REPORTE OFICIAL | Enero de 2015

Tengo que confiar en *alguien*, ...¿cierto?

Cómo tratar las amenazas internas a la ciberseguridad

Russell Miller

Merritt Maxim

CA Technologies, Security Management

ca technologies

Tabla de contenido

Resumen

"Cuando uno ocupa cargos con accesos con privilegios, como un administrador de sistemas para este tipo de agencias de la comunidad de inteligencia, se está expuesto a mucha más información, en una escala mayor que el empleado promedio".

– Edward Snowden

Desafío

Aunque muchas organizaciones enfocan sus esfuerzos de seguridad en los límites de la red, son los usuarios internos los que ofrecen mayor riesgo para la ciberseguridad. Desde ejecutivos, administradores de TI y socios de negocios, muchas personas tienen acceso a información confidencial que, si se expone públicamente, podría causar consecuencias significativas para el negocio de una organización, o incluso para su existencia.

Por lo general, la ciberseguridad se entiende como un campo técnico, con defensores altamente calificados que buscan superar a los atacantes en un concurso de intelecto y determinación. A pesar de que hay algo de verdad en esta caracterización, omite lo que quizás represente el aspecto más importante de la seguridad: el elemento humano. Las personas tienden a creer en aquellos que conocen, lo cual los lleva a compartir contraseñas u otros datos que no deberían compartir.

La confianza es un elemento esencial para operar cualquier tipo de organización. Las personas necesitan acceso a información confidencial y sistemas importantes por distintos motivos, y un nivel de confianza debe estar asociado con ese acceso. Comprender y manejar esa confianza es el desafío más importante, y difícil, al momento de tratar con las amenazas internas.

Oportunidad

"Confianza" no significa darles a los empleados acceso no restringido e innecesario a la información. Con los controles de seguridad adecuados, las organizaciones pueden reducir significativamente la exposición al riesgo de amenazas internas. Es fundamental encontrar el equilibrio adecuado entre los controles y las habilitaciones que tiene el empleado, y la responsabilidad de los empleados por sus acciones. Esto requiere un enfoque amplio que le permita a las organizaciones administrar cuidadosamente sus identidades, accesos y datos desde la administración de identidades hasta la gobernanza, la administración de identidades con privilegios y la protección de datos.

El fraude interno es un hecho habitual.

En promedio, las organizaciones han sufrido aproximadamente 55 incidentes de fraude relacionados con empleados en los últimos 12 meses.[1]

– The Ponemon Institute

Beneficios

Los estrictos controles de seguridad no solo reducen los riesgos, sino que permiten que se comparta la información en una organización. El acceso a la información altamente confidencial, por lo general, es muy restringido debido al riesgo de que se expongan los datos. Con los controles de seguridad apropiados, los datos pueden compartirse con un grupo grande de personas, para que puedan ser más eficientes e innovadores.

"En el mundo actual, lo más importante que cualquier persona puede tener es tecnología. Lo más importante que puede hacer este país es proteger sus secretos comerciales".[3]

– Juez de Distrito de EE. UU., Ruben Castillo

Sección 1:

Desafío

Los usuarios internos pueden robar, borrar o exponer información confidencial de forma malintencionada o inconsciente por diversas razones. Al mismo tiempo, los usuarios internos deben tener cierto nivel de acceso para que funcione el negocio o para que la organización opere. Es fundamental comprender las amenazas internas en sus diversos niveles, desde las motivaciones a los ejemplos de daños hasta comprender cómo evolucionaron las amenazas, para abordar de forma inteligente las estrategias de mitigación de riesgos.

Tipos de amenazas internas

Las amenazas internas no son todas iguales. Existen tres tipos de amenazas internas: usuarios internos malintencionados que roban información o causan daños deliberadamente; usuarios internos que, sin darse cuenta, son explotados por partes externas y usuarios internos que son descuidados y cometen errores no intencionados.

