GTS.15 – Grupo Técnico em Segurança de Redes

PCI DSS

Aprimorando a segurança dos dados de cartões de pagamento

Marco Antônio Abade

sobre o Autor

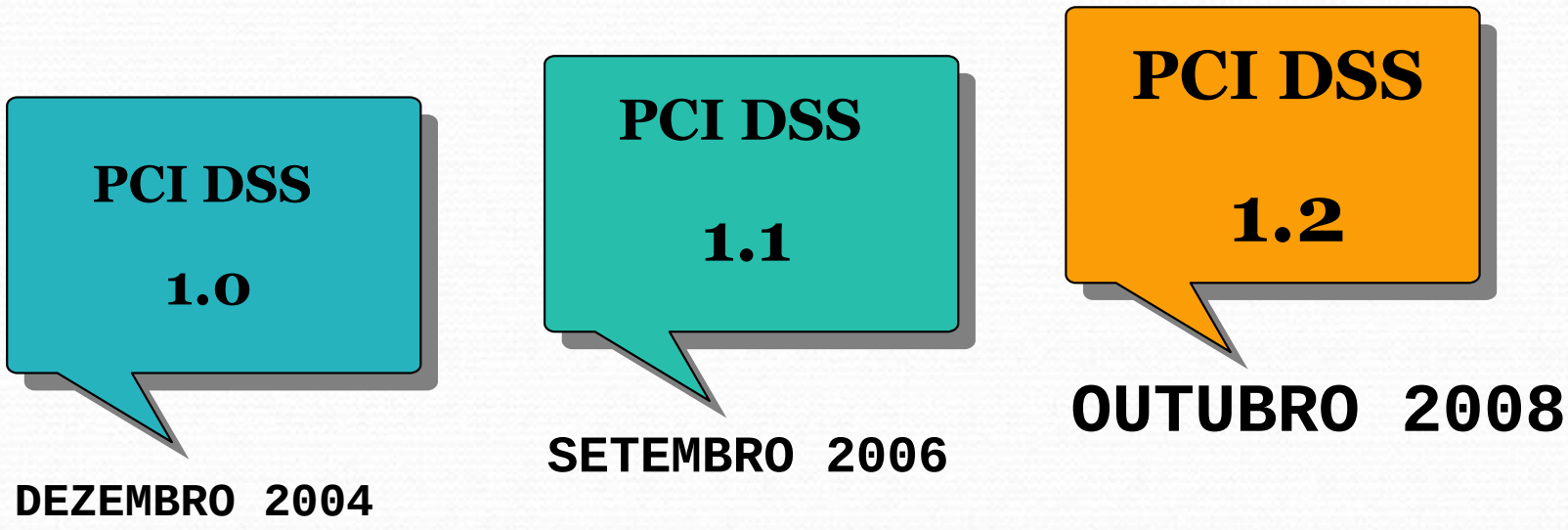
- Bacharel em Análise de Sistemas pela Universidade de Ribeirão Preto e Pós-graduado em Segurança da Informação pelo ITA – Instituto Tecnológico de Aeronáutica;
- Desenvolveu o sistema de internet banking "Net Empresas" do Banco Nossa Caixa (PJ), apresentando fraude Zero desde 2004;
- Auditor de sistemas;
- Implantou o CSIRT-BNC (Computer Security Incident Response Team) em 2005 e a CAF (Central AntiFraudes) em 2009;
- Foi gerente da Divisão de Monitoração e Operação de Segurança, responsável pela execução do projeto de "Prevenção a Fraudes Eletrônicas e Correlação de Eventos de Segurança da Informação" utilizando tecnologia de redes neurais e ferramentas SIEM – Security Information Event Management.

Agenda

- O Padrão de Segurança de Dados da Industria de Cartões de Pagamento – PCI DSS
- Elementos referentes ao comprometimento massivo de dados:
  - Comprometimento descoberto pela vítima
  - Comprometimento descoberto por terceiros
- Propostas de aprimoramento, aplicando processos de monitoração e tecnologia atualmente disponível, para redução da Janela de Intrusão.

