PROGRAMAÇÃO EM AMBIENTES DE REDES DE COMPUTADORES

Raiza Artemam de Oliveira

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS

Introdução à administração de redes de computadores

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Descrever como administrar uma rede de computadores.
- Analisar a importância da administração de redes de computadores.
- Identificar problemas mais comuns em uma rede de computadores sem administração.

Introdução

Nos dias atuais, praticamente tudo está conectado a uma rede, como carros, telefones celulares, computadores, geladeiras, *videogames*, etc., os quais contribuíram para o crescimento acelerado das redes de computadores e levaram à necessidade de monitoramento e gerenciamento, para garantir que a rede esteja sempre disponível.

Neste capítulo, você compreenderá alguns dos problemas comuns em redes de computadores e verificará a importância da administração em redes de computadores, além de conhecer os protocolos mais utilizados para gerenciamento de redes de computadores, seus princípios e métodos mais relevantes, bem como aplicá-los de maneira adequada em uma rede de computadores.

1 Administração de redes

A administração de redes, conforme Forouzan (2008), pode ser definida como o monitoramento, o teste, a configuração e o diagnóstico de componentes de rede para atender a um conjunto de exigências estabelecidas por uma organização. Pinheiro (2002) complementa que gerenciamento de redes pode ser caracterizado como a coordenação (controle de atividades e monitoramento de uso) de recursos materiais (modems, roteadores, etc.) e/ou lógicos (proto-

colos), fisicamente distribuídos na rede, assegurando, na medida do possível, confiabilidade, tempos de resposta aceitáveis e segurança das informações. Ainda, Terplan (1992 *apud* SUBRAMANIAN, 2010) descreve que gerenciamento de rede significa implantar e coordenar recursos para planejar, operar, administrar, analisar, avaliar, projetar e expandir redes de comunicação para atender aos objetivos do nível de serviço a todo tempo, a um custo razoável e com capacidade ideal.

O gerenciamento de rede pode ser resumido em três etapas: coleta de dados, um processo que consiste no monitoramento dos recursos gerenciados; diagnóstico, em que se analisam os dados coletados, ou seja, o computador de gerenciamento executa uma série de procedimentos com o intuito de determinar a causa do problema representado no recurso gerenciado; e ação ou controle do gerenciamento de rede, em que, após o diagnóstico do problema, deve-se promover uma ação ou um controle do recurso, caso o evento não tenha sido algo passageiro (um incidente operacional).

A tarefa de gerenciamento de redes torna-se trabalhosa quando do crescimento acelerado dos computadores, tanto em relação ao desempenho quanto ao suporte de conjuntos de serviços. Uma rede sem gerenciamento pode apresentar problemas capazes de afetar o tráfego dos dados e sua integridade, como de congestionamento do tráfego, recursos mal utilizados ou sobrecarregados, problemas com segurança, etc. (PINHEIRO, 2002), mesmo em redes pequenas.

Basicamente, uma gerência de rede deve obter e tratar as informações da rede possibilitando um diagnóstico seguro e, em seguida, o encaminhamento das soluções dos problemas. Para cumprir tais objetivos, as funções de gerência precisam ser inseridas nos diversos componentes da rede, possibilitando descobrir, prever e reagir a problemas (PINHEIRO, 2002).

Para que os sistemas de gerenciamento de redes consigam realizar suas funções como previsto, há modelos de gerenciamento, sendo o mais utilizado o modelo FCAPS, acrônimo de *fault*, *configuration*, *accounting*, *performance* e *security* (PINHEIRO, 2002; SUBRAMANIAN, 2010; FOROUZAN, 2008), as questões que esse modelo enfatiza para solucionar. Os pontos tratados por este modelo podem ser observados na Figura 1.

