



RELATÓRIO BEYONDTRUST DE VULNERABILIDADES MICROSOFT 2020

Conheça os perigos dos direitos de administradores não gerenciados e estratégias para controlá-los



ÍNDICE

1	Introdução e Sumário Executivo	3
2	Destaques de 2019	5
3	Vulnerabilidades por Produto	6
	Internet Explorer & Edge	6
	Windows	7
	Windows Office	8
	Windows Server	9
4	Visão de Cinco Anos	10
5	Análise dos Especialistas	11
	Jane Frankland, Especialista de Cibersegurança	11
	Paula Januszkiewicz, CEO da CQURE	12
	Sami Laiho, MVP e Hacker Ético da Microsoft	13
6	BeyondTrust Endpoint Privilege Management	14
7	Garantindo a Conformidade	14
8	Próximos Passos e Recursos	15
9	Metodologia	16
	Como a Microsoft Classifica as Vulnerabilidades	16
	Precisão dos Dados de Vulnerabilidades	17

1 Introdução e Sumário Executivo

O relatório BeyondTrust de Vulnerabilidades Microsoft 2020, publicado anualmente, analisa os dados de boletins de segurança emitidos pela Microsoft ao longo do ano anterior. Todas as terças-feiras, a Microsoft libera correções para todas as vulnerabilidades que impactam seus produtos, e este relatório oferece um compilado anual, fornecendo uma visão holística das tendências relacionadas às vulnerabilidades e, mais importante, quantas delas poderiam ser mitigadas se os direitos de admin fossem removidos das organizações.

2019 marca o sétimo ano de publicação desse relatório, e inclui uma comparação de tendências de cinco anos, provendo um melhor entendimento de como as vulnerabilidades estão crescendo e em quais produtos especificamente.

Sumário Executivo

Confira a seguir as principais conclusões do relatório deste ano, que analisa todos os boletins Patch Tuesday divulgados ao longo de 2019.

- ▶ Em 2019, 858 vulnerabilidades foram descobertas pela Microsoft
- ▶ O número de vulnerabilidades reportado aumentou 64% nos últimos 5 anos (2015-2019)
- ▶ 77% das vulnerabilidades críticas descobertas em 2019 poderiam ter sido mitigadas com a remoção dos direitos de administrador
- ▶ 100% das vulnerabilidades críticas do Internet Explorer e Edge teriam sido mitigadas pela remoção dos direitos de admin
- ▶ 80% das vulnerabilidades críticas que afetam o Windows 7, 8.1 e 10 teriam sido atenuadas pela remoção dos direitos de admin

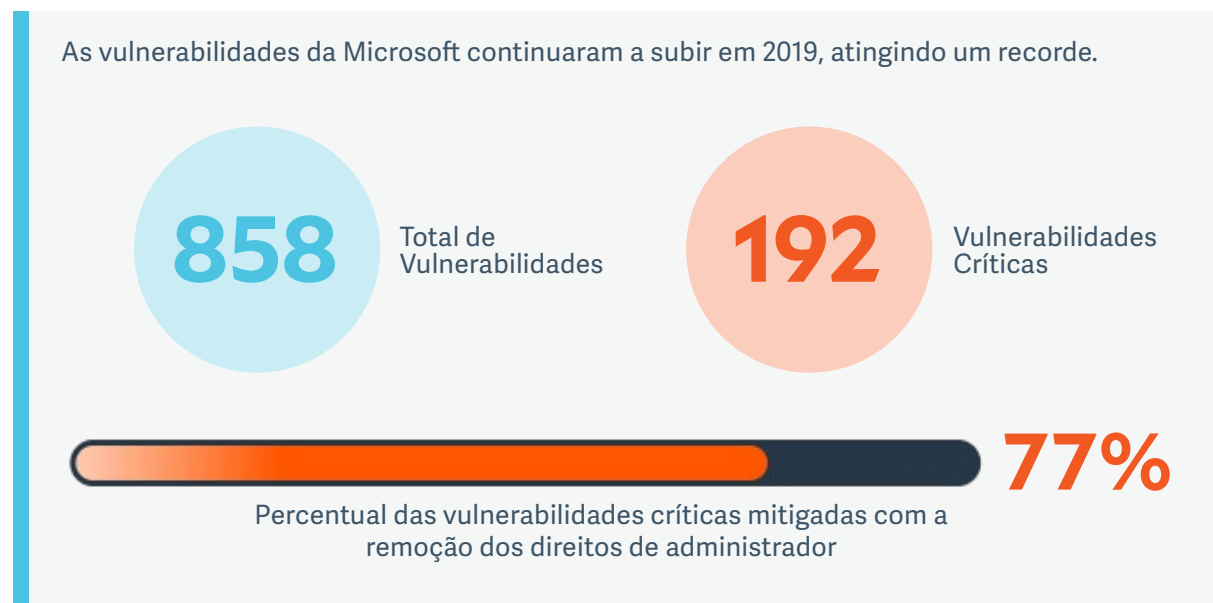


Figura 1: Estatísticas de Vulnerabilidades Microsoft (2019)

Como a Microsoft Agrupa as Vulnerabilidades

Cada Boletim de Segurança da Microsoft é composto por uma ou mais vulnerabilidades, aplicando-se a um ou mais produtos da empresa. Essas categorias, organizadas por tipo de impacto, consistem em: execução remota de código, elevação de privilégios, revelação de informações, negação de serviço, evasão de proteção de segurança, spoofing e tampering.

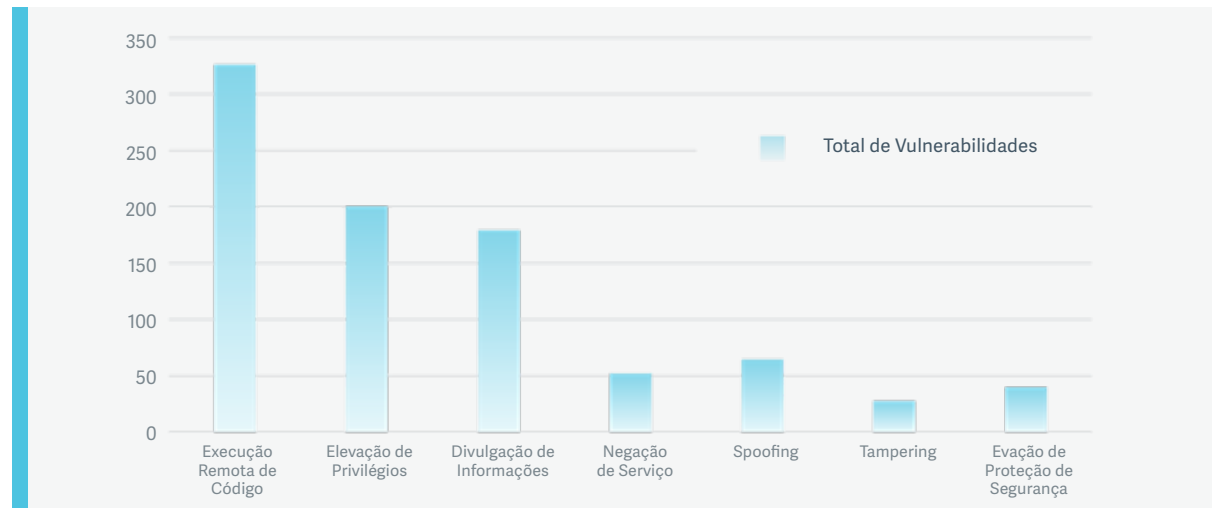


Figura 2: Classificação de categorias de vulnerabilidades Microsoft (2019)

As vulnerabilidades de execução remota de código (RCE) em 2019 atingiram um recorde, enquanto as de elevação de privilégios também aumentaram 37% desde o ano passado

De acordo com relatórios anteriores, a RCE, ou Execução Remota de Código (Remote Code Execution) é responsável pela maior proporção de vulnerabilidades totais da Microsoft ao longo de 2019. Das 323 vulnerabilidades de RCE, 191 foram consideradas críticas. Dessas vulnerabilidades críticas, a remoção dos direitos de admin teria mitigado 76% delas. As vulnerabilidades da RCE em 2019 atingiram um recorde, enquanto as de elevação de privilégios também aumentaram 37% em relação ao ano passado.

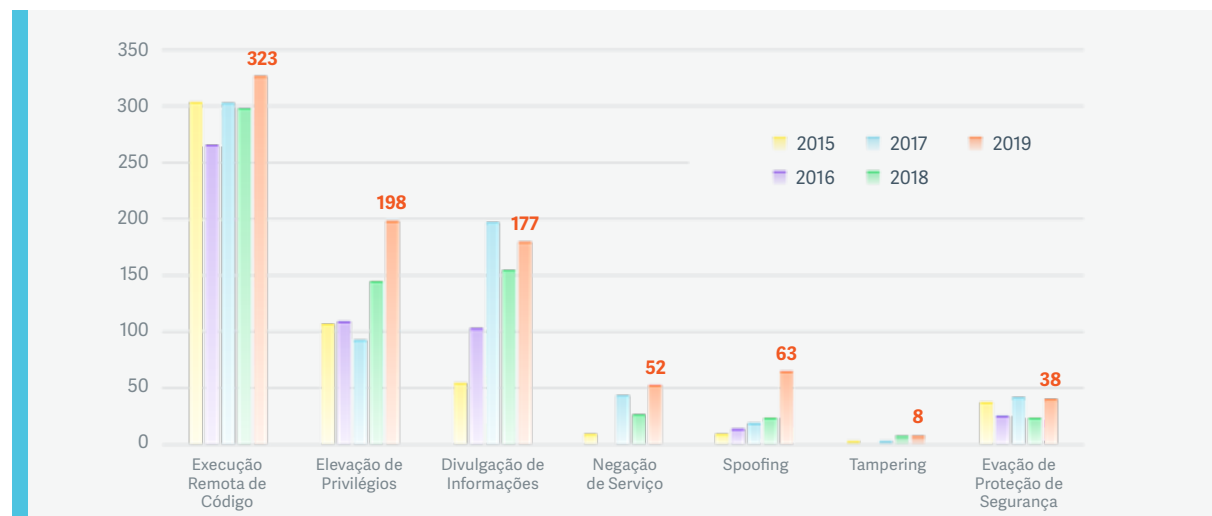


Figura 3: Categorias de vulnerabilidades (2015-2019)

2

Destaques
de 2019

Em 2019, a Microsoft reportou um **número recorde** de vulnerabilidades



858

foi o número total
de vulnerabilidades

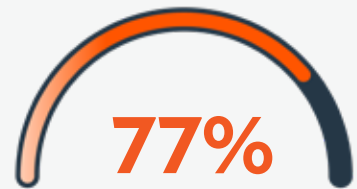


64%



**Foi o Aumento Nos
Últimos 5 Anos**

O número de vulnerabilidades reportadas
subiu de 524 (2015) para 858 (2019)



**Das Vulnerabilidades Críticas
Poderiam ter Sido Mitigadas**

A remoção dos direitos de admin teria
reduzido os riscos significativamente

Como a remoção dos **direitos de administrador** poderia ajudar?



3

INTERNET EXPLORER & EDGE

Vulnerabilidades
por produto

A remoção dos direitos
de admin poderia ter
mitigado 100% do risco.

Apesar do Google Chrome e do Firefox serem os navegadores mais utilizados, o Microsoft Internet Explorer ainda é um navegador bastante popular, mas desde janeiro de 2016 a Microsoft só suporta e corrige a versão mais atual do Internet Explorer. Vale ressaltar que o suporte para o Internet Explorer (IE) terminou em 31 de janeiro de 2020. A partir daí, o IE 11 tornou-se a única versão suportada do Internet Explorer no Windows Server 2012 e do Windows Embedded 8 Standard.

Foram descobertas 33 vulnerabilidades críticas no Internet Explorer 8, 9, 10 e 11 durante 2019. A remoção dos direitos de admin poderia ter mitigado 100% do risco.

As vulnerabilidades críticas do Microsoft Edge aumentaram significativamente desde sua criação, há dois anos, com 86 descobertas no ano passado. Desses 86, a remoção dos direitos de admin poderia ter novamente mitigado 100% do risco.

Em 15 de janeiro de 2020, o Edge mudou para uma nova engine baseada em Chromium, o que significa que tanto o Google Chrome quanto o Edge podem ter as mesmas falhas ao mesmo tempo. Com isso, nenhum desses navegadores podem ser considerados "seguros" para mitigar as vulnerabilidades do Edge.

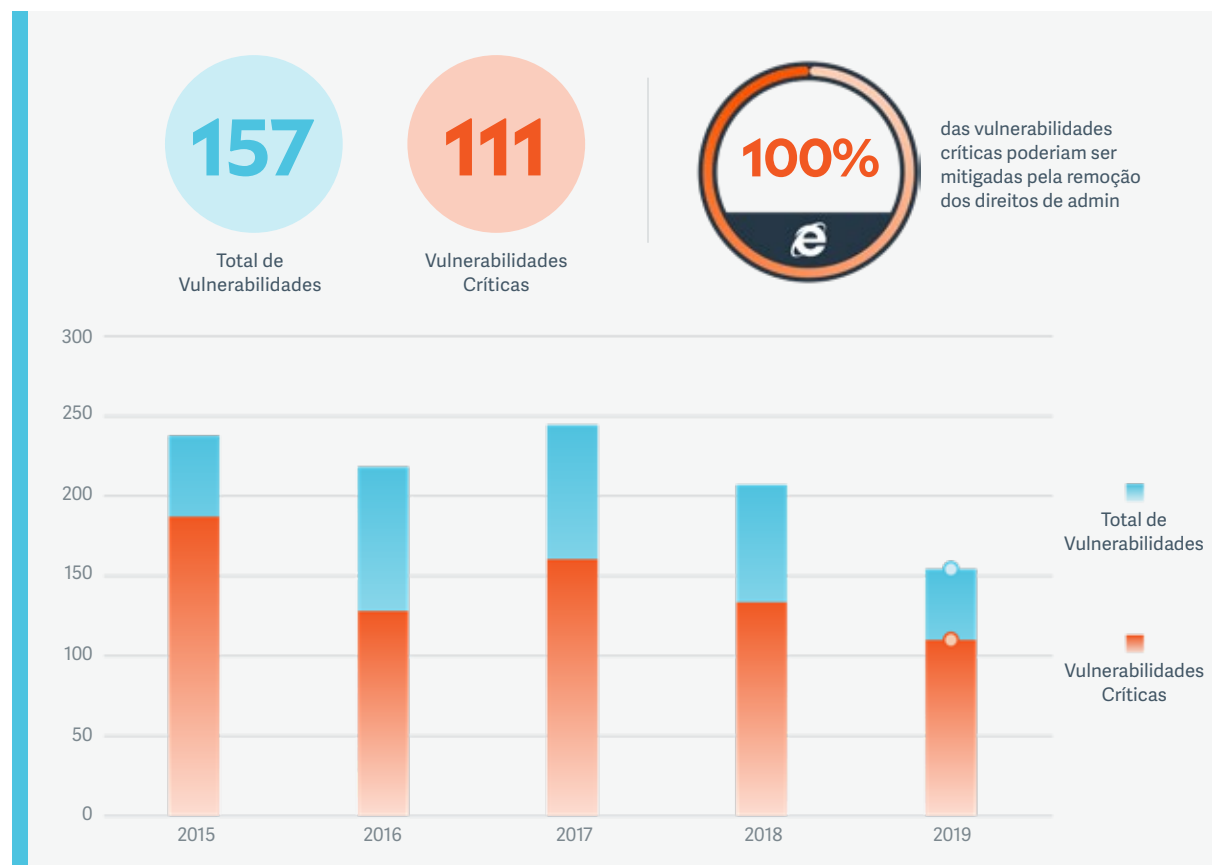


Figura 4: Vulnerabilidades do Microsoft Internet Explorer & Edge (2015-2019)

O Windows 10 foi apontado como o "sistema operacional Windows mais seguro" desde que foi lançado, mas ainda assim experimentou 167 vulnerabilidades críticas no ano passado.

WINDOWS

Em 2019, 667 vulnerabilidades foram relatadas nos sistemas operacionais Windows Vista, Windows 7, Windows RT, Windows 8/8.1 e Windows 10. O Windows 10 foi apontado como o "sistema operacional Windows mais seguro" desde que foi lançado, mas ainda assim experimentou 167 vulnerabilidades críticas no ano passado. De todas as vulnerabilidades do Windows descobertas em 2019, 170 foram consideradas críticas.

A remoção dos direitos de admin poderia ter mitigado 80% dessas vulnerabilidades críticas.

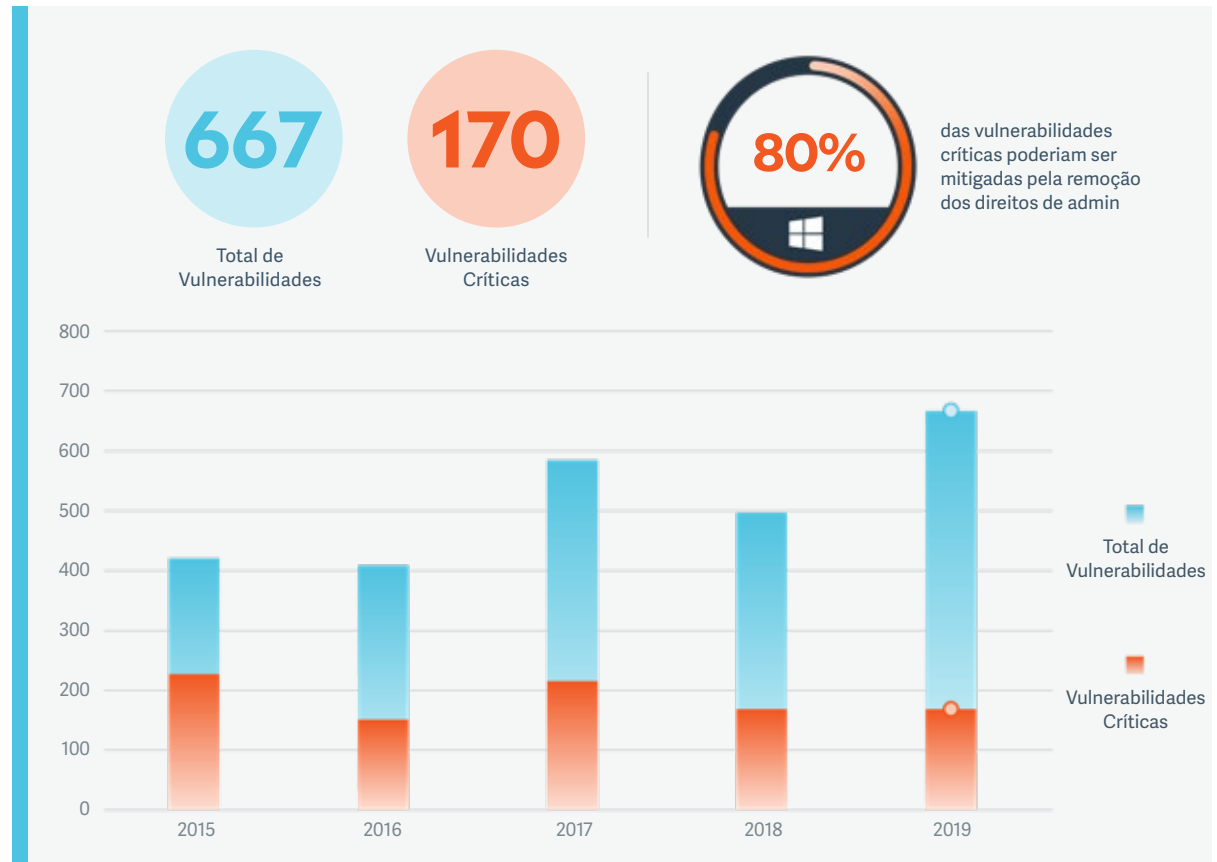


Figura 5: Vulnerabilidades do Microsoft Windows (2015-2019)

"Técnicas de prevenção como a whitelisting de aplicações, a remoção do acesso de administrador e a adoção da estratégia de restrição de privilégios protegem as máquinas individuais dos usuários e reduzem os ataques na rede, mas não restringem severamente a funcionalidade do usuário."

Dr. Eric Cole, Fundador e CEO da Secure Anchor Consulting

WINDOWS OFFICE

Depois de bater um recorde de 102 vulnerabilidades em 2019, o Office viu uma queda de 40% esse ano (60). Das 60, apenas 7 foram consideradas críticas, e a remoção dos direitos de admin mitigaria 100% delas em todos os produtos Office em 2019 (Excel, Word, PowerPoint, Visio, Publisher e outros).



Figura 6: Vulnerabilidades Críticas do Windows (2015-2019)

WINDOWS SERVER

Um total de 668 vulnerabilidades foram relatadas nos boletins de segurança da Microsoft que afetam o Microsoft Windows Server em 2019. Das 171 vulnerabilidades consideradas críticas, 79% poderiam ser mitigadas pela remoção dos direitos de admin.

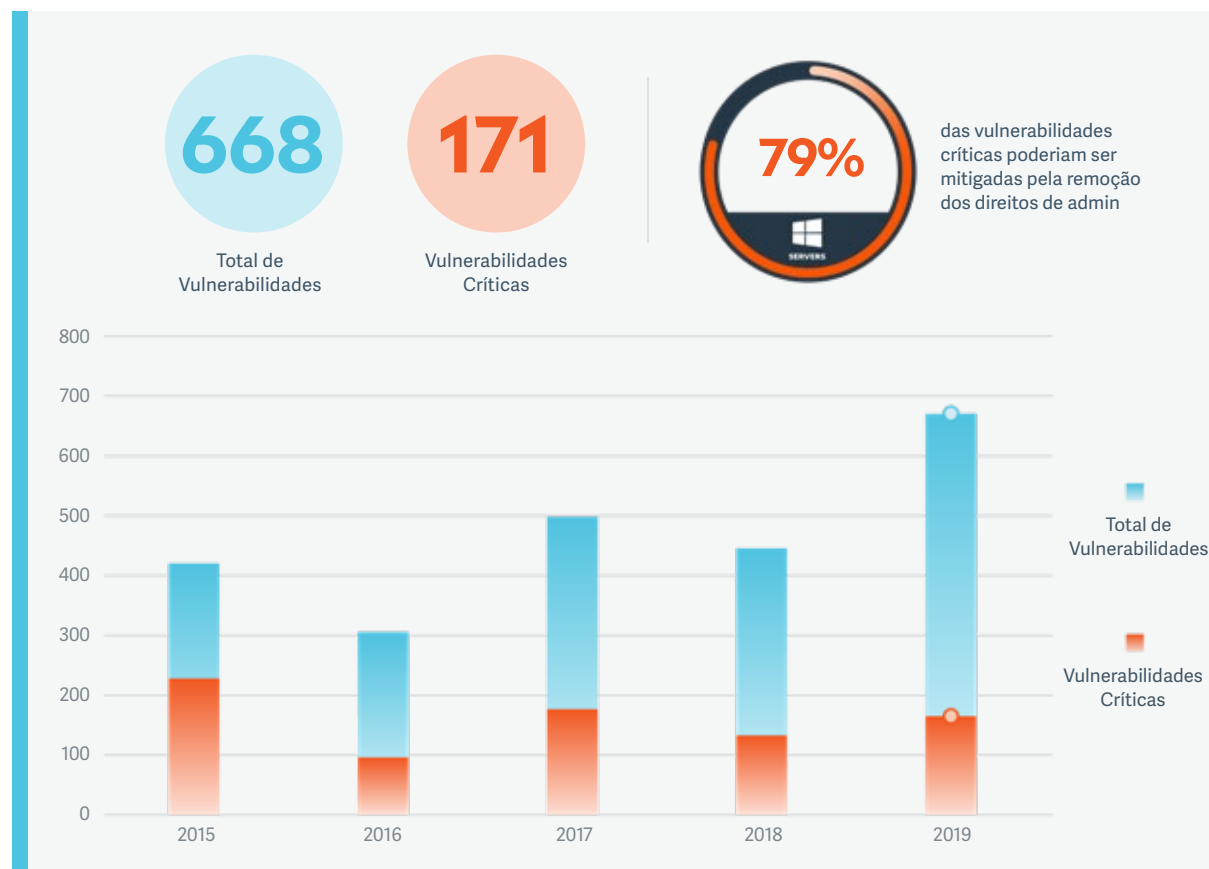


Figura 7: Vulnerabilidades do Servidor Windows (2015-2019)

Em 2013, foram encontradas 252 vulnerabilidades no Microsoft Windows Server – o que significa que houve um aumento significativo das vulnerabilidades nos últimos seis anos.

4 Visão de Cinco Anos

As vulnerabilidades críticas continuam a apresentar riscos e incomodar as organizações que se preocupam em proteger suas redes contra violações de dados. A análise deste relatório indica que a maioria dessas vulnerabilidades pode ser mitigada pela remoção dos direitos de administrador local.

As vulnerabilidades críticas continuam a apresentar riscos e incomodar as organizações que se preocupam em proteger suas redes contra violações de dados.

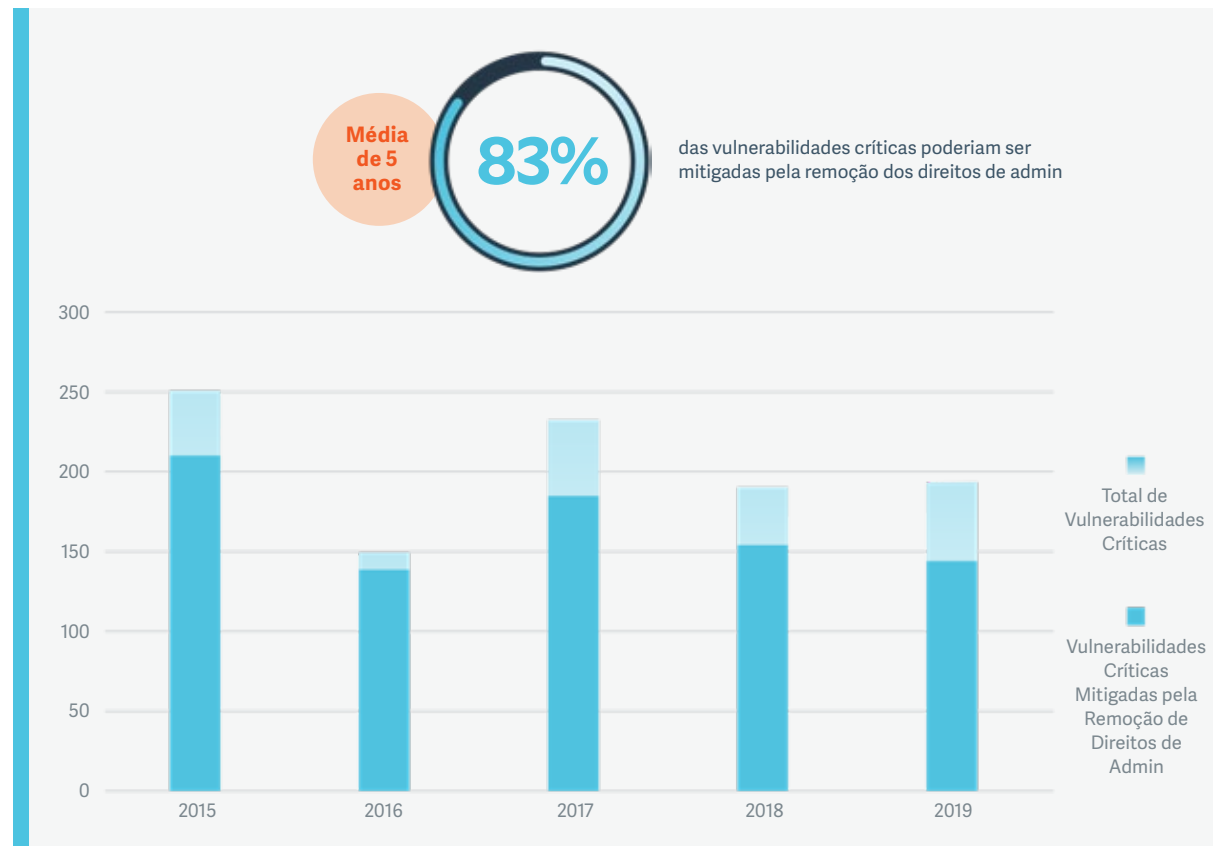


Figura 8: Vulnerabilidades críticas da Microsoft (2015-2019)

5

JANE FRANKLAND

Análise dos Especialistas

*Autora de **IN Security & Renomada Palestrante de Cibersegurança***

A quantidade de dados que produzimos e compartilhamos está crescendo exponencialmente, e a infraestrutura de segurança que protege esses dados está em crescente estresse. Os ataques estão aumentando em volume e qualidade e, sendo persistentes e complexos, a velocidade e a intensidade desses ataques continuam a desafiar todas as partes do nosso ecossistema. O relatório da BeyondTrust demonstra claramente isso e não é surpresa ver as vulnerabilidades aumentando tão significativamente.

Sejam atacantes que estão em busca de pontos fracos, ou colaboradores que acidentalmente colocam em risco a organização através de práticas inseguras, as pessoas têm sido historicamente consideradas como o elo mais fraco. É por isso que praticamente todas as vulnerabilidades exploradas são susceptíveis de serem conhecidas por pesquisadores e especialistas em segurança. Os sistemas sem correção são alvo fácil para os hackers que procuram invadir uma rede e entrar em uma organização. Mesmo após décadas de campanha, o patching – uma prática básica de segurança – ainda não está sendo aplicado efetivamente. Embora a maioria das empresas tenham processos para implantar rapidamente patches críticos no momento de uma vulnerabilidade explorada, muitas ainda se deparam com patches de rotina não críticos. É essa questão que devemos resolver. Patches exitosos reduzem as explorações de vulnerabilidades, paralisações significativas do sistema, problemas de disponibilidade, perdas financeiras e risco de reputação.

“ A remoção dos direitos de admin é uma das medidas mais básicas e poderosas que uma organização pode tomar.



Para reduzir consideravelmente as ameaças, as empresas deveriam adotar como padrão a remoção dos direitos de admin. Muitas vezes, eles desconhecem as vulnerabilidades externas de aplicações e sistemas operacionais não seguros. Mas se elas forem descobertas antes de um hacker, por exemplo, durante um assessment de segurança, poderão ser corrigidas. Caso contrário, é só uma questão de tempo até que um atacante as descubra. E aí é fim de jogo!

A remoção dos direitos de admin reduz os riscos de spyware ou malware, e evita que terceiros façam o mesmo, tornando dados confidenciais inacessíveis, sem possibilidade de modificação ou exportação. Além disso, essa estratégia não deixa que usuários alterem ou bloqueiem usuários fora do sistema ou publiquem conteúdo não autorizado on-line que pode causar danos à marca. É uma das medidas mais básicas e poderosas que uma organização pode tomar.

PAULA JANUSZKIEWICZ**Especialista em segurança cibernética e CEO da CQURE**

Atualmente, técnicas de engenharia social usadas para atingir usuários individuais, como o envio de um anexo malicioso via email, são métodos comumente usados para ter acesso às redes corporativas internas. Este documento mostra essa tendência.

O anexo ou link malicioso podem ser usados para explorar as vulnerabilidades nas aplicações do Internet Explorer, Microsoft Edge ou Microsoft Office. O fato de o usuário abrir o link ou o anexo resulta no acesso direto ao sistema.

Vamos imaginar que este usuário tem privilégios de administrador local. Neste caso, o invasor pode ter acesso não apenas a todos os arquivos do sistema que podem ser baixados ou criptografados, mas também há uma grande possibilidade de reunir credenciais – por exemplo do LSASS – usando-as para atacar outras máquinas na rede. Se o usuário trabalhar com privilégios de administração de servidor ou domínio, o invasor poderá ter acesso a esses hosts e serviços críticos. Este também é um ambiente perfeito para ransomware – se os usuários estiverem operando com direitos de admin, o ransomware pode se espalhar mais facilmente.

Se a restrição de privilégios foi bem implementada, e o usuário não usa privilégios de admin no dia a dia, o invasor teria que se esforçar muito mais para escalar privilégios e realizar movimentos laterais para outras máquinas.

A implementação da restrição de privilégios é uma das tarefas mais importantes que as empresas devem fazer para se proteger das vulnerabilidades mencionadas.

“ Se os usuários estiverem operando com direitos de admin, o ransomware pode se espalhar mais facilmente.



Falando sobre o Gerenciamento de Acessos Privilegiados, também é crucial corrigir softwares e sistemas para remover todas as vulnerabilidades que possam ser exploradas.

O uso de recursos incorporados no Windows 10 também pode ser útil quando se trata de minimizar o risco de ataques. O Windows Defender Exploit Guard é capaz de conter a exploração das vulnerabilidades existentes no software, protegendo os processos. O Credential Guard pode ser usado para isolar as operações de credenciais com o uso da virtualização. Além disso, a lista de aplicações que podem ser executadas na estação de trabalho pode impedir que o código malicioso seja executado.

Para concluir, todas as mitigações juntas podem reduzir com sucesso o risco de ataques maliciosos.

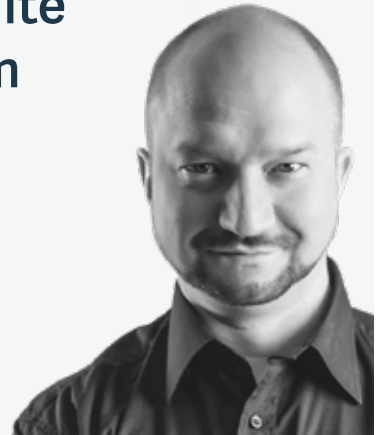
SAMI LAIHO*MVP e Hacker Ético da Microsoft*

As 858 vulnerabilidades descobertas em 2019 são tantas que, embora a correção de sistemas operacionais e aplicações seja importante, a necessidade de proteger proativamente os ambientes é ainda maior. Acredito que a melhor proteção para os ambientes é alcançada por conceitos como restrição de privilégios, whitelisting, MFA e educação/conscientização.

Além do malware comum, o que mais ameaça meus clientes são ransomware e phishing. A maioria dos malwares tradicionais pode ser mitigada removendo direitos de admin. Os resultados são ótimos se comparados com medidas reativas, especialmente quando se trata dos programas e navegadores do Office!

Outro ponto importante: lembre-se que a remoção dos direitos de admin não é apenas uma questão de segurança. Essa estratégia também permite que seus computadores sejam executados de maneira mais rápida, melhor e por mais tempo, com menos reinstalações. Meus clientes também observaram uma redução de 75% na quantidade de chamados ao help desk, depois da remoção dos direitos de admin. Isso significa que você pode ser mais seguro e mais produtivo por longos períodos de tempo!

“ A remoção dos direitos de admin não é apenas uma questão de segurança. Essa estratégia também permite que seus computadores sejam executados de maneira mais rápida, melhor e por mais tempo.



A remoção dos direitos de admin não resolve o problema do ransomware, embora ajude a minimizá-lo. O problema é evidente – você precisa de permissões gravadas para seus dados e, portanto, também pode criptografá-los. A melhor proteção contra o ransomware é a whitelisting. Whitelisting mata ransomware em seus pontos de entrada, como e-mail e navegadores.

Uma das ameaças mais comuns hoje em dia é o phishing. Não é algo que pode ser resolvido apenas com proteções técnicas, pois é difícil garantir que as pessoas não digitem suas senhas nos lugares errados ou reutilizem senhas em vários serviços. A boa notícia é que 99% dos ataques de phishing podem ser mitigados com a implementação da Autenticação Multifatorial (MFA). O 1% restante só pode ser combatido com treinamento e conscientização. E é por isso que ataques simulados de phishing devem ser implementados em todas as empresas combinado com capacitação obrigatória.

6

BeyondTrust Endpoint Privilege Management

As conclusões deste relatório mostram que um grande número de riscos pode ser facilmente mitigado se os direitos dos administradores forem removidos, uma prática recomendada por muitos especialistas do setor. Quais as barreiras que impedem as organizações de enfrentar esses riscos?

A solução de segurança certa pode ajudar as organizações a implementar a abordagem de restrição de privilégios com produtos que não só são implantados rapidamente, mas também atingem o equilíbrio certo entre segurança e produtividade.

Implementar a restrição de privilégios para desktops e servidores é uma etapa crítica para o Gerenciamento Universal de Privilégios, a estratégia BeyondTrust para habilitar o gerenciamento de acessos privilegiados (PAM).

Implementar a restrição de privilégios para desktops e servidores é uma etapa crítica para o Gerenciamento Universal de Privilégios, a estratégia BeyondTrust para habilitar o gerenciamento de acessos privilegiados (PAM). Nesse sentido, o Endpoint Privilege Management é uma solução central do portfólio BeyondTrust PAM.



Figura 9: Portfólio de Soluções BeyondTrust

Com o Endpoint Privilege Management, você pode remover rapidamente privilégios excessivos de usuários Windows, Mac, Unix, Linux e dispositivos de rede, além de reduzir riscos sem impactar a produtividade do usuário.

Com a solução, você também garante a conformidade interna e externa removendo privilégios em excesso, usando whitelisting de aplicações e fornecendo trilhas de auditoria das atividades dos usuários.

Nossa solução Endpoint Privilege Management está disponível via appliance virtual ou físico, e na nuvem (SaaS), para que empresas de todos os tamanhos possam garantir a segurança dos endpoints com uma solução que seja escalável e econômica.



7

Garantindo a Conformidade

Implementar o princípio de restrição de privilégios e remover os direitos de admin são requisitos fundamentais para garantir a conformidade. Os requisitos de conformidade podem ser agrupados em três propósitos principais — proteger, controlar e auditar o uso de recursos de TI e os dados confidenciais que eles contêm.

O uso de uma solução de gerenciamento de privilégios nos endpoints como parte de sua estratégia de segurança permite que as organizações atendam aos seguintes requisitos:

- ▶ Rastreamento, controle, prevenção e correção do uso, atribuição e configuração de privilégios de admin em computadores, redes e aplicações. (CIS, PCI, NIST, HIPAA, GDPR)
- ▶ Implementação de uma única função primária por servidor e permissão apenas para tarefas, protocolos, daemons, etc. necessários, etc. (PCI, CIS)
- ▶ Apuração, gerenciamento e análise de registros de auditoria de eventos que possam ajudar a detectar e entender ataques; os registros de auditoria devem especificar identificação do usuário, tipo de evento, data e hora. (CIS, PCI, NIST, HIPAA, GDPR)

Confira uma lista completa desses requisitos e como as ferramentas da BeyondTrust os habilitam na Matriz de Conformidade.

Próximos Passos e Recursos

- 8** Ao endereçar o problema de direitos de admin não gerenciados, você pode rapidamente alcançar a segurança nos endpoints eliminando as brechas de segurança e atendendo aos requisitos de conformidade, sem prejudicar a produtividade dos usuários.

Entre em contato com a BeyondTrust para agendar uma demo do Endpoint Privilege Management e entender esses recursos.

Whitepaper

- ▶ [A Comprehensive Guide to Endpoint Privilege Management Case Study](#)

Estudo de Caso

- ▶ [How the University of Derby Secure their Endpoints with BeyondTrust](#)

Video

- ▶ [A Two-Minute Overview of our Endpoint Privilege Management Solution](#)

Datasheets

- ▶ [Privilege Management for Windows & Mac](#)
- ▶ [Privilege Management for Unix & Linux](#)

Metodologia

- 9** Cada boletim emitido pela Microsoft contém um Sumário Executivo com informações gerais. Para este relatório, uma vulnerabilidade que pode ser mitigada pela remoção dos direitos de admin é classificada se atender aos seguintes critérios indicados pela Microsoft:

- ▶ Clientes/usuários cujas contas estão configuradas para ter menos direitos de usuário no sistema podem ser menos impactados do que os usuários que operam com direitos administrativos do usuário
- ▶ Se o usuário atual estiver logado com os direitos de admin, um invasor pode assumir o controle de um sistema comprometido

COMO A MICROSOFT CLASSIFICA AS VULNERABILIDADES

Cada vulnerabilidade pode ser encontrada em um ou mais produtos Microsoft, e cada uma delas é atribuída a uma das sete categorias existentes; execução remota de código, elevação de privilégios, revelação de informações, negação de serviço, bypass de recurso de segurança, spoofing, adulteração, que podem variar dependendo do software ou combinação de software comprometidos.

Uma vulnerabilidade de cada tipo geralmente se aplica a uma combinação de diferentes versões de um produto ou produtos, e às vezes todas as versões – por exemplo, todas as versões de clientes Windows. Muitas vezes, uma vulnerabilidade só se aplica a uma combinação de produtos – por exemplo, o Internet Explorer 11 no Windows 7.

A cada vulnerabilidade também é atribuído um nível de gravidade – crítica, importante, moderada – que também varia dependendo de cada software, ou combinação de softwares comprometidos.

O Common Vulnerability Scoring System (CVSS) é um padrão usado por organizações em todo o mundo, e fornece uma maneira de capturar as principais características de uma vulnerabilidade, resultando em uma pontuação numérica que reflete sua gravidade. O score numérico pode então ser traduzido em uma representação qualitativa (como baixa, média, alta e crítica) para ajudar as organizações a avaliar e priorizar adequadamente seus processos de gerenciamento de vulnerabilidades.

Certas vulnerabilidades ocorreram várias vezes ao longo de 2019, geralmente afetando diferentes softwares. Nesses casos, a vulnerabilidade em si só é contada uma vez, com todos os tipos de software afetados atribuídos a essa entrada.

PRECISÃO DOS DADOS DE VULNERABILIDADES

Várias generalizações foram aplicadas para cada vulnerabilidade, considerando o seguinte:

- ▶ Cada vulnerabilidade foi classificada de acordo com o maior nível de gravidade de todas as instâncias dessa vulnerabilidade, caso ela tenha aparecido mais de uma vez
- ▶ Cada vulnerabilidade foi classificada com o tipo mais prevalente para todas as instâncias dessa vulnerabilidade
- ▶ As versões do produto não foram levadas em conta
- ▶ As combinações de produtos não foram levadas em conta
- ▶ As vulnerabilidades foram contadas tanto para o software quanto para a versão, quando apropriado (por exemplo, uma vulnerabilidade para o Internet Explorer 11 no Windows 10 é considerada como vulnerabilidade tanto para o Internet Explorer 11 quanto para o Windows)

SOBRE O ENDPOINT PRIVILEGE MANAGEMENT

O BeyondTrust Endpoint Privilege Management combina gerenciamento de privilégios e controle de aplicações para gerenciar eficientemente os direitos de administrador em dispositivos Windows, Mac, Unix, Linux e rede, sem prejudicar a produtividade. Implemente a estratégia de restrição de privilégios e elimine os direitos de admin locais com controles, garantindo a expansão do seu universo de privilégios, ao mesmo tempo em que cria uma experiência de usuário tranquila.

SOBRE A BEYONDTTRUST

A BeyondTrust é líder mundial em Gestão 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 ataque em ambientes tradicionais, em 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, alcançar conformidade e aumentar o desempenho operacional. Mais de 20.000 clientes confiam na BeyondTrust, incluindo 70% das empresas listadas na Fortune 500, além de uma rede global de parceiros.

beyondtrust.com/pt/