

CONTEÚDO PATROCINADO | WHITE PAPER

Garantindo a segurança de ambientes híbridos e remotos

Empresas com trabalhadores remotos e híbridos enfrentam maiores riscos de segurança. Mas com a abordagem e soluções certas, as empresas conseguem se proteger de maneira eficiente.



CIO

PATROCINADO POR

 TeamViewer

MAIS DA METADE DOS TRABALHADORES EM TEMPO INTEGRAL DOS **ESTADOS UNIDOS** são capazes de trabalhar remotamente, e metade desses são trabalhadores em sistema híbrido, [de acordo com a empresa de pesquisas Gallup](#). Com o aumento atual do número de trabalhadores remotos e híbridos, as empresas enfrentam riscos significativos de segurança, tanto conhecidos como desconhecidos.

As empresas têm alterado suas estruturas de local de trabalho para se adaptarem à empresa estendida, indo além do perímetro tradicional da empresa para lidar com novas demandas, como nuvem, usuários remotos, aplicativos e a internet das coisas/tecnologia operacional (IoT/TO). Por sua vez, isso aumentou a superfície de ataque geral das empresas, que agora se estende a dispositivos domésticos e redes Wi-Fi.

Esses tipos de riscos de segurança são um problema crítico diante do aumento dos ataques de segurança cibernética nos últimos anos. Um estudo mostrou [que o número de violações significativas enfrentados pelas empresas de diversos setores aumentou 20,5% de 2020 para 2021](#). Outro estudo mostra que [trabalhar de casa aumenta a frequência de ciberataques em 238%](#).

[Violações de dados custam caro, tanto financeiramente quanto em relação à confiança do cliente. O custo médio de uma violação de dados aumentou](#) de US\$ 3,86 milhões em 2020 para US\$ 4,24 milhões em 2021 e finalmente, assustadores US\$ 4,35 milhões em 2022. Na presente taxa de crescimento, [estima-se que os danos causados por ciberataques atinjam US\\$ 10,5 trilhões por ano até 2025](#).

A área de TI, por sua vez, muitas vezes se vê sobrecarregada pela crescente necessidade de oferecer suporte, gerenciar e manter a visibilidade de todos os dispositivos remotos e de rede conectados à empresa. Sem medidas robustas de segurança, os dispositivos remotos correm risco, sejam eles de propriedade da empresa ou do funcionário.

"Os departamentos de TI atualmente se deparam com ambientes de TI heterogêneos e distribuídos, que são o oposto da configuração padronizada de trabalho em um ambiente corporativo fortificado e controlado", diz Frank Ziarno, Vice-Presidente de Gerenciamento de Produtos da TeamViewer. "O uso de redes Wi-Fi desprotegidas ou deixar o laptop desacompanhado por um instante pode parecer inofensivo, mas pode ser fatal para a empresa. Para manter uma segurança sólida, os departamentos de TI precisam proteger os dispositivos remotos como se estivessem na sede da empresa, por meio de treinamento e soluções de segurança adequadas."

Os maiores desafios de segurança

Frequentemente, os riscos que começam pequenos podem — e vão — se intensificar, gerando um impacto sério caso não sejam abordados rapidamente. Aqui estão os quatro principais riscos de segurança que as empresas enfrentam ao adotar o trabalho híbrido:

1. Vulnerabilidades de rede e dispositivos remotos

Desatualização do software antimalware é uma das ameaças de segurança mais significativas quando se trata de redes e dispositivos remotos. Outros problemas potenciais incluem sistemas operacionais desatualizados, comportamento anormal da memória e firewalls desativados.

Software desatualizado ou não suportado e soluções de antivírus podem expor as empresas a riscos graves, permitindo que hackers ganhem facilmente o controle de sistemas e dados. Embora o software antivírus desatualizado possa funcionar em certa medida, frequentemente ele não consegue lidar e neutralizar efetivamente malware ou ameaças de segurança.

2. Ciberataques

Terminais como computadores e dispositivos móveis simplesmente não são protegidos da mesma forma que servidores.

Os cibercriminosos reconhecem os dispositivos como lugares vulneráveis para lançar ataques por meio de métodos como phishing, ransomware e exploits de dia zero, que são três dos tipos mais comuns e caros de ataques.

3. Perda de dados

A perda de dados pode ocorrer de várias formas, incluindo perda ou esquecimento de dispositivos. Com frequência, as empresas não fazem backup de seus dispositivos, acreditando que seu software antimalware oferece proteção suficiente. Mas a perda de dados pode também incluir:

- Criminosos cibernéticos roubando dispositivos de casas, escritórios, carros e cafeterias
- Funcionários acidentalmente deletando arquivos de hard drives
- Desastres naturais como enchentes e incêndios

Algumas empresas dependem de seus funcionários para fazer backup de seus dispositivos terminais. Mas isso é um erro. Os funcionários podem não estar treinados ou motivados o suficiente para levar essa tarefa a cabo. Confiar ou depender dos funcionários para isso também significa que a TI não pode controlar os backups que supostamente devem ser feitos em hard drives externos. Não há forma de garantir que esses backups sejam realmente realizados.

4. Supervisão de TI insuficiente

Com frequência, os departamentos de TI não têm visibilidade completa dos dispositivos dos usuários finais. A equipe de TI não consegue facilmente determinar se todos os dispositivos dos trabalhadores remotos e híbridos estão em bom estado de funcionamento, nem quantos estão conectados à rede corporativa em determinado momento.

Com supervisão insuficiente, dispositivos vulneráveis a ataques cibernéticos não recebem as correções necessárias, e os sistemas operacionais e softwares de terceiros não são atualizados. A equipe de TI não consegue realizar auditorias espontâneas de forma eficiente para identificar softwares proibidos ou potencialmente prejudiciais na rede da empresa, identificar dispositivos não autorizados, verificar o status dos backups ou obter informações críticas sobre os dispositivos sem depender das informações fornecidas pelos usuários finais. O risco se aplica não apenas ao dispositivo individual, mas, na verdade a toda a rede.

Soluções que funcionam

Afinal, qual é a resposta? É crucial começar com uma visão holística e abrangente de todos os dispositivos (independentemente do formato, fabricante e sistemas operacionais), incluindo quaisquer dispositivos de propriedade dos funcionários. Aplicativos e ferramentas que permitem monitorar e gerenciar remotamente todos os dispositivos em rede podem melhorar significativamente a eficiência e eficácia da equipe de TI.

"A proteção cibernética sempre será uma batalha," afirma Robert Haist, Diretor de Segurança da Informação da TeamViewer. "Os criminosos cibernéticos não estão parados, e as empresas precisam estar sempre um passo à frente. A estratégia de segurança de uma empresa requer atenção, monitoramento e reavaliação contínua de ferramentas, estruturas e abordagens. Obter e manter uma compreensão profunda de todo o ambiente de TI distribuído é o primeiro passo crucial para alcançar uma postura de segurança adequada e sustentável. Só é possível proteger aquilo que você sabe que existe."

Aqui estão quatro táticas para ajudar a evitar os riscos de segurança associados ao trabalho remoto e híbrido:

1. Seja proativo no monitoramento web

Sem um monitoramento web proativo, os funcionários podem acessar downloads infectados e sites comprometidos durante a navegação.

Uma boa solução de monitoramento web utiliza servidores em todo o mundo para realizar testes ping regularmente no seu site. Se a resposta ao ping demorar muito ou se o ping não receber resposta, isso gera um alerta. Com o monitoramento web proativo, a equipe de TI é informada imediatamente sobre uma ameaça ou interrupção. Uma boa ferramenta de monitoramento web deve ter:

- Scripts automatizados para manter execução impecável de processos.
- Tempos de resposta rápidos com notificações para favorecer rápida solução de problemas.
- Geração de relatórios para análise completa da performance e favorecer otimizações.

2. Aposente sua VPN

Embora uma rede privada virtual (VPN) seja a solução convencional para o acesso dos funcionários aos sistemas corporativos, existem importantes desvantagens. As VPNs são complexas, exigindo um esforço extenso para configuração e instalação. Elas também apresentam desafios em termos de escalabilidade e segurança.

Com uma VPN, quando os usuários baixam arquivos do servidor para seus próprios computadores e fazem alterações nos documentos localmente antes de salvá-los de volta no servidor, podem ocorrer problemas.

Em termos de segurança, nada impede os trabalhadores remotos de salvar documentos em seus dispositivos pessoais. Além disso, as VPNs podem ser interrompidas sem motivo aparente, deixando a conexão entre o servidor e o dispositivo desprotegida.



3. Utilize uma plataforma de monitoramento e gerenciamento remoto.

Com o acesso remoto, os trabalhadores podem acessar diretamente a área de trabalho do escritório, ver uma imagem espelhada do que está acontecendo em seu computador lá e operá-lo de qualquer lugar do mundo.

Todas as sessões e arquivos transferidos são protegidos por criptografia de ponta a ponta. Os funcionários remotos podem trabalhar de forma eficiente, sem latência ou atrasos em ações como transferência de arquivos ou download.

Ao contrário da VPN, que requer configuração e instalação extensivas e deve ser compatível com o seu roteador, as soluções de acesso remoto baseadas em nuvem podem ser configuradas e dimensionadas em minutos, sem exigir manutenção extensiva.

As plataformas de monitoramento e gerenciamento remoto (RMM) mantêm os dispositivos seguros de três maneiras, tudo a partir de um único painel de controle fácil de usar:

- Software antimalware previne e faz remediação de ciberataques
- Gerenciamento de patches elimina as vulnerabilidades de software
- Backups programados garantem que os dados dos dispositivos sejam copiados para a nuvem e estejam disponíveis para restauração e recuperação, mesmo se ocorrerem ataques cibernéticos bem-sucedidos.

Com plataformas de gerenciamento e monitoramento remoto, a equipe de TI pode realizar auditorias espontâneas para encontrar softwares prejudiciais na rede da empresa, coletar informações essenciais sobre os dispositivos e verificar facilmente o status dos backups, atualizações de software e patches.

Conclusão

Os riscos de segurança associados ao trabalho remoto e híbrido são extremamente reais. No entanto, com a abordagem e soluções corretas, as empresas podem proteger-se efetivamente e ajudar a prevenir futuros ataques e interrupções nos negócios.

Você está em perigo? Responda a este breve questionário para identificar quais riscos de segurança relacionados ao trabalho remoto e híbrido sua empresa pode estar enfrentando atualmente.

Sim Não

Você pode garantir que suas conexões estão em conformidade com seus controles de acesso?

Sim Não

Você consegue usar devidamente as funções existentes em suas ferramentas?

Sim Não

Você tem visibilidade da frequência de uso das suas ferramentas?

Sim Não

Você pode aproveitar compras centralizadas e administração delegada?

Sim Não

Você tem acesso a sistemas confidenciais gerenciados mediante aprovação?

Sim Não

Você pode confiar que seus usuários sejam realmente os seus usuários?

Se você respondeu "não" para qualquer uma dessas perguntas, sua empresa está em risco. [Entre em contato com um especialista](#) hoje mesmo para conversar sobre as vulnerabilidades da sua empresa.



CIO

PATROCINADO POR

 TeamViewer