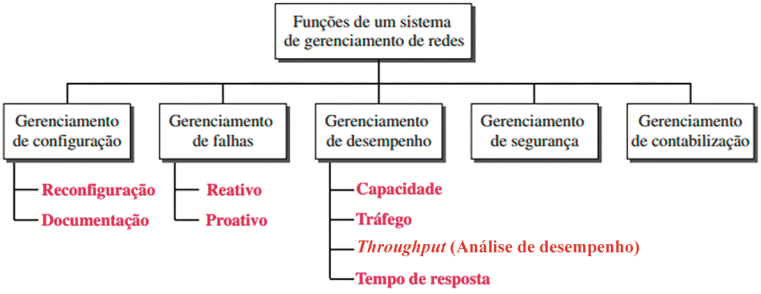

Figura 1. Funções de um sistema de gerenciamento de redes.
Fonte: Adaptada de Forouzan (2008).

Para o gerenciamento de configuração (*configuration*), é necessário conhecer, a todo instante, o estado de cada entidade e sua relação com as outras entidades. Esse gerenciamento divide-se em outros dois subsistemas (FOROUZAN, 2008; PINHEIRO, 2002):

- reconfiguração: promove o ajuste dos componentes e das características de rede, podendo compreender uma atividade diária em uma rede de grande porte. Essa reconfiguração pode ser feita no nível de *hardware*, que envolve, por exemplo, a substituição de um computador da rede ou um roteador; de *software*, que abrange, por exemplo a instalação de um novo *software* no servidor; e de contas do usuário, que envolve não somente a inclusão ou exclusão de um usuário na rede, mas também os privilégios e a participação de grupos na rede;
- documentação: refere-se ao registro das mudanças efetuadas em uma rede, também podendo ser feita no nível de *hardware*, que abrange documentos como diagramas e especificações, devendo atentar-se a inserção de número de série, fornecedor, data de aquisição e garantia do *hardware*; de *software*, que também deve manter documentadas as informações sobre o *software*, como tipo, versão, hora de instalação e licenciamento; e de contas do usuário, feita por utilitários de sistemas operacionais.

Para que uma rede funcione de modo apropriado, os componentes devem funcionar corretamente tanto individualmente quanto entre si. Para isso, há o gerenciamento de falhas (*fault*), que pode ser reativo e proativo. O primeiro tipo é responsável por detectar, isolar, corrigir e registrar as falhas, efetuando o tratamento de solução de curto prazo para tais falhas, o que ocorre em três etapas: na primeira, realiza-se a localização exata da falha; na segunda, isola-se a falha detectada, para que não afete muitos usuários, o que possibilita que estes sejam notificados sobre a previsão de tempo para realizar a correção; e, na terceira, corrige-se a falha, após a qual também deve haver uma documentação, quando se apontam a localização da falha, a possível causa e as ações tomadas para corrigi-la. Já no tipo proativo, as falhas são previstas e evitadas antes de ocorrerem (FOROUZAN, 2008).

O próximo tipo de gerenciamento, denominado gerenciamento de desempenho (*performance*), está ligado ao gerenciamento de falhas, pois tenta monitorar e controlar a rede para garantir que esteja executando do modo mais eficiente possível. Para isso, utiliza as seguintes métricas (FOROUZAN, 2008).

- Capacidade: garantir que a rede não extrapolará a capacidade em que foi projetada.
- Tráfego: garantir que o tráfego interno (número de pacotes que trafegam na rede) e externo (troca de pacotes fora da rede). Quando há tráfegos excessivos, pode haver interrupções na rede.
- *Throughput:* refere-se à quantidade de dados transferidos em uma rede, podendo ser medido de um dispositivo individual ou de parte da rede. Com isso, faz-se um monitoramento para que não seja reduzida a níveis inaceitáveis.
- Tempo de resposta: medido a partir do instante em que um usuário solicita um serviço até o momento em que o serviço é atendido. Nesse caso, o gerenciamento de desempenho busca monitorar o tempo médio de resposta e o tempo médio em horários de pico. Quando há um aumento no tempo de resposta, pode compreender um indicativo de que a rede está operando acima de sua capacidade.

O gerenciamento de segurança (*security*) corresponde ao controle de acesso à rede, com base em políticas predefinidas, impedindo, assim, que os usuários usem a rede incorretamente, de modo intencional ou não.

E, por último, há o gerenciamento de contabilização (*accounting*), em que se quantificam o acesso e o uso de recursos de rede por seus usuários para fins de tarifação, além de impedir que os usuários monopolizem recursos limitados da rede e utilizem o sistema de modo ineficiente ou permitir que os administradores de redes consigam elaborar planos com base na demanda da rede.

Um protocolo ainda muito utilizado para compreender o que acontece dentro das redes e serviços é o *simple network management protocol* (SNMP, ou, em português, protocolo de gerenciamento simples), que emprega um conjunto de protocolos *transmission control protocol*/*internet protocol* (TCP/IP). Conforme Forouzan (2008), o protocolo SNMP utiliza o conceito de gerente e agente — ou seja, em geral há um gerente, normalmente um *host* que efetua o controle e o monitoramento de um conjunto de agentes, com frequência roteadores (Figura 2).

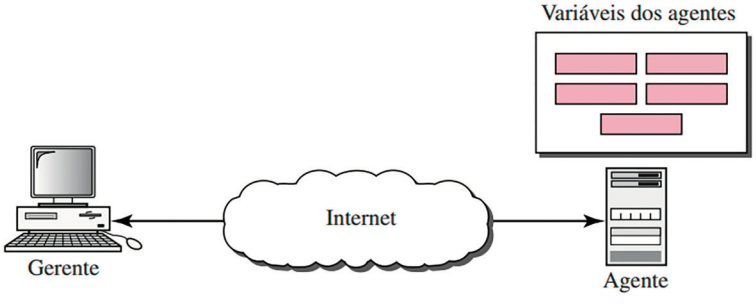

Figura 2. SNMP.
Fonte: Forouzan (2008, p. 877).

Esse protocolo está implementado na camada de aplicação dos modelos arquiteturais de redes, o que possibilita que o gerenciamento de redes por meio do protocolo SNMP torne-se heterogênea, uma vez que não depende das características físicas dos dispositivos gerenciados para funcionar corretamente e da tecnologia de rede subjacente, podendo ser utilizadas em *local area network* (LAN) e *wide area network* (WAN) interligadas por roteadores de diferentes fabricantes.

Link

O modelo FCAPS é definido pelo padrão ISO 7498-4: visite o *site* oficial do padrão para saber mais.

https://qrgo.page.link/bKw9D

Na Figura 2 podemos observar o *host* gerente, no qual é executado um programa-cliente SNMP. No agente representado por outro *host*, mas que também pode ser um roteador, executa-se o programa-servidor SNMP, em que o gerenciamento é obtivo por meio da interação dessas duas entidades. Forouzan (2008) e Pinheiro (2002) apontam que o protocolo SNMP fundamenta-se em basicamente três conceitos, listados a seguir.

1. Um gerente monitora o estado de um agente solicitando informações que refletem o comportamento do agente.
2. Um gerente força um agente a realizar uma tarefa reinicializando valores no banco de dados do agente.
3. Um agente contribui para o processo de gerenciamento alertando o gerente sobre uma situação anormal.

Ainda, o protocolo SNMP utiliza dois outros protocolos auxiliares — o *structure of management information* (SMI, em português, estrutura de informações de gerenciamento) e o *management information base* (MIB, em português, base de informações de gerenciamento) —, ou seja, o gerenciamento da rede mundial é realizado por meio da colaboração desses três protocolos, cada um com um papel definido, como descrito a seguir (Figura 3).

- **SNMP:** define o formato do pacote que será enviado, interpreta o resultado e cria estatísticas (geralmente utilizando o auxílio de outro *software* de gerenciamento). Nos pacotes enviados, há os nomes dos objetos, denominados variáveis, e seus estados, chamados valores.

- **SMI:** define e padroniza regras universais para nomear objetos, listar seus tipos de dados (que podem ser armazenados) e apresenta o modo como codificar objetos e valores, para que computadores com arquiteturas diferentes que transmitem, recebem ou armazenam valores possam comunicar-se. Para utilizar o SNMP, é necessário utilizar tais regras, funcionando, assim, como uma diretriz para o SNMP.
- **MIB:** enquanto o protocolo SMI é responsável por criar as regras, o protocolo MIB define o número de objetos, nomeia-os de acordo com as regras e associa um tipo a cada objeto nomeado. Assim, cria um conjunto de objetos definidos para cada entidade de modo similar a um banco de dados, ou seja, promove um conjunto de objetos com nomes, tipos e relações entre si para uma entidade a ser gerenciada.

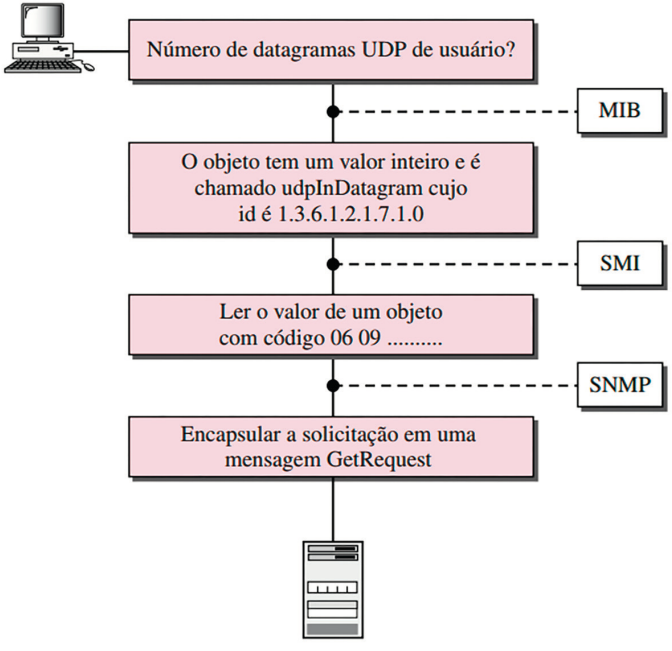

Figura 3. Uso dos três protocolos no gerenciamento de redes.

Fonte: Forouzan (2008, p. 881).

Na Figura 3, é possível observar, de modo geral, o processo de gerenciamento em uma rede: o protocolo MIB determina o objeto que armazenará o número de datagramas — a unidade básica de dados no nível IP, UDP — recebidos pelo agente, o SMI, com suas regras, codifica o objeto, e o SNMP, por sua vez, cria a mensagem e promove o encapsulamento da mensagem já codificada.

Conseguimos perceber que o SNMP constitui um protocolo muito importante para o gerenciamento de rede, ainda que trabalhe de maneira limitada, já que o gerente obtém somente as informações de determinado equipamento, enquanto o protocolo RMON (*remote monitoring*) captura as informações do tráfego da rede como um todo, permitindo, assim, o gerenciamento remoto do SNMP. Os agentes que implementam o RMON MIB contêm cinco funções, listadas a seguir.

1. Execuções *off-line:* permite que o agente execute suas tarefas mesmo que a comunicação com a estação de gerenciamento não seja possível ou esteja com problemas.
2. Gerenciamento proativo: possibilita executar diagnósticos contínuos e manter *logs* do desempenho da rede a fim de desenvolver a função de manter históricos das operações e, em seguida, fazer uma análise para identificar eventuais problemas.
3. Detecção e registro de problemas: permitem reconhecer determinadas condições da rede, efetuando constantes averiguações para informar ao gerente eventos e situações de erros significativos para a rede.
4. Valorização dos dados coletados: possibilita realizar análises específicas sobre os dados coletados na rede.
5. Múltiplos gerentes: fornecem um nível maior de disponibilidade, pois o diagnóstico poderá ser feito por meio de uma ou mais estação gerente. Com isso, permite também a execução de diferentes funções ou o gerenciamento por meio de diferentes departamentos em uma empresa.

2 Importância da administração de redes

Nos dias atuais, redes de computadores com um crescimento constante e veloz são cada vez mais comuns, o que dificulta e torna o seu gerenciamento mais complexo, já que passam a ser mais dispositivos para monitorar e mais recursos para gerenciar, exigindo que o administrador de uma rede utilize

software para auxiliar nesse controle, e, para fazê-lo de maneira eficiente, deve aprender seus recursos e saber utilizá-los de acordo com suas necessidades.

O gerenciamento de redes constitui um assunto amplo, uma vez que não se limita somente a dados de redes locais ou de área ampla, mas também a telecomunicações (tráfego de voz). Hoje, praticamente todas as empresas utilizam a tecnologia de alguma maneira, tendo compreendido a importância de um setor ligado à tecnologia. Como exemplo, pensemos em grandes lojas de departamento especializadas em vendas de roupas, que exigem um departamento de um setor de tecnologia para operar o sistema de caixa, de controle de estoque, de cadastro de clientes ou até mesmo desenvolver sistemas próprios da loja, como aplicativos para celular ou investir em vendas *on-line*. Ainda, pode haver uma situação em que a loja dispõe de filiais em outras cidades, que se comunicam por meio de uma rede privada.

Observando a necessidade do uso de tais redes, surgiu a necessidade de monitorar e gerenciar equipamentos que formam a rede de computadores das empresas. Como, na economia atual, "tempo é dinheiro", alguns processos precisam funcionar corretamente, e o setor de tecnologia, nesse sentido, deve desempenhar seu papel e dispor de serviços, dispositivos e estruturas organizacionais funcionando o máximo de tempo possível. No exemplo dado, é fácil compreender a importância do controle de recurso de uma rede, tanto para o âmbito da segurança quanto do conhecimento de sua própria rede.

Um correto gerenciamento de rede permite que haja também uma resolução ágil de problemas, além de prevenir possíveis falhas na operação sistêmica da empresa, promovendo uma economia em relação à manutenção dos equipamentos. Uma empresa que conhece sua rede pode ter também o benefício de saber a quantidade de dados que ela suporta e, em uma situação em que o tráfego estiver em um nível elevado, o tomar uma atitude ágil e prevenir lentidão na rede ou até mesmo sua paralisação total. Nesse sentido, listamos algumas vantagens de um gerenciamento de rede:

- **identificar falhas:** ao monitorar uma rede, o setor de tecnologia de uma empresa é notificado sobre possíveis falhar por meio de *e-mail* pré-programados e alertas ou mesmo *dashboards* que apresentam informações sobre a saúde da rede. Assim, os responsáveis pelo gerenciamento da rede ficam sempre atualizado sobre o desempenho a partir de qualquer lugar, podendo atuar sob o problema de forma ágil. Por exemplo, imagine que na rede de uma empresa ocorreu uma falha fora de expediente (no final da noite). Caso a rede disponha de infraestrutura monitorada, o

responsável poderá solucionar o problema de maneira remota e imediatamente para que, no dia seguinte, os funcionários estejam com a rede normalizada para trabalhar. Algumas empresas, ainda, utilizam uma equipe terceirizada para efetuar o monitoramento remoto;

- **agilizar a correção das falhas:** uma rede gerenciada mostra em qual dispositivo pode estar a falha, reduzindo, assim, o tempo para identificar onde está o problema e solucioná-lo;
- **identificar tendências:** ao dispor de certa rastreabilidade e monitoramento em redes gerenciadas, o processo de identificar tráfegos duvidosos ou atividades questionáveis quanto à segurança da informação torna-se mais fácil. Assim, em algumas situações, uma avaliação do monitoramento com uma análise forense pode identificar ameaças que poderiam passar despercebidas em redes sem monitoramento. Há, também, situações em que há problemas intermitentes ou apenas em horários de pico, um comportamento de difícil identificação. Quando há o correto gerenciamento da rede, pode-se utilizar os registros como roteiro para descobrir a propensão de desempenho e integridade da rede;
- **planejar manutenções e reparos:** ocasionalmente, equipamentos podem começar a apresentar problemas constantes, prejudicando as tarefas. Desse modo, entende-se que a substituição não se deu no momento correto. Com o gerenciamento da rede, o administrador de rede pode planejar manutenções periódicas ou investimentos em novos equipamentos para prevenir problemas maiores em *hubs*, roteadores, modens ou outros pontos da infraestrutura;
- **compreender a informação:** com relatórios do comportamento da rede, torna-se fácil compreender questões técnicas, resultando em embasamentos para discussões e tomadas de decisões com a equipe de gestão da empresa.

Link

No *link* a seguir, há algumas sugestões de *software* que auxiliam o administrador no gerenciamento da rede.

https://qrgo.page.link/ap4pr

3 Problemas comuns em redes de computadores

As redes de computadores existem para possibilitar a comunicação entre dispositivos a longas distâncias e o compartilhamento de informações e recursos, contudo, como atualmente são muito extensas e com uma alta conectividade, tornaram-se mais complexas e passíveis a falhas. Quando há uma falha em determinada rede, as máquinas conectadas a ela ficam "ilhadas", o que, muitas vezes, pode prejudicar um dia inteiro de produtividade em uma empresa. Como pudemos anteriormente, uma rede de computadores que dispõe de uma gerência de rede fica mais resistente a falhas, uma vez que se torna possível detectar e solucionar problemas rapidamente ou mesmo prevenir as falhas antes que ocorram (SUBRAMANIAN, 2010).

Redes sem gerenciamento de rede podem apresentar as falhas descritas a seguir.

- **Congestionamento de tráfego:** ocorre em uma sub-rede quando há tráfego de mais pacotes do que a rede suporta. Quando a rede opera com uma carga de tráfego de pacotes dentro de sua capacidade, todos os pacotes são entregues. Quando o tráfego extrapola a capacidade da rede, os roteadores não conseguem gerenciar e acabam perdendo os pacotes.
- **Lentidão:** o congestionamento de tráfego pode ocasionar lentidão na rede.
- **Problemas com segurança:** uma rede instável é uma porta aberta para ataque de *hackers*.
- **Perda de arquivos:** quando há congestionamento de tráfego, os roteadores não conseguem entregar os pacotes, levando à perda de arquivos.
- **Retrabalho:** com a perda de dados, os funcionários precisam perder tempo refazendo arquivos ou processos, o que gera retrabalho e diminui a produtividade.
- **Instabilidade de sistemas e acesso à Web:** a indisponibilidade da rede pode ocasionar perda de horas ou dias de trabalho, já que não será possível acessar sistemas, *software* e outras soluções conectadas à rede.
- **Falhas em equipamentos de redes:** muitas vezes, um roteador ou um *hub* pode falhar. Quando a rede não dispõe de um gerenciamento, o processo de detectar a origem da falha fica mais caro. Com isso, em vez de um dispositivo que poderia ser rapidamente substituído ou passado por uma manutenção preventiva, perdem-se dias em busca da causa da falha para executar uma ação.

Nesses casos, se houver uma política de gerenciamento de rede, poderemos identificar falhas e indisponibilidade, emitir relatórios e métricas de desempenho, enviar mensagens, reinicializar processos, identificar problemas de desempenho, realizar tomada de decisão ágil, etc.

Quando o administrador de rede for notificado sobre uma anomalia na rede, poderá seguir alguns passos para a investigação do problema, buscando informações relevantes capazes de auxiliar na detecção do problema e a sua localização, etapa na qual a rede com gerenciamento consegue potencializar os resultados, uma vez que pode indicar várias informações sobre a rede, buscar por recorrências do problema na rede, elaborar hipóteses, testar as hipóteses levantadas, solucionar o problema, testar a solução e, por fim, documentar as atividades executadas para a solução do problema, caso venha a ocorrer o mesmo problema futuramente.

Como exemplo de problemas em um dia comum de trabalho em empresas, há o *stress* de endereço IP, uma rede em que o limite de endereços disponíveis foi excedido e que, por consequência, algumas máquinas ficarão sem acesso à rede. Outro problema relacionado a IP são conflitos de configuração, em que mais de um dispositivo assume o mesmo IP e os dispositivos com IP duplicados ficam sem acesso à rede. Normalmente, alguns sistemas operacionais apresentam uma caixa de texto informando que há uma duplicação de endereço IP na rede. Em uma rede que não há gerenciamento, é necessário testar todas as possibilidades, como cabos, placas de rede, roteador, tomadas, etc. até encontrar o problema. Em uma rede com gerenciamento, torna-se mais fácil detectar que o problema foi causado pelo fato de não haver mais endereços IP disponíveis no servidor DHCP (*dynamic host configuration protocol)*, ou, ainda, que esse problema nem viria a acontecer, uma vez que se tem total controle e gerenciamento em tempo real sobre as configurações e métricas da rede.

Outro problema corresponde à lentidão da internet, um problema muito relacionado com conexões de baixa qualidade, ainda que possa não estar diretamente relacionado à exaustão de uma largura de banda, uma vez que uma única porta sobrecarregada em um *switch* ou roteador consegue diminuir o desempenho da rede (TORRES, 2014). Sem um gerenciamento de rede, também seria necessário efetuar vários testes, como a velocidade da internet por meio de *sites*, etc. a fim de encontrar a origem do erro. Em redes com gerenciamento, você saberá exatamente se o problema está localizado na rede como um todo (velocidade) ou em algum componente de rede.

Ainda, outro problema comum estão relacionado à segurança, cuja proporção aumenta conforme o tamanho da rede, pois, quanto mais usuários ativos, os *hackers* podem infiltrar-se em mais *hardware* e roubar informações, como o caso do vírus WannaCry, que afetou diversas máquinas com o sistema operacional Windows, em que mais de 230 mil de sistemas foram infectados por uma falha detectada no sistema operacional que permitia que *hackers* invadissem o computador pela rede e sequestrassem as informações de grandes empresas, pedindo como resgate valores altos em bitcoins (MOHURLE; PATIL, 2017). Com isso, podemos observar que uma rede que dispõe de gerenciamento tende apresentar os pontos dos problemas mais rapidamente para sua correta solução.

Link

Neste *link* você poderá saber mais informações sobre o vírus WannaCry.

https://qrgo.page.link/TpeVk

Referências

FOROUZAN, B. A. *Comunicação de dados e redes de computadores*. 4. ed. Porto Alegre: AMGH; Bookman, 2008. 1134 p.

MOHURLE, S.; PATIL, M. A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, Mandsaur, v. 8, n. 5, p. 1938-1940, May/June 2017. Disponível em: https://www.ijarcs.info/index.php/Ijarcs/article/view/4021/. Acesso em: 15 jan. 2020.

PINHEIRO, J. M. S. *Gerenciamento de redes de computadores*. Volta Redonda: Edição do autor, 2002. 104 p. Disponível em: http://www.allnetcom.com.br/upload/GerenciamentodeRedes.pdf. Acesso em: 15 jan. 2020.

SUBRAMANIAN, M. *Network management*: principles and practice. 2. ed. Noida; New Delhi: Dorling Kindersley, 2010. 726 p.

TORRES, G. *Redes de computadores*: versão revisada e atualizada. 2. ed. Rio de Janeiro: Novaterra, 2014. 1022 p.

Fique atento

Os *links* para *sites* da Web fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Encerra aqui o trecho do livro disponibilizado para esta Unidade de Aprendizagem. Na Biblioteca Virtual da Instituição, você encontra a obra na íntegra.

Conteúdo:

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS