vulnerabilidades e dos riscos apresentados, este estudo descreve uma proposta de metodologia para implementação de um formato próprio para execução de testes de penetração em órgãos da Administração Pública Federal (APF).

Trabalhos Futuros

- Este trabalho, ainda em andamento, não tem a pretensão de ser exaustivo a fim de esgotar todas as ações necessárias para implantar formatos de testes de penetração, assim é essencial que sejam realizados trabalhos que aprofundem este estudo e realizem a aplicação prática e a validação da metodologia.
- Finalizar a definição da ferramentas para a execução do projeto em sua completude.
- Analisar relatórios executados em outros países.

Referências

http://download.volcon.org/volday1/arquivos/palestras/luiz-vieira-ferramentas-livres-para-teste-de-invasao.pdf

http://www.seginfo.com.br/auditoria-teste-de-invasaopentest-planejamentopreparacao-e-execucao/.

http://www.cert.org/vulnerability-analysis/

ISO/IEC 27002. ABNT NBR ISSO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão de segurança da informação. Associação Brasileira de Normas Técnicas – Rio de Janeiro: ABNT, 2005.

MALERBA, C. Vulnerabilidades e Exploits: técnicas, detecção e prevenção. Universidade federal do Rio Grande do Sul – Porto Alegre, 2010.

BROCKE, Jan Vom; ROSEMANN, Michael (Eds). Handbook on Business Process Management: International Handbooks on Information Systems (Vol. 1). Berlin: Springer, 2010.

DSIC/GSIPR. DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO GABINETE DE SEGURANÇA INTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA. *Norma Complementar nº 02/IN01/DSIC/GSIPR*: Metodologia de Gestão de Segurança da Informação e Comunicações. Diário Oficial da República Federativa do Brasil. Brasília, DF, 14 Out 2008, nº 199 – Seção 1. Brasília, 2008.

Referências

DSIC/GSIPR. _____. *Norma Complementar nº 03/IN01/DSIC/GSIPR*: Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Diário Oficial da República Federativa do Brasil. Brasília, DF, 03 Jul 2009, nº 125 - Seção 1**.** Brasília, 2009a.

DSIC/GSIPR. _____. *Norma Complementar nº 04/IN01/DSIC/GSIPR*: Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. Diário Oficial da República Federativa do Brasil. Brasília, DF, 17 Ago 2009, nº 156 - Seção 1**.** Brasília, 2009b.

DSIC/GSIPR. _____. *Norma Complementar nº 05/IN01/DSIC/GSIPR*: Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Diário Oficial da República Federativa do Brasil. Brasília, DF, 17 Ago 2009, nº 156 - Seção 1**.** Brasília, 2009c.

DSIC/GSIPR. _____. *Norma Complementar nº 06/IN01/DSIC/GSIPR*: Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Diário Oficial da República Federativa do Brasil. Brasília, DF, 23 Nov 2009, nº 223 - Seção 1**.** Brasília, 2009d.

DSIC/GSIPR. _____. *Norma Complementar nº 07/IN01/DSIC/GSIPR*: Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Diário Oficial da República Federativa do Brasil. Brasília, DF, 07 Mai 2010, nº 86 - Seção 1**.** Brasília, 2010a.

OBRIGADO!

Democlydes Carvalho – democlydes@gmail.com

http://www.ctir.gov.br

ctir@ctir.gov.br(notificação de incidentes)

cgtir@planalto.gov.br (assuntos diversos)

INOC-DBA: **10954*810**