Segurança Cibernética

Resposta a Incidentes: Continuidade de Negócios

Prof. Dr. Daniel Caetano

2022 - 1

Compreendendo o problema

- **Situação:** Apesar dos investimentos vultosos em infraestrutura, é fatal que algum dia os sistemas falhem. Nesse dia, parecerá que nada funciona...

Mentimeter

O que pode ter ocorrido?

Compreendendo o problema

- **Situação:** Nesse momento é preciso de calma e agilidade: os sistemas precisam voltar ao ar o mais rápido possível.

Mentimeter

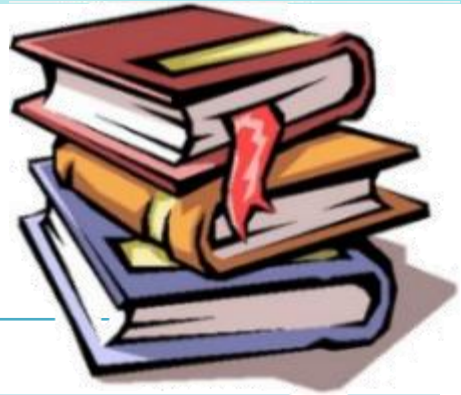
Por onde começar?

Objetivos

- Compreender o que é a e importância de um Plano de Continuidade de Negócios e um Plano de Contingência (Disaster Recovery Plan)
- Conhecer uma sequência de tarefas para resposta a incidentes.

- **Atividade Avaliativa C**

Material de Estudo

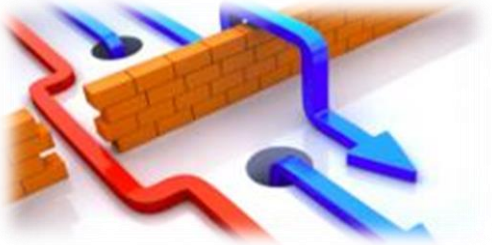


Material	Acesso ao Material
Notas de Aula e Apresentação	https://www.caetano.eng.br/aulas/2021b/ara0076.php (Segurança Cibernética – Aula 10)
Minha Biblioteca	• Segurança de Computadores e Teste de Invasão (ISBN: 978-0-8400-2093-2). Págs. 309, 321 e 324. • Hackers Expostos: Segredos e Soluções para a Segurança de Redes (ISBN: 978-0-07-178028-5). Pág. 669. • Segurança de Computadores: Princípios e Práticas (ISBN: 978-85-352-6449-4). Págs. 520, 528 e 465.
Material Adicional	1) Cartilha TCU – Cap. 3. Disponível em: http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf 2) 5 Erros de Iniciantes. Disponível em: https://youtu.be/wvKXB7eexWg 3) Notificação e Resposta. Disponível em: https://youtu.be/S19Yy_xTWWM 4) Computação Forense. Disponível em: https://youtu.be/BocTBCT11WI 5) Computação Forense. Disponível em: https://youtu.be/UA3tvfrHbmE 6) Auditoria. Disponível em: https://youtu.be/OE54j3BRQN0?t=267 7) Disaster Recovery. Disponível em: https://youtu.be/abF5Rf352eM

Plano de Continuidade de Negócios

Continuidade de Negócios?

- Informações: essenciais
  - Para a empresa funcionar
- Desastres
  - Podem impedir a continuidade dos negócios!
- Até agora: muitos aspectos de prevenção
  - Alguns conceitos e dicas de recuperação



- Como unir tudo?
  - Plano de Continuidade de Negócios (PCN)

Objetivo e Criação do PCN

- Objetivo geral: minimizar impactos
  - Manter a integridade e disponibilidade dos dados
    - Continuar operando em caso de desastre
    - Recuperação ordenada no menor tempo possível.
- Como isso pode ser concretizado?
  - Antever potenciais desastres/catástrofes
  - Planejar solução operacional em cada caso.

Metas de um PCN

- Segurança das pessoas
  - Empregados/colaboradores e visitantes
- Minimizar perdas e danos imediatos
  - Físicas e lógicas
- Rápida restauração das atividades
  - Instalações e equipamentos
- Rápida reativação dos processos críticos
  - Manter o negócio em funcionamento!
- Conscientização e treinamento
  - Responsáveis pela execução do plano!

Insumos para o PCN

- Análise de Risco
  - Identificar todos os desastres possíveis
  - Consequências da interrupção de cada sistema
  - Tempo limite para a recuperação
  - Identificação e priorização
    - Recursos, sistemas, processos críticos...

Insumos para o PCN

- Identificação de Mecanismos de Prevenção
  - No Breaks / Geradores
  - Detectores de incêndio
  - Ar condicionado
  - Cofres à prova de fogo, água e fumaça
  - Armazenagem externa / Backups
  - Criptografia.

Insumos para o PCN

- Estratégias de Recuperação
  - Backups e localidades alternativas
  - Reposição de equipamentos e manutenção (SLA).

Elementos Básicos de um Plano de Contingência (Disaster Recovery Plan)

Forma do Plano de Contingência

- Cinco seções
  1. Informação de Suporte
  2. Notificação/Ativação
  3. Recuperação
  4. Reconstituição
  5. Anexos

PC: Informação de Suporte

- Operação
  - Explicação geral e resumida do processo
- Situações de uso
  - Em que situações deve ser acionado
- Sistemas envolvidos
  - Todos os impactados
- Responsáveis
  - Quem cuida de cada sistema envolvido
- Hierarquia de notificação
  - Quem deve acionar quem para a recuperação.

PC: Notificação/Ativação

- Procedimentos Iniciais
  - "Primeiros socorros"
- Processo de Notificação de Responsáveis
  - Ordem, telefone, informações a passar...
- Avaliação de Danos (Processo para)
  - Causa, nível de emergência, áreas afetadas, tipos de danos etc.
- Ativação
  - Como proceder a ativação...
  - ...quando os danos apurados assim exigirem

PC: Recuperação

- Sequência das atividades de recuperação
  - Ordem detalhada dos procedimentos
- Habilitação de Sistemas Alternativos
  - Síntese dos recursos utilizados
  - Procedimento detalhado
- Recuperação do Sistema Principal
  - Métodos (+ de 1? critérios objetivos!)
  - Procedimento detalhado
  - Testes do sistema reconstituído

PC: Reconstituição

- Desmobilização da Contingência
  - Desativação dos sistemas alternativos
  - Reativação dos sistemas restaurados
- Testes dos Sistemas Principais
  - Avaliação da Recuperação
- Integração de Dados
  - Incorporação dos dados de operação...
  - ...do sistema alternativo para o principal.

PC: Anexos

- Responsáveis pelo plano
  - Qualquer informação adicional pertinente
  - Informações sobre serviços externos e SLAs
  - Apoio alternativo em caso de indisponibilidade
- *Checklists*
  - Listas de acompanhamento
    - Ordem de ligamento/desligamento
- Especificações técnicas
  - Toda inform. útil na recuperação
    - Equipamentos / Software

Requisitos para PCN Funcionar

- Apoio da alta administração
  - Fundamental!
- Treinamento e conscientização
  - Não pode ser novidade na hora do desastre!
- Teste do PCN
  - Evitar pressupostos incorretos, omissões etc.
  - Mudanças!
- Revisões periódicas
  - Ambiente, pessoas, endereços, leis... Tudo muda.

Além do PCN

- Tomar todas as medidas!
  - Proatividade na segurança!
- Atenção ao SLA dos serviços de manutenção
  - Service Level Agreement
- Contratação de seguros
  - Seguro Cibernético.

Mentimeter

Respostas a Incidentes e Desastres

Incidentes e Desastres

- Nem todo incidente...
  - ...se torna um desastre.
- Tentativas de ataques detectadas
  - Demandam um tipo de ação
- Ataques realizados com sucesso
  - Demandam outro tipo de ação

Mentimeter

- Serão dadas algumas dicas...
  - Que podem exigir adaptação no seu ambiente!

Tentativas de Ataques

- Tentativa: ainda não causou desastre
  - Recomenda-se ação tão rápida quanto possível
  - Mas... importante! Mantenha a calma!

Tentativas de Ataques

- Primeiro passo
  - Certificar-se de que as defesas do sistema estão ok
- O que verificar?
  - Firewall está ativo?
    - Se não estiver, suba imediatamente!
  - Antivírus está ativo e atualizado?
    - Se não estiver, atualize.
  - Verifique as portas abertas com o NMAP
    - As portas abertas são as que deveriam?
  - Há uso de SSH é a máquina tem acesso público?
    - Verifique se o SSHGuard está funcional.

Tentativas de Ataques

- Segundo passo
  - Auditoria: identificar os tipos de ataques
- O que verificar em termos de log?
  - Log de sistema (Ex.: syslog)
  - Log de falha de acesso (Ex.: lastb)
  - Logs de aplicações (Ex.: apache, postfix etc)

Tentativas de Ataques

- Terceiro passo
  - Auditoria: identificar se houve sucesso no ataque
- O que verificar em termos do sistema?
  - Execute uma verificação dos arquivos
    - Rkhunter, Lynis etc. (cfg prévia); Antivirus com LiveCD
  - Usuários do sistema (Ex.: passwd)
    - Verifique se não apareceu nenhum indevido!
  - Processos/Serviços automáticos (Ex.: crontab)
    - Para todos os usuários!
  - Verifique os processos em execução (Ex.: top, htop)
    - Tem algum processo estranho?
  - Verifique as conexões ativas (Ex.: netstat -punta)
    - Tem conexões estranhas?

Tentativas de Ataques

- Quarto passo
  - Ações corretivas
- Não houve invasão, mas há método no ataque?
  - Certifique-se de que todo o possível foi feito
    - Configure proteções, instale programas de proteção...
    - Pesquise!.
- Argh! Tem coisa estranha na máquina!
  - Parta para a próxima seção...
    - Procedimentos para desastre!.

Desastre Identificado

- Houve desastre: há comprometimento
  - Primeira ação imediata: desligue a rede
    - Pode ser tirando o cabo, mesmo
    - Se não for possível, desabilite as interfaces de rede.
  - Agora respire fundo e mantenha a calma
  - Sangue frio é importante nesse momento

Desastre Identificado

- Primeiro passo
  - Verificação no restante do sistema
- O que verificar?

  - Todas as máquinas ligadas na rede da empresa
    - No mínimo as da mesma sub-rede
  - Busque a mesma falha da máquina atacada
  - Se localizadas falhas, mesmo procedimento
    - Desligá-las da rede
  - Pode ser feita em paralelo com próximos passos
    - Comande a equipe para realizar esse primeiro passo
    - Próximos passos: aplicados em todas as máquinas

Desastre Identificado

- Segundo passo
  - Subir ambiente alternativo
  - Preparar o recuperado
- Qual ambiente alternativo?
  - Se há, o do **cold site**.
  - O do warm ou hot site pode estar comprometido
- Como preparar novo ambiente?
  - Restaurar o backup mais recente
    - Em nova máquina
    - Em ambiente desconectado ou com firewall fechado

Desastre Identificado

- Terceiro passo
  - Auditoria: verificar extensão de dano imediato
    - Identificar se houve vazamento de informações pessoais
- O que verificar?
  - Execute uma verificação dos arquivos
    - Rkhunter, Lynis etc. (cfg prévia); Antivirus com LiveCD
  - Usuários do sistema (Ex.: passwd)
    - Verifique se não apareceu nenhum indevido!
  - Processos/Serviços automáticos (Ex.: crontab)
    - Para todos os usuários!
  - Verifique os processos em execução (Ex.: top, htop)
    - Tem algum processo estranho?

Desastre Identificado

- Quarto passo
  - Auditoria: identificar como o ataque teve sucesso
- Como começar?
  - Pesquise o que pode ocasionar o problema
    - Oriente-se pelo resultado do terceiro passo
    - Consulte os CVEs!
- O que verificar nos log?
  - Log de sistema (Ex.: syslog)
  - Log de falha de acesso (Ex.: lastb)
  - Logs de aplicações (Ex.: apache, postfix etc)

Desastre Identificado

- Quinto passo
  - Ações corretivas...
  - ...na nova máquina
- Procedimento?
  - Com a nova máquina criada no segundo passo
    - Restauração do backup...!
  - Aplique todas a checklist de segurança da empresa
  - Aplique todas as correções para travar
    - Problemas encontrados no terceiro passo
    - Brechas identificadas no quarto passo

Desastre Identificado

- Sexto passo
  - Ajustando novo ambiente

- Procedimento?
  - Atenção aos CVEs!
  - Verifique se há portas “ouvindo” (netstat –punta)
  - Passe o pente fino na nova configuração do firewall
  - Se for uma VM, faça um snapshot
  - Habilite a nova configuração do firewall
  - Verifique o que está aberto com o NMAP

Desastre Identificado

- Sétimo passo
  - Monitoramento e controle
- Máquina antiga...
  - Nunca mais será confiável
  - Auditoria detalhada (Forense Computacional)
    - Identificar extensão real dos danos
  - Desativar a máquina após.
- Máquina nova
  - Monitorar por um tempo
    - Conexões, tráfego
    - Processos

Desastre Identificado

- Em paralelo do 3º ao 7º passos
  - Se houve dados pessoais afetados!
- Informar a ANPD sobre o incidente
  - Imediato (sugere-se até 72hs) – ou justificar
  - Natureza dos dados, titulares envolvidos, medidas prévias, riscos envolvidos, medidas mitigadoras
- Identificar os usuários afetados
  - Bem como suas informações detalhadas
- Informar a todos os usuários afetados
  - Quais dados foram afetados
  - Medidas tomadas para mitigar impactos
  - Medidas que o usuário pode tomar

Atividade Avaliativa

Atividade Avaliativa C

- Vale: 2,5 na AV2
- Grupo
  - Pesquise 3 CVEs https://cve.mitre.org/cve/search_cve_list.html
    - **CVE-2002-0283**, **CVE-2010-0816**, **CVE-2020-15708**
  - Pesquise também aqui: https://www.cvedetails.com/
  - Verifique se encontra a solução publicada pelo fornecedor
    - Windows: https://msrc.microsoft.com/update-guide
    - Ubuntu: https://ubuntu.com/security/cve
    - Debian: https://security-tracker.debian.org/tracker/
    - RedHat: https://access.redhat.com/security/security-updates?cwe=476#/cve
  - Analise e compreenda a falha e as correções divulgadas
  - Elabore um texto técnico explicando de forma clara a vulnerabilidade e como as correções ocorreram.

ENCERRAMENTO

Resumo e Próximos Passos

- Várias técnicas de proteção
  - Criptografia
  - Hardening
  - Segurança em IoT
  - Atividade Avaliativa
- **Pós Aula**: Saiba Mais, A Seguir... e Desafio!
  - No mural: https://padlet.com/djcaetano/segciber

- Se preparar...
  - Provas finais!

PERGUNTAS?