BeyondTrust

OS 7 PERIGOS dos PRIVILÉGIOS

Armadilhas de segurança comuns
e como evitá-las

> "Os perigos relacionados aos ataques cibernéticos continuam a evoluir, e compreender os riscos subjacentes é fundamental para proteger sua empresa."

Introdução

Os ataques cibernéticos continuam inabaláveis, impactando empresas em todos os setores e regiões. O cenário das ameaças evolui rapidamente, e a mudança em massa para o trabalho remoto, em virtude da pandemia, fizeram com que os hackers agissem rapidamente para explorar novas vulnerabilidades - 94% das empresas sofreram um ataque cibernético em 2020, com impacto nos negócios.

As manchetes sobre violações em grande escala são alarmantes. Alguns casos mais recentes incluem a SolarWinds, Colonial Pipeline o Serviço Nacional de Saúde do Reino Unido (NHS) e a empresa Virgin Media . A lista é interminável — os hackers não discriminam o setor ou o tamanho da empresa.

Apesar dessas ameaças, muitas organizações sofrem para identificar e implementar estratégias e soluções de segurança corretas. Isso pode ocorrer por vários motivos — falta de recursos, problemas de prioridade ou simplesmente uma atitude de desdém do tipo "Isso não acontecerá aqui".

Neste artigo estão descritos "7 Perigos do Privilégio", como eles impactam a segurança da sua empresa e as diretrizes sobre como evitá-los. Independentemente de quais são mais importantes para você, há soluções para evitar ser vítima de um ataque cibernético e como mitigar os riscos.

1 A velocidade da transformação digital

Transformação digital agora, a segurança depois

das organizações estão envolvidas em um projeto de transformação digital [1]

das empresas sofreram um ataque cibernético com impacto nos negócios em 2020 [2]

Fontes: 1. Nominet: Cyber Security in the Age of Digital Transformation, 2019
2. The Rise of the Business Aligned Security Executive Report, Tenable, 2020

De acordo com um estudo da Nominet, 93% das organizações estão envolvidas atualmente em um projeto de transformação digital. Em virtude da pandemia do coronavírus, **a ampla mudança para o trabalho remoto também acelerou a adoção da nuvem** como um fator importante para impulsionar as iniciativas de transformação digital relacionadas à produtividade.

As promessas do que a transformação digital pode atingir para a eficiência dos negócios podem levar as empresas a implantar novas tecnologias sem priorizar sua estratégia de segurança. O ritmo acelerado em que isso aconteceu significa que a segurança pode não ter sido considerada de forma adequada.

> **As promessas dos projetos de transformação digital podem levar empresas a lançar novas tecnologias sem priorizar sua estratégia de segurança.**

O comportamento dos colaboradores ao utilizar seus próprios smartphones ou laptops pessoais (permissão de trazer/utilizar seu próprio dispositivo) também apresenta problemas. Uma pesquisa recente feita pelo Gartner Group revelou que trabalhadores remotos são mais suscetíveis de usar dispositivos pessoais para cometer “pecados de Shadow IT” —, ou seja, encontrando e usando aplicações de terceiros fora dos aprovados pela TI.

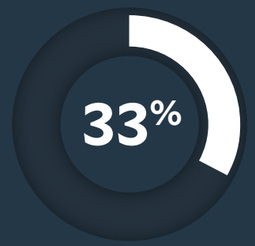
É fundamental que as organizações que estejam realizando projetos digitais considerem a importância da segurança cibernética. Os ecossistemas estão se expandindo, os perímetros estão evoluindo, e a explosão de privilégios contribuiu para a expansão da superfície de ataque. Uma solução completa de Gerenciamento de Acessos Privilegiados pode mitigar esses riscos, gerenciando e controlando os usuários, as sessões e senhas em sua rede, incluindo os envolvidos nos processos de transformação digital ou implantações na nuvem.

Saiba mais: **Proteja sua jornada de transformação digital**

Proliferação na nuvem

Todos esses dados, todas essas nuvens, todos esses privilégios

é o número médio de serviços na nuvem usados por uma organização [3]



de todos os dados existentes estão na nuvem ou passaram por ela [4]

Fontes: 3. Cloud Adoption and Risk Report McAfee, 2019
4. Hosting Tribunal, Big Data Stats for the Big Future, 2021

Atualmente, a maioria das organizações não está meramente em "uma" nuvem - elas estão em muitas nuvens (PaaS, IaaS), e seus usuários consomem dezenas, ou até centenas, de diferentes aplicações do tipo SaaS (Software como Serviço). A grande migração para a nuvem está possibilitando o sucesso do trabalho remoto cada vez maior e impulsionando uma adoção renovada de iniciativas de transformação digital.

Entretanto, com essa mudança em massa para a nuvem, há **mais oportunidades para hackers, com mais vetores de ataque a explorar e vários caminhos para a sua rede.** Se os seus ambientes não possuem arquitetura de segurança e gerenciamento de identidades e credenciais suficientes, os hackers irão explorar brechas para comprometer a rede da sua empresa.

No ano passado, os ataques cibernéticos relacionados à nuvem aumentaram 630%, de acordo com um Relatório da McAfee sobre o risco de adoção da nuvem. A adoção de práticas de segurança com foco na proteção de identidades na nuvem desempenha um papel fundamental para reduzir esses riscos e inclui a aplicação de restrição de privilégios, descoberta e gerenciamento de ativos e contas privilegiadas na nuvem, implementação de controle de aplicações e proteção de ferramentas DevOps.

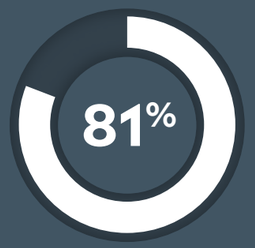
A maioria das organizações utiliza três ou mais nuvens públicas ... isso representa três ou mais vezes o risco de segurança.

Saiba mais: **Guia para gestão de privilégios multicloud**

3

Práticas de senhas arriscadas

Yawn - criar senhas complexas e mudá-las regularmente é realmente necessário?



de violações relacionadas a hackers envolvem senhas roubadas ou fracas [5]

de contas de vítimas de violação de dados usaram 123456 como senha [6]

Fontes: 5. Verizon Data Breach Investigations Report, 2019
6. National Cyber Security Centre (NCSC) Survey, 2019

É necessária apenas uma senha comprometida para iniciar uma violação que pode ter resultados devastadores.

De acordo com um estudo recente da NordPass, **uma pessoa tem em média cerca de 100 senhas que precisam ser lembradas.** Dessa forma, os colaboradores muitas vezes ficam sobrecarregados e podem armazenar as senhas de maneira insegura ou reutilizar a mesma senha para várias contas.

Foi comprovado que o armazenamento inseguro de senhas e a falta de rodízio levam a ataques de phishing e criam brechas de segurança; multiplique esse risco de senhas vulneráveis pelo número de usuários que acessam a rede da sua empresa. Se um colaborador com privilégios de administrador estiver usando uma senha fraca em várias contas, um hacker levará minutos para se infiltrar em uma rede e instalar um ransomware.

Você não pode depender de usuários superando os limites da natureza humana. Para lidar com o risco de senhas, elimine esse ponto problemático para os usuários finais. Em vez de pedir que criem e controlem senhas complicadas para várias contas, ofereça a eles uma ferramenta de acesso ao sistema que não exija que eles saibam a senha. Um ataque de phishing consiste em induzir uma pessoa a clicar em um link ou fornecer suas credenciais por meio de métodos convincentes de engenharia social, assim, um usuário não pode comprometer uma senha que não conhece.

Injeção de credencial é um recurso importante em soluções de gestão de senhas e acesso remoto, permitindo que os usuários simplesmente selecionem uma credencial, a partir de uma lista, para fazer login. Isso elimina a necessidade de armazenar e rastrear credenciais compartilhadas manualmente e cria uma experiência de usuário mais produtiva ao agilizar o acesso a senhas compartilhadas.

Saiba mais: **Explicação da Gestão de Senhas Privilegiadas**

4 Privilégios de administrador em excesso

Todos esses colaboradores precisam realmente de privilégios de administrador?

das vulnerabilidades críticas da Microsoft em 2020 poderiam ter sido mitigadas se os privilégios de administrador fossem removidos [7]

das organizações esperam que as sessões de usuários privilegiados aumentem significativamente nos próximos dois anos [8]

Fontes: 7. Microsoft Vulnerabilities Report 2021, 2021
8. Evolving Privileged Identity Management (PIM) In The 'Next Normal', 2020

A necessidade de acesso é uma questão permanente, e **os usuários geralmente recebem privilégios de administrador para realizar funções que, na realidade, não precisam desses privilégios**. As empresas fornecem aos colaboradores total acesso e controle dos seus sistemas, na esperança de que os usuários nunca precisem incomodar o help desk de TI. O colaborador fica feliz porque se julga autossuficiente. A organização fica feliz porque a produtividade não é afetada. O help desk fica satisfeito porque não é sobrecarregado com solicitações de acesso. Entretanto, essa abordagem apresenta um grande risco de segurança, pois contas com excesso de privilégios são alvos lucrativos para agentes de ameaças.

Para prevenir ataques, é necessário fazer o rastreamento e controle de uso dos privilégios de administrador em computadores, redes e aplicações. Implementar o princípio de restrição de privilégios e remover privilégios de administrador é um requisito fundamental para muitos mandatos de conformidade em todo o mundo, e remover os privilégios de administrador é a melhor ação que você pode fazer para mitigar vulnerabilidades críticas. Entretanto, você também deve considerar o impacto para os usuários - se eles repentinamente ficarem muito bloqueados para concluir suas tarefas diárias, eles ficarão frustrados e o help desk poderá ficar sobrecarregado com tantos chamados.

Soluções eficazes de Gestão de Privilégios de Endpoint podem implementar a restrição de privilégios em horas, sem restringir demasiadamente os usuários ou aumentar os chamados no help desk. As organizações ficam muito mais seguras e a produtividade do usuário final não é afetada - resolvendo eficientemente o equilíbrio entre segurança e produtividade.

Privilégios de administrador em excesso permitem que os ataques de ransomware se propaguem rapidamente e se espalhem pela rede.

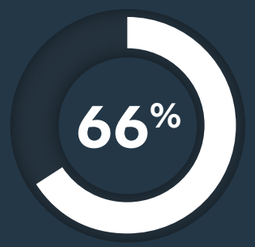
Saiba mais: **Relatório de vulnerabilidades da Microsoft 2021**

5 Colaboradores mal-intencionados

Não há fúria maior do que a de um colaborador desprezado!

$11,45 milhões

é o custo médio total de incidentes relacionados a colaboradores em 2020 [9]



de empresas multinacionais consideram ataques internos ou violações acidentais mais prováveis do que ataques externos [10]

Fontes: 9. 2020 Cost of Insider Threats Global Report, Proofpoint & Observe IT, 2020
10. Tech Journey, Insider Threat Statistics, 2021

Usuários internos mal-intencionados são uma das principais causas de ataques cibernéticos. Eles são classificados como colaboradores atuais ou ex-funcionários que possuem informações sobre as práticas de segurança, dados e sistemas de computação da organização. Embora muitas violações internas sejam resultado de erros não intencionais, no caso desse perigo, é a ira de um ex-funcionário insatisfeito que cria riscos significativos para a segurança cibernética da sua empresa.

Ataques internos são iniciados por colaboradores descontentes que desejam prejudicar suas organizações atuais ou anteriores por meio de roubo de dados e sabotagem - ou para obter algum ganho financeiro.

Recentemente, a Cisco perdeu aproximadamente 1,4 milhão de dólares americanos em custo de mão-de-obra para auditar sua infraestrutura e consertar danos causados por acesso não autorizado de um ex-funcionário. A empresa também teve que pagar um total de 1 milhão de dólares de restituição aos usuários afetados. Este é apenas um dos muitos casos de ameaças internas que ilustram o perigo que está em jogo.

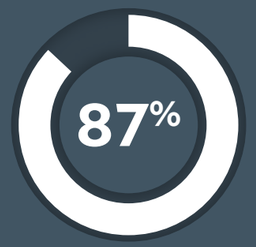
Tomar medidas positivas para mitigar os riscos de ameaças internas incluem a implementação de restrição de privilégios, o rodízio de credenciais privilegiadas com frequência e a contabilização de mudanças de funções de trabalho (incluindo colaboradores que saem da empresa) alterando ou removendo seu acesso em tempo hábil. Gestão de Senhas com Privilégios controlam, monitoram e registram com segurança o acesso a contas com privilégios. Mantenha as senhas atualizadas com um rodízio automatizado - seja de forma programada ou no check-in depois do uso - para eliminar o risco das senhas saírem da organização.

Saiba mais: **Relatório de ameaças a acessos privilegiados**

6 Excesso de confiança

Claro que nossos colaboradores estão vigilantes e cientes das ameaças cibernéticas

das organizações perderam dados em virtude de um ataque de phishing em 2020[11]



de aumento em ataques de phishing contra colaboradores da área financeira em 2020[12]

Fontes: 11. 2021 State of the Phish Report, Proofpoint, 2021
12. Abnormal Quarterly BEC Report Q2, 2020

Mesmo os colaboradores mais diligentes ainda podem cair em uma cilada de phishing por meio de e-mails ou mídias sociais.

Todas as empresas gostariam de presumir que seus colaboradores não seriam ludibriados por um ataque de phishing - entretanto, na realidade 65% das empresas dos EUA relatam ter sofrido um ataque de phishing bem-sucedido . Um relatório recente da Proofpoint revelou que o ataque por phishing continua sendo o tipo de ameaça mais provável para causar uma violação de dados e os hackers sabem disso. O FBI relatou que o phishing foi o tipo mais comum de crime cibernético em 2020, com 241.324 incidentes relatados apenas nos EUA.

Não se trata apenas de phishing. Outras formas de engenharia social em 2021 incluem o aumento de ataques "deepfake". Deepfakes são formas sofisticadas de mídia (vídeo, áudio, fotos e até mesmo sites na internet) que exalam um realismo capaz de convencer o profissional mais experiente. Uma revelação recente mostrando as habilidades preocupantes dos deepfakes foi uma conta falsa (spoof) do TikTok que viralizou, fingindo ser do Tom Cruise.

A Inteligência Artificial (IA) está possibilitando que a tecnologia deepfake ultrapasse nossa capacidade em identificá-la. Poderíamos estar nos comunicando em uma janela de bate-papo com um humano (ou que pensávamos ser uma pessoa), mas na verdade seria um robô mal-intencionado coletando informações confidenciais.

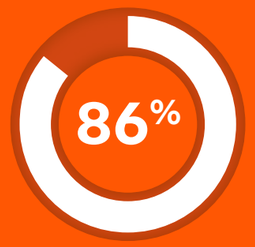
A predominância de phishing, além de métodos cada vez mais convincentes e sofisticados da apresentação de deepfakes, indica que, **até mesmo usuários bem treinados ainda sucumbirão ocasionalmente à essas táticas e basta apenas um deslize para causar uma violação importante.**

O treinamento de conscientização sobre segurança cibernética é um bom passo a ser dado, entretanto ele tem limites. Seus colaboradores são seres humanos, que ainda podem cometer erros, mesmo com amplo conhecimento de ameaças em potencial. Além do treinamento, você pode ativar soluções que reduzem a capacidade de um colaborador ser afetado - mesmo se ele clicar em um link que não deveria - removendo os privilégios de administrador e implementando controles de aplicações.

Saiba mais: **As 5 etapas críticas em sua estratégia de segurança de endpoints**

7 Help desks com falta de pessoal

O help desk de TI tem pessoal insuficiente e com poucos recursos



das equipes de atendimento ao usuário observam que ter um sistema de help desk aumenta sua produtividade[13]

é o tempo médio para fornecer uma primeira resposta a uma solicitação de suporte interno[14]

Fontes: 13. HubSpot, 2020
14. The ZenDesk Benchmark Report

Quando se trata de orçamento e expansão de equipes, **os help desks de TI costumam ser um dos departamentos com menos recursos.** Entretanto, à medida que as outras equipes crescem, o mesmo ocorre com os chamados para o help desk. Mais recentemente, em função da pandemia, a grande mudança para trabalho remoto também gerou uma maior demanda por acesso e suporte remotos. Esses fatores combinados resultam em equipes de TI estressadas, sobrecarregadas e incapazes de fornecer soluções eficientes.

Não são apenas os colaboradores que exigem atenção, os fornecedores que precisam de acesso à rede também pressionam as equipes de TI. Liberar e administrar o acesso de fornecedores pode ser feito de forma manual e ineficiente, e as práticas de segurança das empresas desses terceiros podem ser inferiores que as da sua empresa; 58% das organizações acreditam que provavelmente sofreram uma violação em função do acesso de um fornecedor.

As demandas causadas pela pandemia e a ampla mudança para o trabalho remoto aumentaram as pressões sobre as equipes de TI — e vieram para ficar.

Capacitar as equipes de TI com as ferramentas certas para o acesso e suporte remotos é fundamental para aumentar a produtividade sem comprometer a segurança. Uma solução completa de Acesso Remoto Seguro permite suporte remoto eficiente para resolver problemas técnicos em qualquer dispositivo ou sistema, bem como acesso remoto detalhado para usuários e fornecedores, simples de controlar, gerenciar e auditar — sem a necessidade de uma VPN.

Além disso, implementar uma solução de Gestão de Privilégios em Endpoints não apenas remove os riscos de segurança, como também capacita o help desk a manter cargas de trabalho gerenciáveis, reduzindo a quantidade de chamados. Os usuários podem obter acesso a aplicações conhecidas por meio de listas de permissão atualizáveis e as aplicações são verificadas usando comandos simples.

Saiba mais: **Os 5 principais problemas do acesso remoto**

Proteja sua organização contra esses perigos com o Gerenciamento de Acessos Privilegiados

Quando se trata de segurança, a natureza humana tem seus limites. As constantes pressões no trabalho demonstram que a capacitação e o conhecimento só ajudam você até certo ponto. Entretanto, você pode cercar as brechas de segurança que resultam dos 7 pecados capitais com o Gerenciamento de Acessos Privilegiados (PAM).

O PAM é composto de estratégias e tecnologias de segurança cibernética para exercer controle sobre acessos privilegiados e permissões para usuários, contas, processos e sistemas em um ambiente de TI. Ao controlar contas e credenciais em todo o seu ecossistema, permitindo acesso remoto seguro para colaboradores e fornecedores, além de eliminar privilégios excessivos, o Gerenciamento de Acessos Privilegiados (PAM) reduz significativamente a superfície de ataque ao mesmo tempo que fornece a flexibilidade que os usuários finais necessitam.

Uma estratégia de PAM eficaz ajudará a bloquear múltiplos pontos na cadeia de ataque. Diferentemente das abordagens PAM tradicionais, o modelo exclusivo de Gerenciamento de Privilégios Universais permite que se comece com os casos de uso mais urgentes para a sua organização e, depois atende perfeitamente mais requisitos ao longo do tempo.

O portfólio BeyondTrust PAM é uma solução integrada que simplifica as implantações, reduz custos, melhora a utilização e reduz os riscos associados a privilégios.

> **A riqueza de funcionalidades, a implantação e a escalabilidade tornam a BeyondTrust uma boa opção para empresas multinacionais.**
>
> *— Gartner Critical Capabilities for Privileged Access Management, by Felix Gaehtgens, etc., 16 de julho de 2021*

Gerenciamento de senhas privilegiadas

Descubra, gerencie, audite e monitore contas privilegiadas

Gerenciamento de privilégios em endpoints

Gerencie privilégios em endpoints Windows, Mac, Linux e Unix

Acesso remoto seguro

Gerencie centralmente e proteja o acesso remoto para help desks e terceiros

Saiba mais: beyondtrust.com/solutions

BeyondTrust

Sobre a BeyondTrust

A BeyondTrust é líder mundial em Gerenciamento de Acessos Privilegiados (PAM), capacitando as organizações a proteger e gerenciar todo o seu universo de privilégios. Nossas ferramentas e plataformas integradas oferecem a solução PAM mais completa do setor, permitindo que as organizações reduzam rapidamente sua superfície de ataques em ambientes tradicionais, na nuvem e híbridos.

A abordagem Universal Privilege Management da BeyondTrust protege privilégios por meio de senhas, endpoints e acessos, dando às empresas a visibilidade e o controle necessários para reduzir riscos, obter conformidade e aumentar o desempenho operacional. Nossos produtos permitem o nível ideal de privilégios apenas pelo tempo necessário, criando uma experiência sem atritos para os usuários, aumentando a produtividade.

Com tradição em inovação e firme compromisso com os clientes, as soluções BeyondTrust são fáceis de implantar, gerenciar e escalar conforme os negócios evoluem. Mais de 20.000 clientes confiam na BeyondTrust, incluindo 70% das empresas listadas na lista Fortune 500, além de uma rede global de parceiros

Saiba mais em beyondtrust.com/pt

V2021_07_ENG