AUDITORIA E SEGURANÇA DE SISTEMAS

INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO - UNIDADE 01

As Informações Corporativas fazem toda a diferença para uma empresa. Mas e se essas informações forem divulgadas para um concorrente ou em redes sociais e se tornarem públicas? O que acontecerá com essa empresa? E como isso pode acontecer? São as respostas a essas perguntas que você obterá ao entender como um ataque cibernético ocorre, o que pode ser comprometido e como a segurança da informação pode evitar que isso aconteça.

PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Nada é Totalmente Seguro. Elementos do risco são dinâmicos, seja quando novas vulnerabilidades surgem, seja quando o ambiente muda com novos ativos ou quando a motivação de um agente de ameaça alcança níveis que aumentam a chance de sucesso de um ataque. Dessa forma, aquilo que é seguro, hoje, pode não ser amanhã. Tendo em vista os diversos tipos de informações, os três princípios da segurança da informação são a Confidencialidade, Integridade e Disponibilidade (CID). A Confidencialidade visa que As Informações Não Sejam Reveladas a Indivíduos Ou Entidades Não Autorizados. A Interidade garante que As Informações Devem Permanecer Sempre Em Seu Estado Original . E o princípio da Disponibilidade possui como característica a sua Rápida Percepção Em Caso De Comprometimento.

ELEMENTOS DE RISCO

Existem diferenças entre Ameaça e Vulnerabilidade. Além disso, é preciso diferenciar um Ataque de um Risco e do Agente De Ameaça. Ameaça é algo que pode acontecer e que possui potencial de se concretizar. Você pode fazer uma análogia com a realidade e imaginar um exemplo de ameaça, que pode ser um golpe de loteria, que só acontece se um Golpista (Agente De Ameaça) explora por meio de sua conversa fiada (Ataque), um indivíduo ingênuo e que precisa urgentemente de dinheiro (Vulnerabilidade).

CONTROLES DE SEGURANÇA

Um conjunto de controles de segurança faz parte da estratégia de segurança e pode ser composto por processos, como a Gestão De Identidades e Acessos que envolve o gerenciamento de contas e senhas dos usuários e se trata de um controle essencial, principalmente porque muitos incidentes de segurança visam à obtenção das credenciais de acesso dos usuários. Um outro controle de segurança recomendado seria o tradicional Antivírus, que pode ser aplicado em servidores e nos dispositivos dos usuários. Um exemplo de controle de segurança processual seria a Conscientização De Segurança e Privacidade realizada na admissão de funcionários.

TIPOS DE DADOS

Ataques podem ser realizados para que dados pessoais sejam vazados e a privacidade seja comprometida, bem como podem ocorrer com os Dados Em Processamento (DIU), Dados Em Transmissão (DIM) ou Dados Armazenados (DAR). Ataques a banco de dados visam aos dados armazenados, enquanto ataques à rede visam aos dados em transmissão. Dados em processamento tem a tendência de sofrer ataques muito mais sofisticados.

CONTROLES DE SEGURANÇA E PROTEÇÃO

Os principais controles de segurança e proteção usados atualmente são respectivamente o FIREWALL, Intrusion Detection System (IDS), Intrusion Prevention System (IDS), Autenticação e ANTIMALWARE. Vale ressaltar que o uso de diversas camadas de proteção é recomendado, pois apenas uma pode não ser suficiente para realizar o controle de segurança de forma adequada.

HISTÓRIA DA CRIPTOGRAFIA

A Criptografia é um dos principais controles de segurança da informação e tem uma história fascinante. Esta história tem início no Antigo Egito, com o uso de hieróglifos. Um dos modelos de hieróglifos eram estruturados na forma de pictogramas, que consiste em um conjunto de imagens de objetos, pessoas ou animais que funcionavam como uma palavra. Assim, a Criptografia surgiu há séculos para proteger as mensagens. Atualmente, junto de uma série de outros controles, ela é considerada um Controle De Segurança Da Informação.

ESTEGANOGRAFIA

Consiste no uso de técnicas para ocultar informações ou mensagens dentro de uma outra mensagem. A diferença entre a Criptografia e Esteganografia é que basicamente a Criptografia oculta O Significado Das Mensagens, enquanto a Esteganografia oculta a Existência Da Mensagem.

CRIPTOGRAFIA DE CHAVE PRIVADA OU SIMÉTRICA

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. O algoritmo padrão de Criptografia de chave privada é o Advanced Encryption Standard (AES).

CRIPTOGRAFIA DE CHAVE PÚBLICA OU ASSIMÉTRICA

Uma característica sobre a Criptografia de chave Privada Ou Simétrica é que ela apresenta o desafio da Troca De Chaves, porém é Rápida De Ser Executada. A Criptografia de chave Pública Ou Assimétrica é computacionalmente Mais Pesada, porém é Adequada para ser usada na Troca De Chaves.

Nessa Criptografia existem um Par De Chaves, que são usadas em conjunto para a Cifragem (Com Chave Pública) e Decifragem (Com Chave Privada).

ASSINATURA DIGITAL

Neste processo, é usado uma Chave Privada para fazer o Hash da mensagem e assim verificar integridade das mesmas. Algoritmos realizam um cálculo matemático nas mensagens e formam o seu Hash. Quem recebe a mensagem juntamente com seu Hash deve usar o Mesmo Algoritmo para calcular o Hash da Mensagem Recebida. O Hash Recebido e o Hash Calculado devem ser Iguais. Esse procedimento garante a integridade de uma mensagem.

TROCA DE CHAVES CRIPTOGRÁFICAS

O Gerenciamento Das Chaves Criptograficas é fundamental e geralmente envolvem parâmetros como o Tempo De Validade e Armazenamento. O uso em conjunto das Criptografias de Chave Pública e privada é tradicionalmente usado para a criação de um canal seguro e que por sua vez pode ser servir como ponto para a troca de chaves privadas.

SEGURANÇA DOS SISTEMAS CRIPTOGRÁFICOS

A segurança não pode ser medida somente pelo tamanho da chave, sendo necessário conhecer o algoritmo e a matemática envolvida no processo. A segurança de sistemas Criptográficos depende de uma série de fatores como Geração De Chaves, Mecanismo De Troca De Chaves, Taxa De Troca Das Chaves e Tamanho Das Chaves.

APLICAÇÕES DE CRIPTOGRAFIA

A Criptografia de chave privada e a Criptografia de chave pública têm uma série cada vez maior de aplicações. Algumas delas são a Proteção da comunicação, Proteção de dados armazenados e Proteção de transações. Um dos principais protocolos de segurança para transações é o Hyper Text Transfer Protocol Secure (HTTPS), que consiste no uso do Hyper Text Transfer Protocol (HTTP) sobre uma sessão de Secured Socket Layer (SSL) ou Transport Layer Security (TLS). Este conjunto de protocolos é utilizado para transações WEB com a criação de um túnel seguro por onde trafegam as informações. Além de garantir a confidencialidade, eles podem visar também a integridade dos dados e a autenticidade das partes. Outra aplicação importante de Criptografia para as comunicações é a Virtual Private Network (VPN).

GESTÃO E POLÍTICAS DE SEGURANÇA - UNIDADE 02

Um dos principais instrumentos para a aplicação de segurança da informação nas empresas são as Normas e FRAMEWORKS, os quais apresentam uma visão mais Abrangente das Necessidades e Implementações de segurança da informação, e devem ser seguidos, na medida do possível.

