Proteção Contra Ransomware

Um Guia de Recursos do PCI Security Standards Council

RANSOMWARE É A AMEAÇA DE MALWARE QUE CRESCE MAIS RÁPIDO.

Criminosos atacam empresas com um tipo de malware que sequestra sistemas e dados críticos do negócio até que um resgate seja pago.[1]

1 Fonte: FBI

COMPREENDENDO O RISCO

US$ 1 BILHÃO POR ANO

O custo estimado dos crimes de ransomware em 2016[2]

Em 2015, as vítimas de crimes cibernéticos pagaram

US$ 24 MILHÕES

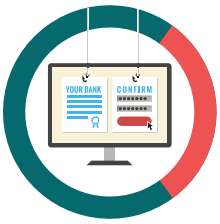
a criminosos praticando ransomware[3]

CRESCIMENTO DE 600%

em novas famílias de ransomware desde dezembro de 2015[4]

2,3: Fonte: ZDNet 4: Fonte: Proofpoint

O ATAQUE



30%

dos usuários abrem e-mails de phishing e mais de 12% clicam nos anexos.

EMAILS DE PHISHING

Os e-mails de phishing são um veículo comum para a prática de ransomware. Estes e-mails parecem ser legítimos, como uma fatura ou fax eletrônico, mas incluem links e/ou anexos maliciosos que podem infectar seu computador e seu sistema.[5]

99%

dos computadores usam softwares vulneráveis a ataques, se não forem atualizados[6]

VULNERABILIDADES DE WEBSITES E DE SOFTWARES

Criminosos praticam ransomware em websites e se aproveitam das vulnerabilidades de softwares para lançar ataques sobre visitantes usando softwares desatualizados, como navegadores e plugins de navegadores.

5: Fonte: 2016 Verizon Data Breach Investigations Report 6: Fonte: Heimdal Security

PCI Security Standards Council

PROTEJA SUA EMPRESA

ESTEJA ALERTA

Treine seus funcionários. PCI DSS 12.6

- Desenvolva um plano que informe seus funcionários sobre as melhores práticas para evitar estes tipos de ataques e como lidar com um ataque quando isso ocorrer.
- Assegure-se de que estejam cientes dos riscos e que entendam que não há problemas em excluir o e-mail, se parecer suspeito.
- Pense antes de clicar. E-mails podem parecer que foram enviados por qualquer pessoa na empresa. Se houver alguma dúvida, sempre entre em contato com a pessoa para confirmar antes de clicar em um link ou abrir um arquivo.

PERMANEÇA VIGILANTE

Teste seus sistemas. PCI DSS 11.3

- Você testou seus sistemas recentemente, para ver se é fácil para alguém invadi-lo? Criminosos são persistentes e você também deve ser.
- Uma vulnerabilidade é como uma porta "quebrada" para que os criminosos entrem. É importante que toda vulnerabilidade encontrada nos testes sejam solucionadas e que você tenha outros controles em vigor para impedir que um indivíduo malicioso invada seus sistemas.

Patch. PCI DSS 6.2

- Seus fornecedores lhe enviam "patches" para resolver problemas em seus sistemas de pagamentos ou outros.
- Quando foi a última vez que você verificou se há novos "patches" de segurança com seus fornecedores de sistemas de pagamento e de software?
- "Patches" fecham as portas que criminosos usam para entrar em seus sistemas. Siga as instruções de seus fornecedores e instale "patches" assim que possível.

Monitore. PCI DSS 11.5

- Você está monitorando as mudanças em seus sistemas? As mudanças suspeitas, não autorizadas ou não aprovadas foram investigadas?
- Monitorar as mudanças em seus sistemas lhe ajuda a ver quando alguém faz uma alteração que você não autorizou ou aprovou. Investigar mudanças assim que elas ocorrem lhe ajuda a encontrar problemas mais rapidamente e a aumentar suas chances de impedir um ataque.
- Um processo de gestão de mudanças lhe ajudará a determinar se as alterações foram aprovadas. Se a mudança não foi aprovada ou for desconhecida, você deve imediatamente investigar para determinar se seu sistema foi corrompido.

Faça "backup" de seus sistemas. PCI DSS 9.5.1, 12.10.1

- Tenha cuidado para que seu "backup" não apague bons "backups" anteriores. Isso pode evitar a fazer "backup" de dados criptografados por ransomware sobre um "backup" bom. A boa prática, independente do método de "backup" é realizar "backups" regulares de todo o disco e "backups" incrementais ("backup" apenas dos dados que forem novos depois do último "backup").
- Para reduzir seu risco, evite fazer "backups" de dados online (conectado ao sistema do qual se está fazendo o "backup"). Ao invés disso, armazene seus dados de "backup" fora da empresa e offline (armazenar seus "backups" na nuvem é um método comum de armazenamento offline; porém, veja o último item). Isso facilita a recuperação de seu "backup" mais recente, caso seus arquivos de dados sejam sequestrados.
- Mantenha várias gerações de "backup" e estabeleça um período de retenção coerente com a capacidade de sua empresa de detectar ransomware e de reconstrução, usando registros antigos.
- Você testou a integridade de seus "backups" recentemente? Você testou o processo de "backup" e de recuperação recentemente? Assegurar que você pode recuperar dados de seus "backups" é crucial, caso seus sistemas sejam sequestrados.
- Ao usar "backups" na nuvem, assegure-se de que seu prestador de serviços de nuvem seja diligente e tenha proteção contra todos os tipos de malware. O armazenamento na nuvem também pode ser afetado pelo atacante, se estiver conectado aos sistemas de "backup" com sincronização persistente.

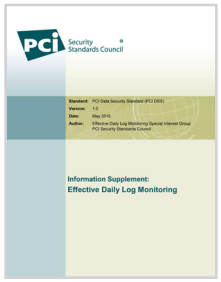
TENHA UM PLANO

Esteja preparado. PCI DSS 12.10

- Você e seus funcionários devem saber como responder a um ataque e o que fazer quando isso acontecer, incluindo quem entrar em contato.
- Assegure-se de ter um plano e de comunicá-lo aos seus funcionários.
- Revise este plano regularmente e faça com que informar seus funcionários seja um compromisso recorrente.

MATERIAIS DE CONTEXTO APROFUNDADOS - PCI

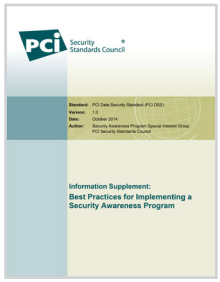
pdf Padrão de segurança de dados do PCI Versão 3.2



pdf Suplemento de Informações: Monitoramento Efetivo dos Registros Diários

pdf Protegendo-se Contra Phishing e Ataques de Engenharia Social

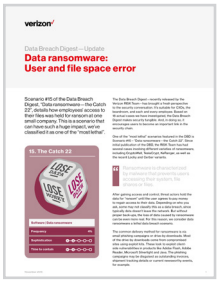
pdf Protegendo os Dados de Pagamento de seus Clientes contra Malware



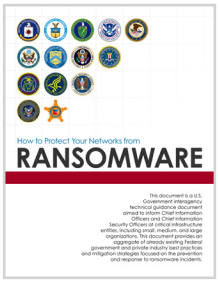
pdf Melhores Práticas para Implementar um Programa de Conscientização de Segurança

pdf Recursos de Proteção de Pagamentos para Pequenos Comerciantes: Guia para Pagamentos Seguros

RECURSOS RELACIONADOS AO SETOR

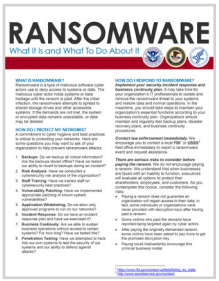


pdf Sequestro de dados: Usuário e erro de espaço em arquivo



pdf Ransomware e Resposta de Prevenção para CISOs

www Projeto No More Ransom



pdf Como Proteger Suas Redes de Malware

Para comentários de especialistas ou dúvida, entre em contato com: press@pcisecuritystandards.org
Para mais informações sobre os Padrões e recursos da PCI, acesse: www.pcisecuritystandards.org.