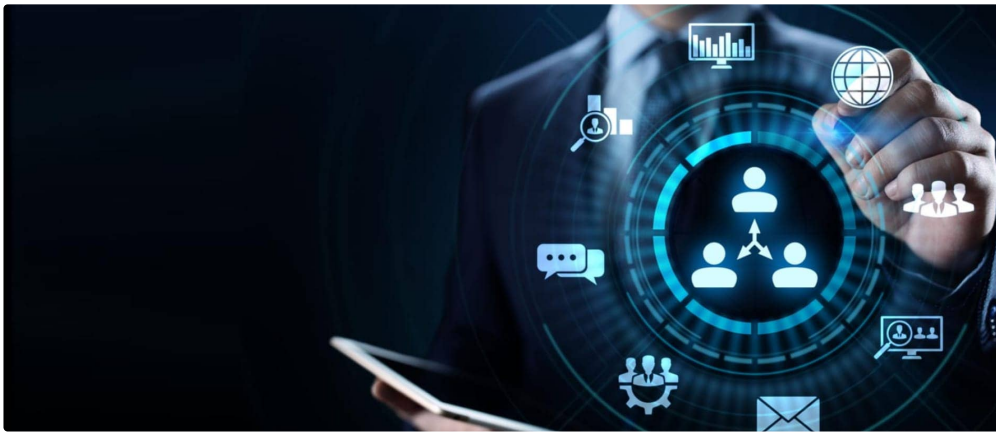


Respostas à incidentes e recuperação (disaster recovery)

Prof. Pedro Eduardo Silva Sá

Descrição

Resposta a incidentes e recuperação de desastres e sua importância para a continuidade de negócios.

Propósito

Não importa quão seguro um sistema possa ser, a ocorrência de um incidente é uma questão de tempo. Os conhecimentos apresentados neste conteúdo vão ajudar você a identificar, responder apropriadamente, investigar e se recuperar de desastres ocasionados por incidentes de segurança.

Objetivos

Módulo 1

Resposta a incidentes

Identificar os princípios básicos de um plano de resposta a incidentes e CSIRT.

Módulo 2

Correção de vulnerabilidades

Identificar as etapas do processo de gestão de vulnerabilidades e do processo de gerenciamento de patches.

Módulo 3

Forense computacional

Descrever os conceitos de computação forense, suas técnicas e ferramentas.

Módulo 4

Disaster Recovery Plan

Descrever o plano de recuperação de desastres e as diretrizes para sua obtenção.

Introdução

A ocorrência de um incidente é um momento pelo qual nenhuma organização quer passar, mas é inevitável que isso ocorra um dia. Nesse ponto, todos os controles de segurança falharam e uma ameaça conseguiu explorar com sucesso uma vulnerabilidade à qual sua organização estava exposta, impactando, de alguma forma, ativos e, consequentemente, os processos de negócio que eles suportam. Entender como lidar com essa situação, bem como responder, investigar e se recuperar de forma adequada é de suma importância para manter a viabilidade da organização frente a um ambiente adverso e, muitas vezes, caótico.

1 - Resposta a incidentes

Ao final deste módulo, você será capaz de identificar os princípios básicos de um plano de resposta a incidentes e CSIRT.

Conceitos básicos de evento e incidente

Um **Sistema de Informação** (SI) é, de forma sucinta, um conjunto de dispositivos eletrônicos (hardware) capazes de processar informações de acordo com uma programação (software) definida por um operador (peopleware). Nesse sentido, podemos entender que existem diversas interações entre os componentes básicos de um SI, e a essas interações damos o nome de **evento**.

Mas você sabe a diferença entre evento e incidente? Veja a seguir.

Evento	Incidente
É qualquer ocorrência observável dentro de um SI.	É todo evento que resulta em uma consequência negativa

Exemplo: a criação de um arquivo, a impressão de uma informação, uma requisição web etc.

para a organização ou o SI.

Exemplo: a indisponibilidade de um sistema crítico, o vazamento de dados pessoais, a ação de malware etc.

Assim, podemos observar que um incidente é uma violação ou ameaça iminente das políticas de segurança da informação, políticas de uso aceitável ou práticas de segurança padrão definidas pela organização.

Comentário

É inevitável que incidentes ocorram. Por isso, a capacidade de resposta é um fator crucial para a sobrevivência de qualquer organização. A reação tempestiva reduz o tempo de indisponibilidade dos sistemas envolvidos e, consequentemente, os prejuízos.

Então, podemos entender que **resposta a incidentes** não é somente "apagar incêndios" do dia a dia, mas deve ser uma prática metodológica, processual e organizada para tratar e gerenciar incidentes de segurança, limitando os danos e reduzindo os custos de recuperação.

Plano de resposta a incidentes e CSIRT

Dado tal cenário, as organizações devem implementar um **plano de resposta a incidentes**, que auxiliará a organização a lidar com um incidente de forma rápida, eficiente e com o mínimo de danos possíveis. Isso é feito observando os seguintes passos:

Identifique e priorize ativos

É crucial que a organização tenha seus ativos de hardware e software inventariados. Depois de identificar os ativos, priorize-os de acordo com a importância e o risco envolvido. Certifique-se de quantificar o valor agregado dos ativos inventariados, pois isso ajudará a justificar o orçamento de segurança.

Identifique os riscos potenciais

Observe as maiores ameaças da atualidade contra os sistemas de negócios da organização. Isso será diferente para cada organização.

Estabeleça procedimentos

Deve existir um conjunto de procedimentos estabelecidos e, principalmente, praticados e treinados. Um funcionário em pânico pode cometer erros cruciais que poderão custar caro para a organização. As políticas e procedimentos para lidar com um incidente devem incluir:

1. Como identificar e conter um incidente.
2. Registro de informações sobre o incidente.
3. Plano de notificação e comunicação.
4. Treinamento dos colaboradores.

Configure uma equipe de resposta

Para lidar com ataques sofisticados e furtivos, incluindo Ameaças Persistentes Avançadas (APT), deve ser composta uma Computer Security Incident Response Team (CSIRT) ou Equipe de Resposta a Incidentes de Segurança em Computadores, equipada e pronta para agir rápido. Essa equipe pode ser interna permanente, *ad-hoc* ou terceirizada.

Os componentes uma CSIRT, com suas responsabilidades básicas, são:

1. **Líder de equipe**

   Coordena todas as atividades da equipe de resposta a incidentes.

2. **Comunicações**

   Gerencia as comunicações em toda a organização e com terceiros, incluindo a mídia. Deve ser treinado ou apoiado pelo departamento de relações públicas.

3. **Investigador líder**

   Reúne e analisa evidências técnicas, determina a causa do ataque e orienta outros analistas e componentes para implementar a recuperação do ativo.

4. **Analistas e pesquisadores**

   Apoiam o investigador, fornecendo inteligência de ameaças e contexto para o incidente. Analistas forenses podem ser necessários para realizar análises profundas em sistemas comprometidos.

5. **Representante jurídico**

   Ter recursos humanos e orientação legal são essenciais para lidar com possíveis acusações criminais derivadas do incidente.

Treinamento

Ter apenas um plano de resposta a incidentes não ajudará muito em um incidente sem o devido treinamento da equipe. Os colaboradores e a CSIRT precisam estar cientes do plano e ser devidamente treinados sobre o que devem fazer.

Dica

Teste o plano de resposta por meio de exercícios controlados. Esses exercícios familiarizam os colaboradores e a CSIRT diante da ocorrência de um potencial incidente. Por meio do teste do plano, é possível identificar e resolver lacunas, bem como ajudar todos os envolvidos a ver como podem melhorar. A hora mais adequada para fazer isso é quando não há risco real para os ativos da organização.

Fases de uma metodologia de resposta a incidentes

O National Institute of Standards and Technology (**NIST**), por meio da publicação *NIST SP 800-61r2 Computer Security Incident Handling Guide*, descreve as etapas do processo de Incident Handling (tratamento de incidentes). Estas etapas são:

Preparação

Esta primeira etapa estabelece objetivos básicos para responder a incidentes de forma mais eficaz. Ela engloba:

1. O estabelecimento de uma política organizacional visando definir o que é um incidente de segurança e se ocorreu ou não um incidente.
2. A criação de um plano de resposta ou estratégia para tratamento de incidentes, incluindo a priorização de incidentes baseados no impacto organizacional.
3. A formação de um plano de comunicação para que os indivíduos e grupos que necessitem ser informados de um incidente ou sua mitigação sejam mantidos cientes sobre os eventos relacionados ao incidente.
4. O estabelecimento de requisitos de documentação para que informações precisas e relevantes sobre cada incidente sejam registradas para referência futura.
5. A formação de uma Computer Security Incident Response Team (CSIRT), ou Grupo de Resposta a Incidentes de Segurança, que deve abranger pessoas de diferentes áreas da empresa para tratar de problemas que podem surgir durante um incidente.
6. A garantia de que a CSIRT tenha o acesso, permissões e ferramentas necessárias para responder de forma adequada aos incidentes.
7. A educação da CSIRT, equipe de TI e usuários finais sobre políticas de segurança, bem como suas funções de relatar e responder a incidentes de segurança.

