Curso em PCI-DSS 3.1

BASEADO NO MODELO PROPOSTO PELO PCI Security Standards

Tendo em vista o aumento dos ataques a empresas que armazenam, processam ou transmitem dados de cartão de crédito, as bandeiras de cartão tem cada vez mais criado clausulas contratuais sobre a proteção de dados, assim como exigências de auditoria e certificação das empresas em relação à proteção de dados do portador de cartão

Em vista deste cenário, as maiores bandeiras de cartão de pagamento do mundo uniram-se para criar um padrão de segurança que pudesse garantir os requisitos mínimos de segurança para estes dados e juntamente a adquirentes, prestadores de serviço e comerciantes fundaram o PCI Council (PCI SSC), orgão responsável pela manutenção do padrão de segurança PCI DSS, que atualmente encontra-se na versão 3.1. A partir deste padrão criou-se um programa de auditoria e certicação em segurança da informação, tanto da empresa como dos profissionais que lidam com estes dados.

Assim, partindo-se da experiência dos facilitadores e criadores deste conteúdo em ministrar os treinamentos oficiais de certificação **ISA (Internal Security Assessor)** e a percepção da necessidade de um treinamento mais focado na implementação dos controles necessários para reforçar a segurança de dados de cartões de pagamento foi criada esta capacitação que tem como meta fornecer todo o conhecimento necessário para obter a certiicação PCI Professional e para certificar a sua empresa como PCI Compliant.

Objetivos

Capacitar o aluno a definir o escopo e aplicar os controles do PCI DSS no ambiente de dados de cartão.

Público alvo

Todo o pessoal técnico envolvido com o manuseio de dados críticos, mais especificamente os custodiantes das informações, normalmente pertencentes à área de tecnologia da informação. Dentre esses profissionais destacamos:

- Gestores, Consultores e Pessoal de Suporte, e gerentes de projeto de serviços de TI;
- Desenvolvedores, Integradores e arquitetos de sistemas;
- Engenheiros e especialistas de rede;
- Profissionais de segurança da informação.

Benefícios

Fornecer subsídios para os alunos entenderem de uma forma prática e objetiva como funcionam as transações realizadas com cartões de crédito e realizarem uma análise de conformidade com o padrão PCI DSS 3.1, permitindo que o mesmo possa ser implantado nas empresas.

Diferenciais:

- Instrutor certificado CISSP-ISSAP, CISM, ISMAS, entre outras;
- Ao final deste treinamento o aluno estará apto para:
    - Realizar uma análise de conformidade com o padrão PCI DSS através das políticas e as tecnologias utilizadas de acordo com este padrão para a proteção de dados críticos na organização;
    - Conhecer medidas de segurança da informação para aumentar a segurança dos dados de cartões de crédito;
    - Adaptar a infraestrutura física e lógica da empresa para a submissão de uma auditoria oficial do PCI DSS.

Metodologia de ensino

Ação educacional com forte conteúdo prático com experimentação das técnicas em exercícios e em casos reais da Organização.

Níveis de Avaliação

Reação: nível de satisfação dos participantes em relação à ação educacional aplicada logo após o seu término.

Formas de Avaliação da Aprendizagem

Avaliação do tipo Formativa com função de orientar, corrigir, informar sobre a aprendizagem do participante da ação através de feedbacks.

Pré requisitos

Conhecimentos básicos de Tecnologia da Informação

Material Didático

- Apostila colorida, impressa com tecnologia ecológica de cera e papel reciclado.

Conteúdo Programático

A narrativa do curso se dá em forma de história, que começa com a chegada de uma nova CEO, com a missão de garantir a segurança de dados de cartão de pagamento na Evolutione.

O Curso é dividido em 7 partes com 28 capítulos, durante os quais as personagens apresentam as políticas e as tecnologias utilizadas para a proteção de dados críticos na organização.

Parte I – Identificando e isolando dados sensíveis

Introdução: A Evolutione e o grupo de colaboradores mais envolvido com a segurança da informação é apresentado aos alunos. Hilda solicita que o CIO da empresa (Willian) faça um levantamento de todos os tipos de dados que a empresa processa e armazena, e em seguida pede que Olívia (Jurídico) identifique as leis, normas e regulamentações relacionadas às atividades da empresa e a esses tipos de dados. Juntos, Olívia e Wallace (CISO) desenham as políticas de retenção de dados e diretrizes para comunicação com portadores de cartão de pagamento para atenderem ao PCI DSS.