Um dos principais desafios da segurança da informação é o Tratamento Dos Variados Riscos, que englobam aspectos de Pessoas, Processos e Tecnologias.

CYBERSECURITY FRAMEWORK

O CYBERSECURITY FRAMEWORK do NIST organiza Diferentes Elementos da segurança da informação, focando no Uso De Direcionadores De Negócios para guiar atividades de segurança, considerando os riscos de segurança da informação. Faz a Ponte entre o nível Executivo com o Operacional e provê uma taxonomia e determinados mecanismos para as empresas alcançarem variados objetivos de segurança da informação. O nível Executivo tem Foco Nos Riscos Organizacionais, enquanto o nível de Negócios e Processos faz o Gerenciamento Dos Riscos Do Ambiente, com o nível de Implementação e Operações Implementando a Segurança. As três partes do CYBERSECURITY FRAMEWORK são Núcleo, Camadas De Implementação e Perfis.

CIS CONTROLS

O CIS Controls funciona como um Conjunto Priorizado De Ações que, de uma forma integrada, estabelecem a Defesa Em Camadas para Mitigar Os Ataques Mais Comuns contra sistemas e redes. Com objetivo de Melhorar O Estado De Segurança, o CIS Controls melhora a segurança e fortalece uma cultura de segurança da informação. O CIS Controls define um conjunto de seis controles considerados básicos, Inventário e Controle De Ativos De Hardware, Inventário e Controle De Ativos De SOFTWARE, Gestão De Vulnerabilidades, Uso Controlado De Privilégios Administrativos, Configuração Segura Para Hardware e SOFTWARE. Porém, considerando que estes controles podem ser difíceis de serem implementados por organizações com Recursos Limitados, a base para as priorizações são os Grupos De Implementação, que são Categorias De Avaliação Própria a partir de alguns atributos relevantes de segurança da informação. Um exemplo de classificação como IG1 são Empresas Familiares Com 10 Funcionários. Uma Organização Regional provendo um serviço poderia ser classificada como IG2. Uma Grande Corporação Com Milhares De Funcionários pode ser classificado como IG3.

FAMÍLIA ISO 27000

Quando falamos sobre segurança da informação, devemos conhecer a família de normas da ISO 27000. Estas normas abarcam ainda a Certificação De Segurança Da Informação, realizada por Auditores Líderes. A Certificação em segurança da informação pode ser concedida para uma organização que segue a norma ISO 27001, onde um Auditor Líder faz a auditoria de certificação.

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

O SGSI é um elemento fundamental para o fortalecimento da cultura de segurança da informação das organizações. E você pode, uma vez estabelecido um SGSI, certificar a sua empresa na ISO 27001.

O Sistema De Gestão Da Segurança Da Informação preserva o CID das informações por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados. O SGSI deve ser criado de acordo com as características específicas de cada empresa. Como estes fatores evoluem com o tempo, é preciso Estabelecer, Implementar, Manter e Melhorar continuamente um SGSI dentro do contexto da empresa

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A LGPD é uma lei que entrou em vigor no Brasil em setembro de 2020, visando proteger os direitos fundamentais de privacidade dos cidadãos brasileiros. A 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 destes dados para garantir a privacidade dos seus usuários. De acordo com a LGPD, os dados pessoais podem ser coletados Mediante FINALIDADE e Base Legal. O titular dos dados pessoais tem direitos, e a empresa que faz o tratamento dos dados pessoais passa a ser a responsável pelos dados pessoais coletados. E essa responsabilidade envolve a proteção, já que qualquer uso irregular, incluindo o seu vazamento, afeta diretamente a privacidade do detentor dos dados. As empresas devem, assim, implementar controles de segurança da informação para evitar incidentes de segurança. A LGPD também estabelece Sanções Para Quaisquer Organizações, sejam elas grandes ou pequenas empresas, Que Não Cumpram Os Requisitos Estabelecidos, envolvendo a transparência nas relações com as pessoas, e vazamentos de dados pessoais, que comprometem a privacidade das pessoas. Essas sanções vão desde Multas, com valores que podem chegar a 50 Milhões De Reais até a Proibição Do Exercicio Das Atividades.

MARCO CIVIL DA INTERNET

O Marco Civil da Internet é a lei que regula o uso da internet no Brasil por meio da previsão de Princípios, Garantias, Direitos e Deveres para quem usa a rede bem como da determinação de diretrizes para a atuação do Estado. O Marco Civil da Internet trata de temas como Neutralidade Da Rede, Privacidade e Retenção De Dados, além de impor Obrigações De Responsabilidade Civil aos Usuários e Provedores. Trata, ainda, da confidencialidade das comunicações privadas, e dá especial atenção aos Dados De Registros De Acesso.

LEI CAROLINA DIECKMANN

A Lei Carolina Dieckmann altera o código penal brasileiro, tornando crime a Invasão De Aparelhos Eletrônicos para obtenção de Dados Particulares, além da Interrupção De Serviço Telemático Ou De Informática de utilidade pública.

CULTURA DE SEGURANÇA

Toda empresa tem a sua própria cultura de segurança e privacidade. Com objetivo de que esta cultura seja fortalecida constantemente, principalmente porque cada vez mais a segurança da informação influencia na resiliência das empresas. O grande desafio é que, como toda cultura, a de segurança e privacidade se torna mais forte com ações da empresa que engajem Todas As Pessoas, dos funcionários aos fornecedores. Um exemplo da influência da cultura de segurança e privacidade no comportamento das pessoas é o caso em que um PENDRIVE USB é encontrado no estacionamento da empresa. O que um funcionário que encontrasse o pendrive faria? Será que ele reportaria o achado como um incidente de segurança? Ou ele inseriria o dispositivo em seu computador para ver o seu conteúdo? Ele sabe que pendrives são um dos vetores de contaminação por Malwares perigosos? Como ele poderia saber que não ele não pode inserir um pendrive em equipamentos da empresa? Vale destacar que a segurança da informação é feita em camadas, com um conjunto de controles de segurança utilizados de uma forma integrada. No caso do pendrive, a principal camada de segurança poderia ser a conscientização dos usuários, com o intuito de prover aos usuários o conhecimento sobre os perigos do uso de dispositivos não autorizados. A crença do perigo real que um pendrive inserido em equipamentos da empresa deve ser incorporada no dia a dia da empresa em um processo de treinamento e conscientização.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Um dos elementos primordiais para fortalecer uma cultura de segurança e privacidade é conhecidada como Política De Segurança Da Informação e Privacidade. Com a definição formal de como a empresa Enxerga e Trata a segurança e privacidade. O que constrói Crença, Conhecimento e Hábitos Necessários fazer com que as definições da política de segurança cheguem a Todos. O que reforça esta crença é a Participação Ativa Da Alta Administração. Um passo importante para o sucesso da política de segurança e privacidade é que ela reflita, da melhor forma possível, as Características De Cada Empresa. Ela deve ser plausível e deve ser aplicável, ou seja, a política deve definir as diretrizes a serem seguidas por todos, e deve definir controles de segurança que deverão ser efetivamente implementados. Políticas de segurança são compostas por documentos que incluem Normas, Diretrizes, Processos, Procedimentos, Termos e Guias. Assim, um fator crítico de sucesso da política de segurança da informação é a Organização De Todo o Seu Conteúdo de modo a tornar mais fácio o seu acesso. A política de segurança e privacidade deve estar Disponível e ser Constantemente Atualizada e Comunicada para Todos Os Envolvidos. A falta de comunicação e de atualização faz com que a percepção seja de que a segurança e privacidade não são tão importantes para a empresa. O reflexo desta percepção é direto e negativo, fazendo com que todos relaxem quanto às suas próprias atitudes, já que percebem que a própria empresa não cuida da segurança e privacidade como deveria.

TERMO OU CONTRATO DE CONFIDENCIALIDADE

O termo ou contrato de confidencialidade, é essencial principalmente nas relações de negócios que existem entre Diferentes Organizações. O termo ou contrato de confidencialidade, geralmente é utilizado quando há Troca De Informações, como em prestação de serviços ou consultorias. Ele garante que há o acesso a informações importantes para a realização da atividade, porém Todo o Conteúdo Deve Ser Preservado e ser Restrito Somente à Execução Das Atividades, não podendo ser utilizado posteriormente, e nem Divulgado Para Terceiros. Importante destacar que os termos e contratos, como os de ciência ou de confidencialidade, são importantes para deixar explícito os objetivos e as preocupações com a segurança e privacidade, constituindo instrumentos importantes para as operações de segurança da informação. Eles têm Valor Legal, sendo essenciais principalmente após um incidente de segurança como um vazamento de informações, que pode estar infringindo o contrato.

SEGURANÇA DA INFORMAÇÃO NO DESENVOLVIMENTO DE SISTEMAS

Independente do modelo de criação de SOFTWARES, seja Desenvolvimento Próprio ou Contratação De Desenvolvimento, é preciso a adoção do ciclo de desenvolvimento seguro, que define Como a Empresa Adquire Ou Desenvolve SOFTWARES De Uma Forma Segura. A diferença entre as duas abordagens é que no caso da Contratação De Desenvolvimento, se deve negociar com a empresa contratada para desenvolver o sistema, as Responsabilidades em cada etapa do desenvolvimento, deixando tudo claro em contrato.

AMBIENTE DE DESENVOLVIMENTO SEGURO

Para o desenvolvimento de SOFTWARE, se deve levar em consideração alguns aspectos importantes. Um deles é o uso de dados para Testes De SOFTWARE. A segurança dos dados utilizados para homologação de sistemas sempre foi uma preocupação, de modo que em muitos casos dados reais são Compilados ou uma Base De Dados De Testes é criada especialmente para o desenvolvimento. Normalmente isso é feito porque há a preocupação do compartilhamento de dados sensíveis para toda a equipe, e também devido a possibilidade de vazamento de dados a partir do ambiente de desenvolvimento. Outro fator importante é o uso de dados pessoais, que devem ser protegidos de acordo com a Lei Geral de Proteção de Dados Pessoais, o que influencia primeiramente no seu uso durante o desenvolvimento, e também impacta fortemente para a segurança, já que em caso de vazamento decorrente de um incidente de segurança, existem sanções previstas na lei. Assim, as empresas devem desenvolver SOFTWARES que não sejam a Fonte De Vazamento de dados pessoais, Seja Na Própria Empresa ou Nos Clientes que usam o SOFTWARE da empresa. Em caso de incidente de segurança, há a responsabilização legal e também a CORRESPONSABILIDADE caso um vazamento ocorra em uma empresa e o seu SOFTWARE seja a fonte do incidente. O ciclo de vida de desenvolvimento seguro envolve elementos de segurança desde o Princípio Do Desenvolvimento, incluindo o Treinamento De Segurança, Estabelecimento De Requisitos De Segurança, Criação De Pontos De Qualidade e Avaliação De Riscos De Segurança E Privacidade.

TENDÊNCIAS E FUTURO

Segurança da informação é uma das áreas mais dinâmicas, com uma evolução que acompanha a forma como o mundo é moldado. A informação sempre precisou ser protegida e com a digitalização, o desafio aumentou. É necessário estar atento para entender os avanços que são introduzidos na sociedade e que tratam fundamentalmente da informação, o que por sua vez leva à necessidade de segurança e privacidade. Algumas destas tendências em andamento e que estão moldando o futuro são a Transformação Digital, e As Novas Tecnologias Emergentes. Assim como há a evolução observada com a transformação digital e as novas tecnologias emergentes, a área de segurança da informação e privacidade também continua a avançar a passos largos. Algumas tendências nessa área são Segurança Em Nuvem, Confiança Algorítmica e Segurança Cognitiva. O futuro também nos mostra as ameaças emergentes, que deverão ser tratadas. Uma evolução natural das ameaças seria o uso de ataques com ideais Políticos e Militares, como um instrumento de instabilidade. Assim, se antes os incidentes de segurança afetavam as pessoas e as empresas, agora os alvos são Cidades, Países, Infraestruturas Críticas, Fábricas e Pessoas. Os impactos estão cada vez mais críticos. Além disso, os Malwares estão cada vez mais avançados, como no caso dos Ransomwares que continuam a fazer cada vez mais vítimas, e deixaram de apenas Cifrar os dados, realizando também o Vazamento, o que amplia muito os impactos envolvidos, deixando de ser somente a Disponibilidade, envolvendo agora também a Confidencialidade. Os avanços tecnológicos também são utilizados pelos criminosos, e o uso da Inteligência Artificial para os ataques cibernéticos, por exemplo, estão em curso. Isto, por um lado, possibilita uma Automatização Dos Ataques, e do outro lado, reforça a Assertividade Dos Ataques Direcionados.

DOS DADOS AO CONHECIMENTO

Os dados são registros que servem como Base para a construção da informação e conhecimento, por meio da Análise, Manipulação e Processamento de dados. A Informação é a estruturação e organização de dados, ou seja, ela é o resultado da Aplicação De Contexto Aos Dados, necessário para compreender determinado assunto em específico. O objetivo da informação é de Esclarecer e Reduzir Incertezas, a fim de Levar Ao Conhecimento e Sabedoria. Já o Conhecimento consiste na Informação Processada e Transformada. Também é resultado de aprendizagem que ocorre quando somos expostos a diversas informações novas, que alteram nosso comportamento e relacionamento com o que está a nossa volta. Em outras palavras, a Informação são os Dados Processados sobre algo ou alguém, e o Conhecimento consiste no conjunto de Informações úteis que foram adquiridas por meio de aprendizados.

DIFERENTES DADOS PESSOAIS E DADOS CONFIDENCIAIS

A Lei Geral de Proteção de Dados Pessoais, visa proteger os Dados Pessoais. Segundo a LGPD, Dado Pessoal é a Informação Relacionada a Pessoa Natural Identificada Ou Identificável.

Um outro tipo de dado importante definido na LGPD e que requer um nível de proteção maior é o Dado Pessoal Sensível, que é o Dado Pessoal sobre Origem Racial Ou Étnica, Convicção Religiosa, Opinião Política, Filiação a Sindicato Ou a Organização De Caráter Religioso, Filosófico Ou Político, Dado Referente à Saúde Ou à Vida Sexual, Dado Genético Ou Biométrico, quando vinculado a uma pessoa. O Dado Sensível é aquele Que Discrimina Uma Pessoa Ou Indivíduo e pode ser usado contra ela ou contra a sua reputação. Dados Pessoais, dizem respeito ao Indivíduo e Dados Confidenciais, envolvem também as Empresas. Uma Informação Confidencial é aquela que, se divulgada tem um Impacto Significativo nas operações ou nos objetivos da empresa. Portanto pode ser acessada somente por um grupo de pessoas.

