CHECAGEM DE SISTEMAS

SEGURANÇA DA INFORMAÇÃO

Informações corporativas fazem toda a diferença para uma empresa. Mas se essas informações forem divulgadas para um concorrente, a empresa será consideravelmente lesada. Ao entender os conceitos relacionados à segurança da informação, podemos evitar que isso ocorra. Assim, o ponto de vista que devemos adotar é o de que nada é totalmente seguro, pois os elementos de risco são dinâmicos. Dessa forma, o que é seguro hoje, pode não ser amanhã.

ATAQUES E TIPOS DE DADOS

Ataques podem ser realizados para que os dados pessoais sejam vazados e a privacidade seja comprometida, bem como podem ocorrer com dados em processamento, dados em transmissão ou dados armazenados. Ataques a bancos de dados visam os dados armazenados, enquanto os ataques à rede visam os dados em transmissão. Dados em processamento tem a tendência de sofrer ataques bem mais elaborados, demandando um maior nível de segurança.

CONTROLES DE SEGURANÇA

Controles de segurança devem fazer parte da estratégia de segurança de todas as empresas. O controle de identidades e acessos envolve o gerenciamento de contas e senhas dos usuários e seu uso é fortemente recomendado. Outro controle recomendado são os antivírus, que podem ser usados em servidores e dispositivos dos usuários. Um controle de segurança processual é a compreensão sobre segurança e privacidade realizada na admissão de funcionários. Devemos ressaltar que o uso de diversas camadas de proteção é recomendado, pois uma pode não ser o bastante para realizar o controle de segurança de forma adequada. Durante a transmissão de dados existem técnicas de criptografia que podem, e devem ser adotadas.

CRIPTOGRAFIA DE CHAVE PRIVADA

Como o uso de um algoritmo e uma chave secreta privada, uma mensagem original é cifrada. O resultado é um texto incompreensível para o atacante. Quem recebe a mensagem cifrada usa a mesma chave secreta para decifrar a mensagem e retornar ao conteúdo original.

CRIPTOGRAFIA DE CHAVE PÚBLICA

Um fato sobre a criptografia de chave privada é o desafio da troca de chaves. Mesmo assim, ela é rápida de ser executada. No entanto, a criptografia de chave pública é computacionalmente mais pesada, porém mais adequada para ser usada na troca de chaves. Nela existem pares de chaves, usados em conjunto para a cifrarem e decifrarem as mensagens.

GESTÃO E NORMAS DE SEGURANÇA

Um dos principais instrumentos para a aplicação de segurança da informação nas organizações são as normas. Elas apresentam uma visão abrangente das necessidades e implementações de segurança da informação, e devem ser seguidas por todos os funcionários da empresa.

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Um sistema de gestão de segurança da informação é fundamental para fortalecer a cultura de segurança das empresas. Quando estabelecido, esse sistema preserva a integridade dos dados por meio de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos estão sendo adequadamente gerenciados. Ele deve ser criado de acordo com as características e normas de cada empresa.

CULTURA E NORMAS DE SEGURANÇA

Toda empresa tem sua própria cultura de segurança e privacidade. Para fortalecer essa cultura de segurança, um dos elementos primordiais a serem adotados são as normas de segurança da informação e privacidade. Um passo importante para o sucesso das normas é que ela aborde as características de cada empresa. Ela deve ser plausível e deve ser aplicável, deve definir as diretrizes a serem seguidas por todos, e deve determinar quais os controles de segurança que deverão ser implementados. Normas são compostas por documentos que incluem processos e guias. Dessa forma, a organização de todo o conteúdo deve tornar mais simples o seu acesso.

LEI GERAL DE PROTEÇÃO DE DADOS

Essa lei estabelece medidas para que haja a transparência na coleta e no tratamento de dados pessoais pelas organizações, que devem então prover a proteção adequada dos mesmos para garantir a privacidade dos seus usuários. As empresas devem, assim, implementar controles de segurança da informação para evitar incidentes de segurança.

SEGURANÇA NA INTERNET

Questões sobre segurança e privacidade na internet passam pelo entendimento dos diferentes elementos que envolvem o que deve ser protegido e os componentes ou ativos de um ambiente que podem ser explorados durante os ataques. Transações partem dos usuários que usam seus dispositivos doravante de algum local em que exista a conexão com a internet, e passam por diversos componentes até chegar ao seu destino. Neste caminho, os agentes de ameaça estão sempre à espreita em busca de oportunidades para roubar dados.

