OBJETIVOS DA SEGURANÇA

João Cândido de Lima <João.candido@ulbra.br>
Universidade Luterana do Brasil (ULBRA) –

Segurança da informação refere-se a um conjunto de medidas a serem tomadas para preservar os dados de um sistema de computador. Estas medidas garantem que a informação será utilizada de maneira correta e pelas pessoas certas na hora certa. Para que estas medidas sejam adotadas de maneira correta, devem-se levar em conta cinco conceitos também chamados de atributos: Integridade, disponibilidade, Confidencialidade, Autenticidade, Não Repudio.

Atributo 1 - Integridade: A integridade visa garantir a preservação da informação em estado de confiabilidade, em outras palavras, a informação é resultado da análise de dados sem a interferência proposital ou acidental de alguém ou de um software. Uma informação não integra nos leva a uma tomada de decisão errada.

Atributo 2 - Disponibilidade: A disponibilidade consiste em dispor a informação aos usuários na hora em que eles precisarem. Para garantir a disponibilidade podemos utilizar técnicas de redundância, replicação de servidores e links espelhamentos entre outros.

Atributo 3 - Confidencialidade: É garantir que a informação será acessada somente por pessoas autorizadas. Essa garantia é atingida através do uso de criptografia, gerenciamento de permissões em um servidor de arquivos. Em alguns casos esse tipo de segurança é obrigado por lei, como as informações referentes ao saldo bancário de alguém não podem vazar sem autorização judicial.

Atributo 4 - Autenticidade: é o meio pelo qual vou garantir que um usuário é ele mesmo, e não uma pessoa passando por ele para ter acesso a dados privilegiados do sistema. Para garantir a autenticidade podemos utilizar identidades digitais como o PROUNI programa universidade para todos do governo federal, onde os alunos com bolsa são cadastrados por um usuário com senha e um cartão com chip em uma leitora, esse cartão possui um certificado digital garantindo que o usuário o possui em mãos.

Atributo 5 - Não repúdio - Consiste no conceito de garantir que a ação efetuada por um usuário não possa ser negada. Se um usuário apagar os dados de um servidor deve-se comprovar através de um sistema que a operação foi realizada pelo determinado funcionário em questão.

Com base nestes cinco atributos, conseguimos promover efeitos de segurança em nosso sistema computacional. Podem-se entender estes atributos como sendo a definição de segurança da informação, pois é através deles abrangemos todo o tratamento de qualquer tipo de informação.

SUSTENTAÇÃO DA SEGURANÇA

João Cândido de Lima <João.candido@ulbra.br>
Universidade Luterana do Brasil (ULBRA) –

Para garantir a segurança da informação, não basta apenas teorias e conceitos, devemos por em prática os mesmos, e devemos considerar diferentes meios de aplicação destes atributos. Visando garantir a implementação da segurança da informação, podemos considerar a idéia de um tripé que também pode ser chamado de pilares da segurança.

Estes pilares demonstram os principais pontos de equilíbrio de um sistema, são eles: Mecanismos, Políticas e Cultura.

Mecanismos: É toda a estrutura utilizada para garantir o funcionamento correto do sistema, pode ser por software ou hardware, podemos considerar como exemplo um servidor RADIUS, que autentica os usuários os identificando na rede, ou ainda um cartão magnético utilizados em algumas escolas para retirar livros da biblioteca. Por tanto mecanismo é a tecnologia em si utilizada para o funcionamento de um sistema.

Políticas: É o método de documentar o funcionamento do sistema, especificando as regras de utilização do mesmo. Podemos pensar em políticas de sistemas como um código a ser seguido e a base para o funcionamento de todo o sistema. Como exemplo pode-se citar o regimento interno de um Laboratório de informática, onde especificaríamos o nível de acesso dos usuários, 1 seria área restrita da rede, 2 utilização apenas na rede interna e 3 acesso somente externo. Com base na política deste laboratório enquadra-se a necessidade de cada usuário quem será de nível 1 ou 2 ou 3.

Cultura: Consiste em quebra de paradigmas, e talvez seja a mais difícil de implantar. Um exemplo clássico é o uso de senhas, quem nunca usou uma senha com o aniversário de alguém ou pior o seu próprio aniversário, isso é uma cultura, fornecer a senha para o colega é outro exemplo. Usar uma senha fraca pode comprometer a estrutura de todo um sistema. Em tese para solucionarmos este problema, devemos explicar aos usuários a necessidade da correta utilização do sistema explicando o porquê da aplicação das políticas previstas para o sistema, isso ajuda a amenizar o problema.

Com o tripé de sustentação da segurança podemos entender o objetivo de protegermos um sistema, garantindo assim o seu funcionamento correto que é o primeiro passo para se estabelecer a segurança da informação.

ANÁLISE DE RISCOS

João Cândido de Lima <João.candido@ulbra.br>
Universidade Luterana do Brasil (ULBRA) –

Quando falamos em análise de riscos é importante lembrar que qualquer investimento as ser feito seja ele de hardware ou software, é precedido pela análise de riscos. Análise de risco é a capacidade de detectar possíveis falhas no sistema que possam agregar prejuízo a informação ou o sistema em si.