DEVEMOS PROTEGER OS DADOS EM TODOS OS SEUS ESTADOS

Os dados existem em diferentes estados. Quando um dado está em Processamento, existe uma aplicação realizando as operações nos dados. Já quando um dado está em Transmissão, existe um rede envolvida. E quando um dado está Armazenado, existe um banco de dados ou um servidor de arquivos. Você deve conhecer estas possibilidades de existência dos dados, em seus diferentes estados para definir e implementar os controles de segurança mais adequados, de acordo com uma visão de riscos. Considere que um agente de ameaça sempre chega aos dados, que estão em um ativo físico ou lógico. Os Controles De Segurança podem ser aplicados nos tanto nos Dados, quanto nos Ativos Físicos Ou Lógicos. Os Acessos aos ativos podem ser Controlados com Mecanismos De Controle De Acesso, que envolvem Identificação, Autenticação e Autorização. Um Banco De Dados é um exemplo de ativo que gerencia os dados. O controle de acesso faz com que os dados sejam acessados somente por Usuários Legítimos. Porém, em caso de Vulnerabilidades no banco de dados, ou de qualquer outro componente que faz parte do sistema, o Agente De Ameaça pode acessar indevidamente os dados. Neste caso, é importante fazer o uso de Controles De Segurança como a Criptografia, que protege a Confidencialidade dos dados, tornando o sistema mais seguro.

MASCARAMENTO, ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Na Payment Card Industry Data Security Standard, o Mascaramento é um método para Ocultar um segmento de dados ao ser exibido ou impresso. Já o Truncamento é um método que Remove Permanentemente um segmento dos dados no armazenamento. Caso haja o Armazenamento, há o Truncamento ao invés do Mascaramento, que é utilizado apenas na sua exibição ou impressão. No atendimento aos clientes dos bancos emissores, em que há o acesso dos atendentes aos dados, os riscos envolvidos podem ser reduzidos com o uso de mascaramento. O atendente pode realizar as operações utilizando os dados com mascaramento, o que limita a possibilidade de vazamentos e posterior uso indevido dos cartões. Como no Truncamento usado no armazenamento a remoção é Permanente, as substituições podem ser feitas de uma forma mais Geral, Sem Indicar o Número De Algarismos Substituídos.

ORIGINAL - 1234 1234 1234 1234

MASCARAMENTO - 1234 12XX XXXX 32

TRUNCAMENTO - 1234 12 - 34

Outra técnica de proteção de dados é o uso da Anonimização. Segundo a Lei Geral de Proteção de Dados Pessoais, a anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado Perde a Possibilidade De Associação a um indivíduo. A Pseudonimização é tratada pela lei como o tratamento por meio do qual um dado Perde a Possibilidade De Associação a um indivíduo, Senão pelo uso de Informação Adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Uma forma simples é que no caso da Anonimização o processo inverso, ou seja, o Retorno Ao Dado Original Não é Possível, enquanto no caso da Pseudonimização é possível retornar ao dado original com o uso de uma informação adicional. Por exemplo, José, Paulo, Maria e Rita podem ser Anonimizados, como XXXX. Já no caso de serem Pseudonimizados, eles são identificados como sendo respectivamente, N1, N2, N3 e N4. No caso do uso da Anonimização, são armazenados os dados referentes ao nome anonimizado e os demais dados necessários. Qualquer necessidade de uso destes dados não possibilita o processo reverso de Identificar o Titular Dos Dados. A empresa que adota esta técnica não pode trabalhar com dados Individualizados. No caso do uso da Pseudonimização, são armazenados os dados referentes ao nome pseudonimizado e os demais dados necessários. Além disso, há uma Outra Base com informações de Nome e Nome Pseudonimizado, que Permite A Reversão e a Identificação Do Indivíduo. Essa base adicional deve ser mantida Separadamente pela empresa em ambiente Controlado e Seguro.

CLASSIFICAÇÃO DA INFORMAÇÃO

A informação deve ser classificada levando em cosideração diversos aspectos e deve prezar por evitar Modificações ou Divulgações não autorizadas. Um exemplo de esquema de classificação da informação define quatro níveis sendo respectivamente informações Públicas, Internas, Confidenciais e Sigilosas. Os resultados da classificação devem ser Atualizados de acordo com as Mudanças ao longo do seu ciclo de vida. Uma informação pode deixar de ser Sensível ou Crítica após certo período de tempo. A classificação envolve também o uso de Rótulos, considerando informações em formato Físico Ou Digital. A Rotulagem da informação é requisito essêncial para Acordos De Compartilhamento De Informações e deve ser conhecido por Todos Os Colaboradores. Há casos em que se pode dispensar a rotulagem, como em Informações Públicas. Um ponto a ser considerado também é que ativos rotulados são Mais Fáceis De Identificar e Selecionar Para Roubos em caso de ataques.

CICLO DE VIDA E TRATAMENTO DOS DADOS

Um dado possui um ciclo de vida da criação à destruição e envolve os seguintes passos, Criação, Armazenamento, Uso, Compartilhamento, Arquivamento e Destruição. A LGPD define o tratamento de dados como Toda Operação Realizada Com Dados Pessoais.

SEGURANÇA DE DADOS NA NUVEM

O uso de um provedor de nuvem envolve o Provisionamento, Migração e Desprovisionamento. Os dados Não Podem ser acessados indevidamente em nenhum momento pelo provedor de nuvem. Você deve exigir, como cliente, que os provedores façam a Proteção Dos Dados Armazenados em Diferentes Níveis. Os dados estão sob responsabilidade do provedor, existem no Centro De Dados e também em Mídias. Há o Acesso Físico aos servidores e às mídias e um incidente de segurança pode ser decorrente de um atividade maliciosa. Dessa forma, os controles de segurança básicos dos provedores de nuvem são o Controle De Acesso Físico, uso de técnicas como a Ofuscação para tornar a identificação de dados mais difícil e o uso de Criptografia diretamente na mídia física. Outro ponto importante envolvido com o uso de provedores de nuvem é quanto à Eliminação e Destruição Dos Dados. Quando uma empresa utiliza um provedor de nuvem, a Sanitização De Dados deve ser Exigida. A Sanitização, Destruição Ou Eliminação De Dados do provedor de nuvem deve garantir que após o fim do contrato e o Desprovisionamento, os dados não permaneçam com o provedor. Além disso, os dados em Mídias Físicas também devem se descartados adequadamente, pois podem resultar em acesso indevido aos dados. Há o exemplo da Destruição da mídia física em casos mais críticos, em que é feitio um processo de Desmagnetização ou mesmo a Destruição Física.

NAVEGAÇÃO EM DADOS COM CRIPTOGRAFIA

O uso de Criptografia para proteger os dados é importante. Porém, é preciso considerar uma série de elementos que fazem com que o nível de segurança seja corretamente avaliado. Os dois principais elementos são a Chave Criptográfica para decifrar os dados e a Possibilidade De Vulnerabilidades em ativos relacionados que dão Acesso a estas chaves. Os Dados Em Trânsito são tradicionalmente protegidos com o HTTPS, que é baseado em Criptografia. No HTTPS, as chaves Criptográficas são geradas Dinamicamente, para cada sessão. No caso dos Dados Armazenados, há diferentes possibilidades de uso da Criptografia. Os dados armazenados em um banco de dados passam do Usuário para uma Aplicação, que se conecta ao Banco De Dados. Nesse caso existem três pontos que podem gerenciar a Criptografia e as suas chaves Criptográficas Usuário, Aplicação e Banco De Dados. Você pode desenvolver uma aplicação em que a Criptografia é feita, e a chave Criptográfica é definida pelo Próprio Usuário. Assim, no caso de o usuário Esquecer Ou Perder Esta Chave, os Dados Também São Perdidos. Os dados só podem ser acessados pelo próprio usuário de modo que nem a empresa, nem o provedor de nuvem possui o acesso aos dados em claro. O desafio é o Gerenciamento De Chaves, e o que se deve evitar ao máximo é Armazenar a Chave Criptográfica na Própria Aplicação, pois isso facilita o acesso indevido aos dados.

