6. Use uma estação de trabalho de administração segura (SAW)

Uma estação de trabalho de administrador segura é um sistema dedicado que só deve ser usado para realizar
tarefas administrativas com sua conta privilegiada.
Não deve ser usado para verificar e-mails ou navegar na Internet. Na verdade ... não deveria nem ter
acesso à internet.

Que tarefas você faria em um SAW :

- Administração do Active Directory
- Política de grupo
- Gerenciando servidores DNS e DHCP
- Qualquer tarefa que requeira direitos de administrador nos servidores
- Direitos de administrador para sistemas de gerenciamento, como VMware, Hyper-v, Citrix
- Administração do Office 365

Você entendeu a ideia.
Basicamente, quando você precisa usar sua conta privilegiada para realizar tarefas administrativas,
você deve estar fazendo isso a partir de um SAW.
As estações de trabalho de uso diário são mais vulneráveis ao comprometimento da passagem de hash,
ataques de phishing, sites falsos, keyloggers e muito mais.
Usar uma estação de trabalho segura para sua conta elevada fornece proteção muito maior contra esses vetores de ataque.
Como os ataques podem vir de internos e externos, é melhor adotar uma postura de segurança contra violação.

Devido às ameaças e mudanças contínuas na tecnologia,
a metodologia de como implantar um SAW continua mudando.

Há também PAW e servidores de salto para tornar ainda mais confuso.

>> Aqui estão algumas dicas para ajudá-lo a começar:

- Use uma instalação limpa do sistema operacional (use o sistema operacional Windows mais recente)
- Aplicar linha de base de segurança de proteção
- Ativar criptografia de disco completo
- Restringir portas USB
- Use firewall pessoal
- Bloquear internet
- Use uma VM - o Terminal Server funciona bem
- Software mínimo instalado
- Use dois fatores ou cartão inteligente para acesso

Restrinja os sistemas para aceitar apenas conexões do SAW

Aqui está meu fluxo de trabalho típico usando um SAW:

Faça login em meu computador com minha conta normal para verificar e-mail e ver novas
solicitações de suporte. Tenho um pedido para dar a um usuário permissões para uma pasta compartilhada.

Vou entrar no meu SAW com minha conta privilegiada que tem direitos para modificar a associação do
grupo AD e adicionar o usuário ao grupo de segurança AD necessário.

Muito simples, certo?

Pode parecer um incômodo, mas na verdade acho mais conveniente dessa forma. Posso entrar remotamente
quando estiver fora da rede e ter um servidor com todas as ferramentas de que preciso. Eu também não
preciso me preocupar em reinstalar todo o meu software de suporte se precisar recriar a imagem do meu
computador.