SEGURANÇA DA INFORMAÇÃO

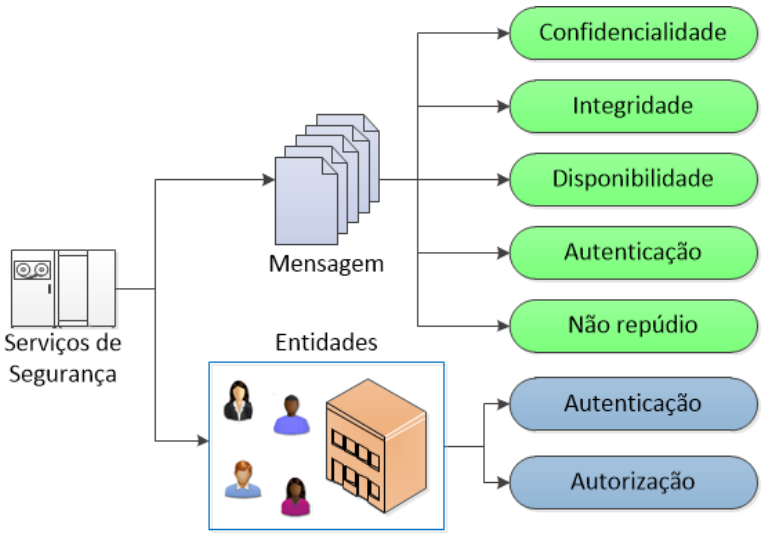
Prof. Luis Gonzaga de Paulo

TEMA 1 – SERVIÇOS DE SEGURANÇA

Para prover a segurança da informação é necessário um conjunto de medidas e recursos. Dentre esses recursos, estão os serviços de segurança, relacionados na Figura 1. Esses serviços têm como objetivo preservar as características básicas da informação, visando a confidencialidade, a integridade, a disponibilidade, a autenticação, o não repúdio e a autorização.

Os serviços são divididos entre aqueles que atuam junto à **mensagem** – ou seja, na infraestrutura tecnológica que suporta a informação – e aqueles que atuam junto às **entidades** – isto é, com os indivíduos e as organizações que tomam parte no ciclo de vida da informação. Esses serviços incluem também autenticação e autorização, conhecidas como *identity and access management* (IAM) – ou gerenciamento de identidades e acesso.

Figura 1 – Serviços de segurança de mensagem e de entidades



Fonte: Adaptado de Forouzan, 2010.

1.1 Serviços de segurança da mensagem

Os serviços de segurança da mensagem atuam em todo o ciclo de vida da informação, desde sua origem até o descarte. Esses serviços, como já dissemos, têm como objetivo preservar as características básicas da informação no que se refere à segurança: confidencialidade, integridade, disponibilidade, autenticação e não repúdio.

1.1.1 Confidencialidade

A confidencialidade é também denominada **privacidade da mensagem.** Trata-se do sigilo entre o emissor e o receptor da mensagem, ou seja, a mensagem deve ser útil e acessível somente aos envolvidos no processo de comunicação. Forouzan (2010) confirma que a forma de obter a confidencialidade ou a privacidade da mensagem não mudou e tem sido preservada há milhares de anos: “A mensagem deve ser criptografada no emissor e descriptografada no receptor”. Isso quer dizer que a mensagem deve ser ininteligível para as partes não autorizadas a acessá-la.

A privacidade visa impedir que um possível intruso no processo de comunicação – ou um interceptador – consiga acessar o conteúdo original da mensagem. Como já vimos, para garantir a confidencialidade, usamos tanto a criptografia de chave simétrica como a criptografia de chave assimétrica.

1.1.2 Integridade

Esse serviço de segurança procura garantir que a mensagem que chega ao receptor seja exatamente igual à que foi enviada pelo emissor, sem sofrer alterações durante o processo, sejam essas alterações de origem acidental, sejam de origem mal-intencionada. No momento atual da tecnologia, em que as transações comerciais eletrônicas crescem vertiginosamente e fazem intenso uso de troca de informações monetárias e financeiras, uma falha de integridade pode resultar em uma catástrofe. A integridade da mensagem deve ser preservada em uma comunicação segura, porém, sabemos que a criptografia pode garantir o sigilo e a confidencialidade, mas não a integridade.

Entretanto, em algumas ocasiões, a integridade da informação é mais necessária do que a sua confidencialidade. “Por exemplo, Alice poderia redigir um testamento para distribuir suas propriedades após sua morte. O testamento não precisa ser criptografado. Após sua morte, qualquer um poderá examinar o documento. Todavia, sua integridade deve ser preservada” (Forouzan, 2010).