Veja, a seguir, os itens que compõem o checklist desta etapa:

- ✓ Todos foram treinados com base nas políticas de segurança?
- ✓ As políticas de segurança e o plano de resposta a incidentes foram aprovados pela gerência apropriada?
- ✓ A CSIRT conhece suas funções e as notificações necessárias para fazê-lo?

- [ ] Todos os membros da CSIRT participaram de simulações?

Detecção e análise

Esta fase possui enfoque na identificação de desvios e na análise sobre a possibilidade de tais desvios serem considerados incidentes ou não. Isto inclui:

1. Uso de arquivos de registro, mensagens de erro, alertas do IDS (Intrusion Detection System, ou Sistema de Detecção de Intrusão), alertas de firewall e outros recursos ou sensores para identificar um possível incidente de segurança. Essa etapa engloba a operacionalização e ajuste fino de ferramentas de correlacionamento de logs ou Security Information and Event Management (SIEM).
2. Comparação dos desvios com as métricas preestabelecidas para reconhecer incidentes e seus escopos.
3. Notificação da CSIRT e estabelecimento dos canais de comunicação entre a equipe e a parte gerencial da organização.
4. Definir o responsável pela avaliação e coleta de evidências (analista forense).
5. Assegurar que os responsáveis pelo tratamento dos incidentes documentem todos os aspectos dos processos de detecção e escopo.

Veja, a seguir, os itens que compõem o checklist dessa etapa:

- [ ] Quando o evento aconteceu?
- [ ] Como foi detectado?
- [ ] Quem o descobriu?
- [ ] Alguma outra área foi impactada?
- [ ] Qual é o escopo do comprometimento?
- [ ] Isso afeta as operações em qual nível?

- A fonte (vetor de entrada) do evento foi descoberta?

Contenção

Esta fase foca na limitação de perdas e prevenção de mais danos. Ela inclui várias subetapas, e cada uma delas é vital para a mitigação completa e a preservação adequada das evidências. Veja a seguir:

Contenção de curto prazo

Limita o dano assim que possível, bem como isola um único ativo ou um determinado segmento de rede. São medidas imediatas e tempestivas que devem ser tomadas na ocorrência de um incidente.

Backup do sistema

Cria uma imagem duplicada do sistema afetado (snapshot) antes de qualquer outra ação, para garantir a preservação das evidências.

Contenção de longo prazo

Deixa o sistema afetado temporariamente desativado para reparo, de forma que os processos de negócio suportados por ele possam ser retomados por meio do restante do processo de resposta de incidente.

Veja, a seguir, os itens que compõem o checklist desta etapa:

- O que foi feito para conter o incidente em curto prazo?
- O que foi feito para conter o incidente em longo prazo?
- Algum malware descoberto foi colocado em quarentena do resto do ambiente?
- Que tipo de backups existem?
- Todas as credenciais comprometidas foram revisadas quanto à legitimidade e reforçadas?

Erradicação

Nesta fase, os sistemas afetados são removidos ou restaurados. De forma geral, este estágio inclui:

1. Realização de todas as etapas consideradas necessárias para fazer com que os sistemas retornem ao estado operacional esperado. Isto pode ser tão simples quanto aplicar uma correção de software, ou tão complexo quanto reconstruir um sistema do zero.

2. Implementação de controles de segurança adicionais de forma a mitigação de incidentes repetitivos.

3. Atualização da documentação de incidentes para descrever todas as etapas realizadas durante o estágio, objetivando diminuir o tempo de reação no caso de uma ocorrência semelhante. O registro cuidadoso dos custos, bem como horas de trabalho, aquisições de software ou hardware podem ajudar a determinar o impacto geral do incidente.

Veja, a seguir, os itens que compõem o checklist desta etapa:

- [ ] Os artefatos do invasor foram removidos com segurança?
- [ ] O sistema foi “hardenizado”, sanitizado e as atualizações de segurança foram aplicadas?
- [ ] O sistema pode ser refeito?

Recuperação

Esta fase reintroduz os sistemas afetados ao ambiente de produção. O teste e o monitoramento cautelosos ajudam a garantir que os sistemas não se mantenham comprometidos. As informações necessárias nesta etapa incluem:

1. O tempo para que as operações sejam restauradas, que deve ser uma decisão de consenso entre a CSIRT e a área de negócio à qual o sistema atende.

2. Quais as ferramentas de teste e medidas devem ser usadas para garantir que cada sistema esteja totalmente funcional.

3. O tempo para monitorar os sistemas em busca de desvios.

Veja, a seguir, os itens que compõem o checklist desta etapa:

- [ ] Quando os sistemas podem retornar à produção?
- [ ] Os sistemas foram corrigidos e testados?

- O sistema pode ser restaurado a partir de um backup confiável (íntegro)?
- Por quanto tempo os sistemas afetados serão monitorados e o que será monitorado durante esse tempo?
- Quais ferramentas garantirão que incidentes semelhantes não ocorram novamente?

Atividades pós-incidente

Esta fase conclui todo o processo, com o objetivo de garantir que o incidente foi controlado com sucesso. Isto envolve:

1. Uma reunião com a CSIRT e a gestão para finalizar o cronograma do incidente. Esta reunião deve ocorrer o mais breve possível após o incidente ser considerado “sob controle”, de forma que os eventos decorrentes estejam frescos na mente de todos os envolvidos.
2. Identificação do incidente e escopo, bem como as etapas realizadas para conter, erradicar e recuperar.
3. A eficiência da CSIRT e do plano de resposta a incidentes, particularmente o que funcionou bem e o que precisa de melhorias.
4. Conclusão da documentação do incidente para fornecer uma descrição abrangente do incidente e qual foi a resposta final da CSIRT.

Algumas questões a serem respondidas nesta etapa:

- Quais mudanças precisam ser feitas?
- Como o treinamento dos colaboradores e da CSIRT deve ser melhorado?
- Qual vulnerabilidade foi explorada?
- Quais garantias devem ser empregadas para que incidentes semelhantes não ocorram novamente?

Como mitigar prejuízos devido aos incidentes de segurança

No vídeo a seguir, conheça a definição de incidentes de segurança e o modo como a organização de equipes de tratamento podem mitigar prejuízos nas organizações.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

Um dos membros da equipe de segurança de TI informou que um servidor de aplicações do escritório tem apresentado comportamento estranho. Alguns dos serviços em execução no servidor estão configurados incorretamente e não atendem à baseline de segurança. Todos os membros da equipe de TI que têm acesso ao servidor negam terem feito qualquer alteração. Essa ocorrência é classificada como?

A Evento

B Incidente

C Acontecimento

D Log

E Ocorrência

Parabéns! A alternativa B está correta.

%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cp%20class%3D'c-paragraph'%3EIncidente%20%C3%A9%20todo%20evento%20que%20resulta%20em%20uma%20consequ%C3%AAncia%20negativ

Questão 2

Quais das etapas abaixo não faz parte da metodologia de resposta a incidentes?

A Preparação

B Detecção e análise

C Contenção e erradicação

D Gestão de mudanças

E Recuperação

Parabéns! A alternativa D está correta.

%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cp%20class%3D'c-paragraph'%3ESegundo%20a%20publica%C3%A7%C3%A3o%20NIST%20SP%20600-61r2%2C%20as%20etapas%20do%20processo%20de%20resposta%20a%20incidentes%20s%C3%A3o%3A%20Prepara%C3%A7%
incidente.%3C%2Fp%3E%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20

2 - Correção de vulnerabilidades

Ao final deste módulo, você será capaz de identificar as etapas do processo de gestão de vulnerabilidades e do processo de gerenciamento de patches.

Processo de gestão de vulnerabilidades

Por definição, **vulnerabilidade** é qualquer falha ou fraqueza em um ativo que possa ser explorada por uma ameaça. Por si, uma vulnerabilidade não provoca qualquer incidente, mas seu potencial em causar perdas não pode ser desprezado.

Diante de um fluxo constante de novas informações, como, por exemplo: novos ativos, novas ameaças, atualizações de software, novas vulnerabilidades, zero days, boletins de ameaças, patches etc., a compreensão e o gerenciamento de vulnerabilidades se tornam atividades contínuas. Essas atividades demandam tempo, atenção e recursos significativos, culminando na necessidade de implantação de uma metodologia de gestão dessas vulnerabilidades.

A correção de vulnerabilidades é uma das etapas de um **processo de gestão de vulnerabilidades** e um processo importante para qualquer organização, uma vez que pode inviabilizar que um agente de ameaça possa explorá-la, acarretando em um incidente. Esse processo também auxilia a organização a corrigir uma vulnerabilidade que foi explorada em um incidente.

Comentário

O processo de gestão de vulnerabilidades pode ser definido como um conjunto de ações e atividades com a finalidade de reduzir, a níveis aceitáveis, o risco associado às vulnerabilidades encontradas em algum ativo.

