Fundamentos de administração e segurança em rede de computadores

Prof. Sérgio dos Santos Cardoso Silva

Descrição

Princípios teóricos de segurança e administração de redes de computadores. Ferramentas para o alcance de um nível adequado de segurança e gerência de redes.

Propósito

Conhecer os riscos da operação e da utilização de redes de computadores, bem como os protocolos de segurança e os tipos de ferramentas adequadas para a administração e o gerenciamento de tais processos.

Objetivos

Módulo 1

Riscos de segurança nas redes de computadores

Identificar os riscos de segurança nas redes de computadores.

Módulo 2

Softwares e equipamentos para diminuição dos riscos

Selecionar softwares e tipos de equipamentos adequados para a diminuição dos riscos de segurança nas redes.

Módulo 3

Arquitetura de gerenciamento de redes

Reconhecer a arquitetura de gerenciamento de redes.

Introdução

A internet é uma rede comercial que pode ser utilizada por qualquer pessoa ou empresa em todos os cantos do mundo. Com isso, possíveis problemas de segurança afloram.

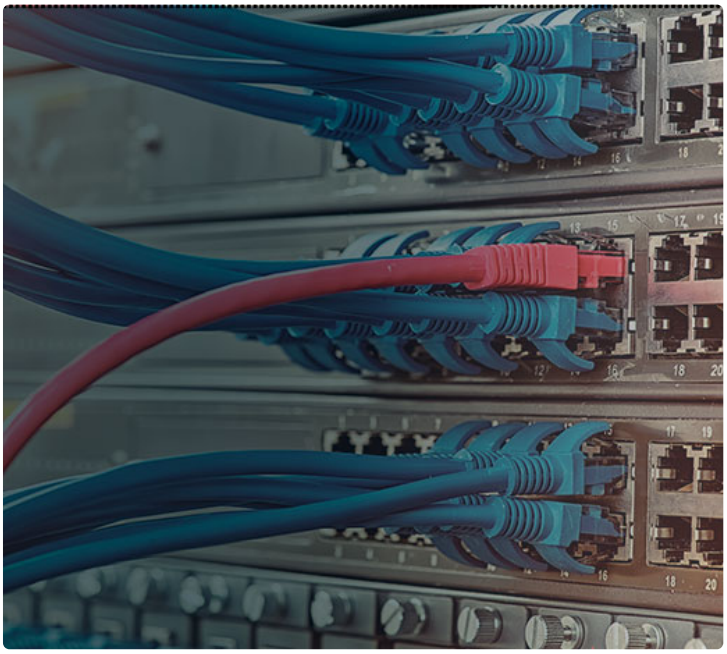
Pessoas mal-intencionadas utilizam essa rede para realizar atividades maliciosas, como roubo de informações e de identidade, paralisação de serviços etc.

Por isso, o tópico segurança destaca-se atualmente como uma das grandes preocupações dos administradores de redes. Garantir a segurança na comunicação de dados passou a ser uma das questões cruciais na utilização da internet.

É fundamental que tanto usuários quanto profissionais de tecnologia da informação (TI) tenham conhecimento dos riscos

no uso da rede e saibam identificar ferramentas capazes de minimizá-los.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



1 - Riscos de segurança nas redes de computadores

Ao final deste módulo, você será capaz de identificar os riscos de segurança nas redes de computadores.

Definições

Para identificar os riscos relacionados ao uso de uma rede de computadores, é importante conhecer algumas definições. Por conta disso, iremos nos basear na norma ABNT NBR ISO IEC 27001:2013, reconhecida mundialmente como uma referência na área de segurança. Essa norma apresenta as seguintes definições:

Conceitos de segurança da informação

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Ameaça

Causa potencial de um incidente indesejado que pode resultar em danos a um sistema ou organização.

Ataque

Tudo aquilo que tenta destruir, expor, alterar, desativar, roubar, obter acesso não autorizado ou fazer uso não autorizado de um ativo.

Ativo

Qualquer coisa que tenha valor para uma pessoa ou organização. Exemplo: os dados do cartão de crédito, um projeto de uma empresa, um equipamento e até mesmo os colaboradores de uma empresa podem ser definidos como ativos humanos.

Como é possível perceber nessas definições, a **ameaça** está relacionada a algo que pode comprometer a segurança, enquanto o **ataque** é a ação efetiva contra determinado ativo.

> **Um incidente de segurança ocorre quando uma ameaça se concretiza e causa um dano a um ativo.**

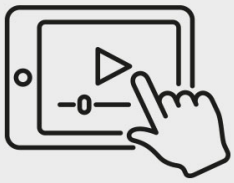
Se uma ameaça se concretizou e causou um dano, isso significa que alguma propriedade da segurança foi comprometida.

Três propriedades são tratadas como os pilares da segurança: Confidencialidade, Integridade e Disponibilidade (CID).

Além delas, outras propriedades também são importantes no contexto de segurança. A norma ABNT NBR ISO IEC 27001:2013 destaca as seguintes:

Propriedades da segurança da informação

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Confidencialidade

Propriedade cuja informação não está disponível para pessoas, entidades ou processos não autorizados. A confidencialidade está relacionada ao sigilo dos dados. Somente entes autorizados podem acessá-los.

Integridade

Propriedade que protege a exatidão e a completeza de ativos. Trata-se da indicação de que o dado não foi adulterado. Exemplo: um ativo permanece intacto após ser armazenado ou transportado.

Disponibilidade

Propriedade de tornar o dado acessível e utilizável sob demanda por fontes autorizadas. Se uma pessoa ou um processo autorizado quiser acessar um dado ou equipamento, ele estará em funcionamento.

Autenticidade

Propriedade que assegura a veracidade do emissor e do receptor das informações que são trocadas. A autenticidade assegura que quem está usando ou enviando a informação é realmente determinada pessoa ou processo. Em outras palavras, garante a identidade.

Não repúdio ou irretratabilidade

Propriedade muito importante para fins jurídicos. Trata-se da garantia de que o autor de uma informação não pode negar falsamente a autoria dela. Desse modo, se uma pessoa praticou determinada ação ou atividade, ela não terá como negá-la. O não repúdio é alcançado quando a integridade e a autenticidade são garantidas.

Confiabilidade

Propriedade da garantia de que um sistema vai se comportar segundo o esperado e projetado. Exemplo: se determinado equipamento foi projetado para realizar uma operação matemática, esse cálculo será realizado corretamente.

Legalidade

Propriedade relacionada com o embasamento legal, ou seja, ela afere se as ações tomadas têm o suporte de alguma legislação ou norma. No caso do Brasil, podemos citar o Marco Civil da

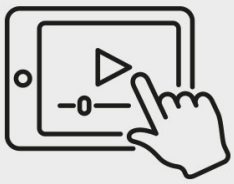
Internet, a Lei Geral de Proteção de Dados (LGPD) e o conjunto de normas 27.000 da ABNT.

Os mecanismos de proteção se relacionam a práticas, procedimentos ou mecanismos capazes de proteger os ativos contra as ameaças, reduzindo ou eliminando vulnerabilidades. Além disso, eles evitam que uma dessas propriedades sejam comprometidas.

Tipos de ataques

Veja as principais características dos ataques ativos e passivos.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Para haver a identificação dos riscos, será necessário entender e classificar os tipos de ataques que podem ser realizados contra uma rede de computadores.

Interligadas, as tabelas a seguir apresentam os critérios de classificação desses tipos de ataques e as suas descrições:

ATAQUES	DESCRIÇÃO	TIPOS
ATIVOS	Tentam alterar os recursos do sistema ou afetar a sua operação.	Ataques de interrupção
		Ataques de modificação
		Ataques de fabricação ou personificação
		Ataques de repetição

ATAQUES	DESCRIÇÃO	TIPOS
PASSIVOS	Tentam descobrir ou utilizar as informações do sistema sem o objetivo de afetar seus recursos.	Ataques de interceptação

Classificação primária dos tipos de ataques.

CRITÉRIOS	TIPOS	DESCRIÇÃO
PONTO DE INICIAÇÃO	Ataques internos (inside attack)	Realizados dent da própria rede. atacante e a víti estão na mesm rede (doméstica corporativa).
	Ataques externos (outside attack)	Feitos a partir d um ponto exterr rede da vítima.
METODO DE ENTREGA	Ataques diretos	O atacante, sem ajuda de terceir realiza uma açã diretamente cor a vitima.
	Ataques indiretos	O atacante emprega terceir ou seja, outros usuários da red para que o ataq seja realizado.
OBJETIVO	Ataques de interceptação	Buscam obter informações qu trafegam a rede atacando a confidencialidad

CRITÉRIOS	TIPOS	DESCRIÇÃO
	Ataques de interrupção	Seu objetivo é indisponibilizar ou mais serviço de rede sobrecarregand os sistemas, as redes ou simplesmente desligando o equipamento.
	Ataques de modificação	Ocorrem quand um atacante ter acesso não autorizado a um sistema ou a um rede e modifica conteúdo das informações ou configurações d um sistema.
	Ataques de fabricação ou personificação	Buscam quebra principalmente, autenticidade de um serviço, um dispositivo ou d uma rede.
	Ataques de repetição	Uma entidade maliciosa intercepta e rep uma transmissã de dados válida que trafega atra de uma rede par produzir um efe não autorizado, como a repetiçã de pedidos de u item ou o proce de *login* em um ambiente.

Classificação primária dos tipos de ataques.

Terceiros

O uso de terceiros pode amplificar o poder de ataque ao, por exemplo, aumentar o volume de tráfego contra a vítima em um ataque contra a disponibilidade.

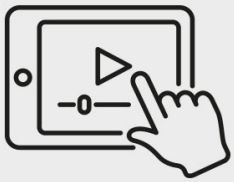
Etapas de um ataque

Precisamos dividir um ataque em **sete etapas** para poder analisá-lo de forma mais criteriosa:

- Reconhecimento
- Armamento (*weaponization*)
- Entrega (*delivery*)
- Exploração
- Instalação
- Comando e controle
- Ações no objetivo

Etapas de um ataque

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Os atacantes passam a ter mais privilégios no alvo à medida que avançam nas etapas. Portanto, pelo lado da defesa, o objetivo é pará-los o mais cedo possível para diminuir o dano causado.

Vejamos a seguir cada etapa de um ataque:

Reconhecimento

Na primeira etapa, o ator da ameaça realiza uma pesquisa para coletar informações sobre o local a ser atacado. Trata-se de uma fase preparatória na qual o atacante procura reunir o máximo de informações sobre o alvo antes de lançar um ataque ou analisar se vale a pena executá-lo. As informações podem ser obtidas por meio de diversas fontes: sites, dispositivos de rede voltados para o público, artigos de notícias, anais de conferências, meios de comunicação social.

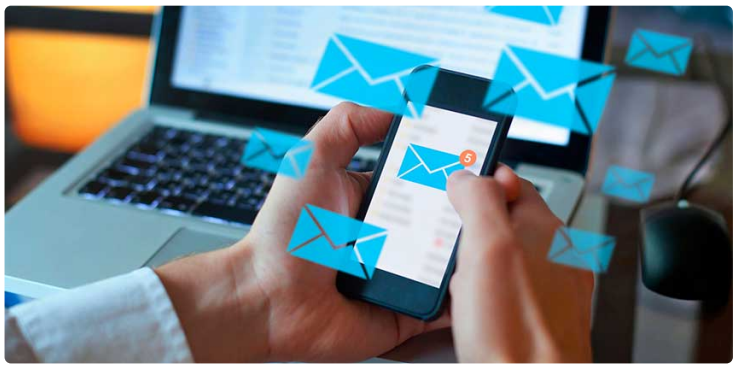
Qualquer local público é capaz de ajudar a determinar o que, onde e como o ataque pode ser realizado. O atacante escolhe alvos negligenciados ou desprotegidos, pois eles possuem a maior probabilidade de serem penetrados e comprometidos.

Armamento (*weaponization*)

Após a coleta de informações, o atacante seleciona uma arma a fim de explorar as vulnerabilidades dos sistemas. É comum utilizar a expressão *exploits* para essas armas, que podem estar disponíveis em sites na internet ou ser desenvolvidas especificamente para determinado ataque.

O desenvolvimento de uma arma própria dificulta a detecção pelos mecanismos de defesa. Essas armas próprias são chamadas de *zero-day attack*.

Após o emprego da ferramenta de ataque, espera-se que o atacante tenha conseguido alcançar seu objetivo: obter acesso à rede ou ao sistema que será atacado.



Entrega (*delivery*)

Nesta fase, o atacante entrega a arma desenvolvida para o alvo. Para essa entrega, podem ser utilizados diversos mecanismos. Eis alguns exemplos: mensagens de correio eletrônico (e-mail), mídias USB, websites falsos ou infectados, interação nas redes sociais.

O atacante pode usar um método ou uma combinação de métodos para aumentar a chance de entrega do exploit. Seu objetivo é fazer com que a arma pareça algo inocente e válido, pois ludibria o usuário e permite que ela seja entregue.

Uma prática comum para essa entrega é o uso de *phishing*. Tipicamente, são enviados e-mails com algum assunto aparentemente de interesse da vítima. Nesta mensagem, existe um link ou um anexo malicioso que serve de meio de entrega da arma na máquina alvo.

Exploração

A etapa de exploração ocorre quando o atacante, após entregar a arma, explora alguma vulnerabilidade (conhecida ou não) na máquina infectada em busca de outros alvos dentro da rede de destino. As vulnerabilidades que não são publicamente conhecidas são chamadas de *zero-day*.

No caso do emprego de *phishing*, a exploração ocorre quando o e-mail recebido é aberto e o usuário clica no link ou abre o anexo, instalando um software malicioso que infecta a sua máquina. Isso permite o controle dela por parte do autor do ataque.

A partir desse momento, o atacante obtém acesso ao alvo, podendo obter as informações e os sistemas disponíveis dentro da rede atacada. Os alvos de exploração mais comuns são aplicativos, vulnerabilidades do sistema operacional e pessoal.

Instalação

A partir da exploração da máquina realizada na fase anterior, o atacante busca instalar algum tipo de software que permita a manutenção do acesso à máquina ou à rede em um momento posterior.

Para essa finalidade, é instalado no sistema alvo um *Remote Access Trojan* (RAT). Conhecido também como *backdoor*, o RAT permite ao atacante obter o controle sobre o sistema infectado.

Pelo lado do atacante, é importante que o acesso remoto não alerte nenhum sistema de proteção e permaneça ativo mesmo após varreduras por sistemas de segurança da rede de destino.

Comando e controle

A partir do momento em que um RAT (*backdoor*) é instalado no sistema alvo, o atacante passa a ter um canal de comunicação com o software instalado no alvo.

Denominado **comando e controle**, tal canal possibilita o envio de comandos para realizar ataques na própria rede local ou para atacar a rede de terceiros, caracterizando, assim, um ataque indireto

Ações no objetivo

Quando o atacante chega à última etapa, isso é um indício de que o objetivo original foi alcançado. A partir de agora, ele pode roubar informações, utilizar o alvo para realizar ataques de negação de serviço, envio de spam, manipulação de pesquisas ou jogos on-line, entre outras atividades.

Nesse ponto, o agente de ameaças já está profundamente enraizado nos sistemas da organização, escondendo seus movimentos e cobrindo seus rastros.

É extremamente difícil remover o agente de ameaças da rede quando ele já chegou a esta fase.

Vamos analisar a noticia a seguir:

> “
>
> Brasil sofreu 15 bilhões de ataques cibernéticos em apenas três meses. A questão não é mais ‘o que podemos fazer se sofrermos um ataque cibernético?’, mas, sim, ‘o que podemos fazer quando sofremos um ataque cibernético?
>
> **(TECMUNDO, 2019)**

Ao analisarmos o caso, percebemos a importância da análise dos riscos relacionados ao uso de uma rede de computadores sem a devida proteção.

Pesquise outras situações similares e procure perceber a intervenção dos mecanismos de proteção nesses casos.

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

Os ataques podem ser classificados de diversas formas: ativo ou passivo, interno ou externo, direto ou indireto. Os passivos são os de interceptação; os ativos, os de modificação, interrupção, personificação ou repetição. Considere que você esteja realizando a compra online de uma caneta. Ao verificar o extrato de sua conta, percebe que havia duas cobranças do mesmo valor. Esse tipo de evento pode ser associado ao ataque de

A modificação, porque o atacante modificou a transação, permitindo que a operação fosse executada duas vezes.

B repetição, pois o atacante capturou os pacotes com as informações de pagamento e os enviou novamente para a cobrança no banco.

C interceptação, uma vez que o atacante monitorou a transação e, percebendo a troca de informações financeiras, repetiu a operação.

D personificação, já que o atacante assumiu a identidade da loja on-line, repetindo a operação financeira.

E interceptação, pois o atacante modificou os dados do carrinho de compras inserindo duas unidades.

Parabéns! A alternativa B está correta.

O ataque de repetição permitiu que fosse debitado duas vezes o mesmo valor de sua conta. Como o atacante capturou os pacotes que realizam a transação financeira, ele pôde modificar a conta de destino e – considerando que os dados da transação estivessem presentes no pacote – receber o valor cobrado. Esse mesmo ataque pode ser utilizado quando um atacante captura pacotes de autenticação, permitindo o acesso a determinada rede ou sistema.

Questão 2

Uma das grandes ameaças existentes na internet é a chamada APT. Sigla para *Advanced Persisten Threat*, ela se refere a ataques direcionados de organizações a determinadas organizações e empresas.

Imagine que você, após ser convocado para analisar as ações de uma APT, tenha percebido que ela estava enviando e-mails a

determinada empresa com um anexo possivelmente malicioso.

A etapa de ataque identificada está relacionada com:

A conquista, porque a APT obteve acesso a um endereço de e-mail válido da empresa.

B instalação, pois a APT enviou a arma para obter acesso ao alvo.

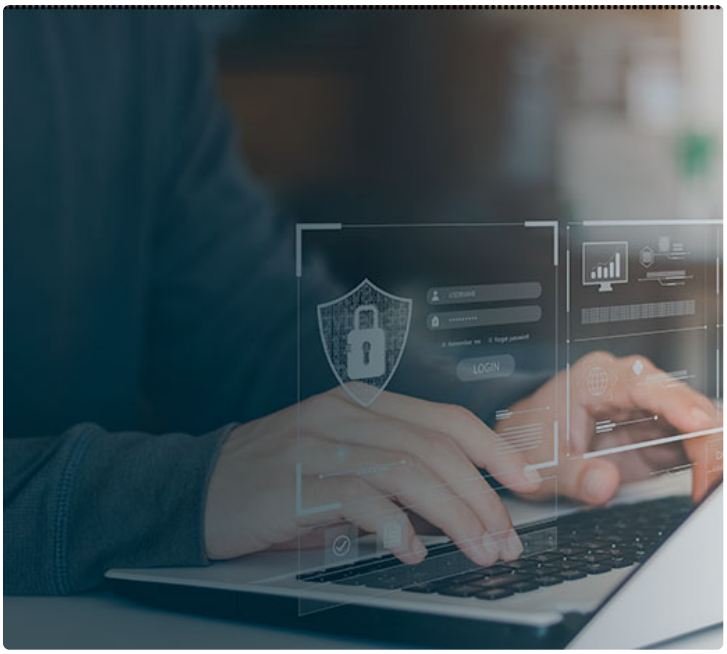
C exploração, uma vez que a APT se aproveitou de uma vulnerabilidade no sistema de e-mail.

D entrega, já que a APT utilizou um meio de entregar a arma a seu alvo.

E comando e controle, porque a APT utiliza do serviço de correio eletrônico para trocar comandos.

Parabéns! A alternativa D está correta.

O entendimento das fases dos ataques é de suma importância na segurança da rede. Quanto mais cedo o ataque for detectado e interrompido, menos danos ele causará, porque o atacante (no caso ilustrado, uma APT) terá tido uma menor penetração na rede e comprometido menos o ambiente.



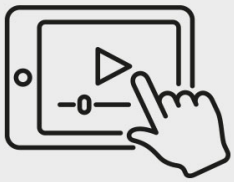
2 - Softwares e equipamentos para diminuição dos riscos

Ao final deste módulo, você será capaz de selecionar softwares e tipos de equipamentos adequados para a diminuição dos riscos de segurança nas redes.

Segurança física

Segurança física x Segurança lógica

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Estar conectado à internet nos expõe a diversos riscos, como roubo de informações e de identidade, adulteração de informações etc. De acordo com a norma ABNT 27001:2013, para minimizar os riscos dessa conexão, é necessário implementar mecanismos de controle a fim de garantir a segurança dela.

Esses mecanismos podem ser divididos em dois tipos:

Mecanismos de controle físicos

Evitam ou dificultam as falhas nos equipamentos e instalações.

Mecanismos de controle lógicos

Evitam ou dificultam as falhas relacionadas aos softwares utilizados.

Vejamos agora a aplicação desses mecanismos na manutenção da segurança de uma conexão.

Segurança física abrange todo ambiente em que os sistemas de informação estão instalados. Seu objetivo principal é garantir que nenhum dano físico ocorra nos equipamentos. Por exemplo: roubo de equipamentos, incêndio, inundação e qualquer ameaça às instalações físicas.

A norma ABNT NBR ISO/IEC 27002:2013 divide a segurança física em dois itens principais:

- **Áreas seguras**: Previnem o acesso físico não autorizado, os danos e as interferências em instalações e informações da organização.
- **Equipamentos**: Impedem perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.

A segurança física envolve outras áreas da Engenharia, como a civil e a elétrica, ao permitir a projeção de prédios com paredes adequadas à proteção dos equipamentos, sistemas de para-raios, aterramento, limpeza da área para evitar incêndios etc.

Alguns exemplos de **mecanismos de controle físicos** podem ser encontrados no emprego de:

Sistemas de refrigeração e de combate a incêndio

Projetados para os equipamentos poderem operar em condições adequadas de temperatura e umidade. Ainda garantem que os casos de incêndio possam ser combatidos o mais rápido possível.

Sala-cofre

Espaço construído com paredes corta-fogo, sistemas de refrigeração e de forma hermética para proteger equipamentos críticos de TI.

Sistemas de energia redundantes

Funcionam como *no-breaks* (*Uninterruptable Power Supply* - UPS) e geradores. Ambos são necessários ao permitirem que, em caso de queda de energia, os equipamentos permaneçam em operação. Isso garante tanto o fornecimento constante de energia quanto a manutenção dela dentro da tensão recomendada.

Preparação do ambiente contra alagamento

No caso de chuvas fortes.

Limpeza da área externa

Para evitar incêndios.

Segurança lógica

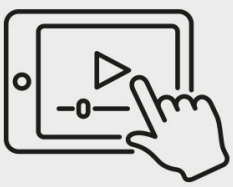
A segurança lógica **envolve o emprego de soluções** baseadas em softwares para garantir a CID. Entre os diversos mecanismos existentes, destacaremos os oito listados a seguir:

1. Autenticação
2. Sistemas de controle de acesso
3. Criptografia
4. Funções de hash
5. Assinatura digital
6. Certificado digital
7. Redes Virtuais Privadas (VPN)
8. Firewall, sistemas de detecção de intrusão e antivírus

Vamos entender agora o funcionamento de cada mecanismo.

Autenticação

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Está relacionada à garantia da propriedade da autenticidade, evitando que terceiros possam fingir ser uma das partes legítimas a fim de

acessar sistemas ou informações não autorizadas.

A autenticação diminui o risco de um ataque de personificação ou fabricação. Para realizá-la, podem ser utilizados os seguintes mecanismos: senhas, controles biométricos, *tokens*, certificados digitais.

O mecanismo escolhido deve se adequar ao objetivo de segurança a ser alcançado. Atualmente, os controles biométricos são considerados os mais eficientes, mas é recomendado que seja utilizada a chamada autenticação de dois fatores.

A autenticação de dois fatores utiliza dois mecanismos para autenticar um usuário, por exemplo, utilizando senha e um código enviado por e-mail.

Exemplo

Digitais, reconhecimento de íris, palma da mão e certificados digitais.

Sistemas de controle de acesso

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Gerenciam os usuários que podem acessar sistemas e redes, **autorizando apenas** o acesso às informações que lhes couberem. Desse modo, a confidencialidade dos dados está garantida.

Exemplo

O uso de senhas nas redes wi-fi garante que somente as pessoas autorizadas possam utilizá-las.

Para que o controle de acesso seja efetivo, deve-se empregar um mecanismo de autenticação a fim de validar a identidade e – caso o acesso esteja autorizado – restringir os direitos de acesso para cada indivíduo de acordo com o seu perfil de uso.

Criptografia

Entendendo a criptografia

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Assim como a criptoanálise, que não discutiremos aqui, a criptografia é uma vasta área que compõe a criptologia.

A criptografia é uma área que estuda técnicas para esconder não a mensagem real, mas o seu significado. Ela pode ser, inclusive, utilizada para garantir a CID. A propriedade a ser garantida depende do mecanismo utilizado e de que maneira ele foi empregado.

Funções

Para entendermos o processo criptográfico, iremos, inicialmente, identificar duas funções principais:

Ciframento

Transforma um escrito simples, cujo alfabeto comum é utilizado para compor a mensagem original, em um texto cifrado. Nesse texto, as letras originais são substituídas pelas do alfabeto cifrado, escondendo, dessa forma, o conteúdo da mensagem. A função do ciframento é responsável pela criptografia da mensagem original. Já a substituição das letras da mensagem original é feita pelas cifras (Qualquer forma de substituição criptográfica aplicada ao texto original da mensagem.).

Deciframento

Realiza o processo oposto. Como o texto cifrado é transformado no original, o conteúdo de sua mensagem pode ser entendido. A função de deciframento é a responsável pela decriptografia da mensagem cifrada.

As técnicas modernas de criptografia envolvem o uso de um **algoritmo de criptografia associado a uma chave**. O segredo do processo não está no algoritmo em si, mas na chave utilizada para a realização do ciframento.

Classificação

Quanto ao modelo de chave empregada, os algoritmos criptográficos podem ser classificados como:

- **Algoritmos de chave simétrica ou de chave privada**: Empregam uma **única chave**. Dessa forma, a mesma chave que realiza a cifragem faz a decifragem. Alguns exemplos de algoritmos simétricos: DES, 3DES, Blowfish, RC4, RC5, IDEA, Rinjdael e *Advanced Encrytion Standard* (AES) - Algoritmo padrão adotado por diversos governos e várias empresas para garantir a confidencialidade.
- **Algoritmos de chave assimétrica ou de chave pública**: Utilizam **duas chaves** (pública e privada): uma para cifrar e outra para decifrar. Dependendo da ordem em que ambas são empregadas, o algoritmo pode garantir a confidencialidade ou a autenticidade. A exemplo temos o algoritmo Rivest-Shamir-Adleman (RSA), que é o padrão utilizado para transações comerciais, financeiras etc.

Vamos entender melhor o que ocorre com o uso de cada modelo de chave, de acordo com a ordem na qual são utilizadas:

Chave pública

Quando a chave pública é utilizada na função de cifragem, apenas a privada pode decifrar. Como o nome sugere, a chave privada fica restrita à entidade.

Exemplo: pessoa, empresa ou equipamento.

Neste caso, está garantida a confidencialidade, porque só quem possui a chave privada pode decifrar o conteúdo.

×

Chave privada

Quando a chave privada é empregada no processo de cifragem apenas a pública pode decifrar. Como a chave usada para decifrar é a pública, qualquer pessoa pode possuí-la e, portanto, decifrar a mensagem.

Neste caso, não há como garantir a confidencialidade, mas sim a autenticidade. A aplicação das chaves nesta ordem permite o emprego da assinatura digital.

Funções de hash

Conhecendo as funções de hash

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

O objetivo das funções de resumo de mensagem ou de hash é a **garantia da integridade** das informações. Para calcular o resumo, pode ser utilizado qualquer algoritmo que pegue uma mensagem de qualquer tamanho e a mapeie em uma sequência de caracteres de tamanho fixo.

Exemplo

Você tem um arquivo chamado *aula.doc* e quer calcular o resumo dessa mensagem. Uma das funções de hash bastante utilizadas é o *Message-Digest Algorithm 5* (MD5). Então, caso você tenha instalado em seu computador o MD5, pode utilizar o seguinte comando:

md5sum aula.doc

A saída desse comando é uma sequência de caracteres:

5 9 5 f 4 4 f e c 1 e 9 2 a 7 1 d 3 e 9 e 7 7 4 5 6 b a 8 0 d 1

Essa saída será permanente enquanto não ocorrer nenhuma alteração no arquivo. Portanto, toda vez que quiser verificar se ele foi modificado, basta executar novamente a função de hash e compará-la à sequência original. Se ela permanecer a mesma, isso demonstra que o arquivo é íntegro; caso contrário, é uma evidência de que ele foi modificado.

Uma propriedade desejável na função de resumo é que, **diante de qualquer modificação mínima** na informação, o resumo gerado deve ser totalmente diferente. As funções de resumo também são utilizadas como auxiliares no processo de autenticação.

Alguns sistemas usam o hash para armazenar a senha de um usuário. Portanto, quando ele cadastra uma senha, o sistema calcula o hash e

armazena esse valor. Quando o usuário for digitar sua senha para entrar no mesmo sistema, o sistema calculará o hash, enviará essa informação e comparará com o que está armazenado. Se for igual, o seu acesso será autorizado.

A vantagem dessa solução é que a senha do usuário não fica armazenada no sistema nem trafega pela rede. Quem o faz é o hash.

Outra propriedade desejável das funções de resumo é que ela **não é inversível**, ou seja, se temos o hash da mensagem, não conseguimos descobrir a mensagem original. Dessa forma, podemos afirmar que ele configura uma função criptográfica, pois esconde o conteúdo de uma mensagem. Então, quando ocorre o envio do hash da senha, não há como um atacante descobrir a senha original.

Entretanto, o uso isolado dele na autenticação pode gerar uma facilidade para o ataque de reprodução. Um atacante que conseguir obter o hash das assinaturas poderá repetir o seu processo, enviando o resumo e obtendo a autorização de acesso.

Além do MD5, outras funções de resumo muito utilizadas são as seguintes:

1. Secure Hash Algorithm version 1 (SHA-1)
2. Secure Hash Algorithm version 2 (SHA-2)
3. Secure Hash Algorithm version 3 (SHA-3)

Assinatura digital

O que é Assinatura Digital

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

O objetivo do emprego da assinatura digital é **assegurar a autenticidade** e a integridade das informações. Automaticamente, está garantido o não repúdio. A assinatura ainda garante a validade jurídica dos documentos, pois existe a certeza de que eles não sofreram qualquer adulteração, estando íntegros e completos, e a certeza quanto a sua autoria, asseverando que eles realmente foram assinados por determinada pessoa.

O processo utilizado para realizar a assinatura digital combina o emprego da criptografia assimétrica com as funções de resumo da mensagem. Para que um documento seja assinado digitalmente, o usuário deve seguir estes passos:

Calcular

Calcular o resumo da mensagem.

Cifrar

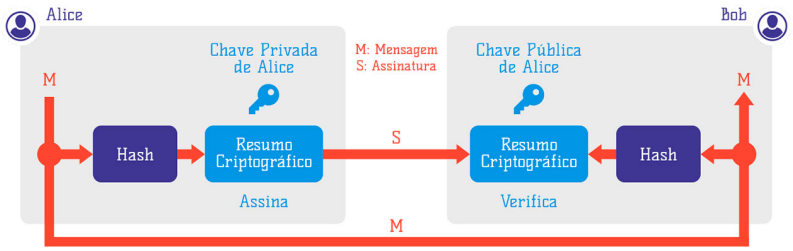
Cifrar esse resumo com a chave privada do emissor do

documento.

Enviar

Enviar a mensagem com o resumo criptografado, que é a assinatura digital.

O esquema a seguir ilustra esse processo:



Assinatura digital de um documento.

Ao receber o documento, o receptor precisa realizar o seguinte processo para o validar:

O usuário deve calcular o hash da mensagem e decifrar o outro recebido com a utilização da chave pública do emissor. Em seguida, ele vai comparar os dois hashes. Se forem iguais, há a garantia de que o documento não foi modificado e o emissor é autêntico. Caso sejam diferentes, algum problema ocorreu. Mas não é possível garantir se o problema reside na modificação dele ou na autenticidade do emissor. Estabelece-se apenas que o documento não é válido.

Certificado digital

O que é o Certificado Digital

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

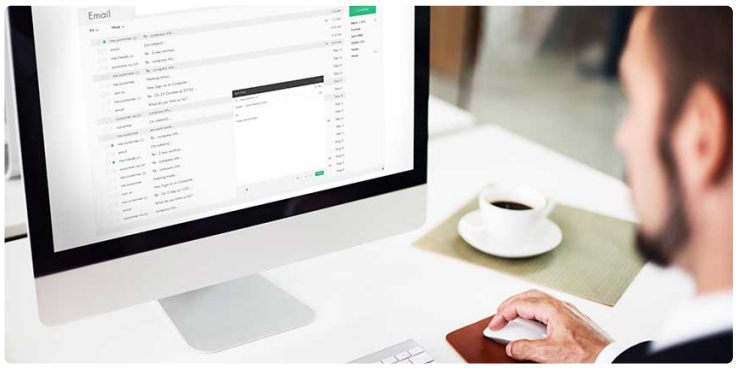
Ele é utilizado para **vincular a chave pública a uma entidade**, como pessoa, empresa, equipamento etc. O certificado contém a chave pública da entidade, que é assinada digitalmente por uma terceira parte confiável chamada de Autoridade Certificadora (AC).

A existência da autoridade certificadora é importante para garantir um ataque conhecido como "homem no meio" (MITM - *Man In The Middle*). O MITM ocorre quando um atacante pode interceptar o envio da chave pública e ter acesso às informações.

Vejamos a descrição deste problema:

Autoridade certificadora (AC)

Cartório eletrônico que garante a segurança de todo o processo na troca das chaves públicas.



Alice quer enviar um documento para Bob. Ela solicita a chave pública dele para poder cifrar a mensagem.

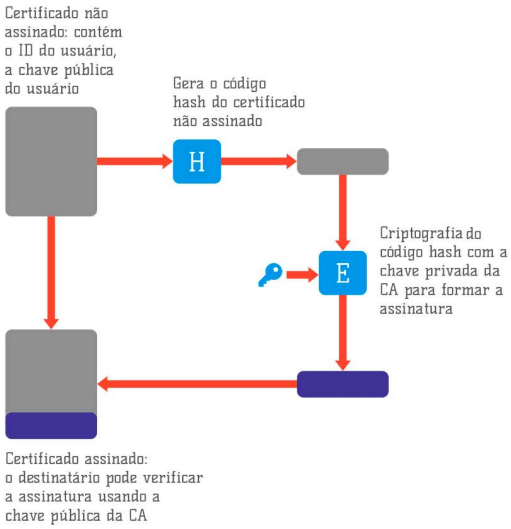
Darth, enquanto isso, realiza um ataque de interceptação para monitorar a comunicação entre ambos. Quando percebe que houve uma solicitação da chave pública de Bob, Darth envia

para Alice a sua chave. Ao mesmo tempo, se fazendo passar por ela, solicita a Bob a chave pública dele, o que caracteriza um ataque de personificação.

Alice, dessa forma, cifra a mensagem com a chave privada de Darth. Obviamente, ele consegue ler as informações enviadas. Para que o processo continue, Darth agora cifra a mensagem com a chave pública de Bob e a envia. Bob, em seguida, recebe a mensagem e a decifra com sua chave privada.

Ao monitorar a troca de mensagens entre Alice e Bob, Darth conseguiu obter as informações, quebrando a confidencialidade desse processo de comunicação.

Para resolver esse problema, é necessária uma terceira parte confiável: a AC, responsável por armazenar as chaves públicas das entidades envolvidas no processo de comunicação. Dessa maneira, a chave fica assinada digitalmente pela autoridade certificadora. Veja o esquema:



Uso do certificado de chave pública.

Voltemos ao exemplo da comunicação entre Alice e Bob. Agora ela já pode solicitar o certificado digital dele para a AC. Ao receber esse

certificado, Alice verificará a assinatura digital da AC. Se ela estiver correta, é um indício de que Alice possui o certificado correto de Bob, podendo, dessa forma, realizar a transmissão das mensagens.

O processo para obter a chave privada da AC, contudo, pode esbarrar no mesmo problema. Para o processo funcionar corretamente, o usuário deve ir ao site da AC e realizar o download dos certificados – chamados de certificados raiz –, garantindo, assim, a obtenção da chave pública correta.

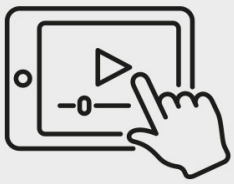
Saiba mais

No Brasil, as ACs estão organizadas na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Trata-se de uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para a identificação virtual do cidadão.

Redes virtuais privadas (VPN)

O que é uma VPN

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



A VPN (*virtual private network*) permite a utilização de um meio inseguro de forma segura. Afinal, quando estamos conectados à internet e desejamos acessar algum serviço ou rede, ficamos vulneráveis a diversos tipos de ataques.

Para minimizar o risco inerente a esse acesso, podemos empregar uma VPN, que utilizará um **túnel de comunicação entre dois dispositivos**. Considere a topologia desta imagem na qual as redes da matriz e da filial desejam trocar informações por meio da internet:

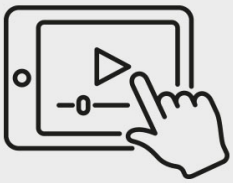
Ao trafegar pela internet, as informações trocadas entre as redes da matriz e da filial estão sujeitas a diversos tipos de ataque. Na utilização de uma VPN, é criado um túnel virtual entre essas redes. Veja:

Na utilização do túnel, as informações trafegadas ficam protegidas, já que os **dados são criptografados**. Além disso, podem ser utilizados mecanismos de autenticação e integridade para garantir tanto a entrada em cada rede só de pacotes autorizados quanto a manutenção de sua estrutura, ou seja, que eles não sejam modificados.

Firewall, sistemas de detecção de intrusão e antivírus

Confira a seguir os mecanismos de segurança lógica.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



Veja o trecho da seguinte notícia:

“PF identifica invasão nos celulares de presidentes de STJ, Câmara e Senado; PGR também foi alvo”. (Fonte: G1, 2019)

Percebemos aqui a importância dos softwares, cuja função é a de garantir a CID nas instituições. Pesquise outras situações similares e procure perceber como foi a intervenção da segurança lógica nesses casos.

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

Você foi contratado por uma empresa para realizar uma consultoria na área de segurança. Durante o trabalho realizado, identificou que ela estava sujeita a ataques contra a disponibilidade por falta de mecanismos de controle físicos ou lógicos.

No relatório, uma de suas sugestões foi a implantação de um mecanismo de controle:

A — físico, com o emprego de no-breaks para garantir o fornecimento de energia.

B — físico, com o uso de assinaturas digitais para garantir a identidade do emissor.

C — lógico, com o emprego de no-breaks para garantir o suprimento de energia.

D — lógico, com a aplicação de firewalls para garantir o controle de acesso físico.

E — físico, com o uso de criptografia para garantir o sigilo da informação.

Parabéns! A alternativa A está correta.

O objetivo dos mecanismos de controle físico é proteger as instalações físicas, ou seja, a destruição, o roubo ou a paralisação de serviços. Os mecanismos físicos podem incluir desde o uso de portões, grades e cadeados até a manutenção do ambiente dentro de condições climáticas adequadas, como a utilização de

equipamentos de refrigeração e o fornecimento de energia ininterruptos graças ao emprego de fontes de energia redundantes (geradores e no-breaks).

Questão 2

Leia o fragmento de texto a seguir:

“Durante um grande surto em maio de 2017, Rússia, China, Ucrânia, Taiwan, Índia e Brasil foram os países mais afetados. O WannaCry afetou tanto pessoas quanto organizações governamentais, hospitais, universidades, empresas ferroviárias, firmas de tecnologia e operadoras de telecomunicações em mais de 150 países. O National Health Service do Reino Unido, Deutsche Bahn, a empresa espanhola Telefónica, FedEx, Hitachi e Renault estavam entre as vítimas.”

Fonte: (AVAST, s.d.)

O WannaCry causou uma grande infecção em diversas empresas no Brasil e no mundo. Esse tipo de ataque sequestrava os dados dos usuários e exigia uma recompensa para que eles fossem disponibilizados novamente.

Para minimizar os riscos de um usuário ou uma empresa sofrer o mesmo tipo de ataque, é necessário o emprego de:

A firewall, já que este tipo de controle impede a invasão à rede, não sendo possível o sequestro dos dados.

B sistema de detecção de intrusão, pois pode monitorar o tráfego da rede, identificando o sequestro dos dados.

C antivírus, porque este tipo de ataque é realizado por um malware conhecido como ransonware.

D sistema de criptografia dos dados, uma vez que o atacante não consegue sequestrar os dados criptografados.

E

sistema de autenticação digital para garantir que somente os donos dos arquivos possam alterá-los.

Parabéns! A alternativa C está correta.

A segurança de um ambiente pode ser considerada completa quando ela emprega um conjunto de mecanismos de controle físico e lógico com o objetivo de garantir a CID. Afinal, os mecanismos de controle lógicos, firewalls, IDS, criptografia, controle de acesso e antivírus são soluções que devem atuar em conjunto. Os antivírus, por exemplo, são os responsáveis pela detecção dos malwares como o WannaCry.

3 - Arquitetura de gerenciamento de redes

Ao final deste módulo, você será capaz de reconhecer a arquitetura de gerenciamento de redes.

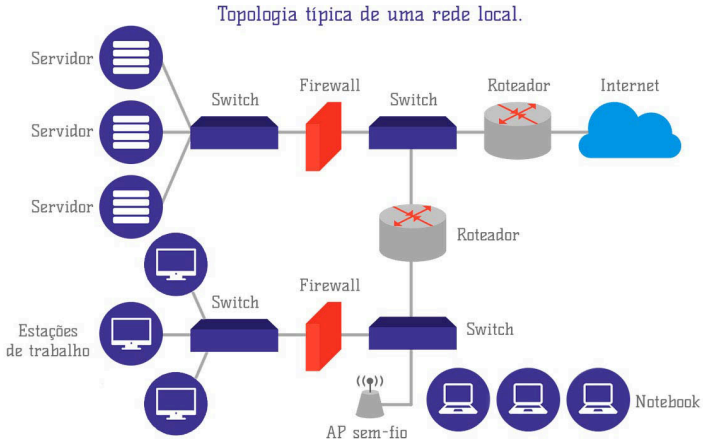
Arquitetura de gerenciamento OSI

A importância do gerenciamento

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Com o crescimento das redes, a administração e o gerenciamento delas passaram a ser atividades de suma importância. Afinal, seus ambientes são complexos e heterogêneos, tendo diversos tipos de equipamentos, fabricantes e protocolos em operação.

Observe o esquema a seguir:



Vemos na imagem diversos servidores e várias estações de trabalho com sistemas operacionais Windows e Linux, firewalls, roteadores, switches e equipamentos para redes sem fio.

Switches

Switches ou comutadores são ferramentas de camada de enlace que conseguem identificar os equipamentos conectados em cada porta e direcionar os quadros para os destinos corretos, segmentando a rede.

> **Imaginemos uma paralisação de algum serviço ou parte da rede. Nesses casos, muitos se perguntam: onde ocorreu a falha? No servidor? No switch? Na estação?**

A gerência de redes auxilia no processo de **identificação das falhas e na correção de problemas**, permitindo que a rede possa operar corretamente e oferecer níveis de serviços adequados à necessidade dos usuários.O objetivo dessa gerência é monitorar e controlar os elementos físicos ou lógicos da rede, assegurando, segundo Stallings (1998), certo nível de qualidade de serviços.

Trata-se do ato de oferecer serviços que atendam à necessidade dos usuários com um funcionamento adequado, bom desempenho e disponibilidade.

Para oferecer uma organização das tarefas de gerenciamento de redes, a International Organization for Standardization (ISO) criou a **M.3400**, um modelo de gerência derivado de recomendação publicada pela International Telecommunications Union (ITU).

Esse modelo se baseia em cinco áreas conhecidas pela sigla FCAPS (*fault, configuration, accounting performance* e *security*). Vamos conhecê-las agora!

Arquitetura de gerenciamento OSI (FCAPS)

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Gerência de detecção e correção de falhas (F = *fault*)

A área de gerenciamento de falhas é importante para **garantir que os serviços e as redes permaneçam em operação**. De acordo com a norma ISO, esta área permite registrar, detectar e reagir às condições de falha da rede. Tal gerenciamento depende do bom funcionamento de cada componente da rede tanto de forma isolada quanto pela interoperação com outros equipamentos dela.

As possíveis falhas nas redes podem ser causadas por problemas de:

Software

Falha no sistema operacional de um servidor ou em um serviço.

Enlace

Paralisação de operação de uma ligação entre uma matriz e uma filial por um rompimento de cabo.

Equipamento

interrupção no fornecimento de energia.

Quando uma falha ocorre, o gerente da rede deve analisar as informações de gerência para identificar a causa raiz do problema, descobrindo, em uma diversidade de equipamentos, softwares e protocolos, o que realmente causou o problema.

O gerenciamento de falhas pode ser dividido em dois subsistemas:

Reativo		Proativo
Trata as falhas no curto prazo (detecção, isolamento, correção e registro de falhas).	×	Monitora a rede para tentar impedir que ocorram falhas.

Gerência de configuração e operação (C = *configuration*)

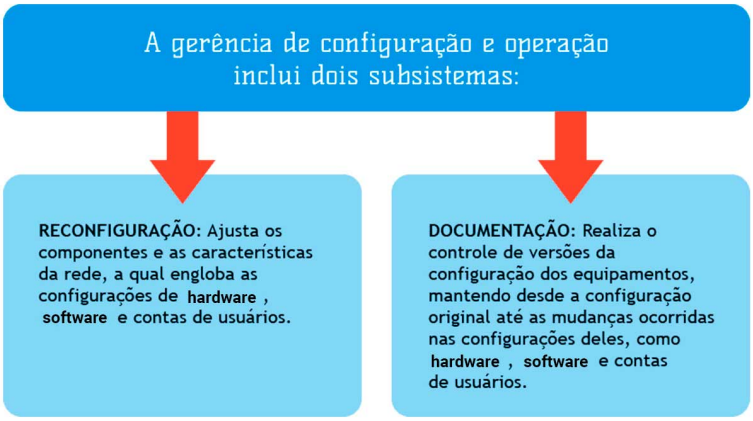
As redes são compostas por diversos equipamentos interligados entre si que possuem uma **configuração**.

Essas configurações devem ser consistentes em todos eles, permitindo que, no caso de uma reinicialização, o dispositivo volte a operar com a configuração correta.

Desse modo, é necessário realizar o gerenciamento das configurações dos equipamentos para:

1. Garantir seu funcionamento com os ajustes corretos.
2. Identificar quais dispositivos estão presentes na rede.
3. Verificar se eles estão com as configurações corretas.

De acordo com Forouzan (2010), um sistema de gerenciamento de configuração precisa saber o estado de cada entidade e sua relação com outras entidades a todo instante.



Gerência de contabilidade e faturamento (A = *accounting*)

De acordo com a ISO, a gerência de contabilidade e faturamento permite **especificar**, **registrar e controlar** o acesso de usuários e dispositivos aos recursos da rede. Por meio desta área de gerenciamento, é possível contabilizar o consumo de determinado recurso da rede.

Exemplo

A franquia de consumo de internet de uma linha telefônica, o que possibilita a tarifação para o usuário.

Este tipo de gerenciamento impede que usuários possam monopolizar os recursos da rede e libera a elaboração de planos de evolução de acordo com a demanda de uso dela.

Gerência de desempenho e otimização (P = *performance*)

O objetivo do gerenciamento de desempenho e otimização é **garantir que uma rede esteja em operação da forma mais eficiente possível**. De acordo com a ISO, sua função é quantificar, medir, informar, analisar e controlar o desempenho de diferentes componentes dela.

Dentro desta área de gerenciamento, é possível realizar dois tipos de avaliação de desempenho:

Avaliação de diagnóstico

Detecta problemas e ineficiências na operação da rede.

Exemplo: Se o gerente da rede percebe um equipamento ou enlace com baixa utilização, ele pode alterar a configuração para permitir que haja uma melhor distribuição de carga. Esse tipo de avaliação auxilia no gerenciamento de falhas, porque é capaz de antever situações que poderiam causar uma falha na rede.

Avaliação de tendências

Auxilia no planejamento da evolução da rede, observando seu comportamento e estimando a necessidade de aumento de determinado recurso.

Exemplo: O monitoramento de um enlace entre matriz e filial poderá indicar a necessidade de um aumento na capacidade dele quando a utilização média ultrapassar determinado valor. Para avaliar a operação da rede, devem ser utilizadas, aponta Forouzan (2010), medidas mensuráveis, como capacidade, tráfego, vazão (throughput) e tempo de resposta.

Gerência de segurança e proteção (S = *security*)

A gerência de segurança e proteção permite controlar o acesso aos recursos da rede e verificar se ela está de acordo com a Política de Segurança da Informação (PSI) da empresa.

> ### Que papel desempenha a segurança nesse contexto?

Ela envolve todas as camadas da **pilha de protocolos TCP/IP**, o que engloba cada dispositivo e informação trafegando pela rede. Por isso, é possível afirmar que esta é a área mais difícil de ser gerenciada.

Arquitetura de gerenciamento em rede

Veja mais sobre segurança e gerenciamento de rede.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

Falta pouco para atingir seus objetivos.

Vamos praticar alguns conceitos?

Questão 1

O diretor da empresa em que você trabalha informou a ocorrência de diversas paralisações na rede, o que prejudica a realização das atividades dos funcionários. Alegando que ela está subdimensionada, ele defende que a rede não consegue atender à demanda de trabalho existente.

Você argumenta que a rede, apesar de constantemente monitorada, possui uma utilização considerada alta (70%), precisando, portanto, ser ampliada para o atendimento dessa demanda.

Essa situação se refere à área de gerenciamento de:

A desempenho, que realiza a avaliação de tendências e auxilia no planejamento da evolução da rede.

B contabilização, que monitora o consumo de recursos da rede, permitindo o uso racional dos dispositivos.

C falhas, que é responsável por realizar um monitoramento proativo da rede, evitando que haja uma sobrecarga dela.

D configuração, que realiza o monitoramento da configuração dos dispositivos, apresentando o consumo da rede.

E detecção, que monitora a rede em buscas de falhas, como a apresentada.

Parabéns! A alternativa A está correta.

A situação apresentada é típica em diversas redes. Por meio dos sistemas de gerenciamento, é possível monitorar o seu uso e planejar os investimentos necessários para que as demandas da rede sejam atendidas, garantindo um nível de satisfação elevado para os seus usuários.

Questão 2

Uma arquitetura de gerenciamento de rede é composta por quatro componentes básicos: estação de gerenciamento, dispositivo gerenciado, base de informações gerenciais e protocolo de gerenciamento.

Tais componentes trabalham em conjunto para permitir que a rede possa ser monitorada e controlada. Para isso:

A o agente envia mensagens para o gerente solicitando informações dos objetos.

B a gerência da rede é realizada pelo protocolo de gerenciamento, permitindo que os comandos sejam executados pelo gerente.

C a base de informações gerenciais mantém informações do estado dos diversos objetos existentes em um dispositivo.

D o gerente emite comandos para a base de informações gerenciais, informando os valores de cada objeto.

E o agente envia comandos para que o gerente possa realizar a coleta de dados dos diversos objetos da rede.

Parabéns! A alternativa C está correta.

A arquitetura de gerenciamento de redes é genérica, mas os sistemas de gerenciamento existentes são baseados nos componentes apresentados. A entidade gerenciadora ou de gerenciamento monitora e controla os dispositivos da rede por intermédio do software gerente. No dispositivo gerenciado, o software agente recebe os comandos do gerente por meio do protocolo de comunicação. Já o conjunto de objetos existentes compõe a base de informações gerenciais.

Considerações finais

Garantir a operação de uma rede é uma tarefa árdua. Afinal, ela deve estar preparada para suportar diversos tipos de ataques mediante o emprego de mecanismos de controle adequados.

Além disso, os sistemas de gerenciamento podem permitir o controle de uma diversidade enorme de dispositivos, protocolos e aplicações. Os mecanismos de controle e gerenciamento adequado das redes, portanto, são fundamentais na manutenção da qualidade e da operacionalidade de seu serviço.

Podcast

Para encerrar, ouça um resumo sobre o conteúdo.

Para ouvir o *áudio*, acesse a versão online deste conteúdo.

Explore +

Confira o que separamos especialmente para você!

Visite a página do **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT)**. Em Publicações, navegue pelos diversos artigos produzidos pelo CERT com recomendações sobre prevenções de ataques;

Acesse a **Cartilha de Segurança para Internet**. Desenvolvida pelo CERT, ela descreve os riscos na utilização da internet e as soluções existentes para isso;

Leia o documento intitulado **Sistema de gerenciamento de rede**: White Paper de práticas recomendadas (2018). Desenvolvido pela Cisco, ele apresenta uma estrutura mais detalhada sobre o processo de gerenciamento de redes;

Saiba2 mais sobre a **Information Technology Infrastructure Library (ITIL)**. Trata-se de um conjunto de recomendações de boas práticas para o gerenciamento dos serviços de TI.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2013** – tecnologia da informação – técnicas de segurança – sistemas de gestão da segurança da informação – requisitos. Rio de Janeiro: ABNT, 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013** – tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013b.

AVAST. **WannaCry**. Avast. s.d. Consultado na internet em: 18 maio. 2022.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Estatísticas dos incidentes reportados ao CERT.br**. CERT.br. Consultado na internet em: 28 maio 2020.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. 4. ed. Porto Alegre: AMGH, 2010.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de computadores**: uma abordagem top-down. Porto Alegre: AMGH, 2013.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet**: uma abordagem top-down. 6. ed. São Paulo: Pearson, 2013.

LUKASIK, S. J. Why the Arpanet was built. **IEEE annals of the history of computing**. n. 33, p. 4-21, 2011.

MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. **Hackers expostos**: segredos e soluções para a segurança de redes. 7. ed. Porto Alegre: Bookman, 2014.

STALLINGS, W. **Criptografia e segurança de redes** – princípios e práticas. 4. ed. São Paulo: Pearson Prentice Hall, 2008.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3 and RMON1 and 2**. 3. ed. Boston: Addison-Wesley, 1998.

Material para download

Clique no botão abaixo para fazer o download do conteúdo completo em formato PDF.

Download material

O que você achou do conteúdo?

Relatar problema