Para termos uma noção de risco real em nosso sistema, podemos utilizar uma simples fórmula, porém muito útil. A formula é a seguinte: risco = vulnerabilidade X ameaça X Impacto

Vulnerabilidade: Seria uma falha no sistema, proveniente de um problema na hora do desenvolvimento, na hora da implantação ou do próprio uso do sistema. As vulnerabilidades podem ser reduzidas com atualizações ou testes no sistema.

Ameaça: Surge da existência de agentes com motivação e conhecimento para explorar as vulnerabilidades. Existem várias motivações que um agente pode ter, como vingança, lucro, curiosidade entre outras. Para reduzir a ameaça podemos duplicar recursos, fazer backup e monitoramento constante.

Impacto: Vem a ser união da vulnerabilidade e da ameaça, no caso de haver um ataque qual o prejuízo? Isto vai depender do valor da informação atacada. No caso do vazamento de informações confidencias uma empresa pode até decretar falência.

A redução de qualquer fator da formula diminui a possibilidade de um ataque, mas a segurança é o inverso da facilidade de uso, no caso de reduzirmos a zero um desse fatores, poderemos complicar a vida de nosso usuário, por tanto uma boa análise resulta em uma manutenção preventiva do sistema e muitas vezes evita a manutenção corretiva.

ATACANTES

João Cândido de Lima <João.candido@ulbra.br>
Universidade Luterana do Brasil (ULBRA) –

A classificação de atacantes pode ser reduzida a praticamente duas categorias hackers e script kids, mas também existem outras como lammer e cracker. Outro fato importante de se analisar é que não existe invasão sem um invasor, e que vai classificar o invasor é o nível de conhecimento e as técnicas utilizadas para invadir.

Hacker: hack em inglês pode ser traduzido como bisbilhotar, logo hacker é um bisbilhoteiro. Esse termo começou a ser utilizado pelos estudantes do MIT, para classificar os usuários que utilizavam os recursos computacionais além dos limites. Um hacker normalmente efetua uma invasão com objetivos bem definidos, mas não chega a ser um cracker que invade com objetivo de causar um dano ao sistema.

Script Kid: diferente do hacker é um usuário sem muito conhecimento que utiliza programas desenvolvidos por hackers com o objetivo de encontrar um alvo fácil para proporcionar o ataque normalmente esta atrás de notoriedade.

Para prevenirmos um ataque devemos conhecer bem o perfil dos atacantes, de preferência entendermos a sua motivação, assim podemos tomar medidas preventivas com eficácia.

ANATOMIA DE UM ATAQUE

João Cândido de Lima <João.candido@ulbra.br>
Universidade Luterana do Brasil (ULBRA) –

Um ataque pode ter duas origens, pode ser interno ou externo e pode usar ferramentas de ataque intrusivo ou não intrusiva.

Um ataque intrusivo pode ser percebido pelo fato do atacante usar ferramentas com comportamento diferente que um usuário comum teria, podemos citar como exemplo o scanport, softwares que fazem varredura através de portas abertas em um servidor procurando possíveis vulnerabilidades no sistema como o software Nmap do Linux. Assim como um martelo pode ser usado uma ferramenta de trabalho, ele pode ser usado para atacar alguém, os scanports podem ser usados para atacar ou simplesmente usados para identificar falhas em nosso sistema, tudo isso depende do usuário.

Já as ferramentas não intrusivas tem atacam utilizando ações comuns de usuários, sendo assim mais difíceis de serem identificadas, por exemplo um hacker acessando um servidor via página HTML buscando informações sobre a empresa, pode ser considerado como a etapa de uma ataque bem como um cliente buscando informações da empresa.

Um ataque divide-se basicamente em quatro etapas:

1- Levantamento de Informações: consiste em obter o maior número de dados possíveis sobre o alvo com o objetivo usar a análise destes dados contra o próprio alvo.

2- Obtenção e teste de ferramentas: Após descobrir as vulnerabilidades de um sistema a próxima etapa é procurar ferramentas que ataquem os pontos fracos encontrados. Normalmente é testado em um sistema em paralelo ao que será atacado, com o objetivo de não levantar suspeitas por parte do alvo.

3- Aplicação contra o alvo: após obter sucesso nas duas etapas anteriores, chega a hora de efetuar o ataque propriamente dito. É quase impossível que o atacante consiga na primeira vez, por isso ele irá tentar várias e várias vezes e é nesse momento que o administrador do sistema pode conseguir detectar o invasor.

4- Exploração dos resultados: após obter sucesso no ataque o invasor ira explorar os resultados obtidos, esta etapa dependerá muito da motivação do invasor e qual o objetivo dele em invadir este sistema. Podemos detectar o ataque nesta etapa também, mas caso isso não aconteça o atacante pode ficar ativo por vários meses ou até meso anos em nosso sistema.

Com a análise destas etapas podemos concluir que é praticamente impossível detectar o atacante nas duas primeiras etapas, e levando em conta que a quarta etapa o ataque já foi realizado e com sucesso, nos resta á terceira etapa para identificarmos o atacante.