SEGURANÇA EM TRANSAÇÕES

No ambiente dos usuários as transações exigem segurança, porque ataques podem capturar e corromper os dados, fazendo com que transações fraudulentas cheguem ao provedor. Assim, o provedor de serviços, além de proteger o seu próprio ambiente, tem o desafio de tratar todas as transações vindas de criminosos. No ambiente de internet, onde o agente de ameaça está sempre presente, é importante dispor de um canal seguro, que deve ser provido pelo provedor de serviços. Conexões devem ser protegidas com o uso de protocolos de segurança.

TESTES DE SEGURANÇA

Testes de segurança é o processo de comparar o estado de um sistema de acordo com algumas regras. Podem ocorrer somente no encerramento ou compor o processo de desenvolvimento do sistema desde o começo. Testes de segurança requerem pensamento fora do padrão, casos de uso normais testarão o comportamento normal do sistema, em que o usuário está usando as funções da forma como é esperado. Mas, é preciso extrapolar as expectativas tradicionais e ter um pensamento atacante visto que, fazer um teste de segurança fraco e considerar o mesmo completo, é tão crítico quanto não fazer teste algum, pela falsa sensação de segurança gerada.

TESTES DE PENETRAÇÃO

Os testes de penetração são realizados no ambiente externo, com o propósito de determinar se e como um agente de ameaça pode obter um acesso não autorizado aos ativos que afetam um sistema, e confirmar se os controles requeridos estão implementados. Envolve ainda identificar meios de explorar falhas para driblar os controles de segurança dos componentes do sistema.

FUNDAMENTOS DE CHECAGEM DE SISTEMAS

Com a constante evolução do ambiente das empresas e o dinamismo das metas de negócios, a checagem dos sistemas é cada vez mais importante. De modo geral, tem como meta checar as atividades, os processos e os sistemas, visando aumentar a eficiência e eficácia dos mesmos.

O processo de checagem visa também confirmar para a alta gestão da empresa que o negócio está funcionando corretamente, assegurando a saúde financeira e operacional da organização aos diversos atores envolvidos. Uma das principais características da checagem é que ela só pode ser feita por profissionais que têm certificação para exercer a função. Outra característica é que ela é independente dos aspectos operacionais, o que proporciona que os pareceres sejam racionais e sem viés sobre a efetividade do ambiente de controle interno. Portanto, a checagem é uma inspeção formal para checar se um padrão ou conjunto de guias está sendo seguido, se os registros estão corretos e se as metas de eficiência estão sendo alcançadas. Um programa de checagem é composto por procedimentos, usados para testar e a efetividade dos controles adotados pela empresa. Esse processo requer a busca por evidências, apuração das forças e fraquezas dos controles, com base nas evidências coletadas, a preparação de um relatório que apresenta todos esses pontos e recomendações para sanar os problemas.

TÉCNICAS E FERRAMENTAS PARA CHECAGEM DE SISTEMAS

As checagens são compostas por metodologias, técnicas e ferramentas, que devem ser usadas para levantar e analisar evidências. Elas devem amparar o profissional responsável a organizar e documentar resultados. Existem técnicas voltadas para interação com pessoas em busca das informações, que complementam as análises manuais e técnicas. Entre as técnicas que tratam as interações com pessoas, estão as entrevistas e dinâmicas em grupo. No que tange a análise manual, podemos recorrer à revisão da documentação, análise das normas, procedimentos e processos, além das revisões gerenciais e de códigos. Para a análise técnica, as ferramentas são um dos principais métodos e exige um amplo conhecimento técnico dos responsáveis.

PCIDSS

Padrão de segurança de dados para empresas de cartões de pagamento. Estabelece requisitos de segurança a serem cumpridos por todos os estabelecimentos que processam, transmitem ou armazenam dados de cartões. Empresas desse ramo devem cumprir todos os doze requisitos de segurança determinados. Sem a conformidade com esse padrão, às mesmas ficam sujeitas a não poderem mais participar do ecossistema de cartões de pagamento, por colocar em risco os demais atores da cadeia e lesar a confiança no sistema.

MASCARAMENTO E TRUNCAMENTO

O mascaramento é um método que serve para ocultar uma parte dos dados, ao ser impresso. O truncamento é um método que remove permanentemente um segmento dos dados. Caso exista o armazenamento, ocorre o truncamento ao invés do mascaramento, que é usado apenas para sua impressão. Como no truncamento usado no armazenamento a remoção é permanente, as alterações podem ser feitas de uma forma mais geral.

ORIGINAL (6393 5080 8685 8382)
MASCARAMENTO (6393 50XX XXXX 8382)
TRUNCAMENTO (6393 50 - 82)