Segurança técnica – tecnologias para defesa e monitoramento em redes corporativas

Apresentar outros elementos que podem ser utilizados para fortalecer o processo de segurança técnica dentro da organização. Uma vez que não existe segurança 100%, é necessário que os componentes e projetos de segurança interajam entre si para, dessa forma, diminuir a possibilidade da ocorrência dos erros e incidentes de segurança.

Funções de cálculo de Hash

Algoritmos de Hash também são conhecidos como menssage digest ou funções unidirecionais. O processo é unidirecional e impossibilita descobrir o conteúdo original a partir do Hash. O valor de conferência ("check-sum") muda se um único bit for alterado, acrescentado ou retirado da mensagem.

A função de Hash também se caracteriza por ser fácil de calcular e difícil de ser invertida. Um exemplo bem simples consiste na elaboração de um resumo de um livro de 1000 linhas. Você consegue gerar o resumo a partir do texto original, porém o inverso é impossível gerar novamente o texto completo.

O MD5 é uma função de Hash

Esse tipo de função é normalmente utilizado em assinatura digital, recebe uma cadeia de caracteres e devolve um número de 128 bits.

A segurança do MD5 assenta no fato de ser impossível (em princípio) determinar a cadeia de caracteres a partir do Hash ou encontrar outra cadeia de caracteres que, transformada, resulte no mesmo Hash.

Por outras palavras, é impossível desencriptar o MD5.

Abaixo segue um exemplo de um algoritmo de Hash aplicado a uma palavra.

Texto original => **Gabriella**, ao aplicar a função MD5 em cima desse texto, é gerado um Hash exclusivo **88f418d385fe30d5a2bfd3e17c732b28**, caso ocorra qualquer alteração no texto, a chave de Hash será modificada.

Texto original => **Gabriela** (note que apenas foi tirado um l que havia sido digitado a mais). O Hash gerado será **3045c3c6443d58c4e72e76fbcbcb2df3** totalmente diferente do Hash gerado pelo texto anterior.

Como visto no exemplo acima, a alteração de apenas um único caractere fez com que o resumo gerado fosse algo totalmente diferente.

Essa possibilidade de garantir que a alteração de qualquer byte de um texto produza um Hash totalmente diferente possibilitou aumentar a segurança na troca eletrônica de dados, uma vez que, se um dado fosse alterado durante o processo de transporte do destinatário até o usuário final, seria possível verificar que essa alteração ocorreu e, com isso, bloquear o uso da informação.

Exemplificando: a técnica de Hash possibilita que, ao ser aplicado em uma mensagem de qualquer tamanho, seja gerado um resumo criptografado de tamanho fixo e bastante pequeno, com, por exemplo, 128 bits. Esse resumo é unido à mensagem original e encaminhado para o destinatário. Ao receber essa mensagem, o destinatário também deve aplicar a mesma técnica e comparar o resumo obtido. Basta agora separar esse resumo que veio com a mensagem e aplicar o algoritmo usado para criar o resumo na origem em cima da mensagem que chegou. Qualquer discrepância desse novo resumo que será criado com o resumo gerado inicialmente indicará que a mensagem sofreu algum tipo de alteração indevida.

Com a função Hash:

- Pode-se garantir que o conteúdo de uma mensagem não foi alterado, que ela está íntegra.
- Não é possível fazer a operação reversa, ou seja, dado um resumo, é impossível obter a mensagem original.
- Duas mensagens diferentes, quaisquer que sejam, não podem produzir um mesmo resumo.
- Deve ser fácil e rápido de ser aplicado.
- Esse tipo de função é normalmente utilizado em assinaturas digitais. Ela recebe uma cadeia de caracteres e devolve um resumo codificado.
- A execução do algoritmo de hashing sobre o mesmo texto sempre vai dar o mesmo resultado, porém, com o mínimo de alteração no texto feito pelo usuário ou remetente da informação, o resultado é alterado.
- MD2, MD4, MD5 (128 bits) e SHA (160 bits) são funções de cálculo de hash.

Para que serve mais o Hash

Alguns sites utilizam essa função para checar a integridade dos seus arquivos e transmitir para o usuário a sensação de segurança, uma vez que por meio do processo de Hash o próprio usuário poderá se certificar de que a informação que ele recebeu está íntegra, ou seja, não sofreu nenhuma alteração durante o processo de transporte.

Como exemplo, podemos citar um site que deixa arquivos disponibilizados para download. Quando o usuário baixa esse arquivo no seu micro pessoal, ele acredita que o arquivo chegou inteiro e está da mesma forma que foi disponibilizado no site. Mas como ter certeza? Com o processo do Hash pode ser disponibilizado o arquivo que deverá ser baixado, bem como o número que foi gerado pela aplicação do Hash no arquivo.

Após baixar o arquivo principal, pode-se novamente ser aplicado o algoritmo de Hash que o site utilizou e fazer uma comparação com o Hash que estava no local de onde o arquivo foi baixado. Se os números forem iguais, está tudo certo e os arquivos são idênticos. Porém, caso os hashs forem diferentes, significa que o arquivo baixado está corrompido ou foi alterado, pois estará com bytes diferentes do original na sua chave de Hash.

Assinatura digital

A assinatura digital é um conjunto de procedimentos matemáticos que possibilitam a inclusão de um código identificador do emitente da mensagem em meio digital. Uma assinatura é algo que só pode ser feito pelo seu autor, provando assim, a sua participação e autoria.

Cartório digital

São empresas especializadas, conhecidas como Autoridades Certificadoras (CA), que emitem certificados digitais, documentos eletrônicos de identidade de pessoas ou empresas na internet. São entidades confiáveis e reconhecidas (VeriSign, Thawte, GlobalSign etc.), que emitem um certificado digital que inclui a chave pública de uma entidade, com dados para identificação confiável dela e assinado digitalmente com a chave privada da CA. Essas empresas necessitam ter em sua infraestrutura um conjunto de itens que garantam a sua segurança tanto física como lógica, por exemplo:

Controle físico, sala-cofre, controle de procedimentos, controle de pessoal, controle de qualidade das máquinas e componentes, segurança na rede: Firewall, IDS, controle dos módulos criptográficos.

Certificado digital

É um arquivo que amarra todos os dados da pessoa ou empresa, como: nome, razão social, data de nascimento etc., identificado numa estrutura inviolável, baseado na tecnologia de criptografia. De uma maneira simples, o certificado é uma chave pública assinada por uma Autoridade de Certificação (CA) que atesta a autenticidade daquela chave pública como pertencente a uma determinada pessoa.

Um dos padrões de certificado utilizado no mercado é definido pela norma ITUT X.509 e possui na sua composição:

Versão do formato do certificado, número serial único associado ao certificado e controlado pela CA; identificação do algoritmo utilizado para assinar o certificado, emissor com informações sobre a Autoridade de Certificação, período de validade inicial e final, informações do usuário, informação sobre a chave pública, assinatura da CA cobrindo todo o certificado. Por segurança, todo certificado leva data de validade.

Todo certificado digital possui um período de validade e, após o vencimento dessa validade, a

autoridade certificadora o inclui no CRL (Certificate Revocation List), ou seja, na lista de certificados revogados, ou, pode também atualizar a sua validade. O CRL é um mecanismo que as CA´S possuem para disseminar informações sobre certificados digitais que foram revogados por algum motivo. Um certificado pode ser revogado quando:

- O usuário é removido do domínio de segurança.
- O proprietário do certificado reconhece que perdeu a chave privada.
- Existe suspeita de ataques.
- Tanto a CA como o usuário podem solicitar o cancelamento do certificado.

PKI – Public Key Infrastructure (Infraestrutura de chave pública)

Não é uma aplicação. É uma infraestrutura usada para habilitar aplicações que necessitem de um alto nível de segurança, utilizando conceitos e técnicas envolvendo chaves públicas e certificados digitais para garantir a segurança do sistema e confirmar a identidade de seus usuários.

Composta por autoridade certificadora, diretório, política de certificados? certificado digital? chaves públicas? chaves privadas? criptografia? assinatura digital.

Quando é apresentado ao navegador um certificado digital, por exemplo, de uma loja de informática que está realizando um comércio, ele consulta a autoridade certificadora que emitiu o certificado digital. Se a autoridade certificadora estiver na lista de autoridade certificadora confiável, o navegador aceita a identidade do site da web e a exibe. Entretanto, se a autoridade certificadora não estiver na lista, o navegador exibe uma mensagem de aviso em que pergunta se você deseja confiar na nova autoridade certificadora.

VLAN (Virtual Local Area Network ou Virtual LAN, em português)

Em consequência da capacidade dos switch´s de implementar uma VLAN, pode-se atribuir a ele a capacidade de funcionar com um dispositivo de segurança para uma rede interna.

