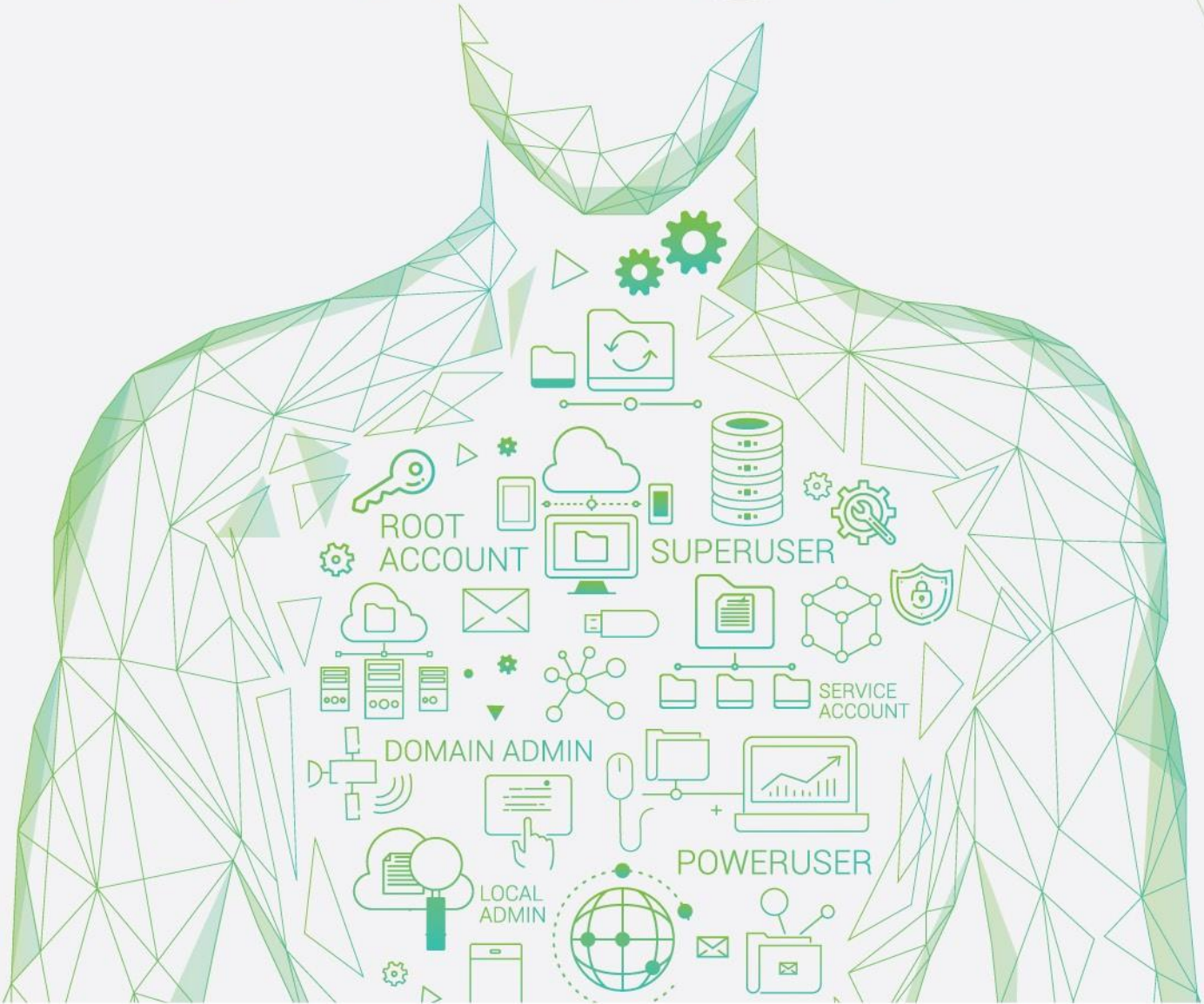
thycotic

ANATOMY
OF A PRIVILEGED ACCOUNT
HACK



Anatomía del Ataque a una Cuenta Privilegiada

Casi todos los usuarios son ahora usuarios privilegiados y los ciberdelincuentes lo saben

Los ciberdelincuentes están hackeando con éxito empresas y gobiernos de todo el mundo en tan solo cuatro pasos utilizando las técnicas más comunes y más baratas para explotar la seguridad, usando el método más sigiloso: esconderse dentro de la red y pasar desapercibidos utilizando las propias soluciones de su víctima para realizar actividades maliciosas.

Los ciberdelincuentes dirigen sus acciones a las personas, buscando formas de manipularlas para que entreguen información confidencial sin ser conscientes de ello. Hacen esto porque es la forma más fácil de acceder a datos valiosos mediante una técnica conocida como ingeniería social. Por lo tanto, no es sorprendente que las personas sean consideradas el eslabón más débil en la ruta de un ataque de seguridad informática, por lo que debemos capacitar a los empleados para que sean la primera y mejor defensa de la compañía.

Los trabajadores remotos, los proveedores externos y los usuarios de negocio con dispositivos tanto corporativos como personales, acceden ahora a cuentas privilegiadas todos los días. Con el paso acelerado al trabajo remoto, casi todos los usuarios ahora se están convirtiendo en usuarios privilegiados y hay que garantizarles un acceso fácil y seguro. Hoy en día el acceso a la nube plantea amenazas de seguridad cada vez mayores debido al uso indebido o abuso por parte de ciberdelincuentes y personas internas malintencionadas.

Según el Informe Verizon Data Breach Investigations del año 2020, las brechas en la nube aumentaron al 24%. Entre estas el 77% involucró credenciales de usuario comprometidas. Y según la firma de seguridad global McAfee, más del 27% de las organizaciones que utilizan plataforma como servicio (PaaS) ha experimentado el robo de datos de su infraestructura en la nube.

Desgraciadamente muchos usuarios de TI no son totalmente conscientes de la criticidad de las cuentas privilegiadas y los riesgos asociados con el mal uso. Eso hace que tanto ellos como sus organizaciones sean mucho más vulnerables a posibles daños económicos y de reputación derivados de las crecientes amenazas.

80% de las **brechas de seguridad** están **relacionadas** con **cuentas privilegiadas**

Tanto las cuentas privilegiadas humanas como las no humanas existen en todos los entornos de TI. Los administradores de TI y los usuarios de negocio las utilizan para automatizar y administrar datos, aplicaciones y servicios de TI críticos. Inicialmente estas cuentas se protegieron dentro de un perímetro definido con firewalls, VPN, etc. Pero actualmente esos perímetros tradicionales han desaparecido ya que la mayoría de las organizaciones dependen hasta cierto punto de soluciones (Infraestructura, Aplicaciones, Servicios, etc..) basadas en la nube. Las cuentas no asociadas a personas con privilegios (por ejemplo, las cuentas de servicio) están acelerando y superando el crecimiento de las cuentas humanas.

Este documento técnico describe la "Anatomía de un ataque a una cuenta privilegiada". Explica cómo los atacantes externos o los internos malintencionados pueden explotar las vulnerabilidades utilizando ejemplos como la contraseña de una cuenta de correo electrónico comprometida que se convierte en una violación total de la seguridad de la red.

LA MAYORÍA DE LOS INCIDENTES DE SEGURIDAD IMPLICAN CREDENCIALES COMPROMETIDAS

Los analistas de la industria estiman que hasta el 80% de todos los incidentes de seguridad implican credenciales y cuentas privilegiadas comprometidas. Aprender cómo los ciberdelincuentes eluden los controles de seguridad y obtienen acceso a los sistemas ayuda a las organizaciones a comprender cómo pueden convertirse en objetivos. Desde Thycotic resaltamos que una buena concienciación de los empleados sobre las últimas técnicas de piratería ayuda a comprender los riesgos y mitigarlos.

Un gran desafío para muchas organizaciones es que continúan utilizando métodos tradicionales para identificar y administrar cuentas con privilegios que aún dependen de tareas manuales y consumen mucho tiempo ya que se realizan de forma poco frecuente o de forma puntual. Las organizaciones deben ir más allá y empezar a utilizar soluciones de seguridad privilegiadas automatizadas. Incluso en los entornos de TI más sofisticados, las cuentas privilegiadas se administran con demasiada frecuencia mediante el uso de contraseñas comunes en varios sistemas, el intercambio no autorizado de credenciales y las contraseñas predeterminadas que nunca se cambian, lo que las convierte en los principales objetivos de los atacantes.

LAS CUENTAS PRIVILEGIADAS CONLLEVAN RIESGOS ESPECIALES

Las cuentas privilegiadas comúnmente se denominan "Las llaves del reino" ya que brindan acceso a datos confidenciales, a los sistemas y redes informáticas. Las cuentas privilegiadas están en todas partes en el entorno de TI y brindan los componentes básicos para administrar redes de hardware y software. Sin embargo, son invisibles para la mayoría de las personas, y que a veces operan en segundo plano, como cuentas de servicio o tareas automatizadas.

Muchos incidentes de seguridad han sido resultado de contraseñas robadas y/o débiles que han facilitado a los atacantes una puerta de entrada a conseguir acceso a cuentas privilegiadas. Las cuentas con privilegios comprometidas les brindan permisos elevados que les permiten moverse a través de la red y los sistemas de la organización para robar, infectar y eliminar información crítica.
Dado que los atacantes parecen ser usuarios legítimos de cuentas privilegiadas, pueden llevar a cabo actividades maliciosas durante semanas o meses sin ser detectados.

Por lo tanto, comprometer una cuenta privilegiada puede ser la diferencia entre una simple violación de la red y una catástrofe.
Cuando un sistema es comprometido, por lo general, es más fácil mitigar, aislar y erradicar el riesgo y restablecer el control. Cuando se viola una cuenta privilegiada, puede provocar daños importantes.

Esto se debe a que cuando una cuenta privilegiada es pirateada, permite al atacante hacerse pasar por un empleado o sistema de confianza y llevar a cabo la actividad maliciosa sin ser detectado como un intruso. Una vez que los atacantes ponen en peligro una cuenta privilegiada, normalmente pueden deambular a voluntad a través de un entorno de TI para robar información y causar graves trastornos.

Al describir la anatomía de un ataque a una cuenta privilegiada, mostraremos cómo los ciberdelincuentes atacan a sus víctimas, qué pueden hacer éstas para reducir su riesgo y prevenir el abuso de sus activos de información crítica.

QUÉ ES UNA CUENTA PRIVILEGIADA

Una cuenta con privilegios puede ser humana, como una cuenta interactiva de Active Directory, o no humana, como una cuenta de servicio.
Permiten a los profesionales de TI administrar aplicaciones, software y hardware. Las cuentas privilegiadas proporcionan niveles de acceso administrativos basados en niveles más altos de permisos. Algunos tipos de cuentas con privilegios no humanos son cuentas de aplicaciones que se utilizan para ejecutar servicios que requieren permisos específicos. Al igual que las cuentas de usuario, las cuentas privilegiadas tienen contraseñas para controlar y autorizar el acceso.

El problema con las contraseñas de usuarios débiles y cuentas privilegiadas es que los atacantes tienen herramientas para descifrarlas. Una vez que obtienen el acceso el daño puede ser catastrófico. El secuestro de cuentas privilegiadas les brinda la capacidad de acceder y descargar los datos más confidenciales de una organización, distribuir malware, eludir los controles de seguridad existentes, borrar los rastros de auditoría para ocultar su actividad, etc.

ANATOMY OF A PRIVILEGED ACCOUNT HACK PASO:

1 CONDUCT ENUMERATION AND RECONNAISSANCE TO CREATE A DIGITAL BLUEPRINT

Cada vez se comparte más y más información acerca de la identidad personal y digital cuando nos conectamos a internet, redes sociales, etc. Esto incluye nombre completo, dirección particular, números de teléfono, dirección IP, detalles biométricos, detalles de ubicación, fecha de nacimiento, lugar de nacimiento e incluso miembros de la familia.
Cuanta más información proporcione on line, más fácil le resultará a un ciberdelincuente utilizar esa información personal para dirigirse a usted y a su organización. Los hackers pueden pasar hasta el 90% de su tiempo realizando un reconocimiento de sus objetivos antes de actuar. Eso significa desarrollar un perfil de su objetivo utilizando recursos online como las redes sociales, Google "Dorking" y otros motores de búsqueda para recopilar la mayor cantidad de información personal posible.

Los atacantes realizan búsquedas tanto en las web pública como en la Deepweb para recopilar información sobre una empresa y sus empleados. Buscan detalles financieros, archivos de sitios web, tecnologías, socios y proveedores, equipos ejecutivos, organigramas, información de contacto, listas de distribución de correo electrónico, plantillas de documentos, formatos de firma, ubicaciones de oficinas, dominios, datos ya exfiltrados y contraseñas robadas que estén publicadas. Algunos incluso van, por ejemplo, a restaurantes y locales cerca de las oficinas de una empresa donde los empleados podrían usar una red Wi-Fi pública durante la comida o un descanso. Toda la información se puede obtener fácilmente con una técnica de evaluación pasiva sin tocar el perímetro de seguridad de la empresa.

Los hackers revisan los datos en busca de los mejores objetivos, esperando que produzcan los resultados más rápidos con el menor esfuerzo, identificando los eslabones más débiles de la organización (empleados o proveedores). Mediante datos personales, formatos de correo electrónico, plantillas de facturas y controles de seguridad existentes planifican su método de incursión.

2 ENGAÑAR A LOS USUARIOS PARA QUE REVELEN SUS CREDENCIALES

Para obtener acceso a la red de una empresa, con frecuencia comienza dirigiéndose a las cuentas de correo electrónico y redes sociales de los empleados o proveedores externos. Un empleado desprevenido recibe un correo electrónico de apariencia auténtica de un proveedor externo o, en muchos casos, a través de un mensaje de redes sociales. Conocido como spear phishing, el mensaje urgente "requiere" que el empleado haga clic en un hipervínculo y escriba sus credenciales. Una vez enviado, el empleado ha entregado su contraseña secreta e identidad digital al ciberdelincuente, quien luego puede eludir los controles de seguridad y hacerse pasar por un empleado de confianza.

También se puede utilizar una víctima secundaria para obtener acceso. Tomemos el ejemplo de un empleado que trae a casa un portátil de la empresa. Su hijo de ocho años usa su dispositivo para jugar en línea y charlar con amigos. De repente, el hijo recibe una nueva solicitud de amistad de un niño mayor que envía algunos enlaces interesantes a nuevos juegos y encuestas divertidas y finalmente envía un enlace a una nueva aplicación.

En lugar de un nuevo amigo, el hacker utiliza al niño de ocho años para obtener acceso a un dispositivo desprotegido en la red doméstica. Una vez comprometido, el hacker generalmente puede acceder a todos los demás dispositivos en casa, explotando las vulnerabilidades y la falta de controles habilitados para la seguridad. Un simple escaneo de Nmap de una red doméstica descubre muchas puertas para obtener acceso rápidamente a múltiples sistemas, incluidos dispositivos inteligentes o cámaras web que les permiten escuchar y ver lo que la familia está haciendo en casa.

El objetivo del atacante es obtener acceso al portátil de la empresa del empleado cuando trabaja desde casa, escanearla en busca de vulnerabilidades, explotarla, instalar malware y luego esperar a que el empleado regrese a trabajar al día siguiente. El perímetro de la empresa ahora se ha visto comprometido y el ciberdelincuente ahora está en la red interna. Cuando el reconocimiento y la enumeración se llevan a cabo de forma cuidadosa y extensa, se necesitan entre 24 y 48 horas para acceder a una red, a menudo a través de una víctima secundaria desprevenida. En la mayoría de las situaciones, suele ser un proveedor o contratista externo. Una ventaja que tiene el atacante es que los profesionales de la seguridad no tienen tiempo ilimitado.
Una vez que el atacante conoce a la víctima y obtiene el acceso a la red de la empresa, normalmente no actúa de inmediato. En lugar de pasar directamente al siguiente objetivo, invierte tiempo para recopilar y aprender más sobre el empleado para obtener una mayor visibilidad.

Una vez que los ciberdelincuentes tienen acceso, pueden aprender sobre el comportamiento del empleado, horarios y operaciones predecibles. Saben cuándo la víctima inicia y cierra sesión, qué aplicaciones ejecuta, qué se instala, a qué privilegios tiene acceso, cómo y cuándo se implementan las actualizaciones de software y cuándo se realizan los análisis de seguridad. Conocer los hábitos de la víctima ayuda al ciberdelincuente a pasar desapercibido y a comprender cómo eludir los controles de seguridad.

3 EXPLORA EL ENTORNO IT CON UN USUARIO LEGÍTIMO

Una vez dentro del entorno de TI como un usuario confiable, los atacantes realizan reconocimientos y aprenden sobre las rutinas diarias de los equipos de TI. Esto incluye observar los horarios regulares, las medidas de seguridad implementadas y el flujo de tráfico de la red.
Eventualmente, el atacante puede obtener una imagen precisa de toda la red y sus operaciones.

Observando y registrando estas rutinas los atacantes están listos para ir al siguiente paso. En la mayoría de los casos comienzan por buscar vulnerabilidades conocidas del sistema ya que a menudo, las empresas confían solo en aplicaciones y sistemas de seguridad orientados al perímetro, pero estas no suelen ser áreas explotadas por los hackers

Los sistemas y aplicaciones que corren mayor riesgo son los que se encuentran en la misma red que el equipo y la identidad digital del usuario comprometido.

Con las credenciales comprometidas, el ciberdelincuente puede abrirse camino a través de la red de la empresa, creando puertas traseras adicionales para el acceso futuro si la víctima elimina el acceso inicial. Y así, una vez dentro de la red de la empresa, pueden moverse sin ser detectados, porque la mayoría de los controles se enfocan solo en proteger el perímetro de la red.

4 ESCALA LA CAPACIDAD DE EXPLOTAR AL ACCEDER A CUENTAS PRIVILEGIADAS

Como se comentó anteriormente, las cuentas privilegiadas son el objetivo de los ciberdelincuentes debido al acceso ilimitado que brindan, pasando de una cuenta de usuario normal a una cuenta privilegiada. Desafortunadamente, algunas empresas han facilitado mucho esta tarea al otorgar a la mayoría de los empleados derechos de administrador local. Este es un paso corto para obtener acceso completo a toda la infraestructura de red.
Algunas organizaciones otorgan derechos de administrador completos para mantener a los usuarios contentos y productivos, aunque no sea necesario. Sin embargo, una vez concedido, el acceso privilegiado se transfiere fácilmente al ciberdelincuente para explotar aún más la red.
Hay muchas formas de elevar los privilegios en los sistemas, ya sea mediante la explotación de servicios, permisos de archivos / carpetas, programador de tareas, credenciales almacenadas en caché, secuestro de DLL o utilizando herramientas como Mimikatz o John the Ripper para secuestrar sesiones o explotar exploits pass-the-hash. La mayoría de los problemas provienen de organizaciones que utilizan la misma contraseña de administrador local en todos los sistemas. Una vez que un administrador local del sistema se ve comprometido, moverse con la misma cuenta es bastante sencillo.

5 MANTIENE EL ACCESO PERSISTENTE

Mantener el acceso a los sistemas una vez que se han visto comprometidos a través de una cuenta de usuario suele ser relativamente fácil. Los ciberdelincuentes pueden descargar herramientas y utilidades para evitar los controles de seguridad existentes. Por ejemplo, un portátil comprometido puede cargarse con estas herramientas durante el Paso 2, lo que facilita mucho el mantenimiento del acceso. Pudiendo además reutilizar las herramientas que encuentren dentro de las organizaciones, como herramientas de acceso remoto, Python, PowerShell, escáneres de vulnerabilidades, etc…

Los ciberdelincuentes también mantienen el acceso a la red creando nuevas cuentas privilegiadas, a menudo llamadas cuentas de puerta trasera, porque son un punto de acceso a la red que el equipo de TI no sabe que existe. O pueden cambiar las contraseñas existentes en las cuentas de servicio o instalar herramientas de acceso remoto que están ocultas detrás de las aplicaciones que utilizan todos los días los empleados. De esta forma, si se descubre y elimina el punto de acceso inicial del atacante, puede dirigirse a una de sus nuevas puertas para acceder en cualquier momento que lo desee.

6 ACTIVIDAD MALICIOSA

Con el acceso establecido y privilegios escalados, las acciones que puede realizar el atacante dependen de él mismo y sus motivaciones, desde querer mostrar sus hazañas o tratar de llegar al siguiente nivel de aceptación dentro de una comunidad. Para el crimen organizado, ganar dinero es la prioridad, incluso mediante la piratería como servicio. La piratería por parte de los estados, que ha ganado tanta notoriedad, se centra en las ventajas económicas, políticas o de inteligencia. Los grupos terroristas también se han convertido en una amenaza significativa, por lo general, buscan robar, dañar o destruir a un adversario.

La principal motivación es el dinero y los incidents ocurridos en el pasado como WannaCry y NotPetya nos son una muestra de cuan extendidos y lucrativos son este tipo de ataques

Mediante técnicas avanzadas, por ejemplo, los ciberdelincuentes se centran en capturar información confidencial para realizar transacciones bursátiles basadas en resultados financieros antes de que se hagan públicas.

Los hackers implementan su plan de ataque mediante el uso de herramientas de resolución de problemas o Help Desk para sistemas operativos que brindan acceso remoto, shells remotos o incluso malware que hace llamadas a un servidor de Command & Control en un horario predefinido, esperando instrucciones de los atacantes.

Las empresas deberían prepararse para ser atacadas antes de designar un equipo de respuesta a incidentes y hacer frente a una brecha de seguridad. La forma en que una organización responde a una brecha a menudo determinará su supervivencia.

7 CUBRE SUS PASOS PARA PERMANECER INDETECTADO

Eliminar cualquier señal o indicación de que una red ha sido pirateada es el paso final para que el ataque sea un éxito. El atacante borra todos rastro de la brecha o planifica cómo volver más adelante para llevar a cabo más actividades maliciosas. En la mayoría de los casos, los ciberdelincuentes cubren su rastro eliminando archivos de registro o cualquier actividad que se pueda rastrear para ver cómo obtuvieron acceso inicialmente. Debido a que un ciberdelincuente tiene acceso a cuentas privilegiadas, puede borrar cualquier rastro de actividad maliciosa con relativa rapidez y facilidad.

Sin embargo, la vida del ciberdelincuente puede volverse mucho más complicada con los controles de seguridad automatizados de una solución de Gestión de Cuentas Privilegiadas (PAM por sus siglas en inglés) que centralizan los registros y segregan los permisos de los usuarios.

Solo las cuentas con privilegios individuales pueden acceder a esos registros y correlacionar los datos del registro para identificar la manipulación o eliminación de registros.

LA SEGURIDAD DEL ACCESO PRIVILEGIADO ES EL NUEVO PERÍMETRO

En el mundo hiperconectado de hoy, las organizaciones ya no pueden confiar en el perímetro de seguridad tradicional como su única protección. El "perímetro de seguridad" de próxima generación debe centrarse en las soluciones de seguridad de Gestión de Acceso Privilegiado. Eso significa soluciones que controlan cuentas privilegiadas, ya que estas son la clave para que los hackers eleven su acceso y puedan moverse por la red. Se requieren soluciones que validen la identidad y el acceso permitido para proteger los sistemas y los datos, que se pueden estar ubicados en cualquier lugar, y poder acceder a ellos en cualquier momento de manera segura.

Las soluciones de gestión de acceso privilegiado pueden ayudar a una empresa a acelerar la adopción de nuevas tecnologías y, al mismo tiempo, ayudar a evitar convertirse en una próxima víctima.

Cinco pasos que puede seguir ahora para reducir los riesgos del abuso de acceso privilegiado:

1. Educar al personal clave sobre la Gestión de Cuentas Privilegiadas
2. Descubrir las cuentas privilegiadas que hay en su empresa
3. Automatizar la gestión y la Seguridad del acceso privilegiado
4. Adoptar e implementar políticas de Gestión de Acceso Privilegiado
5. Ganar una mayor visibilidad del uso de acceso privilegiado

To learn more visit www.thycotic.com.

REAL LIFE STORY:

EL CASO DE LA BOMBILLA INTELIGENTE, DUMB WIFI

Compañía:
Compañía de Gestión Marítima

Evaluado por:
Joseph Carson, CISSP, CSP0, CSP

Antecedentes:
Reconocimos y analizamos la huella digital de la compañía. ¿Siguiente paso? Ganar acceso. Todo fue un juego.

Hace unos años realicé una evaluación de riesgos en una empresa de gestión marítima.
Se había "mapeado" la huella digital del objetivo. Ahora todo lo que teníamos que hacer era acceder. Todos los métodos estaban en juego. Dejamos caer USB en el sitio y visitamos cafés locales para rastrear a los empleados que trabajan con redes inalámbricas no seguras. **Nuestro trabajo consistía en encontrar vulnerabilidades en datos sensibles.**

Cuando se trata de reconocimiento como este, es típico común hacer un barrido de radio definido por software, donde se buscan puntos de acceso inalámbricos, tanto públicos como ocultos. Encontramos una conexión Wi-Fi oculta y, después de escanearla, vimos que estaba configurada en WEP, un protocolo de comunicación antiguo y no seguro. Resulta que una bombilla LED inteligente lo estaba usando para comunicarse con una red Wi-Fi de invitados. Usamos esa bombilla para acceder a la red Wi-Fi mal asegurada, y una vez que se obtuvo la contraseña de Wi-Fi, bueno, se podría decir que el resto es historia.

Obtuvimos fácil acceso a otros dispositivos en la red, incluida una sala de conferencias para invitados, donde encontramos un PC mal protegido.
Aparentemente se usaba para hacer presentaciones.

"Una vez que se obtuvo la contraseña Wi-Fi, bueno, el resto es historia."

Encontramos años de presentaciones, desde presentaciones de proveedores hasta información financiera. Inmediatamente explotamos el equipo, elevando los permisos con Mimikatz para obtener acceso a las cuentas de administrador local.

Pero no habíamos terminado. Analizamos continuamente la red de invitados en busca de nuevos dispositivos, y era solo cuestión de tiempo antes de que ocurriera una reunión. Todos los asistentes se unieron a la red Wi-Fi para invitados y rápidamente obtuvimos privilegios de administrador local en todos los dispositivos, porque todas sus credenciales de administrador local eran las mismas. Accedimos de forma remota a cada dispositivo, instalamos RAT (Remote Access Tool) y, cuando finalizó la reunión, los empleados llevaron sus portátiles comprometidos a la oficina y las conectaron a la red corporativa. En cuestión de minutos, teníamos acceso y control total a toda la red.

Este ataque nos llevó al equipo de hacking ético tres horas desde el momento en que obtuvimos acceso a la red Wi-Fi para invitados hasta la toma de control completa.

APRENDIZAJE: Encuentre sus vulnerabilidades, sepa dónde están sus datos confidenciales, proteja el acceso privilegiado a éstos y proteja y administre cuentas privilegiadas para que no se convierta en una víctima. Tenga siempre un plan de respuesta a incidentes. La rapidez con la que su negocio vuelva a estar en funcionamiento después de un incidente puede determinar su supervivencia y limitará los costes financieros y el daño a la reputación.

REAL LIFE STORY:

EL CASO DE LA HOJA DE CALCULO TODOPODEROSA

Compañía:
Central Energética

Evaluado por:
Joseph Carson, CISSP, CSP0, CSP

Antecedentes:
Sabían que la seguridad era fundamental para proporcionar energía continua y se construyeron una fortaleza. Poco sabían ...

Fui contratado por una central eléctrica. Era relativamente nueva, totalmente automatizada con controles remotos y querían que revisara los controles y sus protecciones en materia de ciberseguridad.

La seguridad física fue impresionante. El sistema de seguridad podía decir cuándo los visitantes estaban a cinco minutos de distancia, qué vehículo conducían y cuántas personas había dentro. Si los visitantes llegaban un minuto antes o después, tendrían que lidiar con el equipo de seguridad armada.

Todas las puertas físicas tenían controles de acceso, incluidas las salas de máquinas. Una vez dentro, cada motor tenía sus propias válvulas de control para cambiar físicamente la presión y el flujo de agua. Las válvulas de control no estaban aseguradas, aunque el riesgo de manipulación era bajo. Los controladores PLC y los sistemas de control SCADA contaban con la más avanzada protección contra amenazas. Invirtieron millones para prevenir ataques de ciberseguridad. **Se habían construido una fortaleza física y cibernética.**

Junto al panel de control había una hoja impresa. Contenía todas las direcciones IP, usuarios y contraseñas para cada estación de control.

El Departamento de Energía de EE. UU. fue hackeado con éxito 159 veces en cuatro años.

Entonces sucedió. Sentado en la mesa junto a los controles había una página impresa. Contenía todas las direcciones IP, nombres de usuario y contraseñas de cada estación de control. No se habían cambiado en más de cuatro años y probablemente el fabricante los había instalado con las credenciales predeterminadas.

Un ciberataque al sector energético de Ucrania provocó un apagón en 86.000 hogares.

Cualquiera podría haber hecho copias de esta lista y podría haber tomado una foto con un teléfono y haberse tomado su tiempo antes de empezar el ataque. ***Ellos nunca lo habrían visto venir.***

El 62% de los ataques provienen de credenciales privilegiadas comprometidas, y el 80% de los hackers dicen que somos las personas las principales responsables de las infracciones de seguridad.

APRENDIZAJE: Proteja sus cuentas privilegiadas con una solución de Gestión de Cuentas Privilegiadas (PAM) que controle el acceso, automatice la rotación de contraseñas y descubra y proteja automáticamente nuevas cuentas..

CÓMO PUEDE PROTEGER LAS CUENTAS PRIVILEGIADAS

Las cuentas privilegiadas se denominan "Las llaves del reino" porque brindan acceso a datos confidenciales y sensibles en los sistemas y redes de la empresa. Las cuentas privilegiadas están en todas partes en el entorno de TI. Brindan la posibilidad de administrar vastas redes de hardware y software que impulsan nuestro negocio dentro de un mundo conectado a Internet e impulsado por la información. Sin embargo, son invisibles para la mayoría de las personas.

RECURSOS GRATUITOS

Plantilla personalizable para plan de respuesta a incidentes de ciberseguridad ayuda a que los equipos de operaciones y de respuesta a incidentes de ciberseguridad formen un frente unido contra un ataque para coordinar acciones y mantener la continuidad del negocio.

Least Privilege Discovery Free Tool
encuentra cuentas con privilegios excesivos en su entorno de TI que son vulnerables a ataques de cuentas privilegiadas.

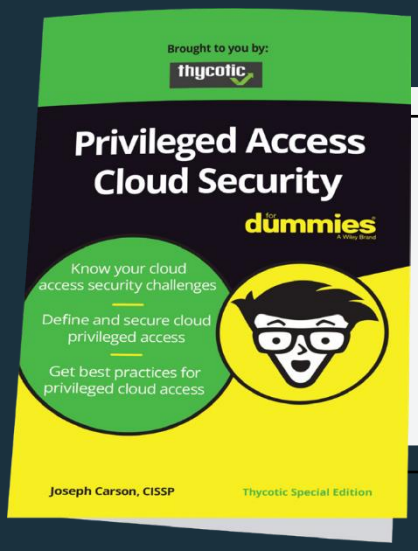
Remote Worker Cyber Security Toolkit
garantiza que las personas puedan acceder a los sistemas y los datos que necesitan, mientras se adhieren a las mejores prácticas de seguridad.

Critical Controls for Modern Cloud Security explica cómo utilizar PAM para mitigar las vulnerabilidades en la superficie de ataque de la nube.

Expert's Guide to PAM Success describe las personas, los procesos y la tecnología necesarios para desarrollar un programa PAM avanzado.

UTILICE ESTE PODER PARA EL BIEN

En este documento técnico, el término hacker se utiliza para representar hackers éticos y hackers criminales que actúan con intenciones maliciosas. La mayoría de los piratas informáticos son buenos ciudadanos y la asombrosa comunidad de piratas informáticos éticos actúa con la intención de identificar riesgos y vulnerabilidades para educar, reducir las amenazas y mejorar la seguridad.



eBOOK GRATIS:

Privileged Access Cloud Security for Dummies

DESCARGAR