BeyondTrust

LOS 7 PELIGROS de los PRIVILEGIOS

Trampas de seguridad comunes
y cómo evitarlas

"Los peligros de ataques cibernéticos continúan en evolución, y entender los riesgos subyacentes es fundamental para la protección de su empresa."

Introducción

Los ataques cibernéticos continúan sin tregua, impactando compañías en todos los sectores y regiones. El escenario de las amenazas evoluciona rápidamente, y la pandemia y el cambio masivo hacia el teletrabajo hizo que los atacantes actuasen rápidamente para explorar nuevas vulnerabilidades - el 94% de las empresas sufrieron un ataque cibernético en 2020, impactando los negocios.

Los titulares están llenos de violaciones en gran escala, desde por exemplo, SolarWinds y Colonial Pipeline hasta el Servicio Nacional de Salud del Reino Unido (NHS) y la empresa Virgin Media. La lista es interminable — los hackers no hacen distinción sobre el tipo de sector o el tamaño de la empresa.

A pesar de tales amenazas, muchas organizaciones luchan para identificar e implementar estrategias y soluciones de seguridad correctas. Eso puede deberse a diversos motivos — falta de recursos, problemas de prioridad o sencillamente una actitud de negación como "Eso no va a pasar aquí".

En este artículo se describen los “7 Peligros de los Privilegios”, cuál es el impacto que causan sobre la seguridad de su empresa y las directrices para evitarlos. Independientemente de cuáles son los más importantes para Ud., hay soluciones para evitar ser víctima de un ataque cibernético y cómo mitigar sus riesgos.

La velocidad de la transformación digital

Transformación digital ahora, seguridad después

de las organizaciones están envueltas en un proyecto de transformación digital [1]

de las empresas sufrieron un ataque cibernético que causó impacto en los negocios en 2020 [2]

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

De acuerdo con un estudio de Nominet, el 93% de las organizaciones están envueltas actualmente en un proyecto de transformación digital. Por causa de la pandemia de coronavirus, **el cambio masivo hacia el teletrabajo también aceleró la adopción de la nube** como un factor importante para dar impulso a las iniciativas de transformación digital relacionadas con la productividad.

Las promesas de lo que la transformación digital puede alcanzar para la eficiencia de los negocios pueden hacer que las empresas implanten nuevas tecnologías sin priorizar su estrategia de seguridad. El ritmo acelerado en que eso sucedió significa que la seguridad puede no haberse considerado de la forma adecuada.

> **Las promesas de los proyectos de transformación digital pueden hacer que las empresas lancen nuevas tecnologías sin priorizar su estrategia de seguridad.**

El comportamiento de los colaboradores cuando utilizan sus propios smartphones o laptops personales (permiso para traer/utilizar su propio dispositivo) también presenta problemas. Una encuesta reciente realizada por el Gartner Group reveló que trabajadores en teletrabajo tienen más tendencia a usar dispositivos personales para cometer "pecados de Shadow IT" —, es decir, encontrar y utilizar aplicaciones de terceros que no fueron aprobadas por TI.

Es fundamental que las organizaciones que estén realizando proyectos digitales consideren la importancia de la seguridad cibernética. Los ecosistemas en expansión, los perímetros en evolución y la explosión de privilegios han contribuido al aumento de la superficie de ataque. Una solución incluyente de Gestión de Accesos Privilegiados puede mitigar esos riesgos, administrando y controlando a los usuarios, las sesiones y contraseñas en su red, incluyendo los relacionados a la transformación digital o implantaciones en la nube.

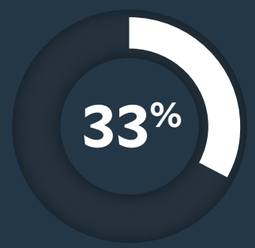
Más detalles: **Proteja su jornada de transformación digital**

2 Proliferación de nubes

Todos esos datos, todas esas nubes, todos esos privilegios

1.935

es el número promedio de servicios en la nube utilizados por una organización [3]



de todos los datos existentes están en la nube o han pasado por ella [4]

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

Actualmente, la mayoría de las organizaciones no está simplemente en "una" nube – están en muchas nubes (PaaS, IaaS), y sus usuarios consumen docenas, o incluso centenas de diferentes aplicaciones SaaS (Software como Servicio). La gran migración para la nube permite el éxito cada vez mayor del teletrabajo y da impulso a una adopción renovada de iniciativas de transformación digital.

Sin embargo, con ese cambio en masa para la nube, surgen **más oportunidades para los atacantes, con más vectores para explorar y diversos caminos hacia dentro de su red.** Si sus ambientes no tienen arquitectura de seguridad y gestión de identidades y credenciales suficientes, los atacantes explorarán brechas para perjudicar la red de su empresa.

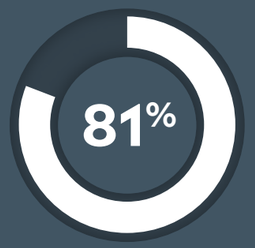
El año pasado, los ataques cibernéticos relacionados a la nube aumentaron el 630%, de acuerdo con un Informe de McAfee sobre el riesgo de adopción de la nube. La adopción de prácticas de seguridad con enfoque en la protección de identidades en la nube desempeña un papel fundamental para reducir esos riesgos e incluye la aplicación de restricción de privilegios, descubrimiento y gestión de activos en la nube y cuentas privilegiadas, implementación de control de aplicaciones y protección de herramientas DevOps.

La mayoría de las organizaciones emplea tres o más nubes públicas... eso representa tres o más veces el riesgo de seguridad.

Más detalles: **Guía para gestión de privilegios multicloud**

3 Prácticas de contraseñas arriesgadas

¿Yawn - Es realmente necesario crear contraseñas complejas y cambiarlas con regularidad?



de violaciones relacionadas a atacantes envuelven contraseñas robadas o débiles [5]

de cuentas de víctimas de violación de datos usaron 123456 como contraseña [6]

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

Solamente se necesita una contraseña comprometida para dar inicio a una violación que puede tener resultados devastadores.

De acuerdo con un estudio reciente de NordPass, **una persona tiene en promedio casi 100 contraseñas que necesita recordar.** De tal forma, los colaboradores muchas veces están sobrecargados y pueden almacenar las contraseñas de manera insegura o reutilizar la misma contraseña para varias cuentas.

Fue comprobado que el almacenamiento inseguro de contraseñas y la falta de rotación de ellas causan ataques de phishing y crean brechas de seguridad; multiplique ese riesgo de contraseñas vulnerables por el número de usuarios que realizan el acceso a la red de su empresa. Si un colaborador con privilegios de administrador estuviera usando una contraseña débil en varias cuentas, un atacante solamente se demorará algunos minutos para infiltrarse en una red e instalar un ransomware.

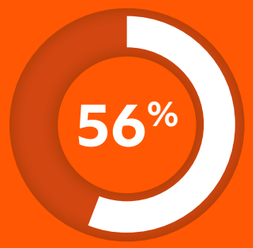
Ud. no puede depender de que los usuarios superen los límites de la naturaleza humana. Para enfrentar el riesgo de contraseñas, elimine ese punto problemático para ellos. En lugar de pedirles que creen y controlen contraseñas complicadas para varias cuentas, ofrézcales a los usuarios una herramienta de acceso al sistema que no requiera que ellos conozcan la contraseña. Un ataque de phishing consiste en engañar a una persona para que haga clic en un link o que informe sus credenciales por medio de métodos convincentes de ingeniería social; por esto, un usuario no puede comprometer una contraseña que no conoce.

Inyección de credencial es un recurso importante en soluciones de gestión de contraseñas y acceso remoto, permitiendo que los usuarios simplemente seleccionen en una lista de credenciales para realizar el login en los sistemas para los que tienen autorización de acceso. Eso elimina la necesidad de almacenar y rastrear credenciales compartidas manualmente y crea una experiencia de usuario más productiva al agilizar el acceso a contraseñas compartidas.

Más detalles: **Explicación de Gestión de Contraseñas Privilegiadas**

4 Demasiados privilegios de administrador

¿Todos esos empleados necesitan realmente de privilegios de administrador?



de las vulnerabilidades críticas de Microsoft en 2020 podrían haberse mitigado si los privilegios de administrador se hubieran retirado [7]

de las organizaciones esperan que las sesiones de usuarios privilegiados aumenten significativamente en los próximos dos años [8]

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

La necesidad de acceso es una cuestión permanente y **los usuarios generalmente reciben privilegios de administrador completos en funciones que no necesitan tales privilegios**. Las empresas proporcionan a los colaboradores control y acceso total de sus sistemas con la esperanza de que nunca necesiten molestar al help desk de TI. El colaborador está contento porque se juzga autosuficiente. La organización está contenta porque la productividad no es afectada. El help desk está satisfecho porque no se sobrecarga con solicitudes de acceso. No obstante, ese abordaje presenta un gran riesgo de seguridad, puesto que cuentas con exceso de privilegios son objetivos rentables para agentes de amenazas.

Pare los ataques realizando rastreo y controlando el uso, la atribución y la configuración de privilegios administrativos en computadoras, redes y aplicaciones. Implementar el principio de restricción de privilegios y retirar privilegios de administrador es la clave para muchos mandatos de conformidad en todo el mundo y retirar los privilegios de administrador es la mejor acción que Ud. puede realizar para mitigar vulnerabilidades críticas de Microsoft. Entretanto, Ud. también debe considerar el impacto sobre los usuarios – si de repente ellos tuvieran mucho bloqueo para concluir sus tareas diarias, ellos se frustrarán y el help desk podrá tener sobrecarga de llamadas de ayuda.

Soluciones eficaces de Gestión de Privilegios en Endpoints pueden implementar la restricción de privilegios en cuestión de horas, sin restringir demasiado a los usuarios o aumentar los pedidos de ayuda al help desk. Las organizaciones se sienten mucho más seguras y la productividad del usuario final no se ve afectada - resolviendo eficientemente el equilibrio entre seguridad y productividad.

Exceso de privilegios de administrador permiten que los ataques de ransomware se propaguen rápidamente y se difundan por la red.

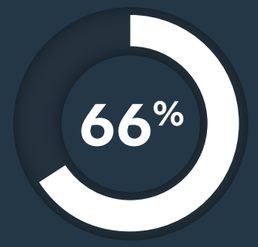
Más detalles: **Informe de vulnerabilidades de Microsoft 2021**

Personas malintencionadas dentro de la empresa

¡No existe en el mundo rabia mayor que la de un empleado despreciado!

$11,45 millones

es el costo promedio total de incidentes relacionados a personas internas en 2020[9]



de empresas multinacionales consideran ataques internos o violaciones accidentales más probables que ataques externos[10]

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

Usuarios internos malintencionados son una de las principales causas de los ataques cibernéticos. Se clasifican como empleados actuales o exempleados – incluso contratistas o socios comerciales - que tienen informaciones sobre las prácticas de seguridad, datos y sistemas de computación de la organización. Aunque muchas violaciones internas sean el resultado de errores no intencionales, en el caso de ese peligro, es la rabia de un exempleado insatisfecho la que crea riesgos significativos para la seguridad cibernética de su empresa.

Ataques internos los inician empleados insatisfechos que quieren perjudicar a las organizaciones en que trabajan o trabajaron por medio de robo de datos y sabotaje - o buscando alguna ganancia financiera.

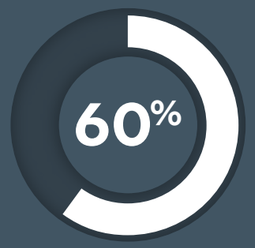
Recientemente, Cisco perdió aproximadamente 1,4 millón de dólares estadounidenses en costo de mano de obra para auditar su infraestructura y reparar daños causados por un acceso no autorizado de un exempleado. La empresa también tuvo que pagar un total de $ 1 millón de dólares de restitución a los usuarios afectados. Este es tan solo uno de los muchos casos de amenazas internas que ilustran las ramificaciones en juego.

Tomar medidas positivas para mitigar los riesgos de amenazas internas incluyen la implementación de restricción de privilegios, la rotación de credenciales privilegiadas con frecuencia y el control de cambios de puestos de trabajo (incluyendo empleados que salen de la empresa) alterando o retirando su acceso de forma oportuna. Soluciones de Gestión de Contraseñas con Privilegios controlan, monitorean y registran con seguridad el acceso a cuentas con privilegios. Mantenga las contraseñas actualizadas con una rotación automatizada – sea de forma programada o en el check-in después de su uso – para eliminar el riesgo de que las contraseñas salgan de la organización.

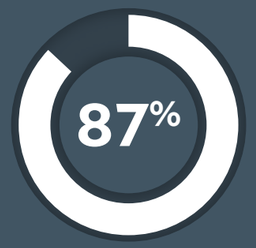
Más detalles: **Informe de Amenazas de Accesos Privilegiados**

6 Exceso de confianza

Claro que nuestros empleados son vigilantes y tienen conciencia de las amenazas cibernéticas



de las organizaciones perdieron datos debido a un ataque de phishing en 2020 [11]



de aumento de ataques de phishing contra empleados del área financiera en 2020 [12]

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

Incluso los empleados más diligentes pueden caer en una celada de phishing hiperrealista vía correo electrónico o redes sociales.

A todas las empresas les gustaría asumir que sus empleados no serían engañados por un ataque de phishing – pero la realidad es que el 65% de las empresas de EE.UU. relatan haber sufrido un ataque de phishing exitoso. Un informe reciente de Proofpoint reveló que el ataque de phishing continúa siendo el tipo de amenaza con mayor probabilidad de causar una violación de datos y los atacantes lo saben. El FBI informó que el phishing fue el crimen cibernético más común en 2020, con 241.324 incidentes relatados tan solo en EE.UU.

No se trata apenas de phishing. En 2021, otras formas de ingeniería social incluyen el aumento de ataques "deepfake". Deepfakes son formas sofisticadas de medios (vídeo, audio, fotos e incluso páginas de internet) con un realismo tal que es capaz de convencer al profesional con experiencia. Una revelación reciente que muestra las habilidades preocupantes de los deepfakes fue una cuenta falsa (spoof) de TikTok y su viralización, fingiendo ser de Tom Cruise.

La Inteligencia Artificial (IA) posibilita que la tecnología deepfake supere nuestra capacidad de identificarla. Podríamos estar comunicándonos en una ventana de chat con una persona (o lo que creíamos que era una persona), pero que en realidad es un robot malintencionado colectando informaciones confidenciales.

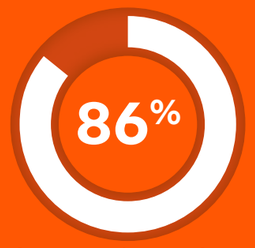
La predominancia de phishing, además de métodos cada vez más convincentes y sofisticados de presentación de deepfakes, indica que **incluso usuarios bien capacitados que sucumbirán ocasionalmente a tales tácticas y que lo único que se necesita es un desliz para tener una violación importante.**

La capacitación para tener conciencia sobre seguridad cibernética es un paso importante, pero tiene sus limitaciones. Sus empleados son seres humanos que pueden cometer errores, aunque tengan un vasto conocimiento de las potenciales amenazas. Además de la capacitación, Ud. puede activar soluciones que reduzcan la capacidad de que un empleado sea afectado, aunque haga clic en un link en el que no debería hacerlo, retirando los privilegios de administrador e implementando controles de aplicaciones.

Más detalles: **5 Pasos Críticos en Su Estrategia de Seguridad en Endpoints**

7 help desks de TI con poco personal

El help desk de TI tiene una plantilla insuficiente y con pocos recursos



de los equipos de soporte al usuario observan que tener un sistema de help desk aumenta su productividad[13]

es el tiempo promedio para dar una primera respuesta a una llamada de soporte interno[14]

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

Cuando se trata de presupuesto y expansión de equipo, **los help desks de TI suelen ser uno de los departamentos con menos recursos.** Sin embargo, a medida que otros equipos crecen, lo mismo sucede con la entrada de pedidos de servicio al help desk. Recientemente, debido a la pandemia, el gran cambio hacia el teletrabajo también generó una demanda de acceso y soporte remotos. La combinación de esos factores resulta en equipos de TI estresados, sobrecargados e incapaces de proporcionar soluciones eficientes.

No son solo los empleados que demandan atención, los proveedores subcontratados que solicitan acceso a la red también colocan presión sobre los equipos de TI. Autorizar y administrar el acceso de proveedores puede realizarse de forma manual e ineficiente y las prácticas de seguridad de esos proveedores pueden ser inferiores a las de su empresa; El 58% de las organizaciones cree que es probable que hayan sufrido una violación debido al acceso de un proveedor.

Las demandas causadas por la pandemia y el cambio masivo para el teletrabajo han aumentado las presiones sobre los equipos de TI — y van a permanecer.

Capacitar a los equipos de TI con las herramientas correctas para el acceso y soporte remoto es fundamental para aumentar la productividad sin comprometer la seguridad. Una solución amplia de Acceso Remoto Seguro permite un soporte remoto eficiente para solucionar problemas técnicos en cualquier dispositivo o sistema, así como el acceso remoto detallado a usuarios y proveedores que es simple de controlar, administrar y auditar — sin necesidad de una VPN.

Además, implementar una solución de Gestión de Privilegios en Endpoints no solo retira los riesgos de seguridad, como también capacita a los equipos del help desk para que mantengan cargas de trabajo administrables, reduciendo la cantidad de órdenes de servicio. Los usuarios finales pueden tener acceso a aplicaciones conocidas por medio de listas de permiso actualizables y las aplicaciones se verifican utilizando comandos simples.

Más detalles: **Los 5 principales problemas del acceso remoto**

Proteja su organización contra esos peligros con la Gestión de Accesos Privilegiados

Cuando se trata de seguridad, la naturaleza humana tiene sus límites. Las constantes presiones en el trabajo demuestran que la capacitación y el conocimiento solamente alcanzan hasta cierto punto. Sin embargo, Ud. puede cerrar las brechas de seguridad que son resultado de los 7 Pecados Capitales con la Gestión de Accesos Privilegiados (PAM).

PAM se compone de estrategias y tecnologías de seguridad cibernética para ejercer control sobre los accesos privilegiados y permisos para usuarios, cuentas, procesos y sistemas en un ambiente de TI. Por controlar cuentas y credenciales en todo su ecosistema, permitiendo el acceso remoto seguro para empleados y proveedores, además de eliminar privilegios en exceso, la Gestión de Accesos Privilegiados (PAM) reduce significativamente la superficie de ataque, al mismo tiempo que proporciona la flexibilidad que sus usuarios finales necesitan.

Una estrategia de PAM eficaz ayudará a bloquear múltiples puntos en la cadena de ataque. Diferentemente de los abordajes de PAM tradicionales, el modelo exclusivo de Gestión Universal de Privilegios permite comenzar por los casos de uso más urgentes para su organización y después atiende de forma transparente otros requisitos en el transcurso del tiempo.

El portafolio BeyondTrust PAM es una solución integrada que simplifica las implantaciones, reduce costos, mejora la utilización y reduce los riesgos asociados a privilegios.

> **La riqueza de funcionalidades, la implementación y la escalabilidad hacen que BeyondTrust sea una buena opción para empresas multinacionales.**
>
> *— Gartner Critical Capabilities for Privileged Access Management, by Felix Gaehtgens etc., 16 de julio de 2021*

Para más informaciones: beyondtrust.com/solutions

Gestión de contraseñas privilegiadas

Descubra, administre, audite y monitoree cuentas privilegiadas

Gestión de privilegios en endpoints

Administre privilegios en endpoints Windows, Mac, Linux y Unix

Acceso remoto seguro

Administre centralmente y proteja el acceso remoto a help desks y proveedores

BeyondTrust

Sobre BeyondTrust

BeyondTrust es líder mundial en Gestión de Accesos Privilegiados (PAM, por sus siglas en inglés), capacitando a las organizaciones a proteger y administrar todo su universo de privilegios. Nuestras herramientas y plataformas integradas ofrecen la solución PAM más completa del sector, permitiendo que las organizaciones reduzcan rápidamente su superficie de ataques en ambientes tradicionales, en la nube e híbridos.

El abordaje Universal Privilege Management de BeyondTrust proporciona seguridad y protege los privilegios por medio de contraseñas, endpoints y accesos, proporcionando a las empresas la visibilidad y el control que necesitan para reducir riesgos, obtener conformidad y dar impulso al desempeño operativo. Nuestros productos permiten el nivel ideal de privilegios tan solo durante el tiempo necesario, creando una experiencia sin fricción para los usuarios que aumenta su productividad.

Con una tradición de innovación y un firme compromiso con los clientes, las soluciones BeyondTrust son fáciles de implantar y de colocar en escala a medida que los negocios evolucionan. Más de 20.000 clientes confían en BeyondTrust, incluyendo el 70% de las empresas listadas en Fortune 500, además de una red global de socios.

Conozca más en beyondtrust.com/es

V2021_07_ENG