Aspectos de Segurança na Internet: Evolução e Tendências Atuais

NIC BR Security Office
nbso@nic.br
http://www.nic.br/nbso.html

Cristine Hoepers
cristine@nic.br
Klaus Steding-Jessen
jessen@nic.br

COMDEX 2001
São Paulo
29 de agosto de 2001

Notas:

Nota sobre a Distribuição desse Documento
É permitido fazer e distribuir cópias inalteradas deste documento, completo ou em partes, contanto que os autores originais sejam citados e esta nota sobre a distribuição seja mantida em todas as cópias. Se este documento for distribuído apenas em partes, instruções de como obtê-lo por completo devem ser incluídas.

Notas:

Aspectos de Segurança na Internet

- Histórico
  - Evolução
  - Mudança do Perfil
- Tendências Atuais
  - Segurança: O Processo
  - Papel dos CSIRTs
- O Cenário Atual

Notas:

Histórico

Notas:

Final do Anos 60 – Internet

- Projeto não considera implicações de segurança
- Comunidade de pesquisadores
- Confiança

Notas:

1986

- "Cookoo's Egg"
  - 30+ sistemas invadidos
  - contas/senhas óbvias
  - vulnerabilidades em softwares
  - tempo e persistência

Notas:

1988

- Internet Worm - Robert Morris Jr.
  - furos do sendmail e finger
  - uso do arquivo `.rhosts`
  - 6000+ computadores atingidos
  - criação do CERT/CC
  - mobilização em torno do tema segurança

Notas:

1989

- WANK Worm
  - VAX/VMS
  - Propagava-se apenas via DECnet
  - Senhas padrão / fracas
  - necessidade de melhor comunicação entre times

Notas:

1991

- Popularização da Engenharia Social
  - solicitação de troca de senhas
  - "programas de teste"
- RPC mountd SunOS
  - buffer overflow
  - acesso remoto ao sistema de arquivos

Notas:

1992

- Vários sites comprometidos
  - roubo de senhas
  - root a partir de conta comum
  - trojans (`su`, `login`, etc)
  - backdoors

Notas:

1993

- Ferramenta de Scanning de Vulnerabilidades
  - Internet Security Scanner (ISS)
  - postada em `comp.sources.misc`
  - procura vários furos: contas default, bugs do sendmail, NFS, NIS, etc

Notas:

1994

- Network Sniffing / rootkits
  - comprometimento de root
  - instalação de sniffers
  - instalação de "rootkits"

Notas:

1995

- IP Spoofing
  - Problema do TCP/IP descrito em 1989
  - Afetam aplicações que usam IP de origem como autenticação

Notas:

1996

- Denial of Service (DoS)
  - UDP (loop entre `chargen` e `echo`)
  - SYN Flood
  - ping com tamanho grande

Notas:

1997

- Ataques a servidores Web (CGI scripts)
  - count.cgi
  - webdist.cgi
  - nph-test-cgi

Notas:

1998

- Buffer overflow em clientes de Mail
  - MIME
  - rodar código arbitrário
- Trojans para Windows
  - Back Oriffice (BO)

Notas:

1999

- Melissa
  - virus de macro Word
  - propaga-se via attachments de mail
  - milhares de hosts infectados

Notas:

1998 – 1999

- aumento significativo de:
  - ferramentas de ataque automático
  - administradores reportando incidentes
  - maior divulgação de incidentes

Notas:

2000

- aumento significativo de:
  - DDoS
  - invasão de DSLs e cable modems

Notas:

1999 – 2000

- aumento significativo de:
  - vírus / backdoors para Windows
  - máquina de usuários finais comprometendo toda a rede
  - vírus se propagando automaticamente
  - usuários finais vulneráveis

Notas:

2001

- Worms
  - velocidade de propagação
  - exploram vulnerabilidades conhecidas
  - máquina infectada vulnerável a outros invasores
- Exemplos: Code Red, Sircam, Ramem

Notas:

Incidentes Reportados ao NBSO em 1999

Mês	Total	axfr	usuário	dos	invasão	web	scan
jan	204	89	5	7	14	22	67
fev	172	75	5	1	6	31	54
mar	203	100	7	5	12	19	60
abr	151	60	8	0	2	0	81
mai	145	68	10	1	7	2	57
jun	192	76	17	2	9	8	79
jul	208	46	26	0	10	14	110
ago	385	74	167	0	35	8	100
set	264	97	85	1	3	4	74
out	269	86	34	1	7	7	134
nov	418	55	148	1	14	18	182
dez	496	19	146	2	9	50	270
Total	3107	845	658	21	128	183	1268

Notas:

Incidentes Reportados ao NBSO em 2000

Mês	Total	axfr	usuário	dos	invasão	web	scan
jan	424	28	108	11	3	57	217
fev	509	61	78	8	11	80	270
mar	541	55	117	14	8	38	309
abr	351	19	93	17	5	22	194
mai	480	12	145	15	11	28	267
jun	641	7	215	8	17	20	374
jul	585	2	80	13	17	22	450
ago	432	2	112	6	13	16	280
set	337	3	90	6	15	12	209
out	468	0	139	4	7	17	301
nov	573	2	167	34	13	57	295
dez	656	9	196	23	7	46	372
Total	5997	200	1540	159	127	415	3538

