10 dicas de segurança para manter seus dados seguros

Os últimos anos viram um crescimento dramático nas ameaças cibernéticas. Segundo um relatório do The New York Times, mais de 200.000 organizações sofreram ataques com ransomware em 2019, um aumento de 41% comparado ao ano anterior.

Para ajudá-lo a se proteger, preparamos uma lista com importantes configurações de segurança de dados que muitas vezes são deixadas de lado. Ao final, incluímos dicas extras para ajudá-lo a garantir a integridade – outro pilar da proteção de dados.

Obs.: A maioria das configurações listadas abaixo somente podem ser acessadas e modificadas utilizando uma conta de usuário com direitos administrativos.

Dica 1: Desabilite a conta padrão admin

Nomes de usuários comuns usados como administrador podem fazer com que a Synology NAS fique vulnerável a entes maliciosos que realizam ataques de força bruta utilizando combinações comuns de nomes de usuários e senhas. Evite nomes comuns como “admin”, “administrador”, “root”* aio configurar a sua NAS. Também recomendamos o uso de uma senha única forte logo após configurar a sua Synology NAS, além de desabilitar a conta admin padrão do sistema **.

Se estiver fazendo o login atualmente utilizando a conta de usuário “admin”, vá ao **Painel de Controle** > **Usuário** e crie uma nova conta

administrativa. Em seguida, faça o log in utilizando a nova conta e desabilite a conta “admin” padrão do sistema.

* “root” não pode ser utilizado como nome de usuário.

** Se configurar utilizando um nome de usuário que não seja “admin”, a conta padrão já será desabilitada.

Saiba mais

Dica 2: Força da senha

Uma senha forte protege seus sistemas contra acesso não autorizado. Crie uma senha complexa que incorpore letras minúsculas, maiúsculas, números e caracteres especiais de uma maneira que só você consiga lembrar.

O uso de senhas comuns para muitas contas também é um convite para hackers. Se uma conta for comprometida, hackers podem facilmente assumir o controle de outras contas. Isso acontece regularmente para websites e outros provedores de serviços. Recomendamos que faça o sign up utilizando serviços públicos de monitoramento como Have I Been Pwned ou Firefox Monitor.

Se tiver dificuldade em memorizar senhas únicas e complexas para diferentes contas, um gestor de senhas (como 1Password, LastPass, ou Bitwarden) pode ser a melhor alternativa. Basta memorizar uma senha – uma senha master – e o gestor de senhas ajudará a criar e preencher credenciais de registro para todas as demais contas.

Se administra uma Synology NAS que conta com autenticação*, é possível customizar a política der senha de usuários de forma a endurecer os requisitos de segurança de senhas para todas as novas contas de usuários. Vá a **Painel de**

Controle > **Usuário** > **Avançado** e marque o campo Limitar a força da senha na seção Configurações de Senhas. A política será aplicada a qualquer usuário que criar uma nova conta.

* Opções similares também estão disponíveis nos pacotes LDAP Server e Directory Server.

Saiba mais

Dica 3: Mantenha-se atualizado e habilite notificações

Fazemos lançamentos de atualizações de DSM regularmente para oferecer melhorias funcionais e de desempenho, e para resolver vulnerabilidades de segurança de produtos.

Sempre que surgir uma vulnerabilidade de segurança, nossa Equipe de Resposta a Incidentes de Segurança de Produto (PSIRT) realizará uma análise e uma investigação em 8 horas e lançará um patch nas 15 horas seguintes para ajudar a evitar potenciais danos de ataques do tipo zero-day.

Para a maioria dos usuários, recomendamos configurar atualizações automáticas para que as atualizações mais recentes de DSM sejam instaladas automaticamente.*

Saiba mais

Muitos dispositivos Synology contam com a opção de executar Virtual DSM no Virtual Machine Manager, de forma a criar uma versão virtualizada do sistema operacional DSM. Utilize o Virtual DSM para criar um ambiente de ensaio, e depois replique ou tente reproduzir seu ambiente de produção nele. Faça um teste de upgrade instalando a versão mais recente do DSM em seu Virtual DSM e verifique a funcionalidade de chave que a instalação atual exige antes de continuar com a atualização em seu ambiente principal.

Outro aspecto importante a considerar é estar ciente das coisas quando elas ocorrem. Configure notificações na Synology NAS e seja notificado por e-mail, SMS, em seu dispositivo móvel, ou por meio do navegador quando eventos específicos ou erros ocorrerem. Se utilizar o serviço DDNS da Synology, é possível escolher por ser notificado quando a conectividade com a rede exterior for perdida. Aja imediatamente quando receber notificações sobre a falta de espaço em espaços de armazenamento, ou quando uma tarefa de backup e restauração falhar, o que é parte importante para garantir a segurança de longo prazo de seus dados.

Também recomendamos configurar a sua Conta Synology de forma a receber nossas newsletters sobre a NAS e segurança, para estar atualizado sobre as atualizações mais recentes em termos de funções e segurança.

* A atualização automática só oferece suporte a atualizações de DSM menores. Atualizações significativas requerem instalação manual.

Saiba mais

Dica 4: Validação em duas etapas

Se quer acrescentar uma camada extra de segurança à sua conta, recomendamos muito que habilite a validação em duas etapas. Para habilitar a validação em duas etapas em sua conta DSM e na Conta Synology, é preciso um dispositivo móvel e um app autenticador que ofereça suporte ao protocolo Time-based One-Time Password (TOTP). O login exige as credenciais de usuário e um código de 6 dígitos com limitação de tempo, a ser emitido por Microsoft Authenticator, Authy, ou outros aplicativos autenticadores para evitar o acesso não autorizado.

Para a Conta Synology, se perder seu telefone com o app autenticador*, é possível utilizar os códigos de backup fornecidos durante a validação em duas etapas para fazer sign in. É importante manter estes códigos em segurança fazendo o download ou imprimindo-os. Lembre-se de manter estes códigos em segurança, mas acessíveis.

Na DSM, se perder seu autenticador, é possível fazer o reset da validação em duas etapas como último recurso. Os usuários que fazem parte dos grupos de administradores podem fazer o reset da configuração.

Se nenhuma das contas de administrador estiver acessível, será necessário fazer o reset das credenciais e configurações de rede em seu dispositivo. Segure o botão RESET em sua NAS por aproximadamente 4 segundos (até ouvir um beep) e depois inicie o Synology Assistant para reconfigurar seu dispositivo.**

* Alguns apps de autenticação oferecem suporte a backup de contas de terceiro e método de restauração. Avalie seus requisitos de segurança comparados à conveniência e opções de recuperação de desastres.

** SHA, VMM, automount de pastas compatilhadas criptografadas, diversas configurações de segurança, contas de usuário, e configurações de portas estarão sujeitos a reset. Leia mais sobre o processo de reset

Saiba mais

Dica 5: Execute o Security Advisor

O Consultor de Segurança é um aplicativo pré-instalado que pode escanear sua NAS em busca de problemas comuns de configuração de DSM, oferecendo sugestões sobre o que fazer em seguida para manter a Synology NAS em segurança. Por exemplo, pode detectar questões comuns como deixar o acesso SSH aberto, a ocorrência de qualquer atividade de log in anormal, e se os arquivos de sistema de DSM foram alterados.

Saiba mais

Dica 6: Funções básicas de segurança de DSM para configurar

É possível configurar diversas configurações de segurança em **Painel de Controle** > **Segurança** de forma a proteger suas contas de usuário.

IP Auto Block

Abra o Painel de Controle e acesse **Segurança** > **Conta**. Habilite a função de bloqueio automático para bloquear automaticamente

endereços de clientes que deixam de fazer sign in dentro de um período e um número específico de vezes. Os administradores também podem incluir endereços de IP específicos em lista negra para evitar potenciais ataques de força bruta ou negação de serviços.

Configure o número de tentativas baseado no ambiente de uso e tipo de usuários normalmente atendidos por seu dispositivo. Tenha em mente que a maior parte das residências e escritórios terão apenas um endereço de IP externo para seus usuários e que os endereços de IP normalmente são dinâmicos e se alteram depois de um certo número de dias ou semanas.

Saiba mais

Proteção de conta

Enquanto a função Bloqueio Automático coloca em lista negra os endereços de IP que falharam em uma ou mais tentativas de autenticação, a função de Proteção de Conta protege as contas de usuário ao bloquear o acesso de clientes não confiáveis.

Acesse **Painel de Controle** > **Segurança** > **Contas**. É possível habilitar a função Proteção de Contas para proteger contas contra clientes não confiáveis depois de um número pré-determinado de falhas de login. Isso melhora a segurança do seu DSM e reduz os riscos de contas vítimas de ataques de força bruta em ataques disseminados.

Saiba mais

Habilitação de HTTPS

Com a habilitação de HTTPS, é possível criptografar e proteger o tráfego de rede entre sua Synology NAS e os clientes conectados, o

que protege contra formas comuns de ataques do tipo eavesdropping ou man-in-the-middle.

Acesse **Painel de Controle** > **Rede**> **Configurações do DSM**. Marque o campo para Redirecionamento automático a conexão HTTP para HTTPS. Assim, a conexão com DSM será feita por HTTPS. Na barra de endereço, você pode perceber que o URL de seu dispositivo começa com “https://” e não “http://”. Observe que o número de porta padrão para https é 443, enquanto http, de forma padrão, utiliza a porta 80. Se tiver algum firewall ou configuração de rede anterior, é possível que haja necessidade de atualização.

Saiba mais

Avançado: regras de customização de firewall

Um firewall atua como uma barreira virtual que filtra o tráfego na rede a partir de fontes externas segundo um conjunto de regras. Acesse **Painel de Controle** > **Segurança** > **Firewall** para configurar as regras de firewall de forma a evitar sign in e acesso a serviço de controle não autorizados. Pode decidir por permitir ou negar acesso a certas portas de rede por endereços de IP específicos, que é uma boa maneira de, por exemplo, permitir acesso remoto a partir de um escritório específico ou permitir acesso apenas a um serviço ou protocolo específico.

Saiba mais

Dica 7: HTTPS Parte 2 – Vamos criptografar

Certificados digitais têm um papel-chave na habilitação de HTTPS, mas muitas vezes têm custo elevado e são de difícil manutenção, especialmente para usuários não comerciais. A DSM conta com

suporte built-in para Let's Encrypt, uma organização emissora de certificados automatizados e gratuitos, de forma a permitir que qualquer um possa facilmente assegurar suas conexões.

Se já tem um domínio registrado ou se utiliza DDNS, acesses **Painel de Controle**> **Segurança** > **Certificado**. Clique em **Adicionar novo certificado** > **Receba um certificado da Let's Encrypt**, para a maior parte dos usuários, é preciso marcar o campo "Definir como certificado padrão"*. Digite seu domínio e receba um certificado.

Depois de receber o certificado, verifique que todo o seu tráfego passa por HTTPS (como listado na Dica #3).

* Se configurou seu dispositivo para fornecer serviços por meio de diversos domínios ou subdomínios, será necessário configurar qual certificado é usado para cada serviço em **Painel de Controle** > **Segurança** > **Certificado** > **Configurar**

Tutorial em vídeo no Youtube

Dica 8: Mude as portas padrão

Embora a mudança das portas padrão de DSM de HTTP (5000) e HTTPS (5001) para portas customizadas não possam evitar ataques, podem deter ameaças comuns que atacam apenas serviços pré-definidos. Para alterar as portas padrão, acesse **Painel de Controle** > **Rede** > **Configurações do DSM** e customize os números de porta. Também é recomendável alterar a porta padrão SSH (22) se utiliza shell access com regularidade.

Também é possível implantar um proxy reverso para reduzir vetores potenciais de ataque apenas para serviços web específicos, aumentando a segurança. Um proxy reverso atua como intermediário para comunicações entre um servidor interno

(usualmente) e clientes remotos, escondendo certas informações sobre o servidor, como o endereço de IP real.

Saiba mais

Dica 9: Desabilitar SSH/telnet quando não estiver em uso

Se é um usuário constante, que requer shell access, lembre-se de desligar a função SSH/telnet quando não estiver em uso. Como o acesso root é habilitado como padrão e SSH/telnet oferece suporte apenas a sign ins feitos por contas admin, hackers podem utilizar força bruta com sua senha para ter acesso não autorizado ao seu sistema. Se necessita de serviço terminal disponível a qualquer tempo, recomendamos definir uma senha forte e alterar o número de porta padrão de SSH (22) para aumentar a segurança. Também deve considerar utilizar VPNs e limitar o acesso SSH apenas para Ips locais e confiáveis.

Saiba mais

Dica 10: Criptografia de pastas compartilhadas

A DSM oferece suporte a criptografia AES-256 para suas pastas compartilhadas de forma a evitar extração de dados a partir de ameaças físicas. Os admins podem fazer criptografia de pastas compartilhadas recém-criadas e já existentes.

Para criptografar pastas compartilhadas existentes, acesse **Painel de Controle** > **Pasta Compartilhada** e Editar a pasta. Configure uma chave de criptografia na aba Criptografia e a DSM começará a criptografar a pasta. Recomendamos guardar o arquivo chave

gerado em um local seguro, uma vez que os dados criptografados não podem ser recuperados sem a frase chave utilizada para o arquivo chave.

Saiba mais

Dica bônus: Integridade de dados

A segurança de dados está ligada à consistência e acessibilidade de seus dados - integridade de dados. A segurança de dados é um pré-requisito para integridade de dados, uma vez que o acesso não autorizado pode levar a interrupção de dados ou perda de dados, o que pode fazer com que seus preciosos dados sejam inutilizados.

Há duas medidas que pode adotar para garantir a exatidão e a consistência de nossos dados: permitir o checksum de dados na piscina e execução de testes S.M.A.R.T. regularmente. Escrevemos sobre estes dois métodos de segurança em nossos blogs anteriores — consulte estes documentos para saber mais.

Mais importante do que nunca

As ameaças online estão sempre evoluindo e a segurança de dados deve contar com diferentes vertentes, como esperado. Quando novos dispositivos forem introduzidos na sala e no local de refeições. Uma vez que mais dispositivos conectados sejam introduzidos em casa e no trabalho, torna-se mais fácil para os criminosos cibernéticos explorar buracos de segurança e ter acesso à sua rede. Manter-se seguro não é uma coisa que se facha às portas trancadas. Manter-se trancado é a melhor opção. Manter-se seguro

não é algo que se faça uma vez e depois se esquece, é um processo constante.