UNIVERSIDADE
FEDERAL DO CEARÁ

AUDITORIA E SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

ISO 27002 8.25-8.35

8.25 Ciclo de vida de desenvolvimento seguro

Para garantir que a segurança da informação seja mantida dentro do ciclo, regras devem ser estabelecidas e aplicadas no desenvolvimento. O desenvolvimento seguro é um pré-requisito para construir serviços, arquiteturas, software e sistemas seguros. Portanto, é interessante considerar alguns aspectos como:

- Separação dos ambientes de desenvolvimento, teste e produção;
- Orientação sobre a segurança no ciclo de vida do desenvolvimento de software:
    - Segurança na metodologia de desenvolvimento de software;
    - Diretrizes de codificação seguras para cada linguagem de programação utilizada.
- Testes de sistema e segurança, incluindo testes de regressão, verificação de código e testes de invasão.

8.26 Requisitos de segurança da aplicação

Assegura que os requisitos de segurança da informação sejam identificados, especificados e aprovados ao desenvolver ou adquirir aplicações. Estes requisitos geralmente são determinados por meio de uma avaliação de risco, desenvolvidos com o apoio de especialistas em segurança da informação. É importante verificar se é aplicável, por exemplo, questões como o nível de confiança na identidade das entidades, requisitos de proteção de informações confidenciais e controle de entrada. Para aplicativos que fornecem serviços transacionais entre organizações e parceiros, devem considerar o seguinte ao determinar seus requisitos de segurança da informação por exemplo, nível de confiança que cada parte requerer em cada identidade declarada pela outra parte e nível de confiança exigido na integridade das informações trocadas ou tratadas e mecanismos de identificação da falta de integridade (verificação de redundância cíclica, hashing, assinaturas digitais);

Além disso, para aplicações envolvendo pedidos eletrônicos e pagamento, devem se considerar requisitos para manter a confidencialidade e integridade das ordens de pagamento e grau de verificação adequado para garantir que as informações de pagamento fornecidas por um cliente sejam verdadeiras

8.27 Princípios de arquitetura e engenharia de sistemas seguro

Este tópico busca garantir que os princípios de engenharia de segurança sejam estabelecidos, documentados e aplicados em todas as camadas de arquitetura. Os princípios de engenharia de sistemas seguros incluem análise de toda a gama de controles de segurança necessários para proteger as informações e os sistemas contra ameaças identificadas, por exemplo. Leva-se em consideração os princípios de engenharia de segurança como a necessidade de se integrar com uma arquitetura de segurança e o custo, tempo e complexidade para atender aos requisitos de segurança. Também é importante que a organização considere os princípios de “confiança zero”, como assumir que os sistemas de informação o da organização já estão violados e, portanto, não depender apenas da segurança do perímetro de rede e

empregar uma abordagem “nunca confie e sempre verifique” para o acesso aos sistemas de informação.

Outras informações relevantes são como os princípios de engenharia segura irão ser aplicados ao projeto, usando a tolerância a falhas e outras técnicas de resiliência e segregação, aplicadas juntamente com as técnicas seguras de virtualização e técnicas de resistência à adulteração.

8.28 Codificação segura

Garante que o software seja escrito com segurança e reduz o número de possíveis vulnerabilidades de segurança no software. As organizações devem monitorar as ameaças do mundo real, bem como os conselhos e informações mais recentes sobre vulnerabilidades de software e orientar os princípios de codificação segura por meio de melhoria e aprendizado contínuos. É necessário que alguns procedimentos sejam adotados estando divididos em três etapas: (1) Planejamento antes da codificação; (2) Durante a codificação e; (3) Após a codificação a análise crítica e manutenção.

(1) Planejamento antes da codificação: práticas e defeitos de codificação comuns e históricos que levem a vulnerabilidades de segurança da informação junto a configuração de ferramentas de desenvolvimento, como ambientes integrados de desenvolvimento (IDE), para ajudar a impor a criação de código seguro.

(2) Durante a codificação: documentação de códigos e remoção de defeitos de programação, que podem permitir a exploração de vulnerabilidades de segurança da informação junto a proibição do uso de técnicas de design inseguras (por exemplo, uso de senhas no código-fonte, amostras de código não aprovadas e serviços web não autenticados).

(3) Análise crítica e manutenção: convém que as atualizações sejam empacotadas e implantadas com segurança junto ao registro de erros e suspeitas de ataques e que os logs sejam analisados criticamente de forma regular, para fazer ajustes no código conforme necessário.

Acima foram listados alguns procedimentos de codificação segura, vale ressaltar que existem outros tipos para garantir a segurança interna e externa de uma organização.

8.29 Testes de segurança em desenvolvimento e aceitação

Garante que os requisitos de segurança da informação sejam atendidos ao implantar um aplicativo ou código em um ambiente de produção. Novos sistemas de informação, atualizações e novas versões devem ser exaustivamente testados e validados durante o processo de desenvolvimento, e o teste de segurança deve ser parte integrante do teste de um sistema ou de seus componentes. Convém que nos testes de segurança deve-se incluir testes de: Funções de segurança, autenticação do usuário, restrição de acesso e uso de criptografia, codificação segura, configurações seguras, incluindo a de sistemas operacionais, firewalls e outros componentes de segurança. Para maior desenvolvimento interno, a equipe de desenvolvimento deve primeiro realizar esses testes e logo após, deve-se realizar testes de aceitação independentes para garantir que o sistema esteja funcionando conforme o esperado. Deve ser considerado os seguintes pontos: Realização de atividades de análise crítica de códigos como

elemento relevante para testes de falhas de segurança, incluindo insumos e condições não antecipadas; realização de varredura de vulnerabilidades para identificar configurações inseguras e vulnerabilidades do sistema e; realização de testes de invasão para identificar código e arquitetura inseguros. Os testes devem ser executados em um ambiente de teste que se assemelhe ao ambiente de produção pretendido o mais próximo possível para garantir que o sistema não introduza vulnerabilidades no ambiente da organização e que o teste seja confiável.

