Segurança de Informações

AULA 01 (Conteúdo Slides):

Introdução à Segurança de Informações

Serviços:

Para garantir a segurança adequada dos sistemas, são necessários alguns serviços de segurança:

♣ Autenticação

♣ Autorização

♣ Confidencialidade

♣ Integridade

♣ Não-repúdio

AUTENTICAÇÃO:

Um serviço de Autenticação garante que durante uma comunicação que uma entidade é quem ela diz (reivindica) ser.

AUTORIZAÇÃO:

Um serviço de Autorização limita o acesso de um usuário legítimo a um recurso protegido.

CONFIDENCIALIDADE:

Um serviço de Confidencialidade de dados garante que as informações não serão divulgadas indevidamente.

INTEGRIDADE:

Um serviço de Integridade garante que uma informação recebida é exatamente a informação enviada por uma determinada entidade.

NÃO-REPÚDIO:

Um serviço de Não-Repúdio previne que um remetente ou um destinatário negue a transmissão de uma mensagem.

MECANISMOS DE SEGURANÇA:

O que são: Serviços de segurança definem políticas de segurança que são implementadas por mecanismos de Segurança;

Exemplos de mecanismos:

Criptografia, Assinatura Digital, Autenticação, Controle de Acesso, Etc.

Temas para estudar:

Exemplo: O que é? Quando utilizar? Quem utiliza? (Minha pesquisa, logo, minhas conclusões!)

Autenticação:

● O que é: É um método de abordagem que garante acesso às pessoas que possuem o nível ou a “chave” para que possam acessar determinados arquivos limitados por quem desenvolveu a abordagem e, de acordo com que o desenvolvedor definiu como parâmetro para separar conteúdos em níveis de acesso, os usuários poderão ter acesso ou não ao nível. Essa abordagem já fez sentido uma vez: quando os usuários acessavam os recursos da empresa através dos dispositivos e da rede da empresa única e exclusivamente; no mundo atual, entretanto, é necessário adicionar novos parâmetros devido ao uso de aplicativos web e mobile para acessar dados de uma empresa, pois, há menos controle em relação ao dispositivo e/ou à rede utilizados pelo o usuário.

● Quando utilizar:

Utiliza-se quando deseja-se criar barreiras para evitar o acesso a dados de outras pessoas. Vale ressaltar que a autenticação em si não protege os dados de todas as invasões, ela mesma atua apenas como uma barreira (mais uma arma dos desenvolvedores para combater o acesso de usuários não permitidos). Ela é fortemente utilizada em processos de registro de contas on-line como e-mails ou perfis sociais, também é utilizada dentro de softwares de sistemas de empresas que podem conceder acesso virtual ou físico como travas de portas. Usar em demasiado excesso não é a melhor abordagem para garantir a proteção de ativos. A melhor forma de utilizá-la é focando no conjunto apropriado a ocasião para satisfazer exigências de segurança de informação e do usuário final

● Quem utiliza: Desenvolvedores ou programadores atuantes na área de segurança de dados a utilizam para precaver o acesso desconhecido a dados de terceiros que utilizam o aplicativo desenvolvido.

Link de vídeo sobre autenticação: <https://www.youtube.com/watch?v=D-bqhu2LdfI>

Programas Maliciosos:

● O que é: Malicious software (Malware) é um programa de computador destinado a acessar um sistema de computador

Alheio, de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações. Malware inclui vírus, worms, cavalos de troia, ransomware, spyware, adware e outros programas maliciosos.

● Quando utilizar: Se suas intenções são obter dados de terceiros de forma ilegal, essas provavelmente serão as suas ferramentas de abordagem. É utilizado por governos e Hackers quando eles pretendem obter dados de pessoas infringindo a privacidade delas sem permissão.

● Quem utiliza:

É utilizado por governos e Hackers.

Controle de Acesso:

● O que é: Controlo de acesso é uma referência à prática de permitir o acesso a uma propriedade, prédio, ou sala, apenas a pessoas autorizadas. Controle pode ser efetivado por meio físico com guardas e seguranças, mecânicos como fechaduras e chaves ou tecnológicos como sistemas baseados em cartões de acesso, biometria ou reconhecimento de retina. Ele é composto dos processos de autenticação, autorização e auditoria; aquela identifica quem acessa o sistema, essa diz o que o usuário fez durante o uso do sistema ou programa e a autorização determina o que um usuário autenticado pode fazer. A identificação e autenticação fazem parte de um processo de dois passos que determina quem pode acessar determinado sistema. Durante a identificação o usuário diz ao sistema quem ele é (normalmente através de um nome de usuário). Durante a autenticação, a identidade é verificada através de uma credencial (uma senha, por exemplo) fornecida pelo usuário. Atualmente, com a popularização tecnológica, reconhecimento por impressão digital, Smartcard, Mi Fare ou RFID estão substituindo, por exemplo, o método de credencial (nome e senha). Dispositivos com sensores que fazem a leitura, a verificação e a identificação de características físicas únicas de um indivíduo aplicam a biometria e fazem agora a maior parte dos reconhecimentos. A identificação biométrica por impressão digital é a mais conhecida e utilizada atualmente por sua fiabilidade alta e baixo custo.

● Quando utilizar:

Quando pretende-se limitar o acesso a locais ou conteúdos através de senhas ou outros processos para confirmar se a pessoa que deseja acesso realmente é quem diz ser.

● Quem utiliza: Programadores em seus programas, governos na confidencialidade de seus arquivos e cargos públicos, e pessoas que desejam proteger seus bens como empresas, casas ou eletrônicos de acessos desconhecidos.

Detecção de Intrusão:

● O que é: Serve como uma segunda linha de defesa à invasão, age depois da constatação de intrusão no sistema. Sistema, nesse caso, pode ser a rede, um servidor ou um computador pessoal analisando as atividades da rede ou do computador em questão. Como há um aumento no uso de sistemas eletrônicos, há também um aumento de possibilidades para uma possível invasão de sistema, mas essa premissa pode nem sempre ser verdadeira, portanto, há uma necessidade de utilizar um sistema detector de intrusão que auxilia no escopo de segurança da rede como um todo, que possa agir após a constatação de uma provável intrusão. Quando nos deparamos com uma intrusão, é aí que se faz necessária a utilização de um mecanismo que identifique e alerte ou responda à atividade maliciosa em questão.

● Quando utilizar:

Quando há a premissa de uma possível intrusão no sistema sendo ela verdadeira ou não, isso quem dirá será o detector, que avaliará as condições e julgará se há alguma alteração, e as ferramentas anti-malware; o detector entrará em ação, logo após a constatação, para encontrar o problema.

● Quem utiliza:

Todos que possuem ou estão encarregados de proteger um sistema ou aplicativo de ameaças que poderão atrasar ou comprometer o desenvolvimento de projetos de uma empresa ou os dados de algum o usuário que o usa.

Link sobre Detecção de intrusão:

<https://www.devmedia.com.br/sistema-de-deteccao-de-intrusao-artigo-revista-infra-magazine-1/20819>

Gestão de Identidades:

● O que é: A gestão de identidade é o processo de automatizar e auditar as concessões de acesso de sua organização no mesmo repositório, através de fluxos integrados a uma plataforma centralizada, com procedimentos automatizados e perfis de acessos de usuários mapeados. Para tanto, é necessário reunir informações sobre cargo, centro de custo e gestor, entre outros dados, para garantir o controle do ciclo das identidades dos usuários.

● Quando utilizar: Quando pretende-se mapear os acessos a um sistema/programa a fim de certificar-se de ou checar se algum registro feito foi ou não foi efetivado pelo seu verdadeiro dono/usuário com o propósito de descobrir se há alguém utilizando uma falsa-identidade no sistema para poder ter acesso há algo.

● Quem utiliza: Programadores e desenvolvedores do aplicativo são os responsáveis que detêm acesso a essa ferramenta e farão uso se precisaram.

Aspectos Legais e Éticos:

● O que é: São um conjunto de normas de conduta que deverão ser postas em prática no exercício da profissão. Existem seis códigos de conduta que são para com: A sociedade em geral: refere-se à preocupação com o bem-estar das pessoas em geral, quando consideradas como usuários de sistemas computacionais (hardware e software) e envolvem, tipicamente, aspectos de segurança, privacidade e interesses econômicos.

Os empregadores: é também chamada de "ética do trabalho" e refere-se à proteção dos interesses do empregador em situações em que muitas vezes o empregador não tem habilidade para supervisionar tecnicamente o trabalho do profissional e a relação é estabelecida em bases de confiança. Os clientes: quando o profissional trabalha como consultor ou prestador de serviço autônomo para um cliente suas obrigações são as mesmas que as relativas ao empregador.

A própria organização (a sociedade de classe) e seus associados: os códigos de associações de classe geralmente solicitam que os afiliados comunguem dos objetivos da associação e sirvam aos seus interesses, para o bem comum de todos os membros. Os colegas: refere-se ao respeito aos colegas da mesma profissão e à colaboração entre colegas, que normalmente partilham os mesmos interesses. A profissão em geral: trata de aspectos do comportamento ético que devem ser evitados para não denegrir a profissão em si.

● Quando utilizar: No momento em que se deparar com um uma situação conflitante que lhe confere opções de caráter moral. Deve-se sempre optar por aquelas que estejam de acordo com os seis códigos de conduta.

● Quem utiliza: O programador e o cliente em uma tentativa de obter soluções positivas para os dois lados.

Criptografia:

● O que é: é o ato de codificar uma mensagem ou uma troca de dados que só faça sentido para quem tem acesso e, portanto, tem a chave de descriptografar a mensagem ou a troca.

● Quando utilizar: é utilizada para evitar que terceiros com o poder de interceptar as mensagens e trocas de dados entendam o real significado delas.

● Quem utiliza: empresas interessadas em proteger seus dados ou que prezam pela privacidade de seu cliente para auferir ao seu público total sigilo na troca de informações enquanto usam sua ferramenta.

Esteganografia:

● O que é: é uma técnica que consiste em ocultar mensagens dentro de outras mensagens.

● Quando utilizar: Quando deseja adicionar mais um nível de segurança a informação, assim as chances de alguém saber o que a mensagem significa pode cair para apenas você e com quem mais sabe como interpretá-la.

● Quem utiliza: Escritores que pretendem manter uma informação em sigilo e compartilha-la com apenas pessoas de confiança.

Hash criptográfico:

● O que é: Uma função de dispersão criptográfica ou função hash criptográfica é uma [função hash](https://pt.wikipedia.org/wiki/Fun%C3%A7%C3%A3o_hash) considerada [praticamente impossível de inverter](https://pt.wikipedia.org/wiki/Fun%C3%A7%C3%A3o_de_m%C3%A3o_%C3%BAnica), isto é, de recriar o valor de entrada utilizando somente o valor de dispersão. Essas funções hash unidirecionais têm sido chamadas de "os operários da criptografia moderna". Os dados de entrada costumam ser chamados de mensagem, e o valor de dispersão mensagem resumida ou simplesmente resumo.

● Quando utilizar: Em assinaturas digitais, código de autenticação de mensagens

● Quem utiliza: programadores que querem impedir o acesso de terceiros às informações confidenciais.

Forense computacional:

● O que é: é a área que abrange/estuda todos os ciber-crimes que acontecem. A Computação Forense consiste, basicamente, no uso de métodos científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital. A aplicação desses métodos nem sempre se dá de maneira simples.