Histórico do PCI DSS

- Originário de cinco programas de segurança distintos:
  - Visa Card Information Security Program (CISP)
  - MasterCard Site Data Protection
  - American Express Data Security Operating Policy
  - Discover Information and Compliance
  - JCB Data Security Program



Objetivos do Conselho PCI

- Entidade independente.
- Assumiu o controle do programa de conformidade em 2006.
- Missão: melhorar a segurança dos dados, através da educação e divulgação do PCI DSS.
- Implementar controles de segurança de TI nas empresas que transitam ou armazenam dados dos cartões.
- Estabelecer critérios de certificação para:
  - QSAs - *Qualified Security Assessors* e
  - ASVs - *Approved Scanning Vendors*.

A quem se aplica o padrão?

- Aos estabelecimentos comerciais e provedores de serviços que **armazenam**, **processam** ou **transmitem** dados de contas de cartões.

- Os requerimentos são **os mesmos** para todos os níveis de estabelecimentos comerciais.

- Eventuais diferenças residem nos prazos de implantação e frequências de relatórios e auditorias.

O padrão PCI DSS

- Estruturado na forma de 12 requerimentos distribuídos em 6 linhas de controles.

- Apresenta abordagem bastante objetiva e clara de como endereçar cada um de seus 12 requerimentos.
  - O PCI DSS v 1.2 contempla 210 sub-itens aos requerimentos
  - Há um total de 261 procedimentos (de testes) recomendados aos QSA - Assessores de Segurança Qualificados.

Controles e Requerimentos

Construir e manter uma rede segura	1: Instalar e manter um configuração de firewall para proteger os dados do portador 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança
Proteger os dados do portador do cartão	3: Proteger os dados armazenados do portador do cartão 4: Criptografar a transmissão dos dados do portador do cartão em redes abertas e públicas
Manter programa de gerenciamento de vulnerabilidades	5: Usar e atualizar regularmente o software ou programas antivírus 6: Desenvolver e manter sistemas e aplicativos seguros
Implementar medidas de controle de acesso rigorosas	7: Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios 8: Atribuir ID exclusivo para cada pessoa que tenha acesso ao computador 9: Restringir o acesso físico aos dados do portador do cartão.
Monitorar e Testar as Redes Regularmente	10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão 11: Testar regularmente os sistemas e processos de segurança
Manter uma Política de Segurança de Informações	12: Manter uma política que aborde a segurança das informações para funcionários e prestadores de serviços

Controles e Requerimentos

Construir e manter uma rede segura	**1: Instalar e manter um configuração de firewall para proteger os dados do portador do cartão** **2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança**
Monitorar e Testar as Redes Regularmente	**10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão** **11: Testar regularmente os sistemas e processos de segurança**

Agenda

- O Padrão de Segurança de Dados da Industria de Cartões de Pagamento – PCI DSS

- Elementos referentes ao comprometimento massivo de dados e ações em caso de ocorrência:
  - Comprometimento descoberto pela vítima
  - Comprometimento descoberto por terceiros

- Propostas de aprimoramento, aplicando processos de monitoração e tecnologia atualmente disponível, para redução da Janela de Intrusão.

Comprometimento de Dados

1980 – 1990	1990 – 2000	2000 - 2009
Cartão roubado Cartão perdido Cartão extraviado (não entregue)	Cartão clonado (ou “skimming”) Cartão extraviado	Cartão clonado Cartão não presente (uso somente da informação)

- Anos 80 - as ações eram voltadas aos cartões de forma individualizada (portador participa na prevenção)
- Anos 90 - predomínio do “Cartão Clonado”
- No final dos anos 90 - comprometimento “Massivo” (captura nas redes de terminais e comércio de dados via IRC).

Comprometimento Massivo de Dados

- Dois tipos de ataque
  - Ataques de Oportunidade
  - Ataques de alvo previamente estabelecidos
    - Utilização de ferramentas sofisticadas, customização de aplicativos e scripts e engenharia social
    - Envolvimento de criminosos ou organizações criminosas

Caso ocorra a invasão, é fundamental que a atividade seja identificada,

imediatamente.