Outra possibilidade é o uso de Criptografia do Banco De Dados, de modo que todos os dados são Gerenciados e Cifrados pelo sistema de banco de dados. Um outro tipo de Criptografia, a Homomórfica, pode tratar, Ao Mesmo Tempo, da proteção de dados Em Trasmissão, Procesamento e Armazenados. Por meio de Operações Matemáticas diretas nos dados cifrados, a Criptografia Homomórfica faz com que os dados permaneçam Cifrados Mesmo Enquanto São Manipulados.

SEGURANÇA NA INTERNET - UNIDADE 03

A segurança e privacidade na internet passam pelo entendimento de diferentes elementos que envolvem o que deve ser protegido e os componentes ou ativos de um ambiente que podem ser explorados em ataques. As transações WEB partem dos usuários que usam seus dispositivos a partir de algum local em que há uma conexão com a internet e passam por variados componentes até chegar ao seus destino. Neste caminho, os agentes de ameaça estão à espreita em busca de oportunidades para roubar os Dados Pessoais, Dados Das Transações Ou Identidades Digitais. Portanto o agente de ameaça busca oportunidades em Três Ambientes, No Ambiente Do Usuário, No Ambiente De Internet e No Ambiente Dos Provedores De Serviços.

SEGURANÇA EM TRANSAÇÕES WEB

Uma transação WEB pode ser uma Compra Online, uma Transação Bancária, a Realização De Algum Serviço Governamental ou até mesmo uma Postagem Em Uma Rede Social e podem envolver diferentes tipos de dados ou informações como Dados Pessoais, Dados Financeiros Ou Dados Confidenciais, que podem sofrer Modificações, Vazamentos Ou Destruições. Os dados e as informações existem em seus três estados, Processamento, Transmissão e Armazenados podendo sofrer ataques em qualquer ponto de um dos três ambientes. No Ambiente Do Usuário, as transações WEB exigem segurança porque Malwares podem capturar e modificar dados a partir da Origem No Próprio Usuário. Neste caso, a transação chega ao provedor de serviços, como um banco, de forma fraudulenta, seja pela modificação da transação ou pelo furto de identidade. O provedor de serviços, assim, além de ter de proteger o seu próprio ambiente tem o desafio de receber uma transação vindo de um criminoso, que furtou a identidade do usuário verdadeiro. No Ambiente De Internet, em que o agente de ameaça pode capturar ou modificar as transações WEB, é importante que elas sejam realizadas com o uso de um Canal Seguro, que deve ser provido pelo Provedor De Serviços. As conexões WEB podem ser protegidas com o uso de protocolos de segurança como o HTTPS. Já no ambiente do Provedor De Serviços, como no caso de bancos, o ambiente pode ser atacado em Qualquer Um Dos Componentes, incluindo as aplicações, os servidores de aplicação, os sistemas operacionais, as máquinas virtuais e os bancos de dados. Toda a estratégia de Segurança Da Informação Corporativa deve ser seguida pelos provedores de serviços. Muito importante que o profissional de segurança e privacidade considere que os ataques podem ter Origem Externa Ou Interna.

GOLPES NA INTERNET

Os golpes na internet visam explorar os usuários, com uso de técnicas de Engenharia Social que levam à instalação de Malwares, ao direcionamento para Sites Falsos e ao Envio De Dados Sensíveis Para Criminosos. O resultado é um conjunto de atividades maliciosas que incluem o furto de identidades para criação de contas fraudulentas em serviços online e bancos, a realização de transações ilegais, o envio de mensagens falsas, o acesso a serviços variados por terceiros, entre outras atividades possíveis a partir das credenciais das vítimas ou dados sensíveis. Alguns dos principais golpes aplicados na internet são Furto De Identidade, Fraude De Antecipação De Recursos, PHISHING Ou Scam, PHARMING, Golpes De Comércio Eletrônico e Hoax. Uma fonte de informações sobre fraudes e outros perigos que existem na na internet é o Catálogo De Fraudes Da RNP que alerta a comunidade sobre os Principais Golpes Em Circulação Na Internet. As principais ações para a proteção contra esses golpes são a notificação para a organização envolvida a fim de se tomar as medidas cabíveis e a busca constante de informação sobre o assunto.

PRIVACIDADE NA WEB

A privacidade na WEB possui visões a serem consideradas. De um lado, há o rastreamento do que as pessoas fazem na WEB, como os COOKIES. Do outro lado, existe a Divulgação Espontânea de informações pessoais em Redes Sociais, que podem resultar em crimes que transcendem o digital e podem afetar diretamente as pessoas com fraudes e crimes diversos. Com a Lei Geral De Proteção De Dados Pessoais, todos devem preservar a privacidade e a proteção de dados pessoais. De uma forma geral, um usuário, ao acessar determinado site, deve saber que um COOKIE está ativo e deve Aceitar o seu uso. No momento de Inserir Dados Pessoais, o usuário deve ter acesso a um Aviso De Privacidade, que diz Quais Dados, a Objetivo Da Coleta e a Forma Como Eles Serão Protegidos. Após o aceite do usuário, a empresa deve proteger os dados coletados para evitar vazamentos.

PROTEÇÃO PARA DISPOSITIVOS MÓVEIS

Um Dispositivo Móvel é um dispositivo computacional Portátil que possui um Formato Pequeno e que pode ser Carregado por um indivíduo, sendo construído para operar Sem Uma Conexão Física, com Armazenamento De Dados Local Não Removível e que funciona por um certo período de tempo com uma Fonte De Energia Própria. Pode incluir capacidades de comunicação por voz e sensores que possibilitam a captura de informação e tem a capacidade de sincronização com locais remotos. As principais características de dispositivos móveis são Portabilidade, Comunicação Sem Fio, Armazenamento Local e Funcionamento Por Bateria. Essas características influenciam diretamente nos aspectos de segurança e privacidade, devido ao aumento dos Perímetros Das Empresas, que se Expandem com o uso dos dispositivos móveis. Os principais componentes dos dispositivos móveis são o Hardware, Firmware, Sistema Operacional e Aplicação. Cada um destes componentes representa pontos que podem ser atacados.

AMEAÇAS E SEGURANÇA EM DISPOSITIVOS MÓVEIS

Os principais Riscos envolvidos com o uso de dispositivos móveis no mundo são o Comprometimento Da Privacidade do Usuário ou dos Dados Sensíveis da empresa. Instalação De Aplicativos Vulneráveis a partir de Fontes Não Oficiais, aumentando a chance de Inserção De Vulnerabilidades no ambiente. Instalação De Malwares a partir de Fontes Não Oficiais, que podem vir Junto De Aplicativos Falsificados ou Cavalos De Troia. E a Interceptação De Tráfego a partir de Conexões Não Confiáveis, que pode resultar em Vazamento De Dados e Furto De Identidades. As ameaças existentes no mundo móvel são muito similares às de outros ambientes, apesar de algumas especificidades. Os níveis de risco das empresas mudam, pelas próprias características dos dispositivos móveis, que Aumentam A Superfície De Ataque ao ampliar os parâmetros da empresa, que passam a ser Mais Distribuídos. Os Dados Corporativos passam a existir Fora Dos Servidores Da Empresa e há a Mistura Com Os Dados Pessoais que podem comprometer a privacidade dos usuários. O Enterprise Mobility Management Ou Mobile Device Management (EMM) (MDM) é um dos principais controles de segurança para dispositivos móveis. Por meio de um Agente Instalado No Dispositivo existe o Provisionamento Dos Perfis de configuração para os dispositivos. O agente no dispositivo pode Enviar Notificações em caso de Configurações Não Conformes Com a Política Da Empresa, e pode Corrigir Automaticamente configurações desta natureza.

