1.Má configuração

Uma das maneiras mais fáceis de comprometer a segurança dos dados é deixá-los expostos na internet sem qualquer proteção. Isso acontece com frequência, e os atacantes aproveitam essa vulnerabilidade realizando varreduras para encontrar informações armazenadas em serviços na nuvem que foram esquecidas sem as devidas configurações de segurança. Um caso notório ocorreu em junho de 2017, quando 14 milhões de registros da Verizon foram encontrados abertos e acessíveis na internet devido à falta de restrições em um repositório de dados no Amazon S3. Felizmente, essa falha foi descoberta por um pesquisador de segurança antes que pudesse ser explorada por criminosos.

Outra ameaça recorrente é a presença de contas administrativas sem proteção adequada. Contas de superusuário, como "root" no Linux ou "administrator" no Windows, representam um grande risco se forem configuradas com senhas fracas ou facilmente adivinháveis, como "123456" ou "password". Para mitigar esse problema, é recomendável desativar o login direto com essas contas e utilizar métodos seguros, como o comando **su** ou **sudo** no Linux, ou a opção "Executar como Administrador" no Windows. Além disso, a quantidade de contas com privilégios elevados deve ser reduzida ao mínimo necessário para limitar a superfície de ataque.

A criptografia desempenha um papel essencial na proteção de dados transmitidos pela rede, mas seu impacto é nulo quando protocolos inseguros são utilizados. Tecnologias como Telnet, FTP e algumas versões de SMTP e IMAP enviam informações em texto puro, permitindo que qualquer atacante com acesso ao tráfego da rede possa interceptar credenciais e outros dados sensíveis. Para evitar esse risco, é fundamental utilizar as versões seguras desses protocolos, como SSH, SFTP e HTTPS. Uma simples captura de pacotes com ferramentas como Wireshark pode revelar se informações estão sendo enviadas de forma protegida ou expostas.

Eventos de segurança, como a conferência DEFCON, frequentemente demonstram a importância do uso de protocolos seguros. Durante o evento, uma prática conhecida como "wall of sheep" exibe publicamente credenciais e outras informações capturadas em redes Wi-Fi devido ao uso de conexões desprotegidas. Esse tipo de exposição mostra o quão fácil pode ser para um atacante obter acesso a dados confidenciais apenas explorando comunicações inseguras.

Além disso, dispositivos conectados à rede frequentemente possuem credenciais padrão que raramente são alteradas pelos usuários. Isso facilita ataques automatizados realizados por botnets, como a Mirai, que escaneia redes em busca de dispositivos vulneráveis, como câmeras, roteadores e campainhas inteligentes, utilizando listas conhecidas de logins e senhas padrão. Como o código-fonte do Mirai foi disponibilizado publicamente, tanto pesquisadores quanto criminosos cibernéticos podem utilizá-lo para identificar e explorar dispositivos inseguros.

A configuração de firewalls também pode introduzir riscos se não for gerenciada corretamente. Cada serviço ativado em um servidor abre uma porta, criando um ponto de entrada potencial para atacantes. O controle desses acessos deve ser feito com regras de firewall bem estruturadas, garantindo que apenas conexões autorizadas sejam permitidas. No entanto, devido à complexidade das regras, erros de configuração podem expor inadvertidamente sistemas que deveriam estar protegidos. Por isso, auditorias periódicas são essenciais para revisar e minimizar a quantidade de portas abertas na rede.

Garantir a segurança digital exige uma abordagem proativa, envolvendo boas práticas na proteção de dados, controle rigoroso de contas administrativas, uso de protocolos criptografados e configuração cuidadosa de dispositivos e firewalls. Qualquer descuido pode resultar em uma brecha explorável, tornando fundamental a implementação de medidas preventivas para minimizar os riscos de ataques cibernéticos.