Formação para Sistemas Autônomos

Tratamento de Incidentes

Licença de uso do material

Tratamento de Incidentes

- Introdução e Terminologia
- Detecção
- Triagem
- Notificação
- Geração, coleta e análise de log
- Análise de incidentes
- Contatos e Whois
- Resposta e recuperação
- Ameaças Internas
- Problemas com e-mail
- Malware

Terminologia

- Notificação de Incidente:
  - Notificação de atividade de segurança ou eventos
- Tratamento de Incidente:
  - Processo de notificar, analisar e responder incidente
- Intrusão:
  - Ganhar acesso não autorizado; Violar política de segurança
- Vulnerabilidade:
  - Potencial falha de sistema que pode gerar um incidente

Terminologia

- Evento:
  - Qualquer atividade dentro da empresa
- Atividade:
  - Evento suspeito que pode estar relacionado ou não a segurança
- Incidente:
  - Evento que necessita de análise e ou tratamento
- Ataque:
  - Tentativa de violação da política de segurança

CSIRT - Computer Security Incident Response Team

- Time ou pessoa que provê serviços e suporte a um público-alvo definido visando prevenir, tratar e responder a incidentes de segurança de computadores
- Importante definir o público-alvo e objetivo
- Não é o suporte técnico da organização
- Tem o objetivo de:
  - Minimizar e controlar o dano
  - Prover ou ajudar na recuperação
  - Atuar na prevenção de eventos futuros
  - Ser ponto de contato único para notificação de problemas
  - Coordenar os esforços de tratamento

Percepção da Situação

- Você precisa saber o que está acontecendo ao seu redor
- É importante correlacionar informações recebidas, às vezes sem relação evidente, com os incidentes que estão acontecendo
- Esta correlação pode ajudar a tomar melhores decisões

Monitoramento Público

- Um incidente na sua organização pode estar relacionado com informações públicas recebidas, como um relatório de vulnerabilidades ou um grande evento ocorrendo na cidade ou país
- Estas informações podem ser fornecidas por outros CSIRTs, fornecedores de software e hardware, sites de segurança e até de mídias não especializadas como jornais e portais

Tratamento de Incidentes

- Habilidade de prover gerência fim a fim de eventos e incidentes por toda a empresa que afetem os ativos de tecnologia da informação e informações dentro de uma organização

Detecção de problemas

- Detecção de atividade suspeita que possa comprometer a missão do público-alvo
- Pode ser feita por detecção reativa:
  - E-mail, telefonema, formulário, outros CSIRTs etc
- Pode ser feita por detecção pró-ativa:
  - Monitoramento de rede, escaneamento de rede, sistemas antivírus, sistema de detecção de intrusão etc

Detecção de problemas

- Flows (nfdump e nfsen)
- Sensores e honeypots (dionaea ou converse com a equipe do CERT.br no próximo GTS)
- Feeds de dados: Shadowserver, Cymru
- Habilitar log de consultas no DNS recursivo
  - Pode permitir detecção de spambots e phishing

Triagem

- Crítico para grupos grandes ou muitas notificações
- Definição de prioridades
  - Crítica, Alta, Média, Baixa
  - Priorizar informações de outros CSIRTs
- Definição de categorias
  - Roubo de Informação, Detecção de Vulnerabilidade, Detecção de Malware, Pedido de Informação, Incidentes Gerais, Outros
- Não crie categorias e prioridades em demasia
- LEMBRE-SE DO SEU OBJETIVO!!!

Notificação

- A Internet depende do bom relacionamento entre ASes
- Quando notificado seja um bom “cidadão da Internet”, ajude na resolução do problema

Geração de logs

- Log sem sincronização de relógio (NTP) é inútil
- Formato de data: RFC3339 ou ISO8601
  - aaaa-mm-ddThh:mm:ss-fhfh:fmfm
  - 2012-12-19T16:39:57-08:00
  - “T” exigido na ISO8601, mas pode ser “ ” na RFC3339
- Coerência de fuso horário

Coleta de logs

- Coletar logs é fácil, mas é preciso planejar o armazenamento para que estes possam ser recuperados adequadamente para a análise
- Os logs devem ser fáceis de usar
- Definir período e tamanho do armazenamento
- Se possível automatizar geração de relatórios
- Na recuperação dos logs:
  - É possível usar scripts?
  - É possível correlacionar logs distintos?
  - É possível gerar alarmes em tempo real?