ATAQUES E DEFESAS EM DISPOSITIVOS MÓVEIS

Os ataques relacionados a ambientes móveis envolvem Todos os aspectos de segurança da informação. O agente de ameaça pode explorar o Lado Do Usuário, por meio do PHISHING, permitindo Explorar o Dispositivo Móvel ou ainda uma aplicação. Pode ainda explorar a Comunicação, atacando o Provedor De Internet ou ainda atacar a Empresa, explorando Vulnerabilidades No Ambiente formado por Sistemas, Serviços e Plataformas, adicionalmente aos Funcionários e Processos da empresa. Existe a necessidade de Configuração Segura dos dispositivos e o provisionamento das Políticas Corporativas De Gerenciamento Dos Dispositivos Para A Defesa. Isto pode ser feito com o Enterprise Mobility Management Ou Mobile Device Management e também por meio da Proteção Dos Dados Armazenados No Dispositivo Móvel, do Gerenciamento Centralizado Para Aplicar Políticas E Configurações Aos Dispositivos, da Avaliação Da Segurança Das Aplicações Móveis, da Proteção Contra O Acesso Indevido Aos Dados Do Dispositivo Móvel, de Configurações De Privacidade Para Proteger Os Dados Dos Usuários e da Proteção Contra Tentativas De PHISHING.

ATAQUES DE CAMADAS DE APLICAÇÕES E ANTIVÍRUS

A Camada De Aplicação de um dispositivo móvel é uma das que podem ser atacadas pelos agentes de ameaça. Ataques na Camada De Aplicação em dispositivos móveis exploram as Vulnerabilidades Técnicas de Aplicativos Instalados Pelo Usuário.

As maiores vulnerabilidades em aplicativos móveis são Uso Impróprio De Plataforma, Armazenamento Inseguro De Dados, Comunicação Insegura, Autenticação Insegura, Criptografia Insuficiente, Autorização Insegura, Qualidade De Código Ruim, Modificação De Código, Engenharia Reversa e Funcionalidade Exposta. Os Antivírus para dispositivos móveis devem ser Considerados uma Camada De Proteção, Não podendo ser considerado uma Solução para os problemas de segurança e privacidade. Muitos Antivírus fazem a detecção de MALWARES com base em Assinaturas, o que significa que somente aqueles Conhecidos Poderão Ser Detectados. Novas ameaças são Detectadas Com Dificuldades pelos Antivírus e Outros Mecanismos devem ser utilizados pela empresa para Complementar a Proteção.

ENGENHARIA SOCIAL

A Engenharia Social explora a Atenção, Curiosidade, Caridade, Medo Ou Possibilidade De Obtenção De Vantagem Financeira. O criminoso se passa por um Banco, Empresa Ou Site Popular. Envolve a Possibilidade de inscrição em Serviços De Proteção De Crédito, ou o Cancelamento De Cadastro, Conta Bancária ou Cartão De Crédito, e Leva a Vítima a Páginas Falsas em que entregam suas Credenciais, Senhas Ou Informações Sensíveis.

ANÁLISE DE VULNERABILIDADE E PENTEST

O Risco é a Probabilidade de um Agente De Ameaça Explorar Vulnerabilidades de ativos utilizando alguma Técnica De Ataque, o que faz com que uma ameaça se torne um Incidente De Segurança, causando impactos à empresa. Uma das principais formas de reduzir os riscos das empresas é o Tratamento Das Vulnerabilidades, para que elas não possam ser exploradas.

GESTÃO DE VULNERABILIDADES

As vulnerabilidades têm natureza complexa, já que são descobertas o tempo todo, surgem e são criadas em uma velocidade ainda maior. Com os ambientes mudando o tempo todo e com uso e integração de diferentes tecnologias, há sempre novas vulnerabilidades a serem descobertas. Assim, é importante que as elas sejam tratadas por um Processo De Gestão De Vulnerabilidades que organiza as ações para a Descoberta Das Inúmeras Vulnerabilidades em diferentes ativos. A gestão de vulnerabilidades engloba os seguintes processos Descoberta, Priorização De Ativos, Avaliação, Relatório, Remediação e Verificação. A identificação é o início dos trabalhos para proteger as empresas e pode ser feita de diferentes formas. Uma vez descoberta e validadas as vulnerabilidades, elas devem ser tratadas com os Controles De Segurança. Os controles de segurança a serem aplicados na remediação das vulnerabilidades podem ser dos tipos Físico, Tecnológico Ou Processual.

TESTES DE SEGURANÇA

Teste De Segurança é o processo de Comparar o Estado De Um Sistema Ou Aplicação De Acordo Com Um Conjunto De Critérios.

Eles podem ser feitos no Final Do Desenvolvimento ou fazer parte do Ciclo De Desenvolvimento Desde o Início, Com a implementação de Requisitos e Testes De Segurança Automatizados. É preciso ter a mentalidade correta para os testes de segurança. Testes De Segurança requerem um Pensamento Fora Do Padrão. Casos de uso Normais testarão o comportamento Normal da aplicação em que o usuário está utilizando as funções da forma como é esperado. Em testes de segurança, é preciso ir além das expectativas tradicionais e ter um Pensamento De Atacante. Um teste de segurança é estruturado tipicamente com as seguintes fases Preparação, Obtenção De Informações, Mapeamento, Exploração e Relatório. Fazer um teste de segurança Superficial considerando ele Completo é tão Crítico quanto não fazer Teste Algum, pela Falsa Sensação de segurança gerada. É importante que as vulnerabilidades encontradas sejam Validadas, já que as Falhas Não Encontradas São Fatais e as Falhas Apontadas, mas Que Não Existem tiram a Credibilidade Dos Resultados como um todo.

ANÁLISE DE VULNERABILIDADES

A análise de vulnerabilidades compreende a busca por vulnerabilidades nos ativos de uma forma Manual ou com o uso de Ferramentas Automatizadas. Os tipos de análise de vulnerabilidades são as Análises Estáticas e Dinâmicas. A Análise Estática (SAST) envolve a análise dos componentes do sistema Sem A Sua Execução, pela análise Manual ou Automatizada do Código Fonte. A análise Manual possibilita a Identificação De Vulnerabilidades especialmente quando o código é Tecnicamente Seguro, mas com Falhas Na Lógica, que São Difíceis de serem Detectados por Ferramentas Automatizadas. Já a Análise Automatizada é feita com Ferramentas que checam o Código Fonte por Conformidade com um Conjunto Definido De Regras ou melhores práticas da indústria. A Análise Dinâmica (DAST) envolve a análise do sistema Durante a Sua Execução, em tempo real, de forma Manual ou Automatizada. Normalmente, a Análise Dinâmica Não Provê as Informações que a Análise Estática provê. Ela detecta elementos com Ponto De Vista Do Usuário. Os resultados são referentes a problemas de Confidencialidade No Trânsito, De Autenticação e Autorização, Além De Erros De Configuração Do Servidor.