8.30 Desenvolvimento terceirizado

Garante que para o desenvolvimento do sistema, deve certificar-se de implementar as medidas de segurança da informação exigidas pela organização. Ao terceirizar o desenvolvimento do sistema, as organizações devem comunicar e concordar com os requisitos e expectativas e monitorar e verificar continuamente se a entrega do trabalho terceirizado atende a essas expectativas. Os seguintes pontos devem ser considerados em toda a cadeia de suprimentos externa da organização: contratos de licenciamento; propriedade de código e direitos de propriedade intelectual relacionados com o conteúdo de terceiros; provisão de evidências de que níveis mínimos aceitáveis de segurança e capacidades de privacidade estão estabelecidos (relatórios de garantia); contratos de custódia para o código-fonte do software (por exemplo, se o fornecedor sair do negócio); direito contratual para auditar processos e controles de desenvolvimento. Nesse sentido estes pontos estão listados como os principais, vale destacar que é possível encontrar pontos diferentes pois organizações podem adotar outros.

8.31 Separação dos ambientes de desenvolvimento, teste e produção

Entende que os ambientes de desenvolvimento, testes e produção sejam separados e protegidos, com o propósito de proteger o ambiente de produção e os dados de comprometimento através de desenvolvimento e teste. A orientação é que os níveis de separação entre os ambientes de produção, teste e desenvolvimentos necessários para evitar problemas na produção devem ser implementados, da seguinte forma: separando adequadamente os sistemas de desenvolvimentos, produção e operação em diferentes domínios; definir, documentar e implementar regras e autorização para a implantação de software do desenvolvimento ao status de produção; testar alterações nos sistemas de produção e aplicações e prepará-los antes de serem aplicados aos sistemas de produção; não testar em ambientes de produção, exceto se tiverem sido aprovadas; exibir de etiquetas de identificação de ambiente adequadas nos menus para reduzir o risco de erro; não copiar informações sensíveis nos ambientes de desenvolvimento, a menos que sejam fornecidos controles equivalentes para os sistemas de desenvolvimento e teste.

De qualquer maneira, os ambientes de desenvolvimento e teste são protegidos considerando patches e atualização de todas as ferramentas de desenvolvimento, configuração segura de sistemas e software, controle do acesso aos ambientes, monitoramento da mudança no ambiente e código armazenado nele, monitoramento seguro e backup das informações dos ambientes. Uma única pessoa não tenha a capacidade de fazer alterações tanto no desenvolvimento quanto na produção sem uma análise crítica e aprovação prévias

8.32 Gestão de mudanças

Tem o objetivo de preservar a segurança ao executar mudanças na aplicação, ou seja, na implantação de novos sistemas ou em atualizações de sistemas pré-existentes. É importante que todo o processo de desenvolvimento seja bem documentado e oficializado, incluindo as especificações de requisitos e testes de software, para garantir o controle de qualidade. Além disso, é fundamental aplicar procedimentos de controle de mudanças para garantir confidencialidade, integridade e disponibilidade.

Os procedimentos de controle seguem as seguintes orientações:

1. As mudanças devem ser devidamente descritas e autorizadas;
2. Antes de implementar as mudanças, é necessário avaliar os impactos de todas as dependências;
3. Os critérios de verificação devem incluir testes de verificação de aceitação;
4. Planos de contingência devem ser criados para lidar com problemas;
5. Como etapa final, é imprescindível registrar todos os registros das etapas anteriores.

8.33 Informações de teste

Gerenciar de forma adequada as informações de teste é importante para garantir a relevância dos testes e proteger as informações operacionais usadas durante o processo. É importante a seleção apropriada das informações para garantir a confiabilidade dos resultados e a confidencialidade das informações. Dados que sejam confidenciais, em especial dados pessoais, não devem ser copiados em ambientes de desenvolvimento ou teste. Para proteger as cópias das informações de produção usadas nos testes, use os mesmos procedimentos de controle de acesso usados na produção, obtenha permissões separadas para cada cópia das informações de produção e recomenda-se que as informações de uso e confidenciais sejam registradas com máscara de proteção ou mascaramento. Remova adequadamente as informações operacionais do ambiente de teste após o teste. Essas medidas são projetadas para garantir a segurança e eficácia do teste e para evitar o uso não autorizado de informações de teste.

8.34 Proteção de sistemas de informação durante os testes de auditoria

A realização de testes de auditoria e outras atividades de garantia em um sistema operacional requer planejamento prévio e acordo entre os testadores e a gerência responsável. O objetivo é minimizar o impacto dessas atividades nos sistemas e processos de negócios e para atingir isso, é importante seguir algumas diretrizes. Deve haver acordo sobre os requisitos de gerenciamento para testar o acesso a sistemas e dados, bem como controlar a cobertura do teste de auditoria técnica. O teste deve ser limitado ao acesso somente leitura ao software e aos dados e, se isso não for suficiente, um administrador experiente pode realizar o teste em nome do auditor. Antes de conceder o acesso, é fundamental estabelecer e verificar os requisitos de segurança do dispositivo utilizado, como a presença de patches e software antivírus atualizado.

O acesso fora do modo somente leitura deve ser concedido apenas para cópias separadas de arquivos do sistema. Esta cópia será deletada ao final da vistoria ou acompanhada dos devidos backups, se necessário, para manutenção de acordo com a documentação exigida. Esses princípios garantem uma execução de teste segura e controlada, mantendo a integridade do sistema operacional e dos processos de negócios.