As principais etapas do processo de gestão de vulnerabilidades são:

Identificar/rastrear ativos (inventário de ativos)

Manter um inventário dos ativos de informação é a primeira etapa para reduzir a superfície de ataque de uma organização, uma vez que não se controla aquilo que não se gerencia.

Categorização de ativos em grupos

Categorias ou grupos de ativos podem ser criados a partir do inventário de ativos. Os grupos de ativos são usados para verificar ativos específicos e relacionados. Essas categorias também permitem a customização da varredura de vulnerabilidade, abordando ativos que suportam processos de

negócio específicos e auxiliando na atribuição de classificações de risco das vulnerabilidades encontradas.

Varredura de vulnerabilidades

A varredura de vulnerabilidades é projetada para testar e analisar sistemas e serviços para vulnerabilidades conhecidas. A varredura compreende uma lista de tipos de varredura (portas, protocolos e características comportamentais de pacotes de rede). As varreduras de vulnerabilidades, em geral, são realizadas por meio de ferramentas automatizadas que examinam os sistemas, aplicativos e dispositivos de uma organização para determinar seu estado de operação atual e a eficácia de todos os controles de segurança.

Classificação de riscos

As ações devem ser priorizadas de acordo com o nível de risco calculado. Para ativos e grupos de ativos devem ser atribuídos uma classificação de relevância para o negócio. O esforço de remediação da vulnerabilidade é, subsequentemente, priorizado com base no risco identificado. Por exemplo, um servidor web suscetível a uma vulnerabilidade que concede acesso de nível administrativo deve ser corrigido antes de um sistema interno que exija um patch de segurança de baixa criticidade.

Gerenciamento de patches

Patches jamais devem ser aplicados de forma imediata! Os patches devem ser testados em um ambiente de não produção, para determinar se há problemas de compatibilidade com o sistema, assegurar a sua efetividade e evitar efeitos adversos que não possam ser tolerados. Os patches testados devem, então, ser migrados para produção e aprovados para instalação.

Varredura de correção e acompanhamento

Após a implementação dos controles recomendados para cada uma das vulnerabilidades encontradas no escopo analisado, uma nova varredura sob demanda deve ser executada, a fim de avaliar e validar as correções implementadas nos ativos impactados.

Classificação de vulnerabilidades

Conforme abordado no tópico anterior, dentro do processo de gestão de vulnerabilidades, existe uma etapa de classificação de risco.

Atenção!

É na etapa de **classificação de risco** que uma vulnerabilidade encontrada em determinado ativo é contextualizada com a relevância do mesmo para o objetivo do negócio da organização. Nesse contexto, faz-se necessário ranquear, seguindo um padrão, as vulnerabilidades encontradas.

A grande maioria das ferramentas de varredura utilizam os padrões CVE (Common Vulnerabilities and Exposures) para referenciar e CVSS

(Common Vulnerability Scoring System) para classificar em nível de severidade das vulnerabilidades publicadas.

CVE – *Common Vulnerabilities and Exposures*

CVE é um programa a nível global da MITRE Corporation para identificar, definir e catalogar vulnerabilidades de segurança divulgadas publicamente. Existe um registro CVE para cada vulnerabilidade catalogada. As vulnerabilidades são descobertas e, então, atribuídas e publicadas por organizações de todo o mundo que têm parceria com o Programa CVE. Os parceiros publicam registros CVE para comunicar descrições consistentes de vulnerabilidades.

Comentário

Profissionais de tecnologia da informação e cibersegurança de todo o mundo usam registros CVE para garantir que estão discutindo o mesmo problema e para coordenar seus esforços na priorização e resolução das vulnerabilidades.

Um registro CVE possui as seguintes informações e formato:

- Número Único no formato CVE-AAAA-NNNNN (CVE-ANO-NÚMERO).
- Descrição.
- Severidade.
- Referências.
- Histórico.
- Data de publicação.

CVSS – Common Vulnerability Scoring System

> **O CVSS é uma estrutura aberta para comunicar as características e pontuar a severidade das vulnerabilidades publicadas.**

A estrutura do CVSS possui três grupos de métricas: **Base, Temporal** e **Ambiental**.

As métricas Base produzem uma pontuação que varia de 0.0 a 10, que pode, então, ser modificada, pontuando as métricas Temporal e Ambiental.

Comentário

Uma pontuação CVSS também é representada como uma string, uma representação textual compactada dos valores usados para derivar a pontuação.

Gerar uma pontuação CVSS é algo complexo e existem algumas calculadoras desenvolvidas pelo NIST e pelo FIRST, mas levando-se em consideração, basicamente, os seguintes atributos:

1. **Vetor de Ataque (AV):** esta métrica reflete o contexto pelo qual a exploração da vulnerabilidade é possível. Esse valor e, consequentemente, a pontuação básica será maior quanto mais remoto (lógica e fisicamente) um invasor estiver para explorar o componente vulnerável.
2. **Complexidade de Ataque (AC):** esta métrica de Complexidade do Ataque descreve as condições que o invasor deve ter para explorar a vulnerabilidade. Tais condições podem exigir a coleta de mais informações sobre o alvo, a presença de certos padrões de configuração do sistema alvo ou exceções computacionais.

3. **Privilégios Exigidos (PR):** esta métrica descreve o nível de privilégios que um invasor deve possuir antes de explorar a vulnerabilidade com êxito.

4. **Interação do Usuário (IU):** esta métrica descreve a necessidade de um usuário, que não seja o invasor, participar do comprometimento bem-sucedido do ativo vulnerável. Assim, determina se a vulnerabilidade pode ser explorada, exclusivamente, por iniciativa do invasor ou se um usuário externo (ou processo iniciado pelo usuário) deve participar de alguma maneira.

5. **Escopo (S):** esta métrica descreve a capacidade de uma vulnerabilidade em um componente afetar recursos além de seus meios ou privilégios.

6. **Impacto na Confidencialidade (C):** esta métrica mede o impacto sobre a confidencialidade dos recursos de informação gerenciados por um ativo devido a uma vulnerabilidade explorada com êxito. Confidencialidade refere-se a limitar o acesso e a divulgação de informações apenas a usuários autorizados, bem como impedir o acesso ou divulgação a usuários não autorizados.

7. **Impacto na Integridade (I):** esta métrica mede o impacto na integridade dos dados, por ocasião de uma vulnerabilidade explorada com sucesso. Integridade se refere à confiabilidade e à veracidade dos dados originais.

8. **Impacto na Disponibilidade (A):** esta métrica mede o impacto na disponibilidade do ativo afetado, resultante de uma vulnerabilidade explorada com êxito. Embora as métricas de impacto de Confidencialidade e Integridade se apliquem à perda de confidencialidade ou integridade de dados usados pelo ativo impactado, ela se refere à perda de disponibilidade do próprio ativo impactado. Como a disponibilidade se refere à acessibilidade dos recursos, ataques que consomem largura de banda da rede, ciclos do processador ou espaço em disco impactam a disponibilidade de um ativo alvo.

> **Dados as suas características e nível de informação, o CVSS é visto como um sistema de medição padronizado para indústrias, organizações e governos que precisam de pontuações de severidade de vulnerabilidade precisas e consistentes.**

Dois usos comuns do CVSS são calcular o nível de severidade das vulnerabilidades descobertas e auxiliar como um fator na priorização das atividades de remediação de vulnerabilidades, aplicando esse valor a etapa de classificação do risco, dentro do processo de gestão de vulnerabilidades.

Classificações de severidade das vulnerabilidades

Atualmente, a estrutura CVSS está em sua terceira versão (v3.1) e possui os seguintes scores de pontuação:

Severidade	Pontuação Base
Nenhuma	0.0
Baixa	0.1 – 3.9
Média	4.0 – 6.9
Alta	7.0 – 8.9
Crítica	9.0 – 10

Tabela Score CVSS. Elaborada por Pedro Sá.

Por exemplo, a depender das variáveis em cada atributo apresentado, a CVE-2016-0051 apresenta as seguintes características:

- **Descrição:** "O cliente WebDAV no Microsoft Windows Vista SP2, Windows Server 2008 SP2 e R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold e R2, Windows RT 8.1 e Windows 10 Gold e 1511 permite que usuários locais obtenham privilégios por meio de um aplicativo, também conhecido como WebDAV Elevation of Privilege Vulnerability".
- **Base Score:** 7.9
- **Severidade:** Alta
- **Vetor CVSS:** CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Gerenciamento de patches

Segundo a norma ABNT NBR ISO/IEC 27002:2013, convém que todos os controles de segurança sejam avaliados em ambiente de homologação quanto à aplicabilidade e ao impacto antes da implementação em ambiente de produção.

Atenção!

Ainda segundo a norma ABNT NBR ISO/IEC 27002:2013, é recomendável que informações técnicas sobre vulnerabilidades em ativos em uso sejam obtidas em tempo hábil; que a exposição da organização a essas vulnerabilidades seja avaliada (superfície de ataque) e que sejam envidados esforços para lidar com os riscos associados às vulnerabilidades.

Ambientes empresariais possuem centenas e até milhares de ativos de informação, seja hardware, software, banco de dados, aplicações e outros. Esse grande volume de ativos implica na existência de incontáveis vulnerabilidades. Varrer todas essas vulnerabilidades existentes de forma manual e sem qualquer método é algo praticamente impossível e, se for feito, as chances erro são muito grandes. Nesse sentido, implementar e operar um processo de gerenciamento de patches é fundamental.

> **Em tradução literal, patch significa remendo. São trechos de códigos disponibilizados pelos fabricantes para corrigir as vulnerabilidades encontradas em seus produtos.**

Patches podem ser classificados como:

Patch de correção

É uma pequena unidade de código suplementar destinado a corrigir um problema de segurança ou uma falha de funcionalidade em um software ou até mesmo em componentes de hardware.

Hotfix

É, normalmente, desenvolvido de forma emergencial para corrigir uma vulnerabilidade específica.

Rollup

É uma coleção de patches de correção e hotfixes emitidos anteriormente, normalmente destinados a serem aplicados em um aplicativo de sistema, como uma ferramenta ou um serviço específico.

Pacote de serviços (Service Pack)

É uma compilação maior de atualizações que, geralmente, incluem aprimoramentos de funcionalidade, novas funcionalidades e todas as

atualizações e hotfixes emitidos até a data de lançamento do Service Pack.

Como boas práticas para um processo de gerenciamento de patches, temos os seguintes passos:

Identifique os ativos

Crie um inventário.

Classifique

Agrupe os ativos, considerando: nível de relevância para o negócio, nível de severidade das vulnerabilidades, quantidade de vulnerabilidades e os riscos. Neste passo, as prioridades de correção devem ser definidas.

Crie ambientes agregados

Utilize ambientes separados para teste, homologação e produção.

Monitore

Acompanhe a avalie os aspectos D.I.C.A. (disponibilidade, integridade, confidencialidade e autenticidade) dos ativos no ambiente de teste e homologação após a aplicação das correções, bem como avalie a efetividade da atualização.

Crie backup

Faça backups regulares dos sistemas em produção antes de aplicar as correções. Tão importante quanto fazer é testar o backup.

Deploy

Aplique as correções no ambiente de produção e mantenha o monitoramento. Acione planos de recuperação de desastres em caso de alguma necessidade.

Continuidade

Mantenha o monitoramento do deploy. Verifique se todos os ativos receberam e instalaram com sucesso os patches aprovados e verifique a estabilidade dos mesmos. Mantenha o inventário

atualizado, pois vulnerabilidades novas surgem a cada dia.

Documente

Documente todos os processos e procedimentos realizados, com a finalidade de rastrear eventos, reverter e manter a continuidade da atividade.

O Center for Internet Security (CIS), em sua publicação *CIS Controls*, recomenda as seguintes práticas para um Programa de Gestão de Vulnerabilidades Técnicas eficiente, eficaz e efetivo:

1. Utilize uma ferramenta atualizada de verificação de vulnerabilidades compatível com Security Content Automation Protocol (SCAP) para verificar automaticamente todos os ativos da rede, semanalmente ou com mais frequência.

2. Execute a verificação de vulnerabilidades autenticadas com: agentes executando localmente em cada sistema; ou com scanners remotos configurados com privilégios elevados no sistema que está sendo testado.

3. Use uma conta dedicada para verificações de vulnerabilidades autenticadas, que não deve ser usada para outras atividades e deve estar vinculada a máquinas específicas em endereços IP específicos.

4. Implemente ferramentas automatizadas de atualização para garantir que os sistemas estejam em execução com as atualizações de segurança mais recentes fornecidas pelo fornecedor.

5. Implemente ferramentas automatizadas de atualização para garantir que softwares de terceiros estejam em execução com as atualizações de segurança mais recentes fornecidas pelo fabricante.

6. Compare regularmente os resultados de verificações de vulnerabilidades para verificar se as falhas foram corrigidas em tempo hábil.

Vulnerabilidades e ataques cibernéticos: como mitigar prejuízos

No vídeo a seguir, abordamos a correlação entre a existência de vulnerabilidades nos sistemas de informação e a ocorrência de ataques, destacando a importância do robustecimento de servidores, serviços e sistemas.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

Ao analisar várias configurações de rede de um servidor, você descobre uma fraqueza desconhecida no sistema operacional do servidor. Esta fraqueza pode permitir que um invasor remoto se conecte ao servidor com privilégios administrativos. O que você descobriu?

A Exploit

B Bug

C Vulnerabilidade

D Elevação de Privilégio

E Um patch

Parabéns! A alternativa C está correta.

%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cp%20class%3D'c-paragraph'%3EVulnerabilidade%20%C3%A9%20qualquer%20falha%20ou%20fraqueza%20em%20um%20ativo%20que%20possa%

Questão 2

Um administrador de rede implementou uma estratégia para que todas as estações de trabalho da rede recebam as atualizações de segurança necessárias regularmente. Qual das opções a seguir descreve melhor o que o administrador de redes implementou?

A Sandbox

B Honeypot

C Virtualização

D Gerenciamento de patches

E Gerenciamento de vulnerabilidades

Parabéns! A alternativa D está correta.

%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cp%20class%3D'c-paragraph'%3ETestar%2C%20homologar%20e%20aprovar%20para%20instala%C3%A7%C3%A3o%20(deploy)%20atualiza%C3%A7

3 - Forense computacional

Ao final deste módulo, você será capaz de descrever os conceitos de computação forense, suas técnicas e ferramentas.

Conceito de computação forense

Após tratar um incidente de segurança, é possível que o ocorrido se desenrole para o início de uma investigação detalhada desse incidente, com o objetivo de identificar todos os agentes envolvidos. Neste módulo, serão apresentados os conceitos e etapas dos processos de coletas e investigação de evidências forenses que podem ser usadas em uma ação legal.

Comentário

O Código de Processo Penal (CPP) determina, em seus artigos 158, 159 e 160, que, quando o ato infracionário deixar vestígios, será

indispensável o exame de corpo de delito, sendo este realizado por perito oficial ou, na ausência deste, por duas pessoas idôneas com formação superior preferencialmente na área específica, possuidoras de habilitação técnica com a natureza do exame.

Sendo assim, no ambiente computacional, define-se computação forense como um misto da Ciência da Computação com a Criminalística, sendo a prática de coletar, custodiar, preservar e analisar dados de diversas fontes com o objetivo de buscar a materialidade, a dinâmica e a autoria do incidente, seja ele doloso ou não.

O processo forense

O local de um crime é o espaço geográfico onde um suposto delito penal foi cometido. Nesse local, podem ser levantadas evidências a fim de esclarecer a **dinâmica** (como), a **autoria** (quem) e a **materialidade** (o que aconteceu).

> **Um local de crime informático é um local de crime com a presença de ativos computacionais que podem ter relação com o fato investigado.**

Sendo assim, dadas as devidas diferenças, o processo investigatório de um incidente computacional deve obedecer todas as etapas investigatórias como qualquer outra investigação.

Antes de abordar o processo forense, é importante definir dos conceitos: ordem de volatilidade e cadeia de custódia.

Ordem de volatilidade

Os dados são voláteis e a capacidade de recuperá-los após um incidente depende da mídia onde estão armazenados. Por exemplo, dados armazenados em fitas de backup ou pen drives podem durar anos, enquanto os dados salvos em memória de acesso aleatório (RAM) podem durar por apenas alguns nanossegundos.

A ordem de volatilidade geral para dispositivos de armazenamento, do mais volátil para a menos volátil, é:

1. Registradores da CPU, cache da CPU e RAM;
2. Caches de rede e memória virtual;
3. Discos rígidos e pen drives;
4. CD-ROMs, DVD-ROMs, fitas magnéticas e impressões.

Cadeia de custódia

É o registro de tratamento da evidência, desde a coleta até o descarte adequado. Componentes de hardware, dados ou sistemas podem ser evidências.

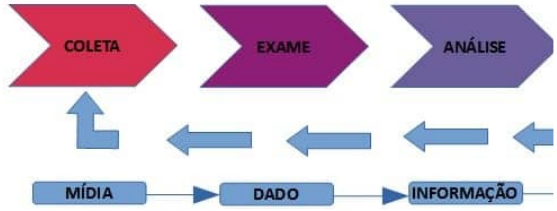
> **A cadeia reforça a integridade e cuidado adequado desde a coleta, análise, armazenamento e, finalmente, apresentação de relatório.**

Todas as pessoas da cadeia, que tratam as evidências, precisam registrar os métodos e ferramentas que elas usaram.

Seguir uma cadeia de custódia pode evitar alegações de manuseio incorreto ou adulteração de evidências, com a consequente impugnação

de provas levantadas. Essa tarefa envolve manter um registro de todos os indivíduos que tiveram custódia física das evidências, registro do momento e ações que realizaram com as evidências, armazenamento das evidências em local seguro, quando em repouso, e realização de exames e análises, fazendo uso apenas dos dados copiados de forma íntegra e fidedigna das fontes originais.

