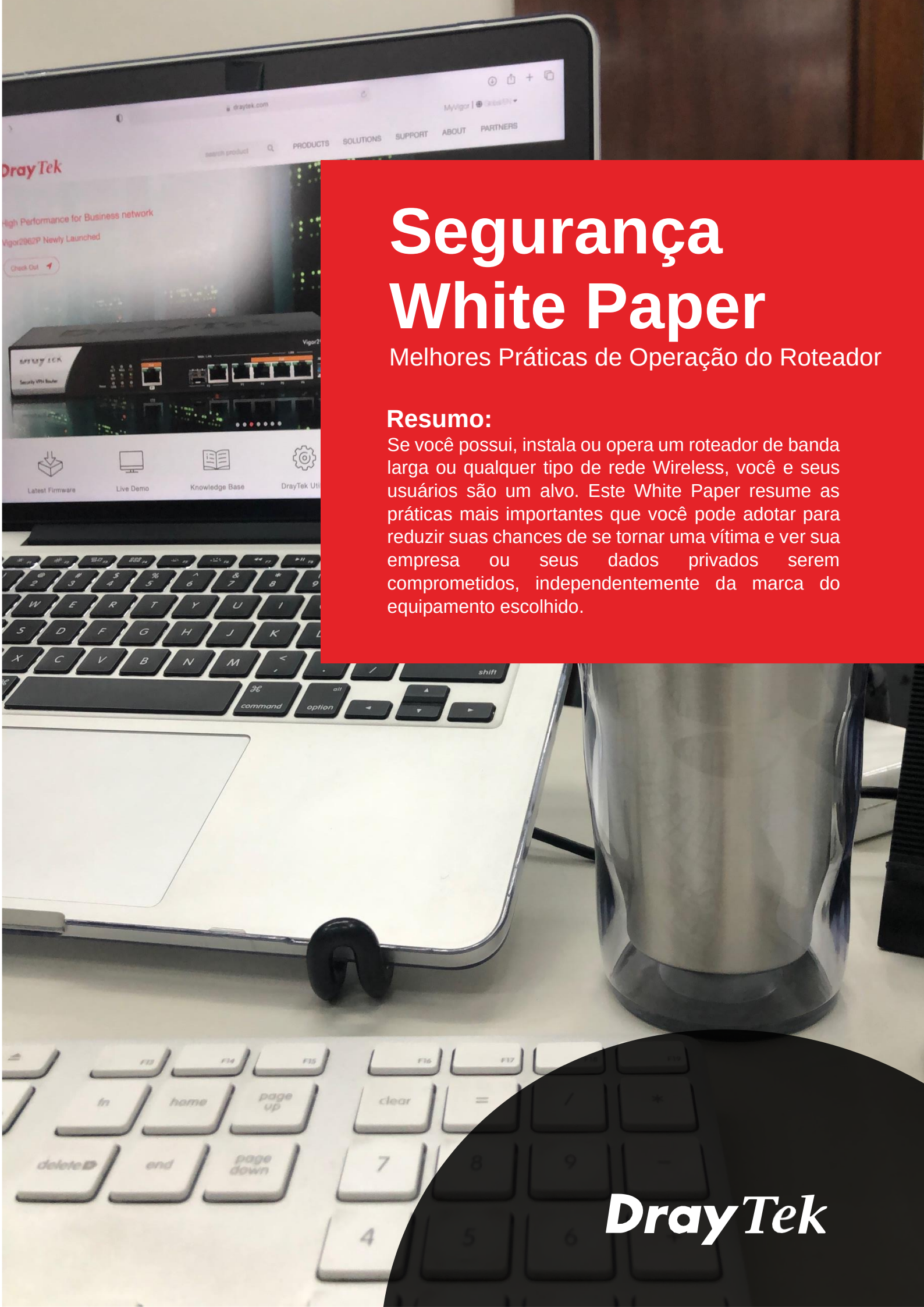



# Segurança White Paper

## Melhores Práticas de Operação do Roteador

**Resumo:**

Se você possui, instala ou opera um roteador de banda larga ou qualquer tipo de rede Wireless, você e seus usuários são um alvo. Este White Paper resume as práticas mais importantes que você pode adotar para reduzir suas chances de se tornar uma vítima e ver sua empresa ou seus dados privados serem comprometidos, independentemente da marca do equipamento escolhido.

DrayTek


DrayTek

# Introdução

Espionagem Corporativa, roubo de dados financeiros ou invasão de governos são as explorações mais interessantes ou mais recompensadoras para um hacker, mas toda rede é uma vítima em potencial. Você pode não ter dados corporativos valiosos para roubar, mas tem transações bancárias, documentos privados ou computadores que podem ser sequestrados por *botnets*. Cada rede ou computador vulnerável é do interesse de um hacker e, se sua rede doméstica estiver conectada à rede de trabalho ou e-mail comercial, expor sua rede doméstica também expõe a rede do seu trabalho.

Mesmo com as melhores fechaduras e portas mais resistentes, se você ou um membro da sua equipe deixar de usá-las corretamente ou não aplicar as práticas recomendadas, elas terão o mesmo resultado de uma porta aberta. Este mesmo princípio se aplica à sua rede de computadores, todos os componentes da sua rede e, em particular o seu roteador, que é o gateway entre os seus usuários e a Internet.

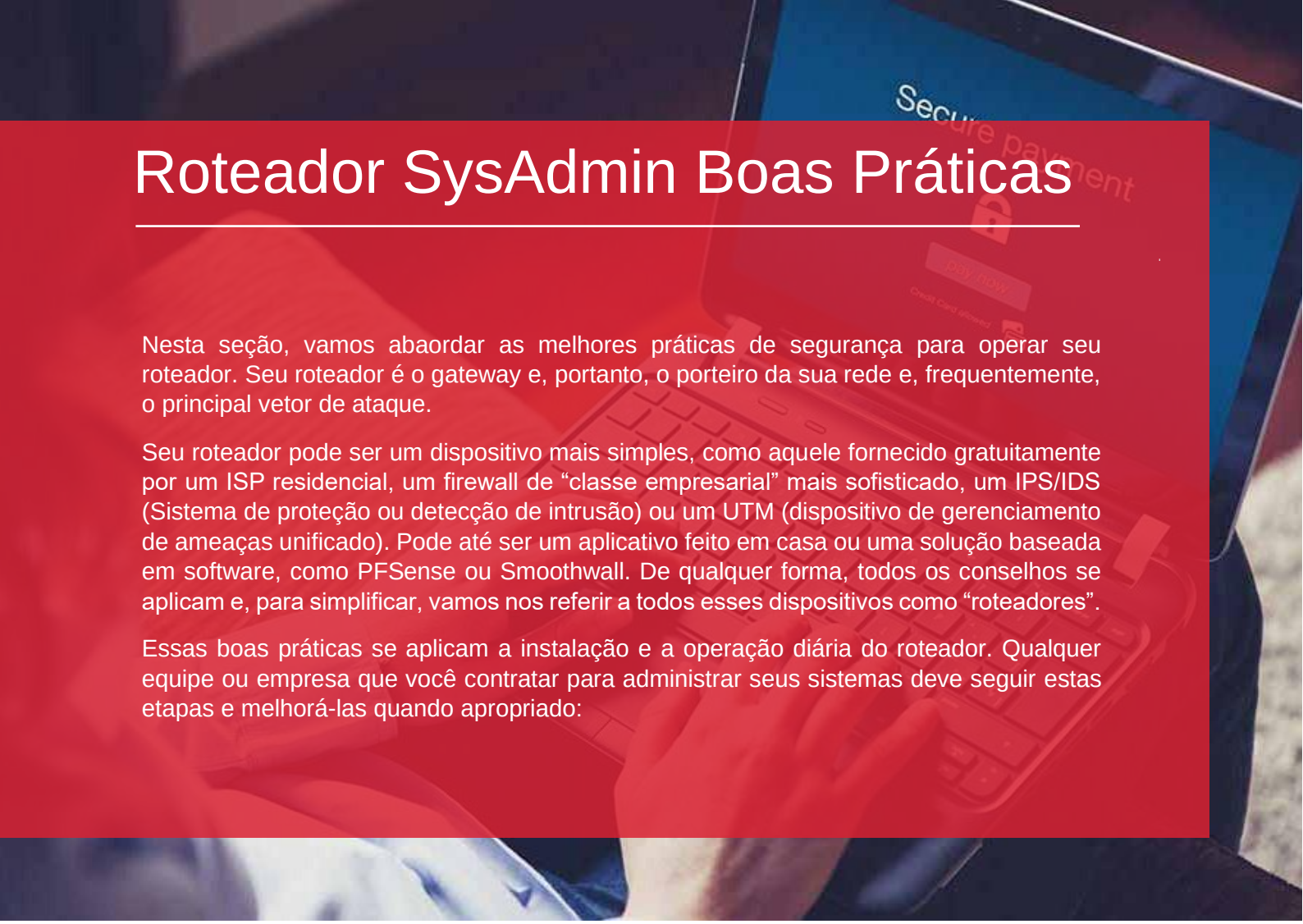
Neste guia, listaremos algumas das “melhores práticas” mais importantes para a operação de seu roteador. É fácil presumir que um roteador saia da caixa com toda a segurança ativada, isso é verdade até certo ponto com a maioria dos produtos, mas eles sempre terão configurações genéricas e você deve melhorar a sua segurança e reduzindo as chances de se tornar uma vítima.

Você deve adotar essas práticas como padrão, ajustando-as e adaptando-as conforme suas necessidades e características específicas. Nenhuma rede pode ser 100% segura, mas a adoção dessas regras reduz significativamente sua vulnerabilidade e demonstra a seus clientes, fornecedores e colaboradores que você tem uma abordagem responsável em relação a segurança.

Recomendamos que você leia todo este guia, mesmo que seja apenas para confirmar o que você “já saiba”. Provavelmente, você já está seguindo muitas das precauções recomendadas. Como dissemos, suas próprias características e hardware irão variar, então este guia não pode ser completo, nem todas as recomendações se aplicam a todas as instalações.

Finalmente, vale reiterar que, embora este guia seja publicado pela DrayTek, essas recomendações se aplicam a todas as marcas de roteadores e dispositivos Wireless, portanto, seja qual for a marca que você escolheu, esperamos que as informações neste guia sejam úteis.

**“A maioria dos ataques, mesmos os mais avançados, não são resultados de vulnerabilidades obscuras ou de hackers brilhantes, mas simplesmente explorando brechas de segurança mais básicas. Garantir a conscientização dos colaboradores sobre os riscos da engenharia social também deve ser uma prioridade.”**



# Roteador SysAdmin Boas Práticas

Nesta seção, vamos abaordar as melhores práticas de segurança para operar seu roteador. Seu roteador é o gateway e, portanto, o porteiro da sua rede e, frequentemente, o principal vetor de ataque.

Seu roteador pode ser um dispositivo mais simples, como aquele fornecido gratuitamente por um ISP residencial, um firewall de “classe empresarial” mais sofisticado, um IPS/IDS (Sistema de proteção ou detecção de intrusão) ou um UTM (dispositivo de gerenciamento de ameaças unificado). Pode até ser um aplicativo feito em casa ou uma solução baseada em software, como PFSense ou Smoothwall. De qualquer forma, todos os conselhos se aplicam e, para simplificar, vamos nos referir a todos esses dispositivos como “roteadores”.

Essas boas práticas se aplicam a instalação e a operação diária do roteador. Qualquer equipe ou empresa que você contratar para administrar seus sistemas deve seguir estas etapas e melhorá-las quando apropriado:

1. Sempre altere a senha padrão do administrador do roteador (em um roteador DrayTek, o padrão é admin / admin). Alterar a senha padrão é a primeira coisa que você deve fazer em qualquer nova instalação. Em alguns produtos, você também pode ter vários logins de administrador para que cada administrador possa usar sua própria senha o que pode ser útil para auditar os acessos ao equipamento.

2. A senha de administrador escolhida deve ser “forte”, assim como todas as outras senhas em seu roteador, incluindo aquelas usadas para contas SIP/VoIP e contas de usuário. Não use a mesma senha em mais de um roteador. Falaremos sobre “Senhas” mais tarde.

3. Sempre saia da interface de administração do roteador (Web ou Telnet) quando terminar de usá-lo e não apenas feche a janela do navegador. Na maioria dos roteadores, há um botão “Logout” na parte superior da página da interface web. Haverá também um comando telnet equivalente se você estiver usando a linha de comando. Isso oferece proteção adicional contra *Clickjacking* e ataques XSS.

4. Não habilite o gerenciamento remoto, TR-069 ou SNMP em seu roteador se você não precisar dele, e se for utilizar apenas temporariamente, lembre-se de desabilitá-lo após uso. Não envie *Syslog*, SNMP ou outros tipos de logs pela Internet (exceto em uma VPN).

5. Para administração do seu roteador use sempre que possível SSL/SSH, em vez de acesso simples e não criptografado. Por exemplo, em seu navegador, o endereço IP do roteador deve ser prefixado com https://. Você pode então desabilitar http/telnet não criptografado. Isso fornece uma proteção muito maior contra espionagens, especialmente se você estiver acessando de uma conexão pública ou pela Internet. Para acesso remoto, você deve usar uma VPN.

6. Se você estiver usando administração remota, restrinja o acesso a endereços IP remotos conhecidos / específicos se o gerenciamento remoto sempre for de locais conhecidos.

7. Monitore a atividade suspeita usando os vários recursos de registro e exibições de status do seu roteador, você pode detectar padrões de acesso ou tráfego suspeito.

8. Sempre mantenha o firmware atualizado. Todos os roteadores atuais passam por um desenvolvimento contínuo e novas ameaças estão evoluindo o tempo todo. O novo firmware pode apresentar novos recursos, mas também melhorias e correções de segurança essenciais.

9. Utilize VLANs para isolar todas as partes da LAN que não precisem se comunicar. Nas configurações wireless, habilite os recursos Isolate LAN (Wlan para LAN) e Isolate Member (Dispositivo para Dispositivo), caso seja apropriado.

10. Limite quem tem acesso de administrador ao seu roteador (ou outros componentes de rede). Alguns dispositivos também permitem logins diferentes para o administrador vs. outros usuários, e também podem suportar o registro de todo o acesso / atividade do administrador para que você tenha uma “trilha de auditoria” da atividade do administrador.

11. Desative todos os protocolos não necessários como o uPnP, WPS, entre outros, deixando ativado apenas aqueles que você realmente precisa usar como os protocolos de VPN (IPSec/SSL), usados para acesso remoto.

12. Existem configurações que você pode desativar, mas sua eficácia ou risco variam. Algumas configurações a serem consideradas incluem desabilitar o DHCP, ping e ocultar o SSID Wireless. Em cada caso, isso pode melhorar a segurança, reduzindo sua superfície de ataque, mas você deve considerar seus próprios requisitos.

13. Publique uma “*AUP - Acceptable Use Policy*” (Política de Uso Aceitável) para que os funcionários, visitantes ou membros da família saibam o que é permitido em sua rede e quais as melhores práticas que eles devem adotar ao usá-la, por exemplo, não fornecer senhas wireless a qualquer visitante ou escrever senhas. Isso deve incluir regras específicas sobre como o e-mail deve ser usado para que armadilhas sejam evitadas, (não apenas com e-mail, mas também com qualquer outro acesso à Web).


14. Para qualquer acesso remoto ou móvel à sua rede, considere a “autenticação de dois fatores (2FA)”. Em vez de usar apenas uma senha, 2FA requer que você faça logon com uma senha e “algo mais” (daí, “dois fatores”). Pode ser um PIN temporário gerado por um dispositivo ou aplicativo em seu Smartphone. Dessa forma, se alguém obtiver a sua senha, não sera capaz de fazer o login, precisando de outro dispositivo ou do seu código PIN. Seu roteador pode suportar 2FA; seu uso é uma escolha entre um pouco mais de inconveniência e aumento de segurança, então seu uso depende de seus próprios critérios. As senhas de uso único *(OTP - One Time Password)* são geradas por um dispositivo de sua posse como, novamente, o seu Smartphone. A senha gerada expira depois de alguns minutos ou assim que você a usar, então um *key-logger*, por exemplo, em um PC seria inútil para registrar senhas.

15. Se você usa VPNs com o seu roteador, considere restringir o acesso a dispositivos locais específicos ou sub-redes separadas em sua LAN. Isso pode ser particularmente relevante para administradores que desejam proteger sua LAN corporativa de dispositivos / atividades mais arriscadas de outros membros convidados que possam comprometer sua LAN.

16. Altere todos os certificados de segurança padrão. Se você estiver usando SSL/TLS (ou acesso HTTPS) para qualquer função do roteador (como deveria ser), forneça ao roteador um certificado de segurança exclusivo, se possível, em vez do padrão com o qual ele vem. Alguns roteadores gerarão automaticamente um novo certificado exclusivo quando instalado ou atualizado pela primeira vez. Você normalmente pode escolher um certificado auto assinado ou emitido por uma autoridade certificadora. É importante não usar os certificados padrões, porque se eles estiverem comprometidos, por exemplo, (a chave privada vazou do fornecedor ou a engenharia reversa do firmware), todos os usuários que usam esse produto ficam vulneráveis – seus dados criptografados podem ser descriptografados.

17. Considere o acesso físico à sua rede: roteador, switches e outras infra-estruturas. Evite tomadas RJ45 ativas em locais sem vigilância que possam ser acessíveis ao público ou visitantes. Se o equipamento conectado a rede for instalado em locais sem supervisão, considere proteger ou esconder os cabos de rede. Considere a segurança adicional do usuário como 802.1x para evitar que dispositivos não autorizados acessem a sua rede. Alguns switches ethernet irão alertá-lo ou (bloquear) se dispositivos desconhecidos estiverem conectados.

18. Se você precisar fornecer acesso temporário ao seu roteador para alguém, por exemplo, equipe de suporte temporária ou técnicos do fabricante, ou se você enviar seus backups de configuração para análise, defina senhas temporárias para eles usarem ou altere a senha depois de terem terminado seu trabalho.

19. Inscreva-se nas listas de e-mail do fabricante / distribuidor. Se uma vulnerabilidade ou *exploit* for identificada, sua lista de e-mail pode conter detalhes da atualização / solução apropriada.

20. Ao usar quaisquer recursos de seu roteador que possuem métodos selecionáveis, sempre selecione o protocolo mais seguro. Muitos dos protocolos mais antigos são agora considerados falhos e inseguros. Por exemplo, use IPSec/AES em vez de PPTP/DES, SHA-1 em vez de MD-5 e WPA3 em vez de WPA2/WPA/WEP (para WiFi). Protocolos como PPTP, WPA2, WPA e WEP são considerados inseguros hoje em dia.

21. Certifique-se de que o relógio em tempo real do seu roteador esteja configurado corretamente e sincronize com um servidor NTP confiável (servidor de horário público) para que os registros sejam precisos e que todos os eventos programados ocorram no horário pretendido.

22. Os servidores DNS não autorizados (para resolução de domínio / endereço da web) são usados para redirecionar o tráfego da web sem que você perceba. Sempre use servidores DNS conhecidos / verificados em seus roteadores e dispositivos. Isso significa usar os servidores DNS fornecidos por seu próprio ISP ou uma fonte pública confiável, como o Google (8.8.8.8 e 8.8.4.4). Seus dispositivos / PCs costumam usar seu roteador como seu servidor DNS, que por sua vez atua como um proxy para o servidor DNS público.

23. Sempre use ferramentas de administração e novos firmwares baixados do site oficial do fabricante, nunca de fontes de terceiros (a menos que aprovado pelo fabricante).

24. Se o seu roteador fornecer recursos de compartilhamento de arquivos, NAS ou armazenamento USB, desative o recurso se não precisar dele (dever estar desativado por padrão) e se você precisar usar, certifique-se de que use senhas fortes para acesso.

25. Mantenha backups da configuração do seu roteador e guarde-os com segurança. Isso sempre permitirá que você retorne a última configuração de que tenha o seu “funcionamento correto”, e economize muito tempo se precisar substituir ou redefinir o hardware.

# Wireless LAN (WiFi) Melhores Práticas

Wireless LAN (WiFi) oferece às empresas, residências e a muitos outros locais, grande liberdade e conveniência, mas essa facilidade de acesso onipresente também pode estar disponível para usuários mal-intencionados ou ações indesejadas.

Existem muitos ataques em potencial contra uma rede insegura. Não importa o quão bom seja seu roteador ou access point, não o operar corretamente e deixar de adotar políticas de segurança adequadas podem deixá-los totalmente desprotegidos, assim como deixar de usar fechaduras de alta segurança nas portas da sua casa ou escritório.

Nesta seção, resumimos as práticas mais importantes que qualquer pessoa deve adotar em uma rede WiFi, bem como conselhos para usar um dispositivo wireless na rede de outra pessoa ou um serviço WiFi público (como em uma cafeteria, aeroporto ou hotel).

1. Mesmo que você não esteja usando o ponto de acesso sem fio, altere a senha padrão Wireless do seu roteador ou access point. Se você não pretende usar, desabilite este recurso.

2. Use a criptografia wireless mais forte disponível. Embora seu roteador possa oferecer suporte a métodos de segurança mais antigos, como WEP, WPA e WPA2, eles são relativamente fáceis de quebrar hoje em dia. Você deve usar WPA3 Personal sempre que possível ou outros métodos mais fortes.

3. Considere definir uma programação automática para desativar a wireless LAN durante um determinado período, por exemplo, durante a noite quando seu escritório estiver fechado.

4. Altere o nome SSID padrão e use um nome que não identifique facilmente sua identidade pessoal, empresa, localização ou a marca do roteador/access point, exceto para acesso wireless de convidados isolados, onde geralmente se espera um nome reconhecível.

5. Crie uma rede convidados isolada. Crie redes adicionais com e sem fio isoladas do tráfego privado da rede corporativa. Isso também deve ser usado para os funcionários ao usar seus próprios dispositivos para uso pessoal (smartphones, tablets e etc.) A rede de convidados deve estar em uma sub-rede separada com VLAN para que seja impossível alcançar a sua rede privada.

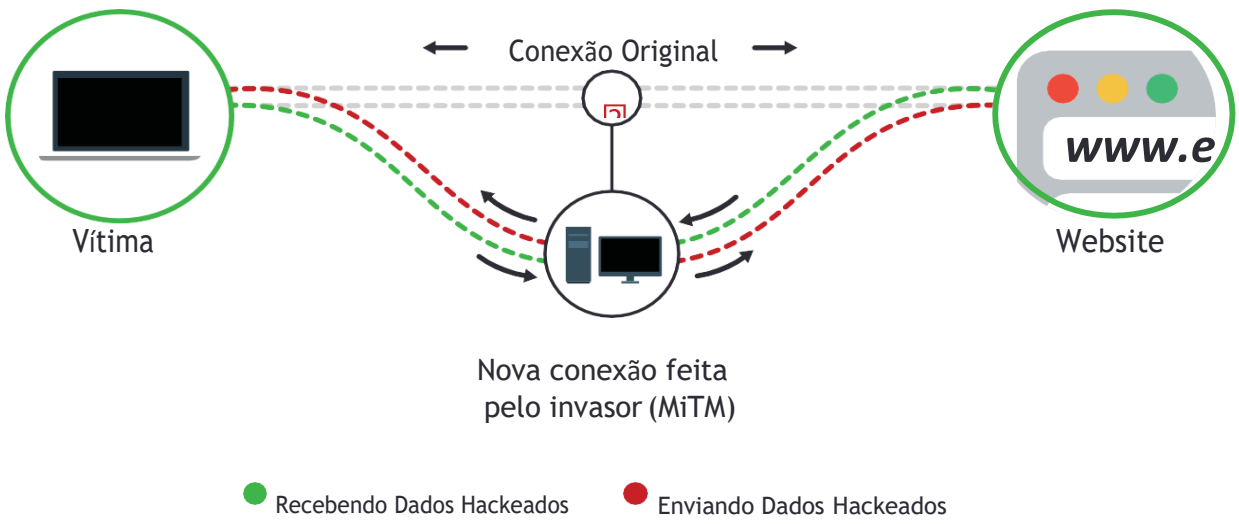
6. Se você configurar uma rede/SSID para convidados, os dispositivos convidados não devem ser autorizados a se comunicarem entre si (a menos que você queira especificamente permitir isso). Nos roteadores/access points DrayTek, isso é chamado de *"Isolate Member"* nas configurações wireless, mas pode ter nomes diferentes em outras marcas.

7. Altere suas senhas periodicamente. Não mantenha a mesma senha wireless por anos, especialmente se você tiver mudanças regulares de funcionários ou funcionários temporários.

8. Se você permitir que funcionários ou convidados acessem sua rede e, portanto, precisam da senha wireless, isso também significa que usuários não convidados também podem obter acesso. Funcionários e seus familiares podem não perceber as implicações de fornecer a senha para um convidado para que ele possa apenas "verificar seu e-mail", então, assim como uma *"AUP - Acceptable Use Policy"* (Política de Uso Aceitável) publicada para funcionários, faça uso de recursos de segurança adicionais como whitelists, 802.1x ou bloqueio por MAC.

9. Se o seu roteador/access point estiver fisicamente acessível, desative o WPS. WPS é uma maneira conveniente de conectar clientes wireless ao seu roteador/access point e também pode eliminar a necessidade de divulgar sua senha de acesso (dependendo da implementação), mas essa conveniência também pode ser um risco de segurança se uma pessoa não autorizada também puder pressionar esse botão.

10. Ao usar WiFi público, certifique-se de qual rede você está usando ou pretende usar para evitar o logon em impostores ou "armadilhas". Qualquer um pode configurar uma conexão wireless chamada "WiFi público gratuito" para atrair vítimas. Qualquer operadora de rede pode interceptar seus dados; a possibilidade de ataques MiTM (man-in-the-middles) está sempre presente, mesmo quando usando criptografia.



11. Se você usa wireless LAN (Wi-Fi) na casa de outra pessoa, no escritório ou em um ponto de acesso público (estações de trem, cafeterias), lembre-se de que o proprietário e outros usuários da rede podem detectar/capturar seu tráfego, mesmo se a criptografia WPA3 estiver em uso (porque eles também sabem a chave!). Use métodos criptografados (por exemplo, SSL, HTTPS, VPNs) para todos os dados confidenciais. Você pode criar uma VPN de volta para o roteador de sua casa / escritório ou usar um serviço de VPN público e enviar todos os dados pela VPN, em vez de diretamente pela rede convidado.

12. Muitos dispositivos wireless (telefones, tablets) agora armazenam senhas Wi-Fi e fazem backup delas na nuvem. Isso é conveniente se você usar vários dispositivos ou precisar restaurar uma configuração, mas isso também significa que o Google (para Android), Apple (para iOS), Microsoft (para Windows) agora têm a senha para provavelmente a maioria das redes wireless do mundo. Isso é útil se você for uma agência de segurança nacional e quiser espionar suspeitos de crimes, mas se essa informação cair nas mãos erradas (seus concorrentes, governos estrangeiros hostis, etc.), tavez por um agente desonesto dentro de uma dessas entidades, então é potencialmente um grande problema. Portanto, se você tiver dados confidenciais da empresa, longe de proibir o acesso wireless por completo, considere não armazenar / salvar senhas Wi-Fi em dispositivos, o que requer a cooperação de sua equipe.

13. O Windows10 tem um recurso chamado “Wi-Fi Sense” que permite que você compartilhe senhas Wi-Fi com seus contatos. Ele é ativado por padrão – considere desativá-lo, a menos que você queira usá-lo. Esteja sempre ciente do que seus sistemas operacionais e aplicativos/software estão registrando, armazenando e compartilhando com seus desenvolvedores (seja desktop, telefone ou tablet).

14. Use todas as ferramentas de diagnóstico que sua instalação Wi-Fi fornece, por exemplo, listas de dispositivos conectados ou volumes de tráfego para verificar se não há muitas conexões não reconhecidas, indicando que você tem um problema de segurança.

# Práticas Recomendadas de Senha

Nas duas seções anteriores, nos referimos a “senhas fortes” de várias maneiras. Como eles são tão vitais, esta seção explica o que queremos dizer com uma senha “forte” e porque você deve usá-las. Mesmo além do seu roteador, o uso de senhas fortes e exclusivas é absolutamente vital para todos os serviços, incluindo bancos on-line, comércio eletrônico, mas também quaisquer contas de administração que você tenha em outro hardware.

Grande parte da sua atividade online depende de acesso seguro ou controlado e grande parte dele será protegida por senha. O acesso às interfaces de administração/configuração do roteador, incluindo web e telnet, são todos controlados por senha. Como seu roteador é um gateway para toda a sua rede, é claramente vital que ele seja protegido com uma senha adequada.

## Cuidando das suas Senhas

As senhas devem ser rigidamente controladas e divulgadas apenas quando necessário. Por exemplo, se você estiver configurando o roteador de um colaborador para acesso VPN de sua casa, eles não precisam necessariamente saber a senha VPN – você, como SysAdmin, pode colocá-la para eles. Isso não é adequado em empresas maiores, onde os administradores de sistemas não devem saber as senhas dos usuários – novamente, é tudo sobre um plano de segurança apropriado para o ambiente específico.

Ironicamente, se você criar senhas complexas para contas de usuário que devem ser digitadas manualmente, será provável que os usuários as anotem. Então não crie senhas digitadas manualmente muito complexas, tenha bom senso sobre a complexidade da senha para evitar constrangimentos.

Não use a mesma senha para dispositivos ou serviços diferentes, cada um deve ser único, caso contrário, se um serviço tiver segurança fraca e estiver comprometido, o hacker pode tentar a senha revelada em outro lugar. Você não deve usar um padrão comum. Por exemplo, se você usa “ebay1234” e “amazon1234”, é fácil para um hacker adivinhar que pode também usar “twitter1234”.

Os usuários nunca devem compartilhar ou contar a ninguém suas senhas. Os usuários devem compreender totalmente que, administradores de sistemas / equipe técnica nunca pedem sua senha e você nunca devem fornecê-la para ninguém, isso é particularmente importante para evitar impostores e ataques de engenharia social.

Os usuários devem ter certeza de que nunca serão repreendidos por recusar ou contestar qualquer coisa que acredite ser contrário às políticas de segurança, mesmo quando forem levados e acreditar que alguém ou a empresa terá grandes problemas se não cooperar. Em empresas maiores, a equipe deve sempre desafiar ou confirmar a identidade de qualquer pessoa que alega precisar de acesso aos seus sistemas, especialmente se a visita ou chamada for inesperada.


## Cofres de Senha

A maioria de nós agora tem muitas senhas para lembrar. Como explicaremos mais tarde, você não deve se sentir tentado a usar a mesma senha para serviços/sites diferentes. As senhas devem ser únicas, use um “*Password Safe*”, que é um software ou aplicativo que permite armazenar senhas e outros segredos em um banco de dados fortemente criptografado. Existem cofres de senha disponíveis para todos os sistemas operacionais e plataformas móveis. Selecione um que seja reconhecido e respeitado. O acesso ao cofre de senha é protegido com uma senha mestra, que você insere sempre que deseja abrir o cofre.

Essa senha mestra deve ser única, não compartilhada e, obviamente, nunca a anote, guarde-a em seu cérebro.

## Senhas Únicas

Senhas únicas são vitais, ou seja, uma senha diferente para cada serviço, plataforma e provedor diferente. É inconveniente, mas se um serviço for comprometido (hackeado ou dados roubados de alguma forma), os malfeitores podem acessar seus outros serviços. Sabendo que muitas pessoas usam senhas comuns, os hackers tentarão sua senha de um serviço em outros serviços.

O problema com senhas compartilhadas foi demonstrado em 2014 com a vulnerabilidade Heartbleed. Sites que não foram afetados, tinham que aconselhar seus clientes a alterar / redefinir suas senhas se eles tivessem usado a mesma senha em sites que eram vulneráveis. Além disso, nem todos os provedores de serviço operam com a mesma segurança. É prática padrão criptografar senhas com uma “*one-way salted hash*”, mas mesmo hoje, alguns provedores de serviço ainda não fazem isso, como demonstrado por alguns hacks em grande escala.


## O que é uma senha “Forte”?

Várias de nossas recomendações neste documento fazem referência para senhas “fortes”. As senhas devem ser as mais longas e complexas que você puder suportar – misturar letras, maiúsculas e minúsculas, números e caracteres:

**GhYu!.(@_:dy562gtUi**

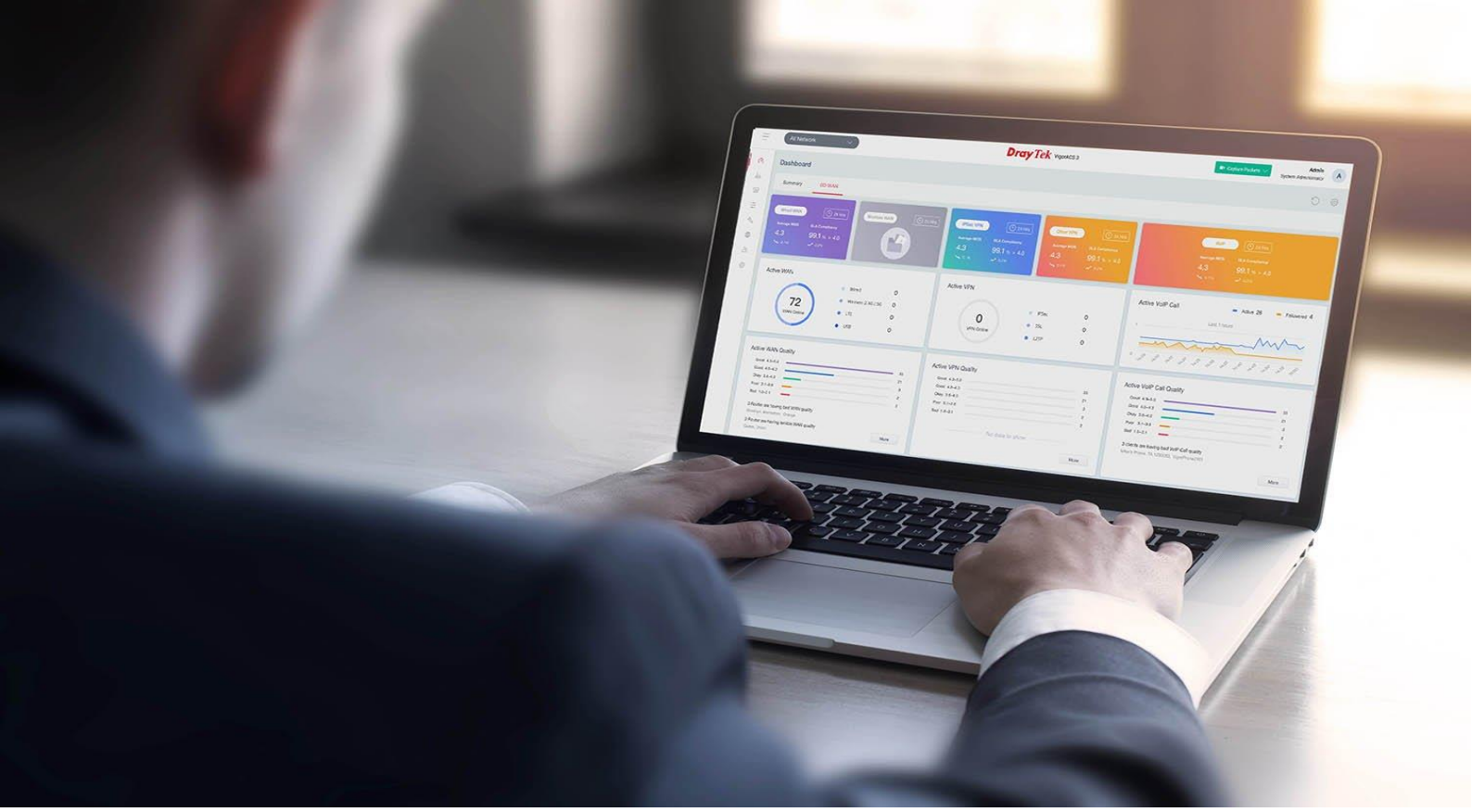
É uma senha boa e complexa (embora talvez um pouco extrema, mas essa é a ideia). Certamente evite palavras isoladas, datas ou mesmo apenas duas palavras juntas. No mínimo, misture maiúsculas e minúsculas, letras e números.

**Nunca anote as senhas.**

# Resumo das Senhas Relacionadas ao Roteador

A senha de administração do roteador é a senha mais óbvia no contexto deste documento, mas existem muitas outras que você usa. Este é um resumo das senhas mais comuns relacionadas ao roteador. Você terá, é claro, inúmeras outras senhas para outros sites (redes sociais, comércio eletrônico etc.), cada um dos quais também deve usar uma senha forte e única.

- Senhas administrativas do roteador (para acesso Web/Terminal);
- Senhas de criptografia Wireless LAN;
- Senhas de ramais SIP/ SIP Trunk (VoIP);
- Senhas VPN (pre-shared keys, site to site e host to lan);
- Painel de administração DrayTek (Portal MyVigor);
- Senhas de portais e fóruns de suporte;
- TR-069/SNMP e outras senhas de gerenciamento de rede;
- LDAP/ Usuários de Acesso e senhas de contas;
- Senhas de acesso à Internet (ISP);
- Senhas de servidores DDNS e SMS;
- Senhas de e-mail (IMAP/POP3);



## Os Dias das Senhas estão contados?

Sugere-se que as senhas em si são realmente apenas SBO, veja abaixo, que a propensão das pessoas para compartilhar senhas, usar senhas fracas ou ser descuidada sempre fornecerá aos hackers uma superfície de ataque confiável. A autenticação de dois fatores (2FA) em que, normalmente, uma senha e "outro fator" são sempre mais fortes porque, mesmo que um hacker tenha ou adivinhe sua senha, eles ainda precisam do outro fator de correspondência, por exemplo, (um PIN gerado por um dispositivo ou um certificado digital). A autenticação em dois fatores pode se tornar padrão dentre alguns anos tornando a senha única obsoleta. Muitos serviços populares já oferecem 2FA.

## Segurança por Obscuridade ("SBO")

Há um ditado comum e frequentemente argumentado em segurança da informação de que "segurança por obscuridade não é segurança de forma alguma", o que basicamente significa que ocultar coisas ou dificultar sua localização não é "segurança" e você precisa usar métodos de segurança "adequados". Aqueles que condenam a segurança por obscuridade ("SBO") apontam que qualquer hacker determinado pode facilmente contornar tais medidas e, recomendar seu uso pode lhe dar uma falsa sensação de segurança.

Claro, é verdade que a obscuridade não é a segurança em si, mas tornar os alvos mais difíceis de atacar e colocar obstáculos extras no caminho pode reduzir as chances de uma tentativa.

Um exemplo de SBO é desabilitar o DHCP, isso não é segurança, mas dá ao invasor um obstáculo extra para superar, com o qual um ataque automatizado pode não se preocupar. O mesmo se aplica à mudança do range de IPs padrão do roteador. Se o código de ataque CSRF (*Cross-site Request Forgery*) for codificado para atacar LANs com a sub-rede 192.168.1.0 comum, ou pelo menos começar aí, o uso de algum outro intervalo de sub-rede pode impedir ou retardar o ataque. Novamente, você tem que pesar a inconveniência da metodologia contra os benefícios.

## Cuidado com a Tecnologia Obsoleta

A tecnologia está em constante evolução. A alta segurança de hoje e o “padrão ouro” da criptografia são as vulnerabilidades de amanhã. Isso acontece devido ao aumento do poder de processamento disponível para usuários regulares. Quando a criptografia DES foi introduzida na década de 1970, ela foi considerada inquebrável com sua chave de 56 bits. Ataques de força bruta de uma chave de 56 bits são viáveis com os computadores acessíveis de hoje. Protocolos de tunelamento como PPTP nem sequer incluíam criptografia originalmente porque foi introduzido quando as redes não eram acessíveis através de uma Internet pública, e o risco e a consciência de hacking não eram reconhecidos. Há também WEP, criptografia para o seu WiFi – que foi substituída pela WPA, que também foi substituída pela WPA2 e hoje estamos na WPA3.

O SSL é outra tecnologia considerada obsoleta. Observe que estamos falando sobre as tecnologias específicas chamadas de SSL (como SSL 3.0), mas o termo “SSL” é geralmente usado genericamente para se referir ao tráfego criptografado da web/Internet, como páginas HTTPS, que agora usam principalmente o método de criptografia TLS1.2. Em 2014, uma vulnerabilidade (chamada Poodle) no TLS foi descoberta por meio da qual um cliente poderia ser induzido a voltar para o protocolo SSL 3.0 (inseguro). A solução foi que todos os principais navegadores emitiram atualizações que desabilitaram SSL 3.0 completamente.

A conclusão aqui é que seu roteador ou outra tecnologia podem suportar vários protocolos para permitir a compatibilidade com versões anteriores e terceiros, mas você deve sempre usar os protocolos mais seguros disponíveis (levando em conta considerações de desempenho e risco) e desativar quaisquer protocolos desnecessários (por exemplo WEP e WPA / WPA2 para WiFi). Outro exemplo: se você configurar uma conexão VPN, desative todos os métodos desnecessários.

## Não Ignore a IoT

Em uma pesquisa de 2016 sobre publicações de sites de segurança, a nova frente de ataque mais comumente prevista foi a IoT – a Internet das Coisas. Essa é a nova onda de dispositivos conectados em sua casa ou escritório - campainhas, geladeiras, lâmpadas, assistentes virtuais e assim por diante. Esta é uma área de crescimento enorme e emocionante para a tecnologia, mas grande parte dela é imatura e parece que na pressa de ser o primeiro a ser comercializado, as considerações de segurança são muitas vezes mais baixas na lista de prioridades do que deveriam ser. Assim como seus PCs e hardwares de rede, seus dispositivos IoT devem se comunicar com segurança na Internet e devem usar senhas para controle e acesso.

Verifique se o seu fabricante está comprometido com atualizações regulares para corrigir vulnerabilidades e continuará o desenvolvimento do produto.

# Antivirus é Importante

Com todo o nosso foco na segurança do hardware, é importante lembrar a importância de cada dispositivo ainda estar equipado com um software antivírus (AV), competente e atualizado. Softwares de antivírus estão disponíveis para todas as plataformas, incluindo mobile e, de fato, seu dispositivo mobile pode ser infectado como um PC Desktop. Manter e usar antivírus é especialmente importante, pois a sofisticação e a natureza insidiosa de vírus e trojans são maiores do que nunca (um Trojan é um vírus escondido dentro de algo inocente olhando, como no Cavalo de Tróia). Os tipos mais comuns de vírus podem ser zumbis DoS (relés), zumbis de spam e ladrões de dados, como: *ransomware ou keylogger.*

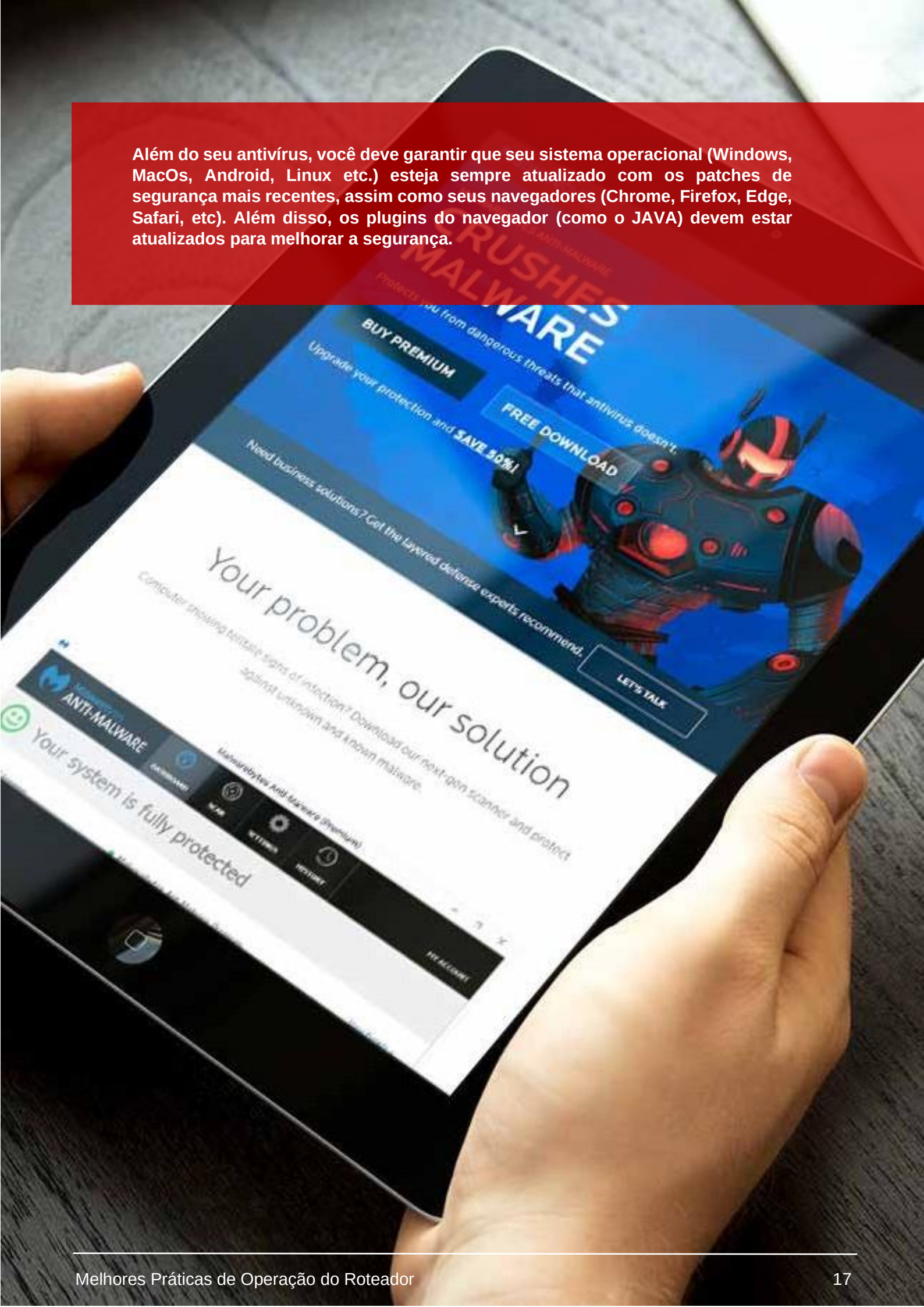
Um “zumbi” é um programa normalmente adormecido, à espera de instruções de um comandante em outro lugar na Internet. Ao chamar dezenas de milhares de zumbis, o centro de comando pode transmitir rapidamente grandes quantidades de dados de muitos locais em direção a um alvo, sobrecarregando a conectividade da vítima alvo (negando assim o serviço a eles). Isso é conhecido como um ataque de negação de serviço distribuído (DDoS). Como os ataques vêm de milhares de locais, que não são responsáveis pelo ataque, é impossível pará-lo (mas pode ser mitigado). Um Zumbi também pode ser usado como um retransmissor de e-mail para enviar spam ou e-mails de *phishing*, tornando-o indetectável.

A combinação mais recente de engenharia social e vírus significa que é fácil até mesmo para os profissionais mais experientes serem enganados por um e-mail ou dispositivo de memória que parece inócuo ou legítimo, então você será infectado. Os vírus são mais comumente contidos em executáveis ou documentos “office” (“Por favor, baixe a sua fatura anexada…”), mas até mesmos arquivos PDF podem ter conteúdo invasor. Controle sua curiosidade se você suspeitar de alguma coisa; esteja sempre alerta.

Às vezes, você pode verificar os cabeçalhos de e-mail para expor uma fonte falsa, mas se o vírus foi enviado de um contato conhecido infectado, até mesmo o cabeçalho parecerá legítimo. Se você não tem certeza sobre o anexo de e-mail de uma pessoa conhecida, tenha cuidado. Se for uma pessoa desconhecida, fuja, exclua o anexo – **NÃO** fique tentado a abri-lo esperando que seu antivírus o proteja.

Mesmo com o antivírus instalado, um vírus novo ou mutante pode ainda não ser reconhecido, por isso é vital reduzir sua chance de ser infectado. As melhores práticas em relação a anexos de e-mail e visitas a sites comprometidos são essenciais. Seu roteador/firewall pode fornecer serviços de filtro de conteúdo (WCF – Web Content Filter no caso do Draytek) que bloquearão sites comprometidos em tempo real. Os sites comprometidos mais comuns são aqueles que parecem estar oferecendo algum serviço ou download sem exigir algo em troca.

**Além do seu antivírus, você deve garantir que seu sistema operacional (Windows, MacOs, Android, Linux etc.) esteja sempre atualizado com os patches de segurança mais recentes, assim como seus navegadores (Chrome, Firefox, Edge, Safari, etc). Além disso, os plugins do navegador (como o JAVA) devem estar atualizados para melhorar a segurança.**



## Backups e Ransomware

Fazer backup de seus dados é um conselho antigo, mas ainda é um ótimo conselho e está além do escopo deste documento, mas com o crescimento de ataques *ransomware* o backup um item extremamente importante. O *ransomware* é um fenômeno relativamente novo em que um vírus criptografa silenciosamente todos os seus dados e, uma vez feito isso, aparece para exigir pagamento para desbloqueá-los. Os criminosos normalmente exigem pagamento em criptomoeda como o *Bitcoin,* não rastreável, e há exemplos de bugs dentro do prórpio *ransomware* que impedem a descriptografia, mesmo quando o resgate é pago, ou os criminosos apenas pegam o dinheiro e não fornecem as chaves de descriptografia. O efeito disso foi imenso para algumas vítimas, tanto em grandes empresas como em particulares. Imagine dados de empresas ou documentos pessoais sendo perdidos.

Com o *ransomware*, a prevenção de infecções é obviamente necessária (consulte a seção anterior), mas se o pior acontecer, você ficará feliz com os backups, embora esperemos que você já esteja fazendo backups de seus dados, se prevenindo dos riscos mais tradicionais como, (falha de disco, roubo do dispositivo, etc.). Seus backups precisam ser regulares, recentes e offline. Cada uma dessas características é vital:

- Você precisa que os backups sejam regulares e recentes, para que você perca a quantidade mínima de dados possível.

- Os dados de backup precisam estar “offline”, ou seja, não armazenados em seu PC ou em qualquer dispositivo ao qual seus PCs (ou outros dispositivos) tenham acesso, caso contrário, o ransomware também pode criptografar seus backups. Se você mantém seus backups na nuvem, bloqueie esse armazenamento para que o seu PC não tenha acesso ao diretório, caso contrário o ransomware pode criptografar isso também.

- Você precisa se certificar de que possui vários backups. Se você mantiver apenas um backup, você pode estar fazendo backup de dados bloqueados / criptografados e substituindo um backup anterior que esteja integro, então mantenha os backups anteriores quando possível, por exemplo, os backups dos últimos 7 dias, os backups das últimas 4 semanas e os últmos 6 meses de backups.

- Faça testes regulares de recuperação de dados através do backup para ter certeza que os backups estão sendo realizados e seus dados estão íntegros.

# Aproveite ao Máximo o seu Roteador/Firewall

Seu firewall deve estar provavelmente fornecendo proteção *Stateful* por padrão no lado da LAN isso significa que, uma fonte externa (ou invasor) não pode “enxergar” seus dispositivos internos de fora, ele só passará dados recíprocos, que são dados recebidos como uma resposta para uma solicitação de saída. O roteador mantém o estado de todas as sessões externas portanto, *Stateful,* no entanto, ele pode fazer mais do que apenas um firewall automático. A filtragem de IP adicional são regras para bloquear ou permitir o tráfego com base em seus endereços de origem e destino, ou tipo de tráfego.

Considere configurar filtros de IP adicionais para bloquear ou permitir o acesso a destinos específicos onde os dispositivos não precisam de acesso total à Internet. Por exemplo, um servidor interno que não precisa de acesso à Internet, pode bloqueá-lo, exceto para serviços essenciais (sites de atualização para o OS, antivírus, backup em nuvem, etc.).

Se você tiver câmeras de CFTV IP ou telefones IP em sua rede, bloqueie o acesso à Internet se eles não precisarem, (você pode definir um gateway falso para isso). Se você estiver usando VPN, defina filtros de IP para que os usuários remotos só tenham acesso aos recursos necessários, por exemplo, apenas servidores específicos e protocolos como o RDP - Remote Desktop, de que eles precisem. Bloqueie qualquer outro dispositivo remoto através de uma VPN se eles não precisarem ter acesso a sua LAN.

Você pode bloquear todos os dispositivos em sua LAN, exceto servidores de e-mail, que precisam enviar e-mails usando os protocolos SMTP (portas 465, 587). Isso pode impedir que *bots* (zumbis) distribuam *spam* através da sua rede.

Grande parte do tráfego da Internet agora usa criptografia SSL/TLS. Isso também criptografa o endereço da web ou URL, por exemplo, www.google.com, portanto, certifique-se de que, se estiver usando qualquer filtro de conteúdo, seu dispositivo seja capaz de detectar e bloquear URLs que estão sendo acessados por meio de uma conexão criptografada.

Os roteadores também fornecem muitos outros recursos de segurança, como filtragem de conteúdo, mitigação DOS, time scheduling e etc, e você deve fazer o uso adequado deles. Habilite os logs para que você possa ver o quanto esses filtros estão sendo usados. Se você estiver usando IPV6, lembre-se de que cada dispositivo LAN tem um endereço IP público – certifique-se de que você esteja se protegendo com uma regra de bloqueio padrão (exceto para servidores voltados para o público, permitindo apenas os protocolos necessários).

# Tor

Tor (originalmente chamado de “The Onion Router”) é um serviço de anonimato para o tráfego de Internet. O Tor fornece anonimato para usuários e serviços, retransmitindo seu tráfego por meio de várias retransmissões aleatórias até, eventualmente, sair da rede Tor para chegar ao seu destino (em um nó de saída). Desta forma, cada extremidade da conexão não pode rastrear o ponto de origem, então o seu endereço de IP é ocultado. O Tor pode ser usado para acessar qualquer site de forma anônima.

Podem existir serviços dentro da própria rede Tor, para que eles não sejam acessíveis pela rede Internet normal. O Tor possui seu próprio sistema DNS para localização de serviços de rede.

A “Dark Web” é o nome coletivo dos sites nesta rede. A “Deep Web” é um subconjunto dos serviços secretos / não listados. A “Dark Web” é famosa por ser usada por criminosos envolvidos com pornografia ilegal, pirataria, hacking, comércio de dados roubados, venda de armas de fogo e Drogas ilegais. O Tor também é amplamente utilizado por hackers. Nem todos que usam Tor são criminosos: algumas pessoas usam o Tor para falar abertamente contra a opressão, digamos, dentro de um regime específico, onde haveria consequências se fossem identificados, incluindo denunciantes, dissidentes políticos ou jornalistas.

Tor é um protocolo de tunelamento, que oferece um desafio para qualquer empresa, escola ou casa que esteja tentando controlar o tráfego de rede ou a atividade do usuário. Os pacotes Tor se parecem com o tráfego HTTPS / TLS (SSL) padrão, portanto, não são facilmente identificados. Isso significa que, se você tiver medidas para ajudar a bloquear determinados serviços, um usuário pode ser capaz de fazer um túnel através do Tor e contornar essas medidas. Sua organização corre o risco de permitir o acesso a sites ou atividades ilegais ou ofensivas que você pensou ter bloqueado.

Portanto, você precisa evitar que o Tor seja usado em sua rede. Você deve controlar todos os dispositivos para evitar que o Tor seja instalado, mas onde os usuários têm liberdade de instalar softwares ou usar seus dispositivos pessoais, isso fica muito difícil de ser controlado. Neste caso, identifique cada nó de saída do Tor e aplique regras de firewall que filtrem estes destinos.

Acima de tudo, se você quiser banir o Tor, lembre-se do elemento humano. Certifique-se de que a *“AUP - Acceptable Use Policy”* (Política de Uso Aceitável) de seus usuários proíba especificamente a instalação ou o uso do Tor. Se sua equipe sabe que isso é estritamente proibido, é muito menos provável que eles tentem instalá-lo ou contornar bloqueios.

# Resumo & Conclusões

Como uma visão geral, este guia nunca será totalmente abrangente, nem pode cobrir a topologia específica de sua própria rede e ambiente, mas esperamos ter demonstrado que existem muitas precauções simples que você pode adotar para aumentar significativamente sua segurança. Este guia também não cobre a configuração específica e o uso dos recursos de segurança fornecidos pelo seu roteador. Você deve aplicar todas as medidas apropriadas e seguir conselhos específicos de seus especialistas em segurança ou estudar os manuais de seus produtos.

No que diz respeito aos hackers, os White-hat Hackers são hackers que prestam serviços a empresas para testar resiliência e segurança de redes, em oposição aos hackers "Black-hat", que são bandidos que causam danos, caos, roubo, constrangimentos, entre outras perdas. Você pode querer considerar a contratação de um "White-hat" para "pen test" (Teste de Invasão) para usa rede / segurança de TI, mas verifique com quem você está lidando, seja claro em seus termos de serviço e políticas de NDA - Non Disclosure Agreement (Contrato de Confidencialidade), faça referências e seja claro em sua missão.

Você deve realizar avaliações de risco regulares de todos os seus usuários e do seu ambiente TI. Este guia foi produzido pela DrayTek – onde os principais produtos são roteadores, então esse é o nosso foco, mas é claro, há muito mais em sua TI do que apenas roteadores, Wireless LAN e senhas. Cada equipamento de TI pode ser um ponto de vulnerabilidade, mesmo algo aparentemente tão inocente como uma impressora.

Claro, mesmo que são seja equipamento de TI pode ser um ponto de vulnerabilidade, como fechaduras de portas e janelas. Estamos acostumados a mantê-los e avaliá-los regularmente, então a TI não deve ser diferente, mas os sistemas digitais oferecem mais oportunidades para contravenções não detectadas, então considere, se você tem meios adequados (mas proporcionais) para detectar e reagir a ataques.

Você também deve considerar qual o nível de histórico, logs ou auditoria é apropriado para sua rede, por exemplo, se você deve registrar todas as conexões dos dispositivos, logins remotos, serviços DHCP, etc. Na verdade, é mais comum que a falta de cuidado do usuário ou falta de consciência de risco, em vez de contravenções deliberadas o deixem em risco, portanto, adotar uma *"AUP - Acceptable Use Policy*" (Política de Uso Aceitável) apropriado (ver anteriormente) e conscientizar os usuários / equipe sobre a importância de uma operação prudente é vital.

# Obrigado!

Obrigado por ler este guia, esperamos que você tenha achado útil. Por favor, entre em contado se você tiver algum comentário, correções e sugestões. Nós realmente agradecemos seus comentários e recomendamos este guia para parceiros e colegas.

Basta enviá-lo e ajudar todos a terem uma melhor segurança de rede.

# Um CALDEIRÃO
# de soluções tecnológicas