Uma VLAN pode ser formada por um grupo de computadores, servidores e outros recursos de rede que, apesar de às vezes estarem fisicamente muito distantes, se comportam como se estivessem conectados a um único segmento de rede, mesmo não estando.

O tráfego em uma VLAN não pode ser "escutado" por membros de outra rede virtual, já que eles não se comunicam sem que haja um dispositivo de rede desempenhando a função de roteador entre as duas redes. Dessa forma, basta implantar medidas de segurança baseadas na política da empresa dentro desses roteadores e, dessa forma, limitar o acesso a essas redes.

Segurança em redes sem fio

As redes sem fios surgiram para facilitar a vida dos usuários finais, mas infelizmente, para aumentar a dificuldade da implementação de segurança dentro dos ambientes da empresa. Hoje em dia tempos uma série infindável de produtos de tecnologia que pode ser conectados a uma rede sem fio.

Com a necessidade do aumento da mobilidade dos funcionários das organizações, os fornecedores de equipamentos já fabricam seus dispositivos preparados para a conexão sem fio. A grande parte de equipamentos já saem de fábrica com dispositivos de bluetooth, infravermelho e wirelles.

O grande problema é colocar na cabeça das pessoas que na rede "**sem fios**" não existe o conceito de rede privada (isolada), pois qualquer individuo com um equipamento wireless pode ligar-se a ela, desde que tenha "sinal" e permisssão para tal, obviamente.

A utilização desse tipo de tecnologia traz uma série de ameaças para o ambiente das empresas, principalmente com aspectos relacionados a:

- Possibilidade de divulgação de informação confidenciais da empresa.
- Possibilidade de acesso não autorizado a dados localizados dentro dos equipamentos da empresa.
- Possibilidade constante da interrupção de serviço, caso não tenha sido bem configurado por causa de problemas com interferências.
- Uso e acesso desautorizado à internet e abertura de um buraco nas defesas da organização.
- Possibilidade de implementações de Access Points não autorizados, fazendo com que a segurança da empresa fique comprometida.

A segurança é um ponto fraco das redes sem fio, uma vez que o sinal pode se propagar pelo ar em todas as direções, além de poder ser capturado por pessoas não autorizadas.

As paredes e portas de uma casa ou empresa não são suficientes para barrar o sinal wireless que se propaga pelo ar e um Access Point instalado dentro de um escritório pode transmitir um sinal num raio de 300 metros e em todas as direções.

A rede sem fio não restringirá o seu alcance apenas para as salas da empresa, pois os escritórios que estiverem localizados no andar de cima ou abaixo, no mesmo prédio, poderão ter alcance dele também. Dessa forma, durante o projeto de implementação desse ambiente, isso necessita ser considerado.

Rogue APS

Um Rogue Access Point (Rogue AP) é o nome dado a qualquer Access Point estranho e que tenha sido instalado dentro da empresa sem permissão por parte dos administradores da rede.

Esse equipamento, por sua facilidade de aquisição e instalação, é facilmente utilizado sem autorização em uma determinada infraestrutura de rede por parte dos usuários que já estão acostumados com a tecnologia em suas casas e querem trazer essa facilidade para dentro do ambiente da empresa.

Os Rogue Aps estão relacionados com um dos grandes problemas existentes nas organizações, uma vez que os usuários podem criar facilmente redes sem conhecimento dos administradores de segurança e sem atender aos requisitos impostos pelas políticas de segurança.

A segurança em redes sem fio pode ser implementada em dois grandes grupos:
Soluções que vão agir em cima de software e soluções que agirão em cima de hardware.

Para um ambiente de rede sem fio, o cenário ideal é feito com a implantação do máximo de ferramentas possíveis, tanto em nível de software como de hardware, para tentar tornar o ambiente mais seguro ao máximo.

Protocolos utilizados para proteção de redes sem fio

Wired Equivalency Privacy – WEP

É o protocolo original de autenticação e criptografia definido pelo IEEE 802.11, sendo a primeira tentativa de se criar um protocolo eficiente de proteção de redes sem fio, porém foi muito criticado em razão de suas falhas. A criptografia e autenticação são aplicadas ao nível do link da rede sem fio e não proveem segurança fim-a-fim, em outras palavras, só proveem segurança no trecho da rede sem fio.

Esse tipo de protocolo utiliza algoritmo simétrico de chaves compartilhadas no dispositivo cliente e do Access Point. É considerado **fraco**, pois a chave utilizada como parâmetro é a mesma para todos os usuários de uma rede e não possui autenticação do usuário.

Wi-fi Protected Access – WPA

Padrão de segurança que veio tentar solucionar as vulnerabilidades apresentadas pelo WEP. O WPA possui maior controle de acesso por meio da utilização de autenticação com chave dinâmica, além de possuir sistema de criptografia mais aprimorado, em que cada usuário possui uma chave de criptografia exclusiva, que é trocada no decorrer da sessão de forma automática.

Tipos de WPA

Existem dois tipos de WPA, e cada um é utilizado em situações específicas. Logo a seguir discriminaremos os dois tipos:

WPA-Personal / WPA-PSK

É a versão "doméstica" do WPA, em que é utilizada uma chave de autenticação específica.

WPA-Enterprise (ou WPA-RADIUS)

Nesse tipo de solução é utilizada uma estrutura mais complexa, em que o ponto de acesso é ligado a um servidor RADIUS (servidor de autenticação), que é responsável por controlar o processo de autenticação do usuário junto à rede.

Vulnerabilidades do WPA

O WPA possui características de segurança superior ao WEP, porém, ainda assim, possui algumas vulnerabilidades, sendo a principal a possibilidade de utilização de senhas pequenas e de fácil adivinhação.

Porém, pode-se conseguir um pouco mais de segurança aplicando algumas regras básicas em equipamentos de rede sem fio.

Utilização de VPN (Virtual Private Network)

Para aumentar a segurança e garantir o sigilo das informações que trafegarão pela rede sem fio, pode-se pensar na implementação de soluções que permitam a implementação de VPN na conexão. Desse modo, é criado um "tunel" virtual seguro desde o computador do usuário até o Access Point ou gateway do mesmo, continuando pela internet até os servidores e sistemas da empresa.

MAC Address Filtering

Cada estação wi-fi radio tem o seu único endereço MAC alocado pelo fabricante e, dessa maneira, para melhorar a segurança. Um Access Point pode ser configurado para só aceitar conexão de endereços MAC previamente cadastrados. Caso o endereço não esteja cadastrado, a navegação pela rede é cancelada.

Dicas para aumentar a segurança na configuração do Access Point

As dicas servem para melhor a segurança no Access Point, contudo, todas as recomendações de segurança física passadas nas aulas anteriores também devem ser implementadas buscando, com isso, diminuir a possibilidade dos incidentes de segurança.

- Ativar a criptografia.
- Alterar o SSID – elemento que identifica seu ponto de acesso.

- Desabilitar o recurso de Broadcast (transmissão) do SSID.
- Filtrar o endereço MAC.
- Alterar parâmetros de SNMP-padrão.
- Aplicar senhas no compartilhamento dos arquivos.
- Analisar o tráfego da sua rede wireless frequentemente.
- Atualizar no software do Access Point, bem como aplicar os principais patches de segurança.
- Procurar padronizar os dispositivos clientes que têm acesso à rede da companhia.
- Exigir que os usuários utilizem senhas para autenticação.
- Ter um gerenciamento de maneira centralizada dos equipamentos wireless da sua empresa.
- Utilizar criptografia que foram recomendadas pelas políticas de segurança, principalmente nos dados confidenciais armazenados nos notebooks e outros equipamentos que têm acesso à rede.
- Desabilitar a administração do roteador por meio da rede sem fio, sendo essa medida de segurança importante, pois somente as pessoas que estiverem conectadas à rede cabeada poderão administrar o roteador.

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento. Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

Referências

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de segurança da informação: guia prático para elaboração e implementação.* Rio de Janeiro: Ciência Moderna, 2006.

NAKAMURA, Emílo Tissato; GEUS, Paulo. Lício de. *Segurança de redes em ambientes cooperativos*. São Paulo: Berkeley, 2002.

RUFINO, Nelson M. de O. *Segurança em redes sem fio: aprenda a proteger suas informações em ambientes WI-FI e Bluetooth.* São Paulo: Novatec., 2005.

STREBE, Matthew; PERKINS, Charles. *Firewalls*. São Paulo: Makron Books, 2002.

TANENBAUM, Andrew S. *Redes de Computadores*. Rio de Janeiro: Campus, 2006.