Evidência digital entende-se pela informação armazenada ou transmitida em formatos ou meios digitais. Sendo que essa evidência, na maioria das vezes, é frágil e volátil, o que requer a atenção de um especialista certificado ou bastante experiente a fim de garantir que os materiais de valor probatório possam ser efetivamente isolados e extraídos correta e licitamente. Tais materiais podem ser apresentados em um tribunal de justiça como prova de materialidade de um crime, por exemplo; ou mesmo como parte de um laudo pericial.

● Quando utilizar: quando a relato de algum crime virtual, ela entra em ação para combater e encontrar soluções para os problemas.

● Quem utiliza: a área forense de agentes e policiais.

Certificado Digital:

● O que é: é um arquivo eletrônico que serve como identidade virtual para uma pessoa física ou jurídica e, através dele, ele pode se fazer transações online com garantia de autenticidade e com toda proteção das informações trocadas

Um certificado digital é usado para ligar uma entidade a uma chave pública. Para garantir digitalmente, no caso de uma Infraestrutura de Chaves Públicas (ICP), o certificado é assinado pela Autoridade Certificadora (AC) que o emitiu e no caso de um modelo de Teia de Confiança (Web of trust) como o PGP, o certificado é assinado pela própria entidade e assinado por outros que dizem confiar naquela entidade. Em ambos os casos as assinaturas contidas em um certificado são atestamentos feitos por uma entidade que diz confiar nos dados contidos naquele certificado.

● Quando utilizar: quando pretende-se fazer uma troca de informações com segurança, o usuário pode requisitar um certificado(chave) para o destinatário, assim restringe-se ainda mais o escopo de acesso.

● Quem utiliza: contanto que se peça o certificado ou que o ambiente utilizado tenha essa opção, qualquer um pode utilizar.

Boas práticas, normas e padrões:

● O que é: é utilizar a tecnologia que se disponibiliza para propagar dados de forma verídica, sem violar privacidade ou infringir regras e leis

● Quando utilizar: sempre, pois, o objetivo é zelar pela a máxima honestidade virtualmente.

● Quem utiliza: todos os profissionais da área podem e devem, entretanto, nem todos a utilizam.

Assinatura Digital:

● O que é: é uma técnica para utilizar a assinatura pessoal em ambientes virtuais por meio de equipamentos específicos que permitem o uso dela. É um método eficiente de autenticação que pode ser explorado para dificultar o acesso ilegal ainda mais.

● Quando utilizar: em transações bancárias virtuais ou em efetivação de compras na internet.

● Quem utiliza: Qualquer um que disponha de um dispositivo para realizar tal coisa.

Auditoria de Sistemas:

● O que é: Auditoria de Sistemas de Informática ou Riscos Tecnológicos é uma atividade independente que tem como missão o [gerenciamento de risco](https://pt.wikipedia.org/wiki/Gerenciamento_de_risco) operacional envolvido e avaliar a adequação das [tecnologias](https://pt.wikipedia.org/wiki/Tecnologia) e [sistemas de informação](https://pt.wikipedia.org/wiki/Sistemas_de_informa%C3%A7%C3%A3o) utilizados na organização através da revisão e avaliação dos controles, desenvolvimento de sistemas, procedimentos de TI, infraestrutura, operação, desempenho e [segurança da informação](https://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o) que envolve o processamento de informações críticas para a tomada de decisão.  Consiste em reunir, agrupar e avaliar evidências para determinar se um [sistema de informação](https://pt.wikipedia.org/wiki/Sistema_de_informa%C3%A7%C3%A3o) suporta adequadamente um ativo de negócio, mantendo a integridade dos dados, e realiza os objetivos esperados, utiliza eficientemente os recursos e cumpre com as regulamentações e leis estabelecidas.

● Quando utilizar: Sempre que for necessário trabalhar com uma grande quantidade de dados de usuários para facilitar e precaver o extravio de informações

● Quem utiliza: Equipes de desenvolvedores que atuam na área de segurança de dados.