PENTEST

Os Testes De Penetração ou Pentests são também conhecidos como testes de Intrusão e ETHICAL HACKING e são realizados a partir do Ambiente Externo. Os objetivos são determinar Se e Como um Agente De Ameaça pode obter um Acesso Não Autorizado A Ativos que afetam um ambiente, e confirmar se os controles requeridos estão implementados. Envolve ainda Identificar Meios de Explorar Vulnerabilidades para Driblar Os Controles De Segurança dos componentes do sistema. Existem três tipos de Pentests.

TESTE DE CAIXA PRETA

Também conhecido como Teste Com Conhecimento Zero, já que é conduzido Sem Qualquer Informação sobre o ambiente que está sendo testado.

O objetivo é que o profissional faça o teste como se fosse um Atacante Real explorando o uso de Informações Públicas e que podem ser obtidas sem restrição por qualquer atacante. Os resultados dos testes de caixa preta podem impressionar e serem úteis para Demonstrar Como As Vulnerabilidades São Exploradas. Porém, Não são muito efetivos em tornar a aplicação mais segura.

TESTE DE CAIXA BRANCA

Também conhecido como Teste Com Conhecimento Total e é conduzido com Todo o Conhecimento sobre o ambiente. Este tipo de teste é Mais Rápido do que o Teste De Caixa Preta, porque há a Transparência e o Conhecimento que permitem a construção de casos de teste mais Sofisticados. Não simula Ataques Externos, mas simplifica a identificação de Comportamentos Suspeitos ou Anomalias Diretamente No Código.

TESTE DE CAIXA CINZA

Teste em que Alguma Informação é provida para o profissional, como uma Credencial De Acesso, enquanto Outras Informações têm de ser Descobertas. Este teste é bastante comum, devido aos Custos e Tempo De Execução.

METODOLOGIA OWASP TESTING PROJECT

A OWASP Testing Project foca em Aplicações WEB e visa a Construção De Aplicações Mais Confiáveis e Seguras. A metodologia segue as premissas de que a prática de Testar o SOFTWARE deve estar em Todo O Ciclo De Vida de desenvolvimento (SOFTWARE Development Life Cycle) (SDLC) e que uma das melhores maneiras de prevenir problemas de segurança em aplicações em produção é incluir a segurança em cada uma de suas fases.

METODOLOGIA OSSTMM

A metodologia Open Source Security Testing Methodology Manual (OSSTMM) surgiu em 2000 como um FRAMEWORK de melhores práticas. Em 2005 evoluiu para uma metodologia. Em 2006, a OSSTMM se tornou um Padrão que foca na segurança, além de poder ser utilizado para a Conformidade de acordo com um Regulamento ou Legislação específica.

METODOLOGIA PTES

A metodologia Penetration Testing Execution Standard (PTES) é composta por Sete Seções que definem as atividades a serem realizadas. De uma forma geral, as atividades são suportadas por uma Documentação Técnica Detalhada para cada uma das seções. As seções descrevem como Iniciar As Atividades, Obter Informações Para Análise, a Modelagem De Ameaças, as Análises De Vulnerabilidades, a Exploração para passar pelos controles de segurança existentes, o Pós-Exploração para manter o controle do alvo e o Relatório Final.

APLICAÇÃO DOS TESTES DE SEGURANÇA

Os Testes De Segurança são parte importante da gestão de segurança da informação e devem ser feitos por Todas As Empresas, sejam aquelas que Desenvolvem Sistemas ou aquelas que Adquirem Sistemas. A metodologia OWASP Testing Project foca na Segurança no Ciclo De Vida de desenvolvimento de SOFTWARE, com a inserção de testes de segurança em diferentes pontos do processo. O desenvolvimento seguro envolve ainda outros elementos de segurança como o Treinamento De Segurança, o Estabelecimento De Requisitos De Segurança, a Criação De Pontos De Qualidade, a Inclusão De Funções De Segurança, a Avaliação De Riscos De Segurança e Privacidade e o Plano De Resposta a Incidentes após a implantação.

FUNDAMENTOS DE AUDITORIA DE SISTEMAS - UNIDADE 04

Com a evolução constante do ambiente das empresas, junto do dinamismo dos objetivos de negócios, a auditoria é cada vez mais importante. De uma forma geral, a auditoria tem como objetivo Verificar e Validar Atividades, Processos e Sistemas, de acordo com o que está sendo estabelecido, Incluindo Aspectos Legais e Regulatórios, visando também a Eficiência e Eficácia. A auditoria visa ainda Confirmar Para a Alta Gestão da empresa que o negócio está funcionando bem e está preparado para enfrentar os Potenciais Desafios. Visa também assegurar aos Diferentes Atores Envolvidos No Negócio sobre a Estabilidade Financeira e Operacional Da Organização. Uma das principais características da auditoria é que ela só pode ser feita por Auditores, os quais são profissionais que normalmente têm certificação para exercer esta função. Outra característica é que a auditoria é Independente Das Funções Operacionais, o que permite que sejam providas Opiniões Objetivas e Sem Viés sobre a efetividade do ambiente de controle interno. Portanto, a Auditoria é uma Inspeção e Verificação Formal para checar se um Padrão Ou Conjunto De Guias está sendo Seguido, se os Registros estão Corretos e se os objetivos de Eficiência e Eficácia estão sendo Alcançados.

AUDITORIA DE SEGURANÇA E CONTROLES DE SEGURANÇA

Para a segurança e privacidade das empresas, é importante que os Processos Estejam Bem Definidos e a equipe responsável tenha as Competências para as Ações Necessárias. A governança garante que as ações do cotidiano sejam tratadas de modo que as ameaças sejam sempre tratadas e alinhadas com a Alta Gestão. Os Investimentos em Controles De Segurança são Necessários para proteger as empresas contra os ataques cibernéticos. Portanto podemos afirmar que a Segurança Da Informação E Privacidade faz parte da Estratégia das empresas, levando à necessidade de Revisão Gerencial, Avaliação De Riscos e Auditoria Dos Controles De Segurança.

AS FASES DO PROCESSO DE AUDITORIA DE SISTEMAS

O Programa De Auditoria é composto por Procedimentos e Passos específicos que serão utilizados para testar e verificar a Efetividade Dos Controles.

A qualidade do programa de auditoria possui um impacto significativo na Consistência e na Qualidade dos resultados da auditoria, de modo que os auditores devem entender como desenvolver programas de auditoria completos e abrangentes. A auditoria requer que o auditor Busque Evidências, Avalie As Forças e Fraquezas de Controles Internos com base nas evidências coletadas, e prepare um Relatório De Auditoria que apresenta as Fraquezas e Recomendações para a Remediação. As principais fases da auditoria são o Planejamento, Trabalho Em Campo e Relatórios.

PLANEJAMENTO

O Planejamento Da Auditoria é essencial para o sucesso, o Escopo e Objetivos da auditoria devem estar Claros, Entendidos e Aceitos tanto pelo Auditor quanto pelo Auditado. Uma vez que o Propósito Da Auditoria é definido, o Plano De Auditoria pode ser criado, englobando o Escopo Acordado, os Objetivos e Procedimentos necessários para a Obtenção De Evidências que sejam Relevantes, Confiáveis e Suficientes para Construir e Suportar as Conclusões Auditoria. Os Recursos Necessários podem assim ser definidos incluindo o Orçamento Necessário para o trabalho, as Localidades a serem auditadas, as Regras e Responsabilidades da Equipe De Auditoria, o Tempo determinado para Cada Estágio da auditoria, as Fontes De Informação para os testes, os Pontos De Contato para necessidades Administrativas e Logísticas e o Plano De Comunicação da auditoria. O Planejamento Da Auditoria é Finalizado com a Definição Dos Procedimentos, que envolvem a Identificação Da Documentação, dos Requisitos De Conformidade Regulatória, da Lista De Indivíduos Para As Entrevistas e dos Métodos e Ferramentas Para a Avaliação.

TRABALHO EM CAMPO E RELATÓRIOS

Após o Planejamento Da Auditoria, a Execução Dos Passos definidos com o uso dos Recursos é feita na fase de Trabalho Em Campo. Esta fase inclui Obtenção Dos Dados, Testes Dos Controles, Realização Das Descobertas e Validações e a Documentação Dos Resultados. A fase de Relatórios representa a Entrega Da Auditoria. Onde ocorre a Elaboração, Revisão, Entrega e Acompanhamento dos resultados da auditoria.

CONTROLES GERAIS DE AUDITORIA DE SISTEMAS

No contexto da segurança, os controles podem ser Físicos, Tecnológicos Ou Processuais e são aplicados nos ativos para que as Vulnerabilidades sejam tratadas. Os Controles De Segurança são Salvaguardas Aplicadas Em Sistemas para proteger a Confidencialidade, Integridade e Disponibilidade dos sistemas e para Gerenciar Os Riscos de segurança. Os Controles De Privacidade são Salvaguardas Administrativas, Técnicas e Físicas aplicadas em Sistemas E Organizações para gerenciar Riscos De Privacidade e assegurar Conformidade Com Requisitos de privacidade aplicáveis. São definidas, cinco funções da segurança que sendo elas respectivamente Identificação, Proteção, Detecção, Resposta e Recuperação.

COBIT E ITIL

O COBIT é um FRAMEWORK de Governança De TI que trata de uma Visão Organizacional, a qual tem relação com a Segurança e Privacidade. Define os Componentes para Construir e Sustentar um Sistema De Governança, composto por Processos, Estrutura Organizacional, Políticas, Procedimentos, Fluxos De Informação, Cultura, Comportamentos, Qualificações e Infraestrutura. O ITIL é um FRAMEWORK de Melhores Práticas que visa auxiliar as empresas a Entregar e Suportar Serviços De TI, provendo uma Estrutura Alinhada com a Visão, Missão, Estratégia e Objetivos Da Organização. O Gerenciamento De Continuidade De Serviços é uma das 34 práticas do ITIL e tem como objetivo Gerenciar Riscos que podem causar sérios impactos aos serviços de TI. O processo do ITIL assegura que o Provedor De Serviço De TI possa prover sempre um Nível De Serviço Mínimo, reduzindo os Riscos De Desastres para um nível Aceitável e planejando a recuperação dos serviços de TI. Os Subprocessos do Gerenciamento De Continuidade De Serviço são respectivamente o Suporte, Definir Os Serviços Para a Continuidade, Treinamento, Testes e Revisão.

CONTROLES PARA DESENVOLVIMENTO DE SISTEMAS

A complexidade envolvida com Aquisição, Desenvolvimento e Manutenção de sistemas é grande e exige um Conjunto De Controles que precisam ser auditados. Considerando a Essência da segurança, que precisa Proteger Os Ativos Contra a Exploração De Vulnerabilidades Que Resultam Em Incidentes De Segurança, a verificação da Eficiência e Eficácia dos controles de segurança e privacidade é fundamental. Existem normas que definem um Conjunto De Controles De Segurança para a Aquisição, Desenvolvimento e Manutenção de sistemas, com os seguintes controles definidos, Requisitos De Segurança De Sistemas De Informação, Segurança Em Processos De Desenvolvimento e Dados Para Teste. O objetivo de controle dos Requisitos De Segurança De Sistemas De Informação é garantir que a Segurança Da Informação seja parte integrante de Todo o Ciclo De Vida dos sistemas. O objetivo da Segurança Em Processos De Desenvolvimento é garantir que a Segurança Da Informação está Projetada e Implementada no Desenvolvimento Do Ciclo De Vida dos sistemas. O objetivo dos Dados Para Teste é assegurar a Proteção dos dados usados.

CONTROLE DE ACESSO

Os Controles De Acesso são referentes ao Gerenciamento De Contas.

CONTROLES LÓGICOS, FÍSICOS E PROCESSUAIS

Os Controles De Segurança envolvem investimentos em Pessoas, Processos e Tecnologias, principalmente para o desenvolvimento de uma Cultura De Segurança, e podem ser Administrativos, Técnicos ou Operacionais. Alguns exemplos são a Conscientização, Políticas, Registro De Eventos, Varredura De Vulnerabilidades e Classificação Da Informação.

Outra classificação utilizada é os controles de segurança e privacidade serem Lógicos Físicos ou Processuais. Os Controles Lógicos são normalmente Complementados com Controles Processuais em Meios Digitais. Controles Físicos também fazem parte da Proteção Da Informação, como no caso de Dados Em Equipamentos, que podem ser Acessados Fisicamente e Roubados. Neste caso, o Controle De Acesso Físico é essencial. Outro conjunto de Controles Físicos diz respeito à Proteção Contra Ameaças Externas e Do Meio Ambiente, como um Sistema De Supressão De Incêndios.

TÉCNICAS E FERRAMENTAS PARA AUDITORIA DE SISTEMAS

Auditorias são normalmente compostas por um conjunto de Metodologias, Técnicas e Ferramentas, que devem ser usadas para Identificar e para Levantar, Analisar e Validar Evidências. As Metodologias, Técnicas e Ferramentas devem auxiliar o auditor a Organizar e Documentar os resultados. Há técnicas para Interagir Com As Pessoas em busca das informações, que se complementam as análises Manuais e às análises Técnicas. Dentre as técnicas e ferramentas que envolvem Interação Com Pessoas, estão Entrevistas, Questionários, Pesquisas, Perguntas e Dinâmicas Em Grupo. Já a Análise Manual pode ser feita com Análise e Revisão De Documentação, Análise De Políticas, Procedimentos e Processos, Análise De Configurações, Revisões Gerenciais e Análise De Códigos.

APLICABILIDADE DAS TÉCNICAS E FERRAMENTAS

Os procedimentos, técnicas e ferramentas para auditoria de sistemas são usadas de acordo com o Objetivo e Escopo da auditoria, e são definidos no momento de Planejamento. A aplicação das técnicas e ferramentas é feita no Trabalho Em Campo e dependem da Abordagem Da Auditoria, que pode ser baseadas em FRAMEWORKS De Governança como o COBIT, Melhores Práticas como o ITIL ou o Sistema De Gestão De Segurança Da Informação. No caso da segurança da informação, a auditoria visa Assegurar que os controles protejam a empresa de uma Forma Adequada, com base na Gestão De Riscos.

PCIDSS

O Payment Card Industry Data Security Standard é um padrão de segurança de dados da Indústria De Cartões De Pagamento, que estabelece requisitos de segurança que devem ser cumpridos por Todos os estabelecimentos e empresas que Processam, Transmitem ou Armazenam dados de cartões. As empresas devem cumprir todos os Doze Requisitos de segurança definidos. Sem a conformidade com a PCIDSS, as empresas ficam sujeitas a Não Poderem mais Participar do ecossistema de cartões de pagamento, por colocar em risco os demais atores da cadeia e Prejudicar a Confiança No Sistema.