Notas:

Incidentes Reportados ao NBSO em 2001 (primeiro trimestre)

Mês	Total	axfr	usuário	dos	invasão	web	scan
jan	896	5	206	11	17	29	619
fev	1040	2	164	6	18	48	799
mar	1202	0	114	9	19	39	1019
Total	3138	7	484	26	54	116	2437

Notas:

Comparativo dos Incidentes Reportados ao NBSO

Ano	Total	axfr	usuário	dos	invasão	web	scan
1999	3107	845	658	21	128	183	1268
2000	5997	200	1540	159	127	415	3538
2001*	3138	7	484	26	54	116	2437

(*) apenas jan–mar

Notas:

Tendências Atuais

Notas:

Problemas

- Sistemas vulneráveis por "default"
- Complexidade crescente dos sistemas
- Dificuldade em acompanhar todos os patches

Notas:

Problemas (Cont.)

- Ataques não são barrados pela maioria dos firewalls (e.g.: IIS, DNS, Vírus)
- Facilidade em ocultar os passos de uma invasão
- Exploits são lançados antes dos patches

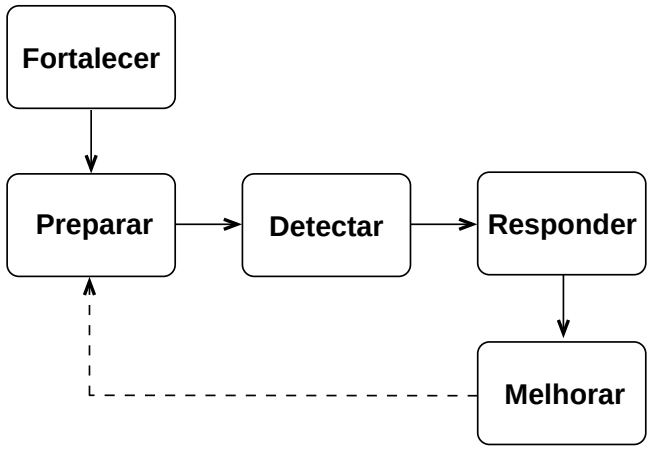
Notas:

Convivendo com os problemas

- Processo de Segurança:
  - Políticas de Segurança
  - Escolha do ambiente
  - Detecção de Intrusão
  - Atualização Constante
- Resposta a Incidentes: CSIRT

Notas:

O Processo



Notas:

Fortalecer

- Escolher softwares cautelosamente
  - segurança X "facilidade"
  - cada sistema possui sua finalidade
- Nunca usar configuração default
- Instalar firewalls, IDSs, etc
- Atualizar o sistema (patches)

Notas:

Preparar

- Estar preparado para detectar ataques não conhecidos
- Conhecer o ambiente
- Monitorar freqüentemente logs e sistemas
- Estar familiarizado com ferramentas de segurança

Notas:

Detectar

- Monitorar logs e sistemas
- Identificar comportamentos não usuais
- Analisar as informações geradas pelas ferramentas
- Investigar incidentes reportados
- Cruzar informações

Notas:

Responder

- Conter os efeitos de uma invasão
- Analizar os efeitos, conseqüências e possíveis causas
- Coletar evidências
- Determinar o escopo do problema
- Recuperar o ambiente

Notas:

Melhorar

- Análise detalhada post-mortem
- Revisar Políticas e procedimentos
- Revisar/alterar configurações e ferramentas
- Possivelmente retornar a todos os passos anteriores

Notas:

CSIRT – Computer Security and Incident Response Team

Um grupo ou organização que provê serviços e suporte para um público bem definido, para prevenção, tratamento e resposta a Incidentes de Segurança.

- Ponto central de contato
- Provê informações para o seu público
- Troca informações com outros CSIRTs

Notas:

Papel do CSIRT

- Coordenar ações
- Determinar o impacto
- Prover recuperação rápida
- Preservar evidências
- Prover recomendações e estratégias

Notas:

Serviços do CSIRT

- Tratamento de Incidentes
- Detecção de Intrusão
- Análise de Artefatos/Vulnerabilidades
- Rastreamento de Invasões
- Auditoria e Teste de Invasão
- Análise de Riscos

Notas:

Autoridade do CSIRT

- Completa
- Parcial
- Indireta
- Sem autoridade

Notas:

Cenário Atual

Notas:

Cenário Atual

- Grande número de vulnerabilidades
- Falta de preocupação por parte das empresas
- Poucos administradores de redes
- Raros CSIRTs estabelecidos
- Falta de Legislação

Notas:

Cenário Atual (cont.)

- Invasores com pouco nível de conhecimento
- Comunicação rápida e eficiente entre invasores (email, WEB, conferências, chats, etc)
- Ferramentas automáticas
  - scans/probes/invasão
  - rootkits
  - ataques coordenados em grande escala

Notas:

Cenário Atual (cont.)

- Banalização do "Consultor de Segurança"
- "ex"-invasores vendendo "proteção"
- "saber" invadir = saber proteger?

Notas:

Leitura Recomendada

- Secrets & Lies – Digital Security in a Networked World, Bruce Schneier, ISBN 0-471-25311-1, http://www.counterpane.com/sandl.html
- Sites de referência http://www.nic.br/links.html

Notas: