




nic.br egi.br

cert.br

INFOESTE 2018
Presidente Prudente, SP
18 de maio de 2018



Backup

o básico cada vez mais essencial

Marcus Vinícius Lahr Giraldi
marcus@cert.br

cert.br nic.br cgi.br

Qual o valor dos dados

- **Difícil mensurar**
- **Geralmente só é percebido da maneira mais difícil**
- **Dados:**
 - possuem valor emocional, financeiro, acadêmico, jurídico, etc.
 - levam tempo ou são impossíveis de serem refeitos
- **Perda pode afetar:**
 - a continuidade dos negócios
 - perda de clientes/pacientes, *downtime*, etc
 - reputação/imagem da empresa
 - moral da equipe
- **Como protegê-los?**
 - impedir que ameaças cheguem até eles

Como proteger os dados

- **Manter os equipamentos seguros**
 - instalar a versão mais nova do sistema operacional
 - aplicar todas as atualizações
 - desabilitar serviços desnecessários
 - instalar antivírus e mantê-lo atualizado
- **Conscientizar os usuários**
 - não abrir arquivos anexos
 - ataques de engenharia social (*phishing*)
 - *zero-days*
- **Backup**
 - cópia de segurança
 - última linha de defesa
 - quando todas as anteriores tiverem falhado

Funções do *backup*

- **Recuperação de versões**

- versão antiga de um arquivo alterado
- imagem original de uma foto manipulada

- **Arquivamento**

- guardar dados raramente alterados e pouco usados

- **Proteção de dados**

- furto/perda de equipamentos
- problemas de *hardware*
- atualização malsucedida de sistemas
- falhas em aplicativos
- apagados sem querer
- apagados por querer: *hackers*, funcionários descontentes, *malware*
- **sequestrados**

NEWS

Lessons learned from 9-11: Disaster recovery dos and don'ts

Ladrão leva computador com estudo inédito sobre vírus da zika

WannaCry Ransomware Demonstrates The Value Of Better Security and Backups

<https://www.forbes.com/sites/tomcoughlin/2017/05/14/wannacry-ransomware-demonstrations-the-value-of-better-security-and-backups/#7b9bfe3a70b8>

<https://noticias.uol.com.br/saude/ultimas-noticias/estado/2016/05/23/ladrao-leva-computador-com-estudo-sobre-zika.htm>

<http://searchwindowsserver.techtarget.com/news/784938/Lessons-learned-from-9-11-Disaster-recovery-dos-and-donts>

Ransomware

- **Impede o acesso aos dados**
 - criptografia dos dados
 - bloqueio do equipamento
 - (MFT, MBR)
- **Exemplos:**
 - CryptoLocker, Cryptowall, WannaCry, Petya
- **Costuma**
 - procurar por extensões típicas de *backup*
 - .back, .bak, .tar, .zip, .gz, .rar
 - cifrar também *backups* na nuvem



Ransomware

- **O que fazer?**

- esquecer dos dados e se conformar
- dar sorte de alguma ferramenta conseguir recuperá-los
- pagar o resgate
 - não garante a recuperação total
 - pode não haver comunicação com o atacante
 - por exemplo, conta de *e-mail* desativada
 - incentivo ao crime
 - pode levar a outros pedidos de extorsão
- **recuperar o *backup* (melhor opção)**

Não basta ter um *backup*

- **Ele deve ser adequado às necessidades**
 - garantir a segurança dos dados
 - adequar-se aos objetivos de quem o realiza
- **Importante conhecer as opções existentes**
 - *backups* inadequados podem resultar em:
 - perdas
 - gastos excessivos
 - esforços desnecessários (operacional)
- **Não existe uma política de *backup* pré-determinada**
 - o que copiar?
 - onde copiar?
 - quando copiar?
 - como copiar?

O que copiar

- **Imagem do sistema**

- sistema operacional, programas instalados, configurações, arquivos dos usuários

- **Dados**

- realmente importantes
 - binários (executáveis e bibliotecas) devem ser evitados
 - podem conter cavalos de troia ou arquivos corrompidos, que serão recuperados na reinstalação
 - criar lista de arquivos que não serão copiados
- apenas os confiáveis

Onde copiar

- **Off-line**

- mídias

- *pen-drive*, CD, DVD, Blu-Ray, disco (interno e externo), cartão SD, fita, etc.

- **Online**

- nuvem

- *datacenter*

- discos de rede

Off-line – Mídias

- **Cuidado com mídias obsoletas**
 - como atualmente recuperar disquetes, CDs????
 - dificuldade de encontrar leitores
 - verificar o tempo de vida útil
- **Manter as mídias etiquetadas e nomeadas**
 - com informações que facilitem a localização
 - tipo do dado armazenado
 - data de gravação
- **Cuidado ao descartar as mídias**

Off-line – Armazenagem das mídias

- **Local**

- ideal para pedidos rápidos e pequenos – mídia facilmente acessível
- manter em lugar
 - seguro e com acesso restrito
 - proteção contra furto e pessoas não autorizadas
 - à prova de fogo
 - bem condicionados
 - proteção contra agentes nocivos naturais (poeira, calor, umidade)

- **Remoto (*off-site*)**

- garante a disponibilidade, em caso de problemas nas instalações
- velocidade de envio depende de:
 - frequência e tempo de restauração
 - finalidade: arquivamento (mídia pode estar distante)
- pode comprometer a confidencialidade e integridade
 - criptografar e gerar *checksum* antes de enviar, verificar antes da restaurar

Online – *Backup* na Nuvem

- **Atenção às senhas**

- ativar verificação em duas etapas

- **Não confundir:**

- **sistemas de armazenamento em nuvem**

- armazenam arquivos na nuvem
- não necessariamente fazem *backup*
 - apesar de poderem ser usados para tal
- oferecem facilidade de acesso
- exemplos: OneDrive, Amazon Cloud Drive, Dropbox, iCloud, Google Drive

- **serviços de *backup* em nuvem**

- fazem cópia dos arquivos na nuvem
- exemplos: Azure Backup, Amazon S3 ou Glacier, iCloud, Google Drive

Off-line ou *Online*

- **Quantas cópias manter?**

- “Quem tem um não tem nenhum”

- **Onde armazená-las?**

- “*There are two kinds of people in the world - those who have had a hard drive failure, and those who will*”- Peter Krogh

- **Regra 3-2-1**

- ter pelo menos três cópias dos dados (uma primária e 2 *backups*)
 - armazenar estas cópias em duas mídias diferentes
 - manter uma das cópias *off-site* (ou ao menos *off-line*)

Como fazer

- **Programar *backups* automáticos**
 - *backups* manuais estão mais propensos a erros e esquecimento
 - certificar-se de que eles estão realmente sendo feitos
- **Programas integrados:**
 - ao sistema operacional
 - ao aplicativo
 - de acordo com a mídia usada
- **Ferramentas**
 - desenvolvidas internamente
 - de terceiros
- **Soluções simples**
 - enviar uma cópia por *e-mail* pode ser suficiente
 - andar com um *pen-drive*

Periodicidade

- **Manter os *backups* atualizados**
- **Conforme a frequência de criação ou modificação**
 - quantos dados você está disposto a perder?
 - quanto maior a frequência das cópias:
 - menor será a perda de dados
 - maiores serão os gastos
 - mais complexa poderá ser a recuperação
- **Sempre que houver risco iminente**
 - mal funcionamento, mensagens de *logs* sobre falhas
 - atualização de sistemas
 - envio a serviços de manutenção
 - grandes alterações no sistema
 - adição de *hardware*, atualização do sistema operacional, etc.

Tipo	Descrição	Vantagens	Desvantagens
Completo	Copia todos os dados; serve como referencial para os demais tipos	Mais básico e completo; cópia de todos os dados em um único conjunto de mídia; recuperação simples	Mais demorado; ocupa mais espaço
Incremental	Copia apenas os dados alterados ou criados após o último completo ou incremental	Menor volume de dados; mais rápido; ocupa menos espaço de armazenamento	Recuperação mais complexa (primeiro um completo e depois todos os incrementais)
Diferencial	Copia os dados alterados ou criados desde o último backup completo	Recuperação mais rápida que o incremental (precisa só do último completo enquanto o incremental precisa do completo e dos incrementais)	Ocupa mais espaço que o incremental e menos que o completo; gasta mais tempo que o incremental e menos que o completo
Progressivo	Similar ao incremental mas com maior disponibilidade dos dados	Recuperação automatizada e mais eficiente (não precisa descobrir os conjuntos a serem recuperados)	Recuperação mais lenta que o diferencial e o completo (precisa analisar diferentes conjuntos para terminar o processo)

Restauração / Recuperação (1/3)

***"No one cares if you can back up,
only if you can recover."***

W. Curtis Preston - Unix Backup and Recovery

Restauração / Recuperação (2/3)

- **Pode ser:**

- parcial (apenas um ou mais arquivos)
- total
 - restauração do zero
 - restaurar um *backup* de sistema completo em um equipamento sem dados
 - reinstalar e após restaurar
 - instalar o sistema operacional básico e recuperar os dados

- **Quando for necessário restaurar um sistema:**

- isolar a máquina da rede
- caso o sistema tenha sido comprometido
 - revisar a configuração após a restauração
 - certificar-se de que não tenha ficado alguma porta de entrada previamente instalada pelo invasor

Restauração / Recuperação (3/3)

Testes

- **Não deixar para perceber o erro quando já for tarde**
- ***Backups* devem ser verificados:**
 - logo após serem gerados
 - posteriormente, em intervalos regulares
 - não apenas para satisfazer auditorias
- **Testes periódicos evitam surpresas**
 - dados corrompidos
 - mídia ou formato obsoleto
 - programas mal configurados
 - cadê o programa de recuperação?

Retenção

- **Por quanto tempo devem ser armazenados**
 - até quando tiver espaço?
 - para cumprir obrigações legais?
 - o que fazer quando não puder/quiser pagar mais?
 - e se o serviço for descontinuado?

Resumo – *Backup* na nuvem

O que considerar ao escolher

- **Realização**

- sistemas suportados
- processo automatizado
- espaço de armazenagem
- restrições de arquivos (tamanho, extensão)
- tempo estimado de transmissão de dados

- **Restauração**

- procedimento (interface Web, aplicativo)
- tempo (imediatamente, horas, dias)
- capacidade de transmissão de dados

- **Armazenagem/Retenção**

- tempo que os arquivos são mantidos
- falta de pagamento

- **Políticas de privacidade e de segurança**

- transmissão e armazenagem (criptografia)

- **Suporte, tempo no mercado, outras opiniões e referências**

The background of the slide is a dark gray circuit board pattern with white lines representing traces and components. The pattern is symmetrical and fills the entire frame.

Lembre-se

cert.br nic.br cgi.br

Backup

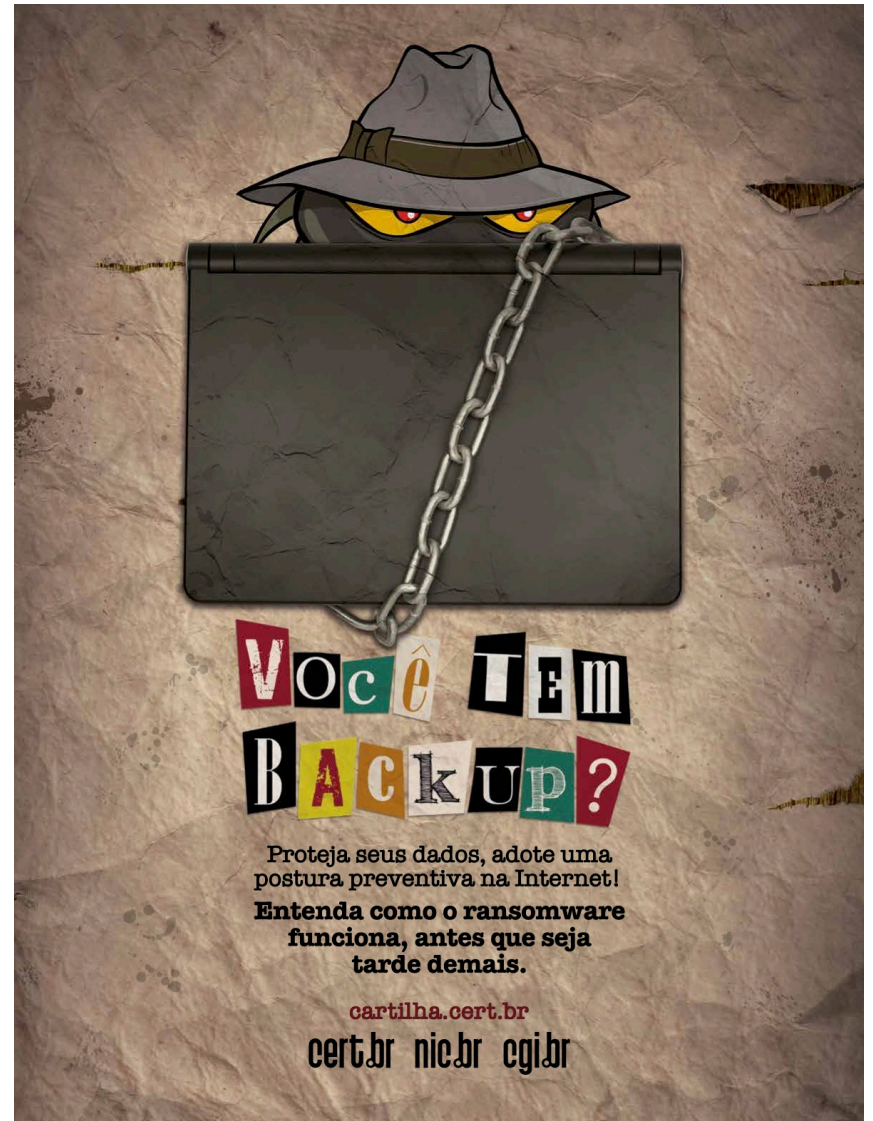
- **Deve ser considerado como última linha de defesa**
 - quando todas as anteriores falharem
- **É essencial:**
 - manter os equipamentos seguros
 - instalar a versão mais nova do sistema operacional
 - aplicar todas as atualizações
 - desabilitar serviços desnecessários
 - instalar antivírus e mantê-lo atualizado
 - conscientizar os usuários
 - *zero-days*
 - ataques de engenharia social

VOCE TEM BACKUP?

Criminosos digitais impedem acesso a informações armazenadas em dispositivos e exigem resgate

<http://nic.br/publicacao/revista-br-ano-08-2017-edicao-12/>

<https://cartilha.cert.br/>



Obrigado

www.cert.br

© marcus@cert.br

© @certbr

18 de maio de 2018

nic.br egi.br

www.nic.br | www.cgi.br