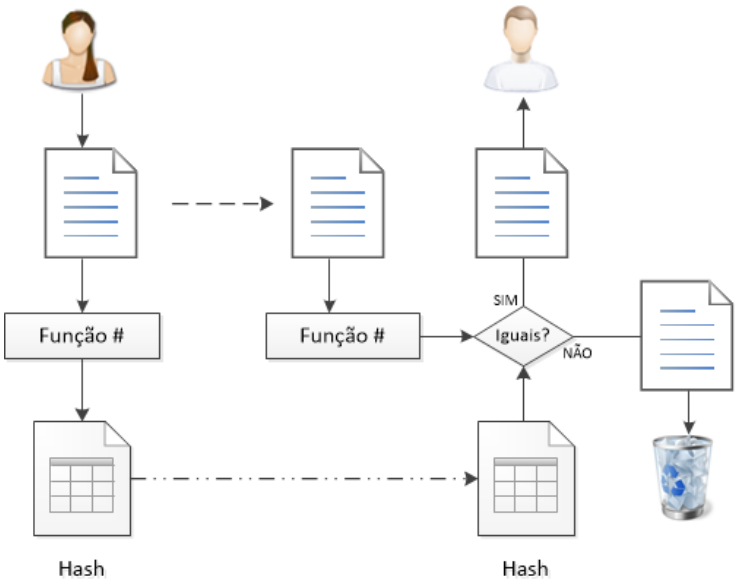
Uma das maneiras mais utilizadas para preservar a integridade de um documento digital é a sua impressão, pois o conteúdo impresso não pode ser modificado. O equivalente eletrônico do par **documento digital** + **impressão** é o par **mensagem** + ***hash***, que é um **resumo criptográfico** ou o ***digest*** da mensagem, também denominado **MDC** (*modification detection code*), ou código

de detecção de modificação. Para ter sua integridade preservada, a mensagem passa por um algoritmo de uma função *hash*, o qual cria uma imagem compactada da mensagem que pode ser usada como forma de garantir sua integridade, tal como se fosse uma impressão.

A Figura 2 mostra a mensagem e o processo de verificação de integridade com o *digest*. O resumo criptográfico deve atender a três critérios básicos:

1. ser **unidirecional**, isto é, garantir que seja possível chegar a um *hash* a partir da mensagem original, porém, que seja impossível reconstituir a mensagem original a partir do *hash*;
2. o *hash* deve ser resistente a **colisões fracas**, isto é, não pode permitir que o emissor ou o receptor (ou um interceptador) possa criar outra mensagem que resulte no mesmo *hash* de modo a falsificar a mensagem original;
3. o *hash* deve ser resistente a **colisões fortes**, isto é, duas mensagens distintas jamais podem resultar em um mesmo *hash*.

Figura 2 – Verificação de integridade com Hash



Fonte: Adaptado de Forouzan, 2010.

O algoritmo mais utilizado para a geração do *hash* é o SHA-1 (*secure hash algorithm 1*), desenvolvido pelo National Institute of Standards and Technology (NIST). Funciona com base no processamento de blocos de 512 bits, do qual é gerado o *digest*. Esse *digest* é processado juntamente com o bloco seguinte e, assim, sucessivamente, até o último bloco. Caso ele não contenha 512 bits, é feito o preenchimento com zeros. Ao término do processo é gerado o *digest* da

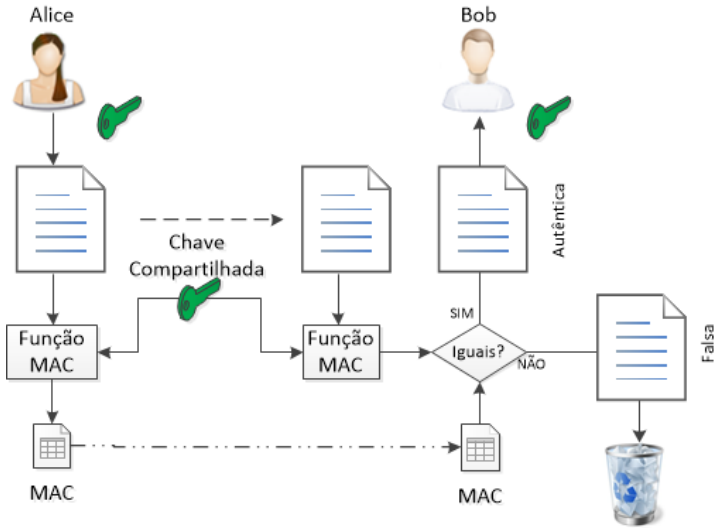
mensagem com 160 bits – cinco palavras de 32 bits.

1.1.3 Autenticação

Na maioria dos processos de comunicação, não é o suficiente garantir a confidencialidade e a integridade da mensagem. Geralmente, quem recebe a mensagem precisa se certificar de sua origem, isto é, o emissor precisa evidenciar a sua identidade. Apenas o *hash* não é suficiente para isso, pois não incorpora informações que possibilitem identificar o emissor no processo criptográfico. Isso se deve ao fato de o *hash* não usar uma chave criptográfica. Então, para que haja possibilidade de o receptor conferir a autenticidade do emissor, é necessário que ambos compartilhem uma chave, criando assim um código de autenticação de mensagem – o **MAC** (*message autentication code*).

Então, se Alice quer enviar uma mensagem a Bob de modo que ele possa se certificar de que foi ela mesmo quem enviou, será necessário que Alice, usando sua chave simétrica compartilhada com Bob, gere um MAC e o envie juntamente com a mensagem. Bob receberá a mensagem e o MAC, e usando a chave compartilhada com Alice, irá gerar um novo MAC a partir da mensagem recebida. Se esse novo MAC for idêntico ao MAC recebido, então Bob terá certeza de que a mensagem procede de Alice. A Figura 3 apresenta esse processo.

Figura 3 – Verificação de autenticidade com MAC



Fonte: Adaptado de Forouzan, 2010.

Um modelo mais atualizado incorpora a própria chave simétrica à mensagem e, usando SHA-1, gera um *hash*. Esse modelo é denominado **HMAC**

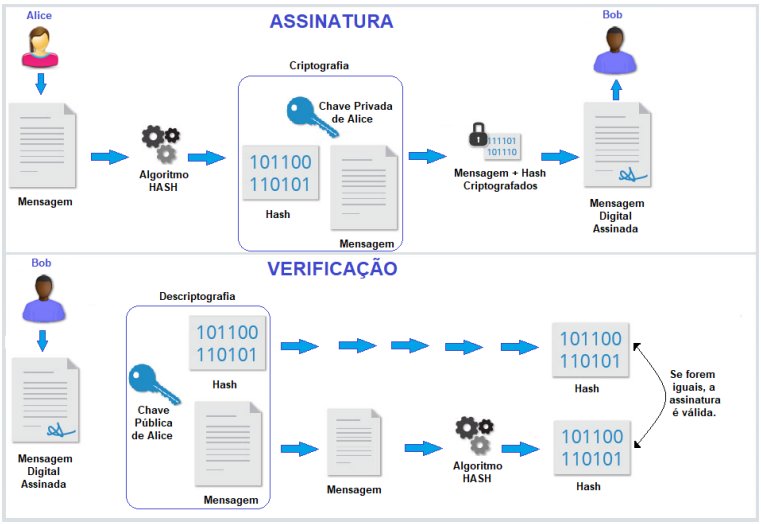
(*hash-based message authentication code).*

1.1.4 Assinatura Digital

Ao receber uma mensagem, é provável que o receptor precise confirmar a identidade do emissor, e se foi ele mesmo quem a elaborou ou aprovou. Essa necessidade não pode ser atendida por *hash* ou MAC. Para isso, é necessário outro processo: o de assinatura digital. De forma semelhante a uma assinatura impressa, a assinatura digital comprova a autenticidade do emissor da mensagem. Porém, diferentemente da assinatura física, uma assinatura digital não faz parte da mensagem, pois é enviada separadamente. Então, o processo requer duas remessas: a da mensagem e a da assinatura.

Diferentemente do que ocorre nos processos anteriores, a assinatura digital requer um sistema de chaves públicas. O emissor usa a sua chave privada para assinar a mensagem, e o receptor usa a chave pública do emissor para verificar a autenticidade da mensagem e validar a assinatura. Porém, é possível simplificar o processo usando um *hash*: em vez de se assinar a mensagem, assina-se o *hash*, e, por meio dessa assinatura, o processo de verificação de integridade e autenticidade se realiza. A Figura 4 mostra esse processo.

Figura 4 – Assinatura digital e verificação



Fonte: Adaptado de Stallings, 2015.

1.1.5 Não repúdio

A irretratabilidade – ou não repúdio – é a característica da segurança da informação cujo objetivo é garantir a autoria e a responsabilidade pela informação

e por seu manuseio, evitando que possa haver negativa ou revogação de ações promovidas com essa informação.

Por exemplo: um cliente realiza uma operação de transferência de dinheiro de uma conta para outra, e o banco requer uma prova de que foi realmente o cliente quem a realizou, que foi realmente ele quem solicitou essa transação. Para isso, é necessário a correta autenticação, mediante procedimentos já discutidos, para a correta identificação do cliente e a autorização do banco para a realização da operação. A autenticação multifator – com login/senha, identificação biométrica e cadastramento prévio aliados à autorização por SMS, tokens e outros meios – procura satisfazer essa necessidade. O recurso de não repúdio pode ser oferecido também por meio de uma terceira parte confiável, com base em criptografia assimétrica, assinatura digital ou certificação digital.

1.2 Autenticação de entidades

De acordo com Forouzan (2010), na autenticação de entidades (ou identificação de usuário), a entidade ou o usuário são verificados primeiro para, só depois, receber autorização de acesso aos recursos do sistema (como comunicação, banco de dados, aplicativos ou arquivos). Ao utilizar o ambiente virtual de aprendizagem (AVA) UNIVIRTUS, você, aluno, é requisitado a informar o seu registro UNINTER (RU) e a sua senha no processo de *logon* ou *login*. A partir desse momento, uma série de recursos é disponibilizada com base em seu *perfil de usuário* e em regras do AVA previamente definidas.

Para o processo de autenticação, a entidade requerente deve se identificar de maneira inequívoca para o verificador usando um conjunto de fatores, tais como:

- **algo que conhece**: uma informação sigilosa conhecida apenas pelo requerente (ou por ambos, requerente e verificador) e que possa ser validada pelo verificador. Normalmente são utilizados senhas, um *personal identifier number* (PIN, ou número de identificação pessoal), a chave criptográfica ou secreta ou mesmo a chave privada;
- **algo que possui**: um documento ou *token* expedido pelo verificador ou por uma outra entidade que tenha a confiança do verificador (fé pública), como uma carteira de identidade, um passaporte, um cartão de débito ou de crédito. Uma chave mecânica ou um dispositivo eletrônico ou

computacional – *smart cards* ou o *smartphone* do requerente também se encaixam nessa categoria;

- **algo que é**: um elemento natural ou da composição física da entidade, inerente à sua existência ou composição, tais como assinaturas impressas (ou mecânicas), impressões digitais, fotos (imagens, traços faciais, retina) voz ou caligrafia. No caso de organizações – ou pessoa jurídica –, essas informações ainda necessitam da associação com a entidade por meio de um contrato e de uma procuração que estabeleça a representação por uma pessoa física.

TEMA 2 – MONITORAMENTO DE TRÁFEGO

Um importante serviço realizado pela segurança de rede é a monitoração das informações que trafegam por ela com o propósito de fazer a classificação e a filtragem de conteúdo. As organizações fazem uso de *hardware*, *software* ou ambos – um *appliance*[1] – para monitorar o tráfego e filtrar os conteúdos. Isso permite o acesso somente àqueles que estão dentro das limitações impostas e evita transmissão e acesso não autorizado às informações críticas.

De acordo com Baltzan e Phillips (2012), as empresas "podem usar as tecnologias de filtragem de conteúdo para filtrar mensagens de e-mails, e evitar a transmissão daquelas que contenham informações confidenciais, seja de forma intencional ou acidental". Esse serviço tem por objetivo adicional evitar a troca de documentos e arquivos que contenham vírus – sendo isso bastante comum em e-mails, tanto naqueles de uso pessoal quanto nos de uso corporativo – e também detectar as comunicações invasivas, falsificadas e não solicitadas: o *spam*.

As redes sociais, os aplicativos de mensagens instantâneas e os dispositivos móveis de uso pessoal são fatores constantes de preocupação nesse sentido. O vazamento de informações e o uso indevido da internet pode arruinar estratégias comerciais, um negócio e mesmo a empresa como um todo. A monitoração do tráfego é algo complexo do ponto de vista tecnológico, uma vez que pode se transformar em gargalo das comunicações; por isso, requer muito cuidado no que se refere à legislação e às relações interpessoais e de trabalho: é muito fácil transpor a tênue linha que separa o controle legal da invasão de privacidade, e o uso indevido das informações obtidas com o monitoramento pode

[1] Um *appliance* é um dispositivo de *hardware* diferenciado e dedicado com um *software* integrado, projetado de modo a fornecer um recurso ou um serviço específico, dedicado.

ser mais catastrófico do que aquilo que se pretende combater.

Os responsáveis pelas – ou com acesso às – ações de monitoramento devem estar sujeitos a regras específicas e rígidas também quanto ao acesso aos mecanismos de monitoramento e controle e às informações por eles geradas, pois trata-se, por natureza, de informações confidenciais e sensíveis.

2.1 Verificação de endereços e de conteúdo

Uma das defesas mais comuns para a comunicação segura e para a prevenção der problemas com a segurança em uma rede é o ***firewall***. De acordo com Baltzan e Phillips (2012), "um firewall é um hardware e/ou software que visa proteger uma rede por meio da análise das informações que entram e saem dessa rede". O *firewall* analisa cada mensagem interceptada – o tráfego da rede –, e só autoriza a sua passagem quando ela não representa riscos, com base em determinados padrões ou marcações específicas.

Firewalls também podem detectar mensagens decorrentes do uso indevido da internet, por exemplo. Em geral, os *firewalls* são instalados na borda da rede interna, entre esta e a rede externa, ou a Internet. Porém, podem ser instalados em perímetros específicos, com vistas a proteger áreas, servidores, banco de dados ou conjuntos de recursos específicos. Também é comum a instalação de *firewalls* em estações de trabalho. Lembre-se: eles são de uso pessoal.

2.2 Detecção e resposta às violações

Para garantir a segurança da informação e de suas comunicações, as organizações podem lançar mão de tecnologias de detecção e resposta aos incidentes. Esses serviços são reativos e sua missão é identificar quando as demais técnicas de prevenção e resistência, tais como filtragem, criptografia e os *firewalls*, falham, ou seja, se há violação de segurança.

O *intrusion detection system* (**IDS**), ou sistema de detecção de intrusão, é o recurso responsável por esse serviço. Trata-se da ferramenta responsável por identificar e alertar os administradores quanto a acessos não autorizados, uso indevido, tentativas ou ataques à rede de dados da organização. O IDS atua como um *sniffer*, capturando e analisando informações da rede e buscando identificar evidências de uma tentativa ou de um ataque em andamento. O IDS pode (e deve) atuar de forma integrada com o *firewall* e outros dispositivos de defesa, interagindo

e ajustando as regras destes de forma dinâmica à medida que são identificadas as anormalidades.