Capítulo 1 – A Evolutione e o PCI Council: Allan, o CSO da Evolutione posiciona a segurança da informação no organograma da empresa, explana sobre o enquadramento da Evolutione nos programas de conformidades das bandeiras de cartões de pagamento e apresenta o PCI Council e seus padrões de segurança para os outros gestores da empresa. Wallace, o CISO, apresenta os componentes de SI (processos, pessoas e tecnologia), os conceitos de defesa em profundidade, o processo de criação de controles de segurança e os tipos e funções das medidas de segurança existentes.

Capítulo 2 – Análise de Riscos: Allan inicia um processo de análise de riscos baseado nas melhores metodologias de mercado, como a ISO 27005 e NIST SP 800-30 revision 1. Para atender ao requisito 12.2 Allan estabelece sistemas de gestão de riscos com um processo de revisão anual dos riscos.

Capítulo 3 – Localização dos dados: Wallace desenha um diagrama de rede que identifica todos as conexões entre o ambiente de dados de portadores de cartão, ou CDE (Cardholder Data Environment), e demonstra o fluxo de dados de cartões dentro dos sistemas e redes. Adicionalmente, Willian se utiliza de ferramentas para identificar dados de cartões que possam estar em outras localidades além das documentadas.

Capítulo 4 – Retenção de Dados: Wallace apresenta os critérios utilizados para armazenamento de dados de cartões de pagamento na Evolutione.

Capítulo 5 – Descarte de dados: Wallace apresenta os controles utilizados para a destruição de dados que não possuem mais uma necessidade legal ou de negócio para serem armazenados.

Parte II – Protegendo sistemas e redes e preparando-se para responder a falhas

Capítulo 6 – Definição de escopo: Wallace apresenta a Hilda as estratégias de segurança relacionadas à identificação do fluxo de dados de portadores de cartão dentro da Evolutione e de todos os componentes por onde estes dados trafegam, são armazenados ou processados.

Capítulo 7 – Configuração dos ativos de rede: Alex apresenta as políticas de configuração dos ativos de rede, incluindo as regras de firewall, NAT, técnicas anti-spoofing e sincronização dos arquivos de configuração. Alex especifica também os protocolos em uso e apresenta os mecanismos de detecção de intrusos nos diferentes segmentos de rede criados através de perímetros que separam diferentes zonas com diferentes níveis de confiança através de firewalls, switches e roteadores.

Capítulo 8 – Configuração padrão: Alex apresenta as políticas definidas para a substituição de senhas dos ativos de rede e dos softwares instalados na Evolutione antes da implantação dos mesmos na rede corporativa.

Capítulo 9 – Configuração de Endpoint: Wallace apresenta as políticas e configurações utilizadas pela Evolutione para a configuração do(s) software(s) em execução nos hosts. Que incluem o antivírus, firewall pessoal e monitor de integridade nos equipamentos dentro do ambiente de dados do portador de cartão.

Capítulo 10 – Criptografia Assimétrica: Samuel, o coordenador de infraestrutura apresenta os fundamentos da criptografia assimétrica, certificados digitais, autoridades certificadoras, Infraestrutura de chaves públicas e assinatura digital.

Capítulo 11 – Criptografia aplicada à transmissão de dados: Samuel continua sua explicação, demonstrando como a Evolutione utiliza a criptografia para atingir os objetivos de conformidade e aumentar a segurança ao transmitir dados de cartões de pagamentos de forma segura, utilizando VPN, SSL/TLS e WPA.

Capítulo 12 – Acesso remoto: Samuel apresenta as políticas de acesso remoto, que incluem autenticação forte, baseada em mais de um fator, as características criptográficas para acesso administrativo.

Capítulo 13 – Controles Físicos: Allan apresenta os controles de segurança física como a proteção do perímetro físico, áreas sensíveis, controles de acesso ao ambiente, CFTV, pontos de rede, estações desbloqueadas, informações nas estações de trabalho, além das políticas de controle de dispositivos de pagamento com lista de dispositivos, e inspeção periódica dos mesmos.

Capítulo 14 – Testes de vulnerabilidades: Samuel apresenta as políticas e as metodologias utilizadas para realizar os testes trimestrais de vulnerabilidades e os testes anuais de invasão no ambiente de dados do portador de cartão.

Capítulo 15 – Provedores de Serviço e Plano de resposta a incidentes: Wallace apresenta as políticas para controle de provedores de serviço, os controles para resposta a incidentes de segurança e apresenta o plano de resposta a incidentes da Evolutione para o caso de vazamento de dados.

Parte III – Segurança em aplicações de pagamento

Willian apresenta os estudos relacionados a vulnerabilidades de softwares, o processo de criação de exploits, zero-days, os procedimentos a serem adotados pelas empresas para mitigar essas ameaças e as melhores práticas de atualização, além das políticas de atualização, hardening e privilégio mínimo da Evolutione.

Capítulo 16 – Configuração: Samuel descreve os procedimentos para criação e manutenção de padrões de instalação e configuração segura (hardening) dos componentes do sistema, assim como os procedimentos criados para que estes sistemas permanecem sempre atualizados e com uma configuração segura em qualquer tipo de componente, incluindo sistemas operacionais, páginas WEB, e firmware de ativos como roteadores e firewalls.

Capítulo 17 - Desenvolvimento: Gabriel, o “Lenda”, explica como os princípios de segurança no design e segurança por default são aplicados nos desenvolvimentos internos da Evolutione. Apresenta também a separação entre os ambientes de desenvolvimento, teste e produção, os procedimentos para gestão de mudanças em software, treinamento de desenvolvedores e os cuidados tomados na validação das entradas dos sistemas para evitar falhas de Buffer overflow, SQL Injection.

Parte IV – Monitoração e controle de acesso aos sistemas

Capítulo 18 – Controle de Acesso: Willian apresenta a política de controle de acesso da Evolutione, as regras para criação e manutenção de senhas seguras e os conceitos de gestão e identidades, identificação única, Need to Know, privilégio mínimo, segregação de funções.

Capítulo 19 – Reference Monitor: Wallace apresenta os conceitos de Reference Monitor, Trile A, DACL's, SACL's, Auditoria de eventos (Logs), assim como o processo e a política de auditoria e os cuidados para sincronização de hosts (NTP).

Capítulo 20 – Autenticação: Willian analisa as diferenças entre os processos de autenticação mais utilizados em sistemas operacionais, como o passwd, SAM, domínios e Kerberos. Discute também, as políticas de acesso a banco de dados e autenticação com Smatcards.

Capítulo 21 – Monitoramento: Alex apresenta as políticas e recursos de monitoramento do ambiente utilizados para detectar alterações em arquivos críticos, redes wireless não autorizadas. O Capítulo aborda tecnologias como Scanners de vulnerabilidades, IDS, IPS e NAC.

Parte V – Proteção dos dados armazenados

Capítulo 22 – Proteção dos dados armazenados: Wallace apresenta as bases da criptografia simétrica, truncagem e hash de dados através da teoria e da demonstração da criptografia de arquivos, bancos de dados, discos e backups utilizada na Evolutione para a proteção dos dados armazenados.

Capítulo 23 – Gerenciamento de Chaves: Samuel apresenta as políticas para geração, transmissão, custódia de chaves criptográficas, conhecimento compartilhado, duplo controle e destruição das chaves.

Capítulo 24 – Tokenização: Samuel apresenta os conceitos de Tokenização e como essa metodologia vem sendo aplicada dentro da Evolutione para diminuir o impacto de um eventual vazamento de dados.

Parte VI – Controles adicionais

Capítulo 25 – Gestão de Mudanças: Wallace apresenta os controles utilizados para garantir uma gestão adequada das alterações realizadas nos componentes dos sistemas da Evolutione, dentre eles a documentação de impacto, aprovação da mudança, teste de funcionalidade e procedimentos de retorno.

Capítulo 26 – Política de Segurança: Allan apresenta o processo de criação e aprovação da política de segurança da Evolutione, assim como a sua divulgação e a capacitação da equipe nos assuntos referentes à segurança da informação.

Parte VII – Documentação do PCI Council

Capítulo 27 – Os documentos de apoio: Allan apresenta os documentos disponibilizados pelo PCI Council para auxiliar as empresas na obtenção da conformidade com os padrões vigentes.

Capítulo 28 – SAQ's, ROC's, AOC's e planilha de controles compensatórios: Allan explica as diferenças entre os Questionários de auto-avaliação (SAQ's) e Relatórios de conformidade (ROC's), e Atestados de Conformidade (AoC), além de demonstrar os requisitos e passos para preenchimento da planilha de controles compensatórios

Veja também:

Curso Introdução ao Gerenciamento de Riscos em TI

Curso Capacitação em Gerenciamento de Riscos de TI

Para conhecer o nosso conteúdo sobre Governança de TI acesse o seguinte link:

http://www.grupotreinar.com.br/treinamentos.aspx?a=1192

Para saber um pouco mais sobre Governança de TI acesse o nosso Blog através do seguinte link:

http://www.grupotreinar.com.br/blog.aspx?filterby=Governan%C3%A7a%20de%20TI