Identificando o comprometimento

- Comunicação realizada **por terceiros**
  - Após uso fraudulento dos dados comprometidos
  - Sem que ocorra uso fraudulento dos dados comprometidos

- Descoberta realizada **pela vítima**
  - Por funcionários durante as atividades normais de trabalho.
  - Por comportamento ou performance não usual do sistema.
  - Pelo monitoramento de eventos ou análise dos logs.

Analisando o comprometimento

- **Fundamental**: Definição de datas relevantes relacionadas à invasão e ao comprometimento de dados ou seja,

Janela de Intrusão

- **Conter** e limitar a exposição de dados;
- **Isolar** os sistemas suspeitos de comprometimento do ambiente de produção;
- **Preservar** todos os logs disponíveis (Firewall, IDS, IPS, Web Server, sistemas operacionais, acessos remotos);
- **Manter** registro detalhado de todos eventos, observações e ações tomadas.

Levantamento de dados

- Realizado através de investigação forense computacional :
  - Número de clientes afetados. Lista completa das contas afetadas.
  - Identificação dos sistemas que sofreram danos (ou **infectados pelas intrusões** maliciosas, se aplicável).
  - O exato tipo de dado comprometido. Cartões de crédito? Documentos de identidade? Informações pessoais? Endereços e telefones?
  - Estimativa de custos para que se possa reparar os danos causados à organização e a seus clientes.
  - Determinação dos padrões de fraudes, se aplicável.

Relatório Verizon 2008 / 2009

- 285 milhões de registros comprometidos em 2008
- 74% dos comprometimentos envolveram ameaças vindas de fontes externas
- 20% originadas internamente
- A maior vítima foi o segmento de serviços financeiros, representando 93% de todos os registros.
  (Onde o dinheiro se encontra)

Fonte: 2009 Data Breach Investigation Report

Relatório Verizon 2008 / 2009

- Descoberta do comprometimento não foi realizada pela vítima e sim por terceiros:
  Relatório de 2008: 75%
  Relatório de 2009: 69%

- 75% dos ataques permaneceram despercebidos por semanas ou meses (**Janela de Intrusão**);

- 66% das vítimas possuíam logs com informações suficientes para descobrir a brecha em seus sistemas;

- 17% ataques = 95% dados comprometidos.

Fonte: 2009 Data Breach Investigation Report

Relatório Verizon 2008 / 2009

- Comprometimento X Janela de Intrusão:
  - Período entre invasão e comprometimento:

    Em Minutos: 27%

    Em Horas: 21%

    Em Dias: 29%

  - Descoberta do comprometimento:

    Em Semanas: 25%

    Em Meses: 49%

Fonte: 2009 Data Breach Investigation Report

Relatório Verizon 2008 / 2009

- Comprometimento X Janela de Intrusão:
  - 8% dos incidentes foram identificados por auditoria, monitoramento e análise de logs;
  - 30% das empresas possuiam IDS;
  - 32% das empresas possuiam R.I.;
  - 13% utilizavam ferramentas SIEM.

Fonte: 2009 Data Breach Investigation Report

Estudo de caso

- Com o objetivo acadêmico, estabelecemos um cenário hipotético de comprometimento massivo de dados.

  (Avaliação de vulnerabilidades e métodos de intrusão que superam os requisitos detalhados pelo Padrão).

- O cenário foi desenvolvido com base em:
  - Padrão PCI DSS;
  - Análise de dados estatísticos obtidos;
  - Metodologia de ataque real descrita em documento conjunto do FBI e Serviço Secreto Americano.

Estudo de caso

- **BANCO das BANANAS**

- Obteve a Certificação PCI DSS, com a abordagem de *check-list* e não de processo de melhoria da segurança;
- Após certificação, devido a fusão com outro banco, o nível de segurança da informação deteriorou rapidamente;
- O banco mostrou-se incapaz de identificar intrusão ocorrida em sua rede, tomando conhecimento somente após comunicação de terceiros.

Estudo de caso - Vulnerabilidades

- Incorporação de infraestrutura de entidades recém adquiridas;
- Re-engenharias resultantes de incorporações;
- Ausência de processo para instalação de *patches;*
- Falta de padrão do parque de computadores;
- Aplicativos de segurança e antivírus com versões diversas;
- Não cumprimento de políticas e cultura de permissividade;
- Nomes de Usuários e Senhas fracas;
- Arquitetura de rede inadequada.

Estudo de caso - Comprometimento

- Invasão dos sistemas do Banco em novembro;
- Identificação ocorreu somente em maio do ano seguinte, comunicado por parceiro de negócios;
- Janela de Intrusão superior a seis meses;
- Invasão realizada através de injeção de código SQL, (explorando vulnerabilidade de *Active Server Page* – ASP);
- Utilização de XP_Cmdshell;
- Obtenção de privilégios;
- Instalação de snnifers.

Agenda

- O Padrão de Segurança de Dados da Industria de Cartões de Pagamento – PCI DSS

- Elementos referentes ao comprometimento massivo de dados e ações em caso de ocorrência:
  - Comprometimento descoberto pela vítima
  - Comprometimento descoberto por terceiros

- Propostas de aprimoramento, aplicando processos de monitoração e tecnologia atualmente disponível, para redução da Janela de Intrusão.

Proposta de Aperfeiçoamento

- É fundamental que a Janela de Intrusão seja reduzida, uma vez que não é possível obter-se um sistema 100% seguro.
- A implementação e conformidade a qualquer Padrão, Norma ou *Framework* não garantem a proteção total dos sistemas.
- A forma de implementação e manutenção dos padrões de segurança tornam-se tão ou mais importantes que seus controles.

São necessários aprimoramentos para maior rapidez e assertividade na identificação de invasões, portanto:

Proposta de Aperfeiçoamento

- Maior relevância ao requisito 11.4 do PCI DSS, transformando-o em um requerimento do controle "Construir e manter uma rede segura"

CONSTRUIR E MANTER UMA REDE SEGURA	
Novo requisito	Instalar e manter uma configuração de IDS/IPS para proteção dos dados

Proposta de Aperfeiçoamento

- Recomendações:
  - Instalação de IDS/IPS na camada de rede na qual estejam armazenados ou trafegando dados de cartões ou de seus portadores;
  - Utilização de HIDS em todos os servidores sensíveis na rede em que se busca proteger;
  - Definição de padrões mínimos de configuração;
  - Processo formal para aprovar configurações ou suas alterações;
  - Topologia da rede **constando** pontos de inserção dos *appliances* de IDS/IPS;
  - Atualização da biblioteca de assinaturas de ataques conhecidos.

Proposta de Aperfeiçoamento

- Ampliar o escopo do requisito 10.6 do controle "Monitorar e Testar as Redes Regularmente", criando novo requisito:

MONITORAR E TESTAR A REDE REGULARMENTE	
Novo requisito	A análise dos registros deve ser realizada de forma automática, utilizando-se de ferramentas de gerenciamento e correlação de logs dos eventos de segurança.

- Ferramentas SIEM, bem configuradas, atuam de maneira que alertas sejam disparados automaticamente agregando valor aos logs.

Conclusão

- A experiência demonstra que Correlação de Eventos (monitoramento) + R. I. é a combinação poderosa para o efetivo conhecimento do ambiente tecnológico;
- Existe a real possibilidade de diminuição da Janela de Intrusão através de processos de monitoramento;
- A identificação de incidentes deve ser reduzida de dias ou semanas para minutos e, em alguns casos, para Real Time, sempre, pela vítima;

Conclusão

- Conformidade deve ser encarada como um processo e não somente como um *check list;*
- A certificação captura um momento, **uma foto;**
- Para que se possa melhorar a segurança da informação é necessário considerar-se o conjunto do dia-a-dia, **o filme;**
- A proposta é utilizar requerimentos que o próprio padrão contempla para, aperfeiçoando-os, obter melhoria da segurança dos dados de cartões de pagamentos, através da **diminuição da Janela de Intrusão.**

marcoabade@yahoo.com
11 8331-7478