Análise de Incidentes

- Lembre-se que um log pode não ter todas as respostas sozinho
- É importante conseguir correlacionar logs, emails, notificações recebidas e até notícias
- Pode ser que você não tenha todas as informações e tenha que interagir com outros CERTs ou empresas para fazer a análise

Contatos e Whois

- Divulgando seus dados:
  - Informações do AS: abuse-c apontando para o CSIRT
  - Informações por blocos IP: abuse-c ou tech-c
  - Informações de domínio: os domínios sobre responsabilidade da sua organização devem conter os dados do CSIRT
- Você pode ser contatado quando um domínio dentro do seu AS ou bloco IP estiver comprometido
- RFC2142: Mailbox Names for Common Services, Roles and Functions
- Seus contatos devem estar atualizados
- E-mails para estes contatos não devem ser filtrados com antispam. Devem ter política diferenciada.

Contatos e Whois

- Contatar a respeito de domínios maliciosos, não use as informações do domínio, mas sim do AS ou do bloco IP
- Se descobriu um problema, notifique o terceiro para ajudar na resolução do problema
- Se precisar de ajuda, contate o CERT.br
- Qualquer AS pode solicitar um VOIP INOC para contato com outros Ases

Resposta a Incidentes

- Analise a situação:
  - Informações recebidas, logs, análise forense, impacto ao negócio, risco ao negócio
- Planeje:
  - Defina o que fazer e quem deve ser contatado
- Coordene:
  - Interaja internamente e com outras equipes para resolver ou mitigar o incidente
- Finalize:
  - Informe aos envolvidos atualizações no incidente e o resultado final
  - Documente o ocorrido, isto pode ser útil em incidentes futuros

Ameaças Internas

- Ex-empregados e empregados atuais, parceiros e terceiros que tem ou tiveram acesso aos seus sistemas
- Eles podem ser responsáveis por fraudes, roubo de informações ou mesmo sabotagem de sistemas
- Controle e monitoramento são as melhores formas de se proteger

Problemas com e-mail

- Spoofing:
  - Parece vir de uma fonte legítima, mas é na verdade uma falsificação
- Spamming:
  - Envio massivo de emails não solicitados, pode ser de propaganda ou de tentativas de fraude
- Phishing:
  - Tentativa de roubo de dados pessoais e financeiros combinando meios técnicos e engenharia social

Malware

- Software que executa em um sistema sem autorização com objetivo malicioso
- Pode buscar obter informações não autorizadas, alterar o comportamento de um sistema, gerar negação de serviço entre outros problemas
- Incluí vírus, cavalos de tróia, worms, backdoors, spyware, botnet etc

Notificações de Direitos Autorais

- Defina sua política com o seu departamento jurídico ou consultor jurídico externo
- Interagir com o notificar para confirmar fuso horário, datas, se o horário estava sincronizado com NTP para validar a notificação antes de proceder para o próximo passo
- Por exemplo, existem ASes que repassam a notificação ao usuário se a mesma for validada, mas que descartam a notificação se não receber validação por parte do notificador

Notificações Policiais e Judiciais

- Se o crime for detectado por sua organização a decisão de contatar a Justiça deve considerar políticas previamente definidas ou decisão conjunta envolvendo a área jurídica
- Se o crime for notificado a sua organização, esta deve oferecer as informações solicitadas e agir com cautela para evitar a destruição de evidências, por exemplo, desligar um computador apaga o conteúdo na memória RAM, salvar arquivo altera um disco etc

Dúvidas?