- **Los usuarios internos malintencionados** son el tipo menos frecuente, pero tienen el potencial de ocasionar daños considerables por su capacidad de acceso interno. Los administradores que tienen identidades con privilegios son particularmente riesgosos. De acuerdo con Ponemon Institute, "las violaciones a la información que son consecuencia de ataques malintencionados son las más costosas"[2].
- **Los usuarios internos explotados** pueden ser "engañados" por partes externas para proporcionar datos o contraseñas que no deberían compartir.
- **Por último, un usuario interno descuidado** puede simplemente presionar la tecla equivocada y borrar o modificar información crítica de manera no intencional.

Las amenazas internas también pueden provenir de usuarios con privilegios (administradores) o de usuarios comunes con acceso a información confidencial. Por lo general, los administradores poseen privilegios completos para realizar esencialmente cualquier operación en los sistemas importantes. Por lo general, personas de todo tipo han acumulado más derechos de los necesarios para sus trabajos actuales, lo cual lleva a un aumento del riesgo que es absolutamente evitable.

¿Qué cambió?

Los riesgos. A medida que nos transformamos en una economía cada vez más basada en la información, la propiedad intelectual y los secretos comerciales son más importantes que nunca para la supervivencia de la organización. El auge de las soluciones analíticas de la "gran base de datos" agudizó este problema. Los negocios ahora almacenan grandes cantidades de datos para detectar patrones y perspectivas que habrían sido imposibles hace solo unos cuantos años atrás. A pesar de que los datos son un diferenciador comercial fundamental, en algunos casos son altamente confidenciales, ya que contienen, por ejemplo, información personal de los clientes, números de tarjetas de crédito, transacciones, comunicaciones e, incluso, ubicaciones. La infracción de seguridad en el almacenamiento de datos de un cliente puede ocasionar el incumplimiento de las leyes de privacidad, juicios por demanda colectiva y daños en la reputación que podrían llevar a la pérdida del negocio.

El CERT (equipo de respuesta ante emergencias informáticas) de la Universidad Carnegie-Mellon ha definido a un usuario interno malintencionado de la siguiente manera: "una amenaza interna malintencionada para una organización es un empleado actual, un exempleado, un contratista u otro socio de negocios que tiene o tuvo acceso autorizado a los datos, los sistemas o las redes de una organización y que abusó o hizo un uso inadecuado de dicho acceso de manera voluntaria de modo tal que afectó negativamente la confidencialidad, la integridad o la disponibilidad de la información o de los sistemas de información de la organización"[4]. Históricamente, el usuario interno era un empleado, pero según lo que el CERT ha observado, el alcance de las amenazas internas se ha extendido más allá de los empleados e incluye la connivencia con personas ajenas a la empresa, socios de negocios "de confianza", etc. Esto, combinado con la naturaleza altamente distribuida y móvil de la fuerza laboral actual, significa que las amenazas internas son más graves que nunca.

Factores de riesgo de los usuarios internos

Todas las organizaciones enfrentan desafíos comunes cuando intentan reducir los riesgos de infracciones de seguridad internas:

Administración ineficaz de usuarios con privilegios. En todos los entornos de TI, existen usuarios con privilegios (administradores, usuarios raíz) que tienen acceso total a los sistemas, las aplicaciones y la información clave. Esto no solo es un riesgo de seguridad, sino que también puede dificultar mucho más el cumplimiento. El uso compartido de contraseñas de administrador es otro problema común que podría dar lugar al acceso inapropiado a sus sistemas y datos, y a la incapacidad de identificar específicamente quién realizó cuál acción en cada sistema.

Asignación inapropiada de funciones y derechos. La administración de funciones y derechos de usuarios es uno de los principales desafíos que muchas organizaciones de TI enfrentan. Las funciones superpuestas o los derechos duplicados incoherentes son problemas comunes que pueden dar lugar a la obtención y el uso inapropiados de información confidencial. Además, la falta de desaprovisionamiento automático puede generar derechos excesivos o cuentas huérfanas, lo que puede proporcionar fisuras a través de las cuales los usuarios internos insatisfechos pueden lanzar un ataque.