Da mesma forma, o *intrusion prevention system* (**IPS**), ou sistema de prevenção de intrusão, é um sistema que monitora uma rede em busca de atividades maliciosas, como ameaças de segurança ou violações de políticas. A principal função de um IPS é identificar atividades suspeitas e, em seguida, registrar informações, tentar bloquear a atividade e, finalmente, relatá-las. Os sistemas de prevenção de intrusão também são conhecidos como *intrusion detection and prevention systems* (IDPS), ou sistemas de detecção e prevenção de intrusão.

Tal qual o IDS, um IPS também pode ser implementado como um dispositivo de *hardware* ou *software*. Idealmente (ou teoricamente), o IPS é baseado em um princípio simples: o tráfego que entra na rede não é confiável, e o tráfego que sai da rede é confiável. Os IPSs são basicamente extensões dos IDSs. A principal diferença está no fato de que, diferentemente do que ocorre em IDSs, os IPSs são capazes de bloquear ou impedir ativamente as intrusões detectadas. Por exemplo, um IPS pode eliminar pacotes maliciosos, bloqueando o tráfego de um endereço IP ofensivo etc.

Outro tipo bastante comum de serviço de detecção e resposta é oferecido por um *software* **antivírus**. A contaminação de um computador por vírus pode colocar em risco toda uma rede e mesmo toda a operação de uma empresa. Geralmente, os vírus não se restringem a contaminar um único computador, mas seu propósito é espalhar-se ao máximo. Os criadores de vírus fazem de tudo para que seus programas maliciosos ganhem acesso a diversos computadores, de preferência com a colaboração ou por meio de descuido dos demais usuários. O antivírus é a ferramenta mais adequada para enfrentar essa ameaça.

A primeira linha de defesa da informação é aquela mais próxima de quem a produz: a pessoa, ou o usuário. Também é necessário que haja uma comunicação segura entre as pessoas, a qual evite que eventuais problemas se propaguem por meio dela, providenciada por um serviço da tecnologia. E o antivírus cumpre parte desse papel, buscando proteger o usuário e seu computador. Por meio dessa proteção, ele evita que ameaças se instalem em um computador ou dispositivo e, mesmo que isso venha a acontecer, impede que se propaguem pela rede.

TEMA 3 – REDES PRIVADAS

Uma rede privada é aquela que atende os interesses de uma entidade, de uma organização. Geralmente, essa rede está circunscrita aos limites físicos da organização; porém, com o avanço tecnológico e a globalização, é cada vez mais comum que esse limite físico seja ultrapassado e a rede se estenda por todo o planeta. Nesse caso, dois termos são usados para definir o ambiente de rede: **intranet** e **extranet**.

3.1 Intranet e extranet

Os conceitos de intranet e extranet foram inicialmente definidos em função do espaço físico e das instalações e construções da organização. Porém, com o passar do tempo e a incorporação de novas tecnologias, esse limite deixou de ser claro. Forouzan (2010) define esses termos da seguinte forma: a **intranet,**

> É uma rede local (LAN) privada que usa o modelo internet. Entretanto, o acesso à rede é limitado aos usuários dentro da organização. A rede usa programas de aplicação e protocolos típicos da Internet, como HTTP, e pode ter servidores, servidores de impressão e servidores de arquivos web (Forouzan, 2010).

Já a **extranet**

> É semelhante à Intranet, porém alguns recursos podem ser acessados por grupos de usuários específicos fora dos limites físicos da organização sob o controle do administrador de redes. Por exemplo, uma organização pode permitir que clientes autorizados acessem especificações, disponibilidade e compra de produtos on-line. Uma universidade ou uma faculdade pode permitir que alunos a distância acessem computadores após a verificação de senhas (Forouzan, 2010).

Como sabemos, uma rede que usa o modelo de internet identifica seus elementos por meio de endereços IP. No caso de uma rede privada, a rede “pode solicitar um conjunto de endereços das autoridades internet e usá-los sem estar conectada à internet” (Forouzan, 2010). Isso permite que se, no futuro, a organização decidir se conectar à internet, poderá fazê-lo com relativa facilidade. Com o uso de endereços do tipo IPv6, essa possibilidade passou a ser considerada por diversas corporações. Entretanto, há uma desvantagem: o espaço de endereços IP da rede privada é subutilizado enquanto a rede está

isolada da Internet.

Uma outra possibilidade é a rede privada “[...] usar qualquer conjunto de endereços sem registrar-se com as autoridades da internet. Como é isolada, os endereços não têm de ser exclusivos” (Forouzan,2010). Essa estratégia apresenta um risco considerável, pois os usuários poderiam confundir endereços locais como parte da internet global, ou vice-versa. Para evitar esses problemas, as autoridades da Internet reservaram conjuntos específicos de endereços que qualquer organização pode usar, sendo desnecessária a solicitação de registro desses endereços.

Esses endereços privados são únicos na rede da organização, mas não exclusivos: outras organizações farão uso deles em suas próprias redes privadas. Entretanto, nenhum roteador encaminhará para a Internet um pacote que tenha um desses endereços como endereço de destino. A Tabela 1 apresenta esses endereços. Convém destacar que essa distribuição foi realizada com base em *requests for coment* (**RFCs**, ou pedidos de comentário) da Internet Engineering Task Force (**IETF**), tornando-se assim um padrão mundial.

Tabela 1 – Endereços de rede privada

Faixa	Endereços Possíveis	Classe	CIDR	RFC
10.0.0.0 a 10.255.255.255	16.777.216	A	10.0.0.0/8	1597 (antiga) e 1918
169.254.0.0 a 169.254.255.255	65.536	B	169.254.0.0/16	3330 e 3927
172.16.0.0 a 172.31.255.255	1.048.576	B	172.16.0.0/12	1597 (antiga) e 1918
192.168.0.0 a 192.168.255.255	65.536	C	192.168.0.0/16	1597 (antiga) e 1918

Fonte: Adaptado de IETF, 2018.

3.2 VPN (*virtual private network*)

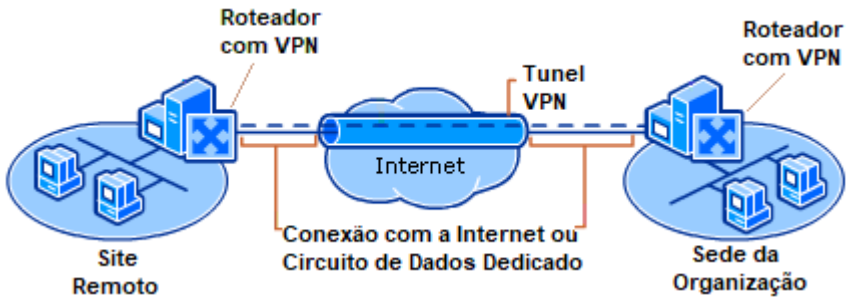
Existem diferentes combinações de redes para atender as necessidades das organizações, cada uma com requisitos técnicos próprios e níveis distintos de privacidade: privadas, híbridas e privadas virtuais. As redes privadas, como já

tratamos anteriormente, são usadas no âmbito da organização. Uma grande organização composta de várias instalações em diferentes pontos geográficos pode lançar mão de uma internet privada. “As LANs [*local area networks*] em locais diferentes podem ser interligadas por meio de roteadores e circuitos de dados dedicados. Em outras palavras, uma internet pode ser formada por LANs e WANs [*wide area networks*] privadas” (Forouzan, 2010).

Entretanto, essas organizações necessitam trocar informações com outras, o que requer a conexão de sua internet à rede global, a Internet, constituindo assim uma rede híbrida: parte privada e parte pública. Essa estratégia é interessante, pois permite que se utilize a Internet – uma rede pública – para conectar diversas instalações ou *sites* da organização. Isso diminui os custos em relação à uma internet privada. De acordo com Forouzan (2010), as WANs privadas são caras. Para conectar instalações em locais diferentes, uma organização precisaria usar circuitos de dados dedicados cujo custo mensal é elevado (Forouzan, 2010).

Para usar uma rede pública e garantir a segurança e a privacidade, a organização utiliza uma *virtual private network* (VPN, ou rede privada virtual), que é financeiramente mais vantajosa e tecnicamente mais fácil de implantar, além de ser mais flexível. Em uma VPN, a rede física é pública, embora virtualmente privada. A Figura 5 mostra uma conexão de rede privada virtual.

Figura 5 – Uma rede privada virtual



Fonte: Adaptado de Tanenbaum, 2011.

Uma VPN fornece conexão entre duas ou mais redes privadas por meio de uma rede pública, como a Internet, por exemplo. Os computadores conectados por VPN comunicam-se por meio de uma rede pública ou compartilhada, porém, o fazem como se estivessem conectados diretamente à rede privada, usando funcionalidades como as políticas de segurança e gerenciamento da rede privada. As conexões virtuais ponto a ponto são estabelecidas com o uso de conexões

dedicadas e criptografia. O acesso aos recursos é feito do mesmo modo que em uma rede interna ou privada, e o usuário não sente nenhuma diferença, exceto com relação a questões de desempenho.

A VPN criptografa o conteúdo do pacote IP por meio de um protocolo de encapsulamento, para então transportá-lo em um pacote não criptografado no trajeto da rede pública. Os dispositivos finais do túnel VPN criptografam e descriptografam os pacotes IP. Há vários benefícios em usar uma VPN e permitir que usuários remotos acessem os serviços da rede privada, entre eles:

- segurança: por usar uma rede pública para conexão e comunicação, a segurança é uma grande preocupação, porém, muito bem tratada na VPN com o uso de protocolos avançados de criptografia e autenticação;
- redução de custos: a criação de túneis VPN para comunicação com outros *sites* da organização é uma opção mais econômica do que a utilização de circuitos de dados dedicados;
- flexibilidade e escalabilidade: além de possibilitar a conexão de *sites*, uma VPN pode ser usada por colaboradores em viagem, por exemplo, ou em eventos ou instalações provisórias.

Além disso, uma VPN atende aos principais requisitos de segurança da informação, como a confidencialidade, a autenticação, a integridade e o não repúdio.

TEMA 4 – *MALWARE*

Um dos maiores riscos aos quais as redes de computadores e os recursos computacionais estão expostos são os *softwares* maliciosos, ou *malwares* – uma contração de *malicious softwares*. “Software malicioso é um software cuja existência ou execução tem consequências negativas ou involuntárias” (Goodrich; Tamassia, 2012). *Malwares* podem ter origem interna, ou seja, pode ser uma falha deliberadamente provocada ou facilitada por alguém que faz parte da organização e que controla ou constrói o *software*.

4.1 Definição

Segundo Goodrich e Tamassia (2012), no contexto de *malware*, um ataque se refere a uma brecha na segurança criada em um sistema ou *software* por um desenvolvedor. Uma falha desse tipo é especialmente perigosa, pois é provocada

por alguém que deveria ser confiável. Infelizmente, há uma ocorrência frequente desses tipos de ataques. O ataque interno pode ocorrer de diversas maneiras, desde o código estar embutido em um programa ou até mesmo ser inserido posteriormente. De qualquer modo, “o malware embutido pode iniciar a escalação de privilégios, pode causar danos como resultado de algum evento ou ele mesmo pode ser um meio de instalar outro malware” (Goodrich; Tamassia, 2012).

4.2 Defesa

Proteger um sistema ou *software* contra esses tipos de ataques não é uma tarefa muito fácil, visto que eles são organizados por uma pessoa de dentro da organização e que conhece o sistema ou *software*. Goodrich e Tamassia (2012) destacam algumas possíveis defesas:

- impedir pontos únicos de falha, como evitar que uma única pessoa administre os *backups* ou gerencie recursos críticos;
- usar inspeções de código, de modo que cada programador apresente seu código para outro programador, linha por linha. Assim, este pode ajudar a identificar omissões, desvios ou erros;
- usar ferramentas de versionamento, arquivamento e documentação. Geradores automáticos de documentação e ferramentas de arquivamento de *software* podem trazer o benefício de revelar ou documentar ataques internos, além de ajudar a produzir *software* de boa qualidade;
- limitar a autoridade e as permissões. Usar o princípio do menor privilégio, que estabelece que cada programa ou usuário do sistema receba o menor privilégio requerido para fazer o seu trabalho de modo eficiente;
- usar sistemas críticos fisicamente seguros. Sistemas importantes devem ser mantidos em áreas com acesso protegido;
- monitorar o comportamento da equipe e dos indivíduos;
- controlar as atualizações e as instalações de *software*. Limitar as instalações de *software* àqueles que tenham sido extensivamente examinados e provenham de fontes confiáveis.

4.3 Tipos

As ameaças causadas intencionalmente por agentes humanos – os ataques comandados por indivíduos mal-intencionados e com maus propósitos

que, explorando fraquezas, falhas de projeto ou falta de proteção adequada – interferem no funcionamento dos sistemas e provocam danos às informações ou aos serviços providos por eles. Boa parte desses ataques fazem uso de *softwares* maliciosos para alcançar seus objetivos. Esse tipo de *software* recebe diversas denominações em função de suas características e propósitos, como as estabelecidas por Lapolla, Martinelli e Sgandurra (2013), a saber:

- vírus: uma sequência de código cuja finalidade é reproduzir-se em áreas importantes dos dispositivos de armazenamento (unidades de disco, *pendrives*, *memory cards* etc.) ou anexar-se a programas e arquivos;
- *worms* (vermes): programas que se propagam por meio de cópias de si próprios para os dispositivos de armazenamento por meio das redes, sem, a princípio, contaminar programas e arquivos;
- *trojans* (cavalos de Tróia): uma forma de *software* com alguma funcionalidade específica e interessante – como recuperação de senhas de programas ou arquivos protegidos (*crackers*), conversão de formatos de arquivos de dados ou geração de números de licença para *software* licenciado – que tem em seu código funcionalidades maliciosas com o intuito de explorar as vulnerabilidades;
- *rootkits*: códigos maliciosos que normalmente infectam o sistema operacional com o intuito de ocultar operações que demonstram a contaminação – por vírus ou cavalos de Tróia, por exemplo –, desabilitar ou superar uma contramedida ou defesa – como antivírus ou *firewalls* – e também permitir que um usuário mal-intencionado tenha acesso ou mesmo controle do dispositivo infectado;
- *botnets* (de *ro**bot net**work*): agentes de *software* autônomos e automáticos cuja finalidade é colocar os dispositivos contaminados a serviço de um controlador, formando assim uma rede de zumbis prontos para executar tarefas como envio de *spam* ou ataques de DoS ou DDoS;
- *spywares*: programas que recolhem informações fornecidas pelo usuário, e sobre o uso que este faz de seu equipamento, e as transmite a uma entidade externa, geralmente na Internet. Essas informações são posteriormente usadas para burlar sistemas de autenticação e verificação de identidade ou como base para trabalhos de engenharia social com o intuito de possibilitar operações fraudulentas baseadas em falsidade ideológica;

- *exploits*: programas ou trechos de código que buscam explorar vulnerabilidades ou falhas de ambientes computacionais – geralmente dos sistemas operacionais – recentemente descobertas para conseguir acesso privilegiado aos sistemas;
- *risktools* ou *riskware*: programas ou funcionalidades de programas cujo intuito é avaliar vulnerabilidades do ambiente computacional para, então, comunicá-las à sua fonte, possibilitando assim a exploração dessas vulnerabilidades de forma mais efetiva. Seu modo de atuação assemelha-se ao dos *trojans*, com a diferença de que geralmente oferecem um apelo à elevação da segurança do ambiente, promovendo falsas notificações de ameaças ou falhas como reforço para a sua instalação;
- *adwares*: programas ou funcionalidades de programas (normalmente *shareware*) que apresentam anúncios de versões mais completas ou outros produtos do fabricante. Muitas vezes, obtêm informações sobre o usuário e o ambiente computacional e as enviam sem o consentimento ou conhecimento daquele para uma base de dados remota, com o intuito de avaliar o perfil e o possível interesse do usuário.

De uma maneira geral, a expressão **vírus de computador** é usado pela mídia e pelo público como sinônimo de ***malware***, representando qualquer *software*, programa ou agente que interfira no funcionamento de um *software* com o propósito de modificar seu funcionamento e obter algum proveito a partir dessa modificação.

TEMA 5 – INVASÃO DE PRIVACIDADE

Um tipo especial de *malware* vem aumentando em muito os incidentes de segurança da informação: aquele que promove a invasão de privacidade e a coleta de informações valiosas dos usuários. Esse *software* pode ser instalado a partir de *sites* não seguros, por um vírus, ou por e-mails. “O software invade o computador do usuário para operar em segundo plano realizando ações de invasão de privacidade ou para obter informação sensível ou valiosa” (Goodrich; Tamassia, 2012).

O objetivo desse *malware* pode ser meramente comercial, como registrar pesquisas sobre certo produto ou preços de passagens aéreas nas buscas pela internet. Isso faz com que vários anúncios (*pop-ups*) apareçam em seu

navegador. Porém o *malware* pode estar orientado a roubar informações sobre o usuário para uso criminoso ou para repassar a outrem. Em outros casos, as violações de privacidade realizadas por um *malware* podem ser por mera curiosidade, ou uma etapa prévia de um ataque mais elaborado. Os principais *malwares* de invasão de privacidade são abordados nos itens a seguir.

5.1 *Adware*

O adware é um tipo de *software* que exibe anúncios durante a navegação na internet sem a solicitação ou a autorização do usuário. Alguns *softwares* têm anúncios embutidos que fazem parte do pacote, mas é importante frisar que o *adware* malicioso exibe anúncios sem consentimento. E a partir da instalação desse *software* podem ser identificadas condições para novos ataques.

5.2 *Spyware*

De acordo com Goodrich e Tamassia (2012), “assim como o *adware*, o *spyware* é instalado no computador sem o conhecimento ou o consentimento de seu usuário e coleta informação do usuário, do ambiente computacional ou do uso do computador”. Nesse caso, a invasão de privacidade é camuflada e muito mais perigosa, pois, geralmente, sua execução continua mesmo após o computador ter sido reinicializado; uma infecção como essa, muitas vezes, envolve a modificação do sistema operacional, de modo que o *software spyware* seja sempre executado como parte da sequência de inicialização do sistema.

Para o usuário leigo, a indicação de que o computador possa estar infectado vem da percepção de lentidão ou respostas aleatórias de *softwares* ou comandos. Porém, até que seja percebido, o *spyware* já pode ter alcançado seu objetivo. “Uma infecção spyware pode mesmo chegar à remoção de adware e spyware concorrentes, assim como dificultar ao usuário perceber que esse software indesejado está executando” (Goodrich; Tamassia, 2012).

REFERÊNCIAS

ABNT. **Coletânea de normas técnicas de segurança da informação**. Rio de Janeiro: ABNT, 2013.

BALTZAN, P.; PHILLIPS, A. **Sistemas de informação**: série A. São Paulo: McGraw-Hill, 2012.

FONTES, E. **Segurança da informação**. São Paulo: Saraiva, 2001.

KIM, D. **Fundamentos de segurança de sistemas de informação**. Rio de Janeiro: LTC, 2014.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw Hill, 2008.

GOODRICH, M. T.; TAMASSIA, R. **Introdução à segurança de computadores**. São Paulo: Bookman, 2012.

INTERNET ENGINEERING TASK FORCE (IETF). **Address Allocation for Private Internets**. Disponível em: <https://tools.ietf.org>. Acesso em: 21 dez. 2018.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **ICP-Brasil**. Disponível em: <https://www.iti.gov.br/icp-brasil>. Acesso em: 21 dez. 2018.

LA POLLA, M., MARTINELLI, F.; SGANDURRA, D. A survey on security for mobile devices. **IEEE Communications Surveys & Tutorials**, v. 15, n. 1, p. 446-471, 2013.

STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

TANENBAUM, A. S. **Redes de computadores**. 5. ed. São Paulo: Pearson Prentice Hall, 2011.