BeyondTrust

Os 5 Principais Problemas de Acesso Remoto

Com o crescente número de dispositivos conectados e as vulnerabilidades rodeando as ferramentas e senhas de acesso remoto, as equipes de TI precisam gerenciar os riscos de segurança, ao mesmo tempo que mantêm os usuários produtivos. A expansão do trabalho remoto deve continuar e os requisitos de segurança relacionados ao acesso remoto seguro são mais críticos do que nunca.

A pergunta é: sua empresa possui ferramentas de segurança adequadas para lidar com problemas resultantes do grande volume de terceiros, colaboradores com privilégios e funcionários remotos que se conectam à sua rede?

1 GERENCIANDO O ACESSO DE TERCEIROS

Em média, os profissionais de TI relatam que cerca de 182 terceiros acessam sua rede interna semanalmente[1]. Esses usuários variam, podendo ser fornecedores de hardware, fabricantes de software ou ainda prestadores de serviços. Em geral, eles contam com o Active Directory ou outras credenciais privilegiadas e, muito provavelmente, uma VPN - permitindo que façam login em sua rede a qualquer momento e permaneçam conectados o tempo que desejarem.

[1]BeyondTrust, "Privileged Access Threat Report", 2019

2 ACESSO PRIVILEGIADO "TUDO OU NADA"

A maioria de seus fornecedores ou usuários só precisa de acesso a sistemas muito específicos. Em geral, o uso de uma VPN permite mais acesso do que o necessário, muitas vezes resultando em "sobras" de acesso quando os usuários são removidos ou substituídos. Essa premissa é ainda mais verdadeira quando muitos usuários internos e fornecedores dependem do acesso remoto para realizar funções críticas de trabalho. Ferramentas como VPNs carecem de controles granulares, e só permitem o acesso "tudo ou nada" na camada de rede, não possuindo recursos para o gerenciamento de aplicações ou sessões.

Minha empresa precisa cumprir os requisitos de compliance.

3 ATENDENDO ÀS DIRETRIZES DE CONFORMIDADE

Muitas empresas seguem padrões de conformidade rígidos, como PCI, LGPD e HIPAA. Os procedimentos de auditoria servem para garantir que os requisitos de conformidade sejam atendidos, e é obrigação da empresa comprovar evidências de que estão seguindo os padrões. Muitas ferramentas de acesso legado, como RDP ou VNC, são incapazes de rastrear ou auditar adequadamente a atividade durante sessões remotas.

Preciso manter os usuários remotos produtivos e capazes de acessar os ativos de TI que precisam para realizar seu trabalho.

4 FACILITANDO O TRABALHO REMOTO

As VPNs não foram criadas para a proteger aplicações, desktops compartilhados e aplicações da web. Além do risco de segurança, seu desempenho pode ser comprometido quando muitos usuários remotos estão conectados. As empresas estão buscando alternativas para que os colaboradores possam trabalhar sem interrupções, proporcionando uma melhor experiência de acesso remoto.

5 AS SENHAS SÃO ARMAZENADAS DE MANEIRA MANUAL E NÃO SEGURA

Contas privilegiadas são um ponto de entrada comum para hackers. Como muitos profissionais de TI usam várias delas para acessar os endpoints na rede, o volume de credenciais para gerenciar e proteger é alto. Essas credenciais costumam ser armazenadas e compartilhadas de maneira não segura por meio de planilhas ou bloco de notas. Elas são esquecidas, repetidas e raramente são alteradas.

Ferramentas Legadas não Possuem Recursos Adequados de Segurança e Produtividade

As soluções de gerenciamento de acesso legado, como VPNs ou RDP, abordam apenas um número limitado de casos de uso, que pode resultar no uso de diferentes ferramentas, dependendo da tarefa a ser realizada. A falta de fluxos de trabalho automatizados pode tornar as equipes de TI ainda mais lentas.

Elas também se deparam com falhas de segurança, como resultado da falta de níveis granulares de acesso ou da incapacidade de criar logs para auditorias de conformidade.

Controle, Gerencie e Audite Acessos Remotos com BeyondTrust

Privileged Remote Access

Permite que as empresas forneçam a seus colaboradores remotos ou terceiros o acesso à rede sem a necessidade de conexão com uma VPN. Os usuários recebem acesso a diferentes segmentos da rede ou sistemas específicos usando privilégios. Esse recurso não apenas mitiga os riscos de uma abordagem ampla para atribuição de privilégios em camadas de rede, como também ajuda as equipes de TI a cumprirem com os requisitos de compliance.

O Privileged Remote Access da BeyondTrust permite ainda que sua empresa elimine pontos cegos de acesso remoto, reduza a superfície de ataque e garanta a produtividade das seguintes formas:

- Com uma política de restrição de privilégios, dando a usuários específicos precisamente o nível de acesso necessário a aplicações, sessões e protocolos, pelo tempo que precisam;
- Permitindo acesso a contas compartilhadas a partir de uma trilha de auditoria para acesso;
- Definindo quais endpoints os usuários podem acessar, quando podem acessá-los e quais aplicações ou ações eles podem usar durante essas sessões;
- Restringindo a configuração e instalação de VPNs para fornecedores, usuários privilegiados e colaboradores remotos, usando dispositivos não gerenciados;
- Controlando e monitorando sessões por meio de um agente seguro, ou usando protocolos padrão para conexões RDP, VNC, Web e SSH

Além disso, a solução também inclui um cofre de senhas que garante que as contas gerenciadas tenham suas senhas alternadas regularmente. Para as contas mais sensíveis, você pode utilizar senhas de uso único, ou seja, cada vez que uma senha é usada, ela é alterada para uma nova.

Permita que os profissionais de segurança controlem, monitorem e gerenciem o acesso a sistemas críticos para usuários privilegiados internos e externos com as soluções da BeyondTrust.

Saiba mais e veja uma demo do Privileged Remote Access em

beyondtrust.com/remote-access

A BeyondTrust é líder mundial em Gestão de Acessos Privilegiados (PAM), capacitando as empresas a proteger e gerenciar todo o seu universo de privilégios. A abordagem da Gestão Universal de Privilégios melhora a segurança e protege os privilégios em senhas e endpoints, oferecendo às empresas a visibilidade e o controle de que precisam para reduzir o risco, atingir os requisitos de compliance e aumentar o desempenho operacional.

beyondtrust.com/pt

2020_11_port