Gobernanza general de identidades inadecuada. La protección eficaz contra el acceso inapropiado a la información, o el uso inapropiado de esta, requiere de un fuerte control de las identidades de usuarios, el acceso y el uso de la información. La mayoría de las organizaciones tienen algunos controles en estas áreas, pero no cuentan con un enfoque unificado y sólido para proteger verdaderamente sus activos de información.

Deficiente clasificación de la información y cumplimiento de políticas. Muchas organizaciones ni siquiera saben dónde se encuentra toda su información confidencial y, por lo general, tienen políticas inadecuadamente definidas y comunicadas acerca de cómo se debe manejar la información confidencial. Sin embargo, lo que es más importante, muchas organizaciones no disponen de controles para detectar y prevenir la transmisión o divulgación inapropiada de información confidencial.

Auditorías y análisis inadecuados. Muchas empresas no tienen forma de auditar continuamente el acceso para asegurarse de que solo las personas debidamente autorizadas obtengan acceso, y que su uso de la información cumpla con la política establecida. Además, aunque tengan herramientas de auditoría, el mero volumen de los datos de registro generados hace que sea muy difícil para las organizaciones examinar los datos e identificar infracciones o amenazas.

Complejidad del registro de auditoría. El mero volumen de los datos de auditoría y registro dificulta la detección y la investigación forenses. Registrar toda la actividad de TI es un primer paso importante para combatir los ataques internos, y los complejos y altamente distribuidos entornos actuales de TI generan volúmenes masivos de datos de registro, pero es muy difícil administrar el volumen total de datos.

Respuesta reactiva. La mayoría de los enfoques actuales para abordar las amenazas internas son reactivos, no predictivos. A pesar de que esto puede ayudar muchísimo en las investigaciones forenses, el problema es que el ataque o robo ya se produjo. Por lo tanto, las organizaciones deben buscar soluciones que puedan ofrecer más capacidades analíticas y predictivas que, aunque no puedan evitar los ataques internos, puedan igualmente identificar a los “usuarios internos de riesgo”, y luego implementar un registro más detallado sobre estos individuos.

Ausencia de políticas de uso aceptable integrales y por escrito. Todas las organizaciones deben tener políticas de uso aceptable detalladas para todos los empleados, y deben exigir a los empleados que revisen y firmen la política una vez por año. Es una medida básica, pero las organizaciones a menudo la pasan por alto. Tener una política de seguridad por escrito no evitará necesariamente los ataques internos, pero puede resultar útil para proporcionar a toda la organización un punto de referencia acerca de lo que es el uso aceptable y de los métodos adecuados para administrar los datos confidenciales.

Alrededor del 65 % de los empleados que cometen robos de IP internos ya habían aceptado empleos en una empresa de la competencia o comenzado su propia empresa al momento del robo. Alrededor del 20 % fueron reclutados por agentes externos que apuntaban a los datos. Más de la mitad roba datos durante el mes en el que abandonan la empresa.

Behavioral Risk Indicators of Malicious Insider IP Theft: Misreading the Writing on the Wall (Indicadores conductuales de riesgo de robo de IP interno malintencionado: malinterpretar los mensajes en el muro),

– Eric D. Shaw, Ph.D., Harley V. Stock, Ph.D.

Por qué es difícil: reducción de riesgo frente a habilitación de negocios

La confianza es fundamental para la operación de cualquier organización. Para que una organización se beneficie de la información confidencial, es necesario que las personas y los sistemas correctos tengan acceso a esta, y las políticas demasiado restrictivas no ayudan a que una organización tenga capacidad de respuesta, sea innovadora e, incluso, funcional. Al mismