ARTIGO

SEGURANÇA NA CONECTIVIDADE: PROTEGENDO REDES E CONEXÕES

POR
Michele Nogueira (UFMG)
michele@dcc.ufmg.br

Vivemos em um mundo hiperconectado em que, através de seus diferentes dispositivos computacionais e da Internet, as pessoas permanecem continuamente conectadas nas ruas, em suas casas, no trabalho e na escola. Isso tem resultado em transformações na sociedade e inovação aceleradas, gerando facilidades e grandes oportunidades para pessoas e instituições [1]. Portanto, a conectividade é a principal sustentação da era digital e desse mundo hiperconectado. Desde a Internet até as redes de acesso existentes em ambientes empresariais, residências, manufaturas, universidades e outros, passando pelos dispositivos da Internet das Coisas (*Internet of Things - IoT*), todo o funcionamento e acesso a serviços diversos depende de uma rede de conexões confiável [1, 2]. Por isso, a segurança na conectividade refere-se à proteção das redes de computadores e dos dados transmitidos por elas contra acessos não autorizados, interceptações e manipulações.

É vital para garantir a segurança das informações em um ambiente digital cada vez mais interconectado. A interconexão entre dispositivos apresenta uma série de desafios, principalmente no que diz respeito à segurança cibernética e, particularmente, relacionados à disponibilidade, confidencialidade e integridade na transmissão dos dados [2]. Assim, este artigo explora de forma abrangente e de fácil leitura os aspectos relacionados à segurança em redes de computadores, suas conexões lógicas e físicas, bem como na interconexão de seus componentes, destacando as melhores práticas, medidas para garantir a confidencialidade dos dados em trânsito, a integridade das mensagens e a disponibilidade da conexão.

As diferentes tecnologias de comunicação, desde Bluetooth, *zigbee*, Wi-Fi até fibra ótica e satélites, interligam nossos dispositivos computacionais cada vez mais diversos, resultando nas redes de computadores. Estas são frequentemente alvos de ataques cibernéticos devido à sua natureza distribuída e à quantidade de dados sensíveis que trafegam por elas. Lembrando que algumas dessas tecnologias possuem limitações em relação à largura de banda, assim como alguns tipos de dispositivos apresentam fortes limitações de recursos computacionais, e, por isto, as redes são facilmente saturadas por ataques como os ataques de negação de serviço (*Distributed Denial of Service - DDoS*) e outros. Para proteger essas redes, é essencial implementar medidas de segurança robustas, incluindo firewalls, sistemas de detecção e prevenção de intrusão (IDS/IPS) e sistemas de prevenção de perda de dados (DLP). Além disso, a autenticação forte, por meio de métodos como certificados digitais e autenticação de múltiplos fatores, é crucial para forçar que apenas usuários autorizados tenham acesso às redes de borda e sistemas. A criptografia desempenha um papel fundamental na proteção dos dados em trânsito, impedindo que informações confidenciais sejam interceptadas e até mesmo modificadas por invasores.

As conexões lógicas entre dispositivos em uma rede também requerem atenção especial quando se trata de segurança cibernética. As conexões lógicas, estabelecidas por meio de protocolos de comunicação, são vulneráveis a ataques de *spoofing* e interceptação. Para mitigar esses riscos, é fundamental implementar protocolos seguros, como o SSL/TLS (*Secure Sockets Layer/Transport Layer Security*), e realizar verificações de integridade dos dados transmitidos. Por sua vez, as conexões físicas, incluindo cabos de cobre e cabos de fibra óptica, também são alvos de ataques como sabotagem, interceptação e mesmo roubo desses componentes [3]. Para proteger essas conexões, é importante implementar medidas de segurança física, como o uso de cabos blindados e a restrição do acesso a áreas onde estão localizados os dispositivos de rede.

A interconexão de componentes em uma rede, via *switches*, roteadores e servidores, é crucial para garantir o funcionamento eficiente do sistema [4]. No entanto, essa interconexão representa um ponto fraco em termos de segurança cibernética, principalmente se não forem implementadas as devidas medidas de proteção. Para protegê-la, é essencial

segmentar a rede em zonas de confiança e aplicar políticas de controle de acesso rigorosas. Essas políticas devem ser definidas considerando visões de governança de toda a instituição e não apenas tomando como base uma visão técnica a fim de evitar inconsistências. Além disso, o monitoramento contínuo do tráfego de rede e a implementação de sistemas de detecção de intrusão ajudam a identificar e mitigar ameaças em tempo real.

Principais Técnicas de Segurança de Conectividade

Conforme mencionado, existem algumas formas principais para assegurar as redes de comunicação e seus componentes. Detalhamos um pouco mais as principais técnicas a seguir.

Firewall: um dispositivo de segurança de rede que monitora o tráfego de entrada e saída da rede e decide se permite ou bloqueia tráfego específico com base em um conjunto definido de regras de segurança. As regras definidas em um firewall pelo administrador da rede/sistema devem estar em consonância com as políticas gerais da instituição, incluindo uma visão de governança da mesma. Existem hoje firewalls que trabalham na camada de rede e outros que trabalham na camada de aplicação, seguindo a terminologia da pilha de protocolos TCP/IP.

Sistema de Detecção de Intrusões (IDS) e Sistema de Prevenção de Intrusões (IPS): sistemas que verificam o tráfego da rede para identificar ataques via análise de anomalias ou com base em assinaturas de ataques e então bloquear ativamente os mesmos. Os IDSs e IPSs fazem isso correlacionando enormes quantidades de dados e o que é considerada uma inteligência global sobre ameaças para não apenas bloquear atividades maliciosas, mas também rastrear a progressão de arquivos suspeitos e malware em toda a rede para evitar a propagação de surtos e reinfecções.

Segurança da carga de trabalho: protege as cargas de trabalho (dados) que se movem entre diferentes ambientes de nuvem e ambientes híbridos. Essas cargas de trabalho distribuídas possuem superfícies de ataque maiores, que devem ser protegidas sem afetar a agilidade dos negócios e operações.

Segmentação de rede: esta é uma forma de dividir a rede de uma organização em diferentes sub-redes. Esta técnica, que também auxilia na organização da rede, permite controlar melhor o fluxo de entrada e saída de dados das sub-redes e implementar firewalls específicos por sub-rede. Essa técnica permite a criação de zonas protegidas, como sub-redes apenas para servidores de grande importância que serão controlados por regras mais rigorosas de acesso. A segmentação de rede usando a tecnologia definida por software coloca o tráfego de rede em diferentes classificações e facilita a aplicação de políticas de segurança. Idealmente, as classificações são baseadas na identidade do endpoint e não apenas em endereços IP. Pode-se atribuir direitos de acesso com base na função, localização e muito mais, para que o nível certo de acesso seja concedido às pessoas certas e os dispositivos

suspeitos sejam contidos e corrigidos.

Rede privada virtual (Virtual Private Network - VPN): uma rede virtual que criptografa a conexão de um terminal a uma rede, geralmente pela Internet. Normalmente, uma VPN de acesso remoto usa protocolos como IPsec ou Secure Sockets Layer para autenticar a comunicação entre o dispositivo e a rede. Essa técnica cria um túnel virtual entre dois endpoints.

Antimalwares: "Malware", abreviação de "software malicioso", inclui vírus, worms, cavalos de Tróia, ransomware e spyware. Em algumas situações, o malware infecta uma rede, mas permanece inativo por dias ou até semanas. Os melhores programas anti malware não apenas verificam malware na entrada, mas também rastreiam arquivos continuamente para encontrar anomalias, remover malware e corrigir danos.

Inteligência artificial aplicada à classificação de comportamento: para detectar um comportamento anormal da rede, muitas vezes é necessário conhecer o que seria considerado o comportamento padrão. Diante de um volume cada vez maior de dados e tráfego de rede, a aplicação de técnicas de inteligência artificial e, particularmente, de aprendizado de máquina, auxilia e torna mais eficiente a classificação de tráfego de rede, inclusive a classificação de tráfego com comportamento anormal. As ferramentas de análise comportamental discernem automaticamente atividades que se desviam da norma. Esse tipo de técnica ajuda e economiza tempo de equipes técnicas de segurança nas organizações que identificam melhor os indicadores de comprometimento que representam um problema potencial e remediam as ameaças rapidamente.

Prevenção de perda de dados: As organizações devem certificar-se de que os seus funcionários não enviam informações sensíveis para fora da rede. As tecnologias de prevenção contra perda de dados, ou DLP, visam impedir que as pessoas carreguem, encaminhem ou até mesmo imprimam informações críticas de maneira insegura.

Melhores Práticas em Segurança de Conectividade

Além das medidas específicas mencionadas acima, existem várias melhores práticas que podem ajudar a fortalecer a segurança da conectividade em uma rede:

1. Atualizações regulares de software: manter todos os dispositivos e sistemas de rede atualizados com as últimas correções de segurança é essencial para evitar vulnerabilidades conhecidas;
2. Políticas de senha fortes: exigir o uso de senhas fortes e alterá-las regularmente pode ajudar a evitar ataques de força bruta e comprometimento de contas de usuário. Essas políticas devem ser definidas seguindo as diretrizes de segurança da instituição;
3. Monitoramento de atividades suspeitas: implementar sistemas de monitoramento de segurança que

alertem os administradores sobre atividades suspeitas pode ajudar a identificar e responder rapidamente a possíveis violações de segurança;

4. Treinamento de conscientização em segurança: educar os usuários sobre as melhores práticas de segurança, como reconhecer e-mails de phishing e evitar o compartilhamento de informações confidenciais, pode ajudar a reduzir o risco de ataques cibernéticos;

5. Backup regular de dados: realizar backups regulares dos dados críticos da rede é essencial para garantir a recuperação rápida em caso de falha de segurança ou desastre.

Considerações Finais

A segurança na conectividade é um aspecto fundamental da infraestrutura de rede moderna. Proteger as redes de computadores, conexões lógicas e físicas, bem como a interconexão de componentes, é essencial para garantir a integridade e confidencialidade dos dados. Ao implementar medidas de segurança robustas e seguir as melhores práticas recomendadas, as organizações mitigam os riscos de ataques cibernéticos e mantém suas redes seguras e protegidas. É importante ter sempre uma visão de futuro e integrar no dia a dia conhecimentos avançados e técnicas inovadoras como aquelas baseadas em Inteligência Artificial a fim de antecipar possíveis ameaças na rede e permitir a proteção mais eficiente das redes e dos sistemas.

Referências

1. Michele Nogueira. Segurança e privacidade dos dados no mundo hiperconectado. Computação Brasil - Revista da Sociedade Brasileira de Computação, no. 45, pg. 36-39, Julho 2021.
2. DE NEIRA, ANDERSON BERGAMINI ; KANTARCI, BURAK ; Nogueira, Michele. Distributed denial of service attack prediction: Challenges, open issues and opportunities. Computer Networks, v. 1, p. 109553, 2023.
3. Conexis Brasil Digital. 2,89 milhões de metros de cabos de telecom foram roubados ou furtados no primeiro semestre de 2023. Último acesso: 28 de abril de 2024.
4. REDES DE COMPUTADORES E A INTERNET: Uma abordagem top-down. 8ª Edição. James F. Kurose e Keith W. Ross. ISBN: 9788582605585
5. Sultan Alneyadi, Elankayer Sithirasenan, Vallipuram Muthukkumarasamy. A survey on data leakage prevention systems. Journal of Network and Computer Applications. Vol. 62, 2016, Pages 137-152. ISSN 1084-8045.

MICHELE NOGUEIRA, D.Sc. é Cientista da Computação atuando na área de redes de computadores e segurança de redes. Possui doutorado em Ciência da Computação pela Sorbonne Université - UPMC/LIP6, França (2009) e realizou Pós-doutorado na Universidade Carnegie Mellon (CMU), EUA. É professora associada do Departamento de Ciência da Computação da Universidade Federal de Minas Gerais (UFMG), membro sênior da Association for Computing Machinery (ACM) e do Institute of Electrical and Electronics Engineers (IEEE). Foi coordenadora da Comissão Especial em Segurança da Informação e de Sistemas Computacionais da Sociedade Brasileira de Computação (SBC) e foi a primeira mulher a coordenar o Comitê Técnico da Internet da IEEE Communications Society (EUA). É líder do Centro de Ciência de Segurança Computacional e coordena o projeto temático MCTIC/ FAPESP MENTORED, no qual um dos objetivos é criar um ambiente experimental acadêmico para Cibersegurança em parceria com a Rede Nacional de Ensino e Pesquisa (RNP).