A publicação especial 800-86 *Guide to Integrating Forensic Techniques into Incident Response*, do NIST, divide o processo forense em quatro fases básicas:



Fases do processo forense.

Veja, a seguir, mais detalhes sobre cada uma dessas fases:

Coleta

1. Identifique o ativo e o rotule.
2. Registre e obtenha detalhes de todo o pessoal relacionado que tenha acesso ao ativo, bem como o material de evidência.
3. Mantenha a integridade dos dados.

Nesta fase, existe a necessidade de **identificar fontes de dados** que podem ser úteis para a perícia forense, ou seja, o que pode ser uma possível fonte de evidências. Terminais pessoais, servidores, celulares, equipamentos de rede e pen drives podem conter dados relevantes.

Após identificar as fontes de dados, é necessário realizar a **aquisição ou apreensão** dessas fontes. Os principais fatores que devem ser levados em consideração no momento da aquisição são: **valor da fonte** – identificar o nível de utilidade da fonte para a investigação; **volatilidade** – a depender da mídia de armazenamento, dados digitais se perdem com o passar do tempo, por conta de diversos fatores; **esforço para aquisição da fonte** – por exemplo, dados de registros de acesso de uma rede local possui um esforço de aquisição menor do que os registros de acessos da provedora de Internet.

Após considerar esses três fatores, é possível determinar qual a fonte de dados mais promissora para se alcançar os objetivos da investigação forense.

Feita a coleta, é muito importante garantir a integridade dos dados obtidos. Para isso, utiliza-se de funções hash para garantir que as cópias efetuadas refletem de forma fidedigna o conteúdo da fonte original. As demais etapas do processo serão executas sob a cópia efetuada.

Exame

1. Utilize métodos automatizados (ferramentas) e manuais para processar os dados coletados.
2. Avalie e extraia as evidências.
3. Mantenha a integridade.

As cópias efetuadas na fase anterior refletem o estado que um ativo estava dentro de um contexto passado. Essa é uma cópia bruta e geralmente possui um volume muito grande de arquivos. Por exemplo,

um log de firewall pode conter milhares de registros, mas somente uma pequena parte pode ser relevante para o cenário da investigação. Cabe ao perito filtrar, identificar e recuperar arquivos que possam conter informações necessárias à perícia.

> **É preciso levar em consideração que possam existir mecanismos de controle de acesso, criptografia e compressão aplicados aos arquivos de interesse, o que eleva ainda mais o esforço para obtenção.**

Análise

1. Analise os resultados da fase de exame usando técnicas e procedimentos legais, ou seja, permitidos por lei.
2. Obtenha informações úteis que justifiquem o motivo da coleta e exame.

Nesta fase, busca-se a identificação de evidências digitais que possuam relação com o fato investigado.

Relatório

1. Relate os resultados da análise forense, incluindo uma descrição das ferramentas e métodos usados, e o porquê dos fatos.
2. Realize recomendações para melhorar os controles de segurança existentes e forneça orientações de melhores políticas, ferramentas, procedimentos e outros métodos para incluir no processo forense.

Note que a mídia obtida é transformada em evidência à medida que as fases avançam no processo, transformando o dado extraído em informação compreensível para análise e, posteriormente, em evidência.

Aspectos, técnicas e ferramentas forenses

Neste ponto serão apresentados alguns aspectos, como as principais técnicas utilizadas nas fases do processo forense, bem como exemplos sucintos de ferramentas utilizadas para alcançar os objetivos esperados.

Coleta e análise de dados não voláteis

Nesta fase, vamos lidar com a mídia na qual o dado de interesse está armazenado. Um aspecto que merece especial atenção é a garantia da integridade da coleta, ou seja, os dados coletados devem refletir o exato estado de quando foram encontrados, pois as demais fases do processo utilizarão a cópia gerada nesta fase. Se a integridade não puder ser garantida, todos os esforços nas fases subsequentes serão nulos.

Cada sistema possui suas particularidades e características, alterando a forma como os arquivos são gerenciados. Contudo, de forma geral, alguns aspectos importantes para a atividade forense permeiam todos os file systems. Veja, a seguir, quais são:

Arquivos deletados

Quando um arquivo é excluído, não necessariamente ele é apagado da mídia de armazenamento. Em vez disso, as informações na estrutura de dados que apontam para a localização do arquivo são marcadas como excluídas. Isso significa dizer que o arquivo ainda está armazenado, apenas o seu ponteiro foi apagado, não sendo mais listado pelo sistema operacional.

Slack space

Sistemas de arquivos usam unidades de alocação de arquivos para armazená-los. Mesmo se um arquivo exigir um espaço menor do que o tamanho da unidade de alocação de arquivo, uma unidade de alocação inteira ainda estará reservada para o arquivo. Por exemplo, se o tamanho da unidade de alocação do arquivo for 512 kilobytes (KB) e um arquivo tiver apenas 12 KB, todos os 512 KB ainda serão alocados para o arquivo, mas apenas 12 KB serão usados, resultando em 500 KB de espaço não utilizado. Esse espaço não utilizado é conhecido como slack space e pode conter dados residuais de arquivos antigos apagados.

Espaço livre

O espaço livre é a área da mídia que não está alocada a nenhuma partição; inclui clusters ou blocos não alocados. Isso pode incluir espaço em mídia onde os arquivos estavam armazenados em um ponto, mas já foram excluídos. O espaço livre ainda pode conter dados.

Como já abordado, a análise forense é realizada em uma cópia fiel da fonte de dados. Quando realizadas por meio de equipamentos e softwares forenses, permitem uma duplicação fiel dos dados e a preservação do material.

As principais formas de cópia de dados são:

Backup lógico

Um backup lógico copia os diretórios e arquivos de um volume lógico. Ele não captura outras informações, como arquivos excluídos ou dados residuais armazenados em slack space.

Imagem

Também conhecida como **imagem de disco**, a imagem gera uma cópia bit a bit da mídia original, incluindo slack space e espaço livre. As imagens exigem mais espaço de armazenamento e demoram mais para serem executadas do que os backups lógicos.

Todas as etapas executadas para criar a cópia da mídia devem ser documentadas, com o objetivo de permitir que qualquer outra pessoa produza uma cópia exata da mídia original usando os mesmos procedimentos. Além disso, o analista forense deve documentar informações complementares, como o modelo e número de série da mídia, capacidade de armazenamento e informações sobre o software de imagem ou hardware duplicador que foi usado. Todos esses cuidados contribuem para a manutenção da cadeia de custódia do caso.

Durante os processos de backups e geração de imagens, a integridade da mídia original deve ser mantida.

Comentário

Para garantir que não haja alteração de dados na fonte original, analistas forenses podem fazer uso de bloqueadores de escrita e

duplicadores forense. Essas ferramentas podem ser tanto baseadas em software como em hardware, e funcionam como uma interface intermediária entre a mídia de destino e a de origem.

Como exemplos de hardware, temos o Tableau Forensic T356789iu, para discos IDE/SATA/SAS/FW/USB/PCIexpress, e Tableau T8u exclusivo para dispositivos USB.

Para ferramentas baseadas em software, o Forensic ToolKit (FTK) e o Encase são soluções compatíveis com o sistema operacional Windows. Para ambiente Linux, existem as distribuições FDTK-UbuntuBr e CAINE, que possuem diversas ferramentas forenses que atendem todo o processo forense, inclusive a fase de coleta.

MAC Times

MAC Times são metadados dos sistemas de arquivos que indicam certos eventos que ocorreram no último instante de determinado arquivo, sendo informações relevantes para a atividade forense.

> É importante saber quando um arquivo foi **modified** (modificado), **accessed** (acessado) e **created** (criado).

O restante do processo envolve extrair e analisar os arquivos coletados. Em uma coleta, podem existir milhares de arquivos e cabe ao analista utilizar seu senso investigativo para determinar arquivos que possam ser relevantes à investigação. Nesse sentido, é importante conhecer os tipos de arquivos mais comuns. Por exemplo, uma imagem pode ter as extensões .JPG, .JPEG, .GIF. Já arquivos de áudio podem ser do tipo .MP3, .MP4, .WAV. No entanto, extensões de arquivos podem ser modificadas e, nesse caso, é preciso levar em consideração o file header, que é, de forma sucinta, uma assinatura que cada tipo de arquivo possui e pode ser acessada por meio de ferramentas forense.

Essa e outras funcionalidades podem ser encontradas nessas ferramentas:

Visualizador de arquivos

O analista pode visualizar o arquivo de forma direta, não precisando de ferramentas específicas para cada tipo de arquivo. Por exemplo, para ver um vídeo, não seria necessário um player específico para este fim. Para abrir um arquivo .pdf, não seria necessário ter um visualizador desse tipo de arquivo.

Acesso a metadados de arquivos

Metadados de arquivos podem conter informações relevantes para a atividade forense. Um arquivo de foto, por exemplo, pode conter metadados que informam a data, local, modelo de câmera fotográfica e outras informações relevantes.

Arquivos compactados

O analista pode examinar arquivos compactados sem a necessidade de um software de descompressão.

Identificar arquivos conhecidos

O objetivo é identificar arquivos com base na sua assinatura. O NIST mantém uma base de dados com hashs de arquivos conhecidos, a National Software Reference Library (NSRL) ou Biblioteca Nacional de Referência de Software.

Visualizador de estrutura de diretórios

A visualização da árvore de diretórios torna a atividade forense mais rápida e fácil para o analista, uma vez que a hierarquia de diretórios pode ser exibida graficamente.

Execução de pesquisas de strings e correspondências de padrões (pattern matches)

Essas pesquisas auxiliam na leitura de grandes quantidades de dados para encontrar palavras-chave ou strings específicas.

Coleta e análise de dados voláteis

Os dados voláteis referem-se aos dados em um sistema alimentado com alguma fonte de energia e que são teoricamente perdidos depois que esta é cortada, como as conexões de redes, arquivos de swap e hibernação, e outras informações armazenadas em memória RAM. O swap, em conjunto com a RAM, compõe a **memória virtual** do sistema. Arquivos de hibernação, por sua vez, são uma cópia da memória RAM do sistema, sendo utilizado para retornar um computador para um estado anterior após sair do estado de hibernação, muito usado em laptops.

No SO Windows, temos os arquivos **pagefile.sys**, **hiberfil.sys** (hibernação) e o **swapfile.sys**.

Comentário

Normalmente, assim como nos file systems, a real deleção de dados na memória não ocorre, e as características como slack space e espaço livre são semelhantes, existindo, nesses endereços de memória, dados valiosos.

Algumas informações que podem ser obtidas através da coleta de dados da memória RAM são:

Configuração de rede

As configurações de rede são dinâmicas por natureza. Por exemplo, hosts recebem endereços IP, dinamicamente, por outro host (DHCP), o que significa que seus endereços IP não fazem parte de configuração armazenada. Hosts também possuem várias interfaces de rede e a configuração de rede atual indica quais interfaces estão em uso.

Conexões de rede

É possível obter uma lista das conexões de rede atuais de entrada e saída. Essa lista pode fornecer endereços de origem e destino, bem como o estado da conexão, aplicação utilizada, protocolo e portas locais e remotas utilizadas.

Processos em execução

Os processos incluem serviços do sistema operacional e aplicativos executados por usuários. Esta lista pode ser estudada para determinar os serviços que estavam ativos no sistema durante a ocorrência do incidente. Identificar os processos em execução é útil para identificar programas que deveriam estar em execução, mas foram desabilitados ou removidos, como forma de evasão de defesas, como, por exemplo, software antivírus e firewalls.

Arquivos abertos

Os sistemas operacionais podem manter uma lista de arquivos abertos, indicando o usuário ou processo que abriu cada arquivo.

Sessões de login

Informações como hora de início e duração de cada sessão, logons anteriores, uso privilegiado e personificação são informações que podem ser recuperadas a partir da coleta e análise de sessões. As informações de login podem ajudar a determinar os hábitos de uso de um usuário e confirmar se uma conta estava ativa quando determinado incidente ocorreu.

Registro de hora

Essas informações podem ser úteis para construir uma timeline de eventos ou correlacionar eventos entre atores. Convêm que administradores de rede utilizem servidores de tempo baseados em protocolo NTP (Network Time Protocol) para fornecer sincronização e registros consistentes de relógios entre diversos ativos da rede.

O file system também é uma das fontes mais ricas de informações para uma análise forense e possui diversos dados voláteis que um analista forense deve verificar. Por exemplo:

Arquivos de configuração

O sistema operacional pode usar arquivos de configuração para armazenar configurações de aplicativos. Por exemplo, os arquivos de configuração podem listar os serviços a serem iniciados automaticamente após a inicialização do sistema e especificar a localização dos arquivos de log e arquivos temporários.

Arquivos de configuração particularmente interessantes são:

Tarefas agendadas

O sistema operacional mantém uma lista de tarefas agendadas que devem ser realizadas automaticamente em determinado horário. As informações que podem ser obtidas são o nome da tarefa, o aplicativo usado para executá-la, opções e argumentos de linha de comando e os dias e horários em que a tarefa foi e deve ser executada.

Arquivos de senha

O sistema operacional pode armazenar hashes de senha em determinados arquivos, por exemplo, o arquivo shadow e passwd, para

sistemas Linux, e registros SAM (Security Account Manager), para sistemas Windows. Vários utilitários de quebra de senha podem ser usados para converter um hash de senha em informação legível e utilizável.

Usuários e grupos

O sistema operacional mantém um registro das contas de usuários e grupos. Esses registros incluem a associação de grupos, nome e descrição da conta, permissões da conta, status da conta e o caminho para o diretório home das contas.

Arquivos de log

Os arquivos de logs registram diversas ações e acontecimentos sobre vários eventos do sistema operacional e também podem conter informações de eventos de aplicações específicas. Uma prática recomendada para auxiliar a atividade forense é que o administrador de rede ative e registre os diversos tipos de logs presentes no sistema operacional.

Arquivos de log interessantes são:

Event Logs

São registros de ações operacionais executadas pelos diversos componentes do SO, como desligar o sistema ou iniciar um processo. Cada evento, geralmente, possui um timestamp (carimbo de data/hora).

Audit Logs

São registros de auditoria contêm informações de eventos de segurança, como tentativas de autenticação bem-sucedidas e malsucedidas, alterações na política de segurança, alterações de permissões de arquivos e outras informações correlatas.

Application Logs

São registros de ações operacionais significativas executadas por aplicativos, como inicialização e desligamento de aplicativos, falhas de aplicações e alterações relevantes nas configurações de aplicativos.

Command History

Alguns sistemas operacionais têm arquivos de log separados, normalmente, para cada perfil de usuário, que contêm um histórico dos comandos executados no SO.

Recently Accessed Files

Sistemas operacionais podem registrar os acessos mais recentes a determinados arquivos, criando, assim, uma lista dos arquivos acessados.

Application Files

Aplicativos podem ser compostos por muitos tipos de arquivos e gerar diversos outros arquivos temporários durante a sua execução. Estes podem incluir contas e perfis de acesso, banco de dados, ações executadas e outras informações dentro do contexto da aplicação.

Dump Files

Alguns sistemas operacionais possuem a capacidade de armazenar o conteúdo da memória, automaticamente, durante uma condição de erro para auxiliar na depuração da falha posteriormente.

Temporary Files

Durante a operação de um sistema operacional ou utilização de um aplicativo, geralmente, são criados arquivos temporários. Embora esses arquivos sejam normalmente excluídos no final do processo, isso nem sempre ocorre. Os arquivos temporários podem conter cópias de outros arquivos do sistema, dados do aplicativo ou outras informações relevantes para a investigação.

Comentário

Durante as etapas de coleta e análise de dados voláteis, diversos softwares podem ser utilizados. As ferramentas mais conhecidas de coleta são o **LiME** (Linux Memory Extractor), para sistemas Linux/Android, e o **DumpIt**, para sistemas Windows. Na etapa de extração e análise de dados voláteis, uma das mais ferramentas difundidas e utilizadas é o aplicativo **Volatility**.

Crimes cibernéticos e os impactos nas organizações

No vídeo a seguir, abordamos o fato de que, sem a devida proteção, as organizações podem ser vítimas de crimes cibernéticos que podem gerar grandes prejuízos.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

Durante uma investigação forense, um analista registra informações sobre cada unidade, incluindo onde foi adquirida, quem fez a cópia forense, o hash MD5 da unidade e outros detalhes. Que termo descreve o processo que o analista está usando ao rotular as evidências com detalhes de quem as adquiriu e manipulou?

A Provas diretas

B Provas circunstanciais

C Registro de incidentes

D Aquisição de provas

E Cadeia de custódia

Parabéns! A alternativa E está correta.

%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cp%20class%3D'c-paragraph'%3EA%20cadeia%20de%20cust%C3%B3dia%20%C3%A9%20o%20registro%20de%20tratamento%20da%20evid%C3%A

Questão 2

Que conceito mede a facilidade de perda de dados?

A Ordem de volatilidade

B Transitoriedade de dados

C Previsão de perda de dados

D Estrutura de Volatilidade

E Hierarquia de memória

Parabéns! A alternativa A está correta.

%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cp%20class%3D'c-paragraph'%3EA%20ordem%20na%20qual%20voc%C3%AA%20precisa%20coletar%20ou%20preservar%20os%20dados%20ap%C3

4 - Disaster Recovery Plan

Descrever o plano de recuperação de desastres e as diretrizes para sua obtenção.

Conceitos, métricas e estratégias de continuidade

Um desastre pode ser entendido como qualquer ação ou omissão, repentina e não planejada, que cause impacto negativo nos ativos críticos para o negócio, acarretando em perdas para toda ou parte da organização, incapacitando esta de entregar serviços essenciais por tempo superior ao tempo objetivo de recuperação.

Seguindo a definição, desastres produzem descontinuidades. Descontinuidades produzem crises, e estas resultam em perdas, sejam humanas, materiais ou financeiras.

A recuperação de desastres é um componente importante na continuidade dos negócios, e se concentra em reparar, reconstruir, restaurar e substituir sistemas; substituir pessoal ou outros ativos depois que um desastre afetou a organização. Nesse sentido, convém que a atividade de recuperação de desastres seja vista sob a luz da **gestão de continuidade**.

Comentário

O processo de gestão de continuidade pode ser entendido como um processo abrangente que busca identificar ameaças potenciais para a organização e os possíveis impactos que elas podem causar nas operações do negócio.

Essencialmente, a gestão de continuidade visa garantir a continuidade e as informações vitais à sobrevivência da organização. Essa gestão é fundamentada na **análise de riscos** e na **análise de impacto no negócio**.

Análise de riscos

Parte de uma infraestrutura de segurança bem planejada envolve conhecer quais ativos precisam ser protegidos e em qual nível. Esse processo envolve identificar o que pode dar errado.

A definição de risco é bastante abrangente. Um risco pode ser um efeito indesejado de uma ação ou a consequência de uma ameaça.

O gerenciamento de riscos é um processo cíclico que inclui quatro fases:

Avaliar

Identificar e avaliar os riscos existentes em um sistema. Nesta fase, é preciso inventariar os ativos, bem como associá-los aos processos de negócio que eles suportam. Identificar as ameaças às quais esse ativo

está exposto. Identificar os controles de segurança existentes, sejam preventivos, detectivos ou corretivos. Identificar as vulnerabilidades existentes, por meio de ferramentas adequadas de varredura. Identificar o impacto que a exploração de uma vulnerabilidade pode causar nos negócios.

Analisar

Analisar os riscos dos potenciais impactos na camada de negócios de incidentes de segurança nos sistemas. Isto deve ser avaliado levando-se em conta as consequências de uma violação dos pilares da segurança da informação (disponibilidade, integridade, confidencialidade e autenticidade) e da criticidade das vulnerabilidades encontradas. Nesta análise, também deve ser calculada a probabilidade de que uma ameaça explore uma determinada vulnerabilidade levantada. A avaliação do impacto será aprofundada na análise de impacto no negócio.

Responder

Formular uma estratégia sobre como responder aos riscos. Assim que um risco for identificado, é necessário definir uma estratégia de resposta para determinar a ação apropriada a ser tomada. Diversas estratégias podem ser combinadas em uma única resposta.

As quatro técnicas de resposta mais comuns estão descritas a seguir:

Aceitar o risco

É o reconhecimento e aceitação do risco e das consequências que o acompanham, se esse risco se materializar. A aceitação não significa deixar um sistema completamente vulnerável, mas reconhecer que o risco envolvido não é totalmente evitável, ou se o custo da mitigação ou prevenção for maior do que o custo da perda.

Transferir o risco

É usado para alocar a responsabilidade do risco para um terceiro, como uma empresa de seguros.

Evitar o risco

É usado para eliminar o risco, juntamente com a eliminação da causa. Isso pode ser tão simples como eliminar a operação ou entidade que está em risco, como desligar um servidor, que é alvo frequente de ataques, ou descontinuar um processo de negócio.

Mitigar o risco

Envolve técnicas que protegem os ativos de possíveis ataques, e são implementadas quando o impacto de um potencial risco é substancial. A mitigação pode vir na forma de defesas ativas, como um firewall, ou medidas de precaução, como fazer backup dos dados sob risco.

Mitigar

Amortecer o impacto dos riscos para segurança futura. Isto pode ser feito determinando, desenvolvendo e implementando controles para

eliminar ou reduzir os riscos. Os controles devem ser economicamente pensados e fornecer o nível de proteção esperado. Em outras palavras, os controles não devem custar mais que a perda estimada, causada pelas ameaças, que possa explorar a vulnerabilidade.

Atenção!

É importante atentar que, mesmo após a mitigação, a maioria das situações retêm risco residual. Poucas medidas de defesa podem reduzir o risco a zero.

Análise de impacto no negócio

Por análise de impacto, entende-se, de forma sucinta, como sendo o processo de analisar os efeitos que uma interrupção ou disrrupção sistêmica pode ter sobre a camada de negócio.

Comentário

Uma **análise do impacto no negócio** – **AIN** ou (**BIA** – Business Impact Analysis) é uma análise sistemática que identifica e determina os efeitos do risco em operações e processos críticos. BIA's devem incluir todas as fases do negócio para garantir que todas as funções essenciais e sistemas críticos sejam identificados e todos os riscos associados sejam tratados.

Conforme um risco é identificado, também são determinadas as chances de ocorrência do risco e, em seguida, determinado o potencial dano organizacional. Por exemplo, se um sistema for atacado por um ransomware e seu backup for corrompido, deixando esse sistema indisponível por **cinco dias**, os custos estimados para a organização precisam ser avaliados (impacto).

Funções e sistemas críticos

As funções e sistemas críticos de uma organização são aqueles que, quando ausentes ou gravemente deteriorados, impedem que a organização opere, ainda que com os níveis mínimos estabelecidos. Por exemplo, para o centro de dados, o sistema de refrigeração deve ter uma classificação de criticidade maior do que o sistema de refrigeração dos escritórios, uma vez que a oscilação de temperatura pode ocasionar uma falha catastrófica nos equipamentos.

À escala de criticidade, pode ser atribuída uma visão tanto **qualitativa** (nominal) quanto **quantitativa** (numeral), de acordo com o quadro a seguir:

Criticidade	Comprometimento
Muito Alta (5)	Poderá afetar toda a organização e as perdas serão catastróficas.
Alta (4)	Poderá afetar um ou mais negócios da organização e as perdas serão graves.
Média (3)	Poderá afetar parte dos negócios da organização e as perdas serão consideráveis.
Baixa (2)	Poderá afetar uma parte pequena e localizada da organização e as perdas serão baixas.
Muito Baixa (1)	Poderá afetar uma parte muito pequena e localizada da organização e as perdas serão mínimas.

Quadro: Classificação da criticidade. Elaborado por Pedro Sá.

Uma maneira de determinar a importância relativa de um sistema ou função é desenvolver dados para comparação. As métricas comuns que devem estar contidas na BIA incluem:

Tempo de inatividade máximo tolerável (MTD – Maximum Tolerable Downtime)

É o período de tempo máximo que um desastre pode durar sem causar uma falha irrecuperável ao negócio. Cada processo de negócio pode ter seu próprio MTD, como um intervalo de minutos ou horas para funções críticas, **24 horas** para funções **urgentes, 7 dias** para funções **normais**, e assim por diante.

Atenção!

Os MTD variam por organização e incidente

Objetivo do ponto de recuperação (RPO – Recovery Point Objective)

É o período de tempo mais longo que uma organização pode tolerar que dados perdidos após um desastre sejam irrecuperáveis.

> **O RPO tipicamente é expresso em horas, e na maioria dos cenários de TI, determina a frequência de backups**

Por exemplo, se o RPO da organização for de 10 horas, então os backups deverão ser realizados pelo menos a cada 10 horas. O intervalo de tempo entre o último backup e o evento não deve exceder 10 horas e, portanto, os dados perdidos neste período estão dentro da faixa de tolerância da organização.

Objetivo do tempo de recuperação (RTO – Recovery Time Objective)

É a duração de tempo dentro do qual as operações e atividades de negócio normais podem ser recuperadas após um incidente. Ele inclui o tempo de recuperação necessário para retornar para o RPO, reinstalar o sistema e retomar o processamento a partir de seu status atual.

Atenção!

O RTO deve ser atingido antes do MTD.

Tempo médio para reparar/substituir (MTTR – Mean Time to Repair)

É o tempo médio necessário para que um dispositivo seja recuperado de um incidente.

> **O MTTR de um componente será menor que o RTO se o dispositivo for relevante para esse esforço de recuperação.**

Em outras palavras, o RTO incorporará o MTTR de componentes vitais no tempo que leva para retornar as operações de negócio ao normal.

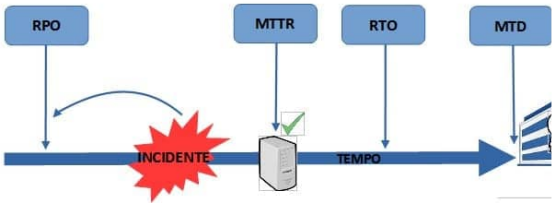


Ilustração do MTTR.

De forma esquemática, podemos visualizar as diversas métricas da seguinte forma:

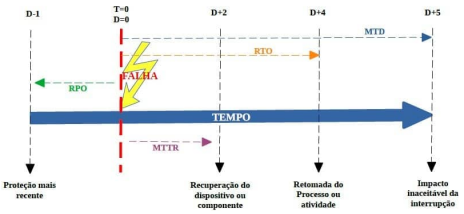


Ilustração das métricas de impacto e continuidade

Após os resultados das análises de risco e análise de impacto, é possível definir as ações a serem executadas para uma adequada recuperação pós-desastre. De forma sintetizada, as principais entradas e saídas desses dois processos são:

Síntese de Análise de Riscos e Análise de Impacto.

Ações a serem tomadas na ocorrência de um desastre

Os procedimentos a serem empregados no **Plano de Recuperação de Desastres** devem ser executados em conformidade com os requisitos de segurança da informação e comunicações necessários à proteção dos ativos críticos, tratando as atividades de forma abrangente, o que inclui as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação e comunicações.

Comentário

A recuperação de desastres é um componente importante da continuidade de negócios, que se concentra em reparar, reconstruir, restaurar e substituir sistemas, pessoal, ambiente e outros ativos, depois que um desastre afetou a organização. Os processos de suporte à recuperação de desastres garantem que a infraestrutura de TI seja trazida de volta a um estado de baseline de trabalho definido como minimamente aceitável até a plena recuperação.

O processo de recuperação de desastres inclui diversas fases e viabiliza o retorno da operação do negócio. Em essência, o passo a passo da recuperação segue o seguinte roteiro:

1

Notificação das partes interessadas

As partes interessadas devem ser informadas sobre a ocorrência de um desastre. Eles podem ser constituídos pelo CEO, membros do conselho, clientes, fornecedores, funcionários e pelo público. Diferentes categorias de partes interessadas são notificadas em diferentes momentos e, a depender da escalada da crise e do nível de detalhes informados, devem seguir os procedimentos definidos em política.

2

Início das operações de emergência

Devem existir etapas detalhadas, relacionadas a serviços de emergência específicos. Por exemplo, pontos de contato externos, canal de suporte técnico, instalações terceirizadas etc. Um gerente de incidentes deve ser nomeado para assumir o controle da situação e garantir a segurança adequada do material.

3

Avaliação das instalações

É necessário avaliar a capacidade da instalação atual para que esta continue sendo o local principal de operações. Se a instalação tiver sido afetada a ponto de ter sofrido perdas significativas, a realocação para um local alternativo pode ser a melhor opção.

4

Início do processo de recuperação

Após notificar as partes interessadas, realizar as operações iniciais de emergência e avaliar o dano e a capacidade de operação da instalação, é hora de iniciar o processo de recuperação.

Locais de recuperação

Para ajudar a garantir a continuidade dos negócios após um desastre, uma organização pode manter locais alternativos, que podem ser usados para restaurar funções do sistema. Veja, a seguir que locais são esses:

Hot site

É uma rede alternativa totalmente configurada, que pode ficar on-line rapidamente após um desastre.

Warm site

É um local inativo ou que executa funções não críticas em condições normais de operação, mas também pode ser rapidamente convertido em local de operações principal se necessário.

Cold site

É um local alternativo predeterminado, onde um ambiente de operações pode ser reconstruído após um desastre.

Tipos de backup

No que diz respeito à recuperação de dados pós-desastre, os processos de recuperação de dados a partir de um backup variam, dependendo dos tipos de backup que foram incluídos no plano de recuperação de desastres. Existem três tipos principais de backup:

Backup completo

Todos os arquivos selecionados, independentemente do estado anterior, passam por backup. Backups totais podem consumir bastante espaço de armazenamento e o processo pode ser lento, e, por isso, tal abordagem deve ser realizada com cautela quanto ao espaço disponível e o RTO.

Backup diferencial

Todos os arquivos selecionados que foram alterados desde o último backup total passam por backup. Quando backups

diferenciais são usados, é preciso restaurar o último backup total mais o backup diferencial mais recente. Backups diferenciais exigem menos espaço de armazenamento e tempo de backup do que os backups totais, mas são mais lentos de recuperar. Mais uma vez, atenção ao RTO.

Backup incremental

Todos os arquivos selecionados que foram alterados desde o último backup total ou incremental, ou o que for mais recente, passam por backup. Quando backups incrementais são usados, é preciso restaurar o último backup total mais todos os backups incrementais subsequentes. Normalmente, um backup incremental leva menos tempo de ser executado do que um backup diferencial, pois ele inclui menos dados, mas também é mais lento quando se trata de tempo para recuperar os dados. Mais uma vez, atenção ao RTO.

Principais diretrizes a respeito dos processos de continuidade e recuperação de desastres

Esteja ciente das vantagens e desvantagens de locais de backup próximos vs. distantes.

1. Esteja ciente das principais ameaças que a organização está exposta.
2. Implemente um processo de continuidade dos negócios em resposta a incidentes reais.
3. Implemente a recuperação de desastres para restaurar as operações após um incidente significativo.
4. Siga um processo de recuperação de desastres notificando as partes interessadas antes de iniciar o processo de recuperação.
5. Forme uma equipe de recuperação com múltiplas funções e responsabilidades.
6. Determine uma ordem de restauração para trazer de volta os sistemas de acordo com seu nível de criticidade para o negócio.
7. Considere manter locais alternativos para restaurar rapidamente as operações quando o local principal estiver comprometido.
8. Escolha entre um hot, warm ou cold site dependendo das necessidades e recursos.
9. Certifique-se de que os processos de recuperação estão seguros contra ataques ou outros comprometimentos.
10. Escolha um tipo de backup de dados que atenda às suas necessidades de velocidade, confiabilidade e armazenamento.
11. Certifique-se de que os backups estão armazenados em um local seguro.
12. Considere as implicações logísticas e de segurança ao manter vários backups.
13. Teste regularmente a integridade dos seus backups.
14. Considere dispor de backups externos.
15. Esteja ciente das vantagens e desvantagens de locais de backup próximos vs. distantes.

Virtualização e backup e a redução do tempo de recuperação em desastres cibernéticos

Veja, no vídeo a seguir, como a virtualização, aliada ao backup sistemático, pode reduzir, significativamente, o tempo de recuperação de indisponíveis.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

Como é conhecida uma análise sistemática que identifica e determina os efeitos do risco em operações e processos críticos?

A Executar uma varredura de vulnerabilidades.

B Criar política de uso seguro.

C Análise de vulnerabilidades.

D Executar uma avaliação de riscos.

E Análise de impacto.

Parabéns! A alternativa E está correta.

%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cp%20class%3D'c-paragraph'%3EUma%20BIA%20%C3%A9%20o%20processo%20de%20analisar%20as%20atividades%20e%20os%20efeitos%20qu

Questão 2

Como é chamado o período de tempo máximo que um desastre pode durar sem causar uma falha irrecuperável ao negócio?

A RTO – Recovery Time Objective

B RPO – Recovery Point Objective

C MTD – Maximum Tolerable Downtime

D MTTR – Mean Time to Repair

E MTBR – Mean Time Between Repair

Parabéns! A alternativa C está correta.

%0A%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%3Cp%20class%3D'c-paragraph'%3EO%20MTD%20%C3%A9%20o%20tempo%20m%C3%A1ximo%20em%20que%20os%20produtos%2C%20servi%C3%

Considerações finais

Como vimos, o processo de resposta a incidentes e recuperação de desastres é muito mais do que uma tarefa cotidiana e corriqueira. Deve ser uma atividade estudada e estruturada de acordo com a realidade da organização, objetivando dar o tratamento adequado durante e após a ocorrência de um incidente. Para atingir esses objetivos, bem como corrigir as falhas exploradas e descobrir os atores envolvidos na exploração, faz-se necessário implementar processos de gestão de vulnerabilidades, que, entre outras atividades, envolve a correção das falhas e implementar um processo de forense computacional, que aborda toda a questão investigativa para determinar quais foram os agentes de ameaças envolvidos no incidente.

Ouça uma entrevista sobre a importância de implantar a cultura do tratamento de incidentes em uma organização.

Para ouvir o *áudio*, acesse a versão online deste conteúdo.

Explore +

Pesquise sobre as CSIRT nacionais, CTIR.GOV e CERT.BR, e veja como elas são estruturadas e os serviços prestados à sociedade brasileira.

Pesquise sobre a Norma ABNT NBR ISO22301:2013, que versa sobre os requisitos para um sistema de gestão de continuidade de negócios.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013:** Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013.

BRASIL. Gabinete de Segurança Institucional. **Portaria nº 93**, de 26 de setembro de 2019. Brasília: 2019. Consultado na internet em: 23 nov. 2021.

BRASIL. **Decreto lei nº 3.689, de 03 de outubro de 1941.** Consultado na internet em: 23 nov. 2021.

CIS, CENTER FOR INTERNET SECURITY. **CIS Controls Version 7.1.** Nova York: CIS, 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST SP 800-61r2** Computer Security Incident Handling Guide. Maryland: NIST, 2012.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST SP 800-86** Guide to Integrating Forensic Techniques into Incident Response. Maryland: NIST, 2006.

Material para download

Clique no botão abaixo para fazer o download do conteúdo completo em formato PDF.

Download material

O que você achou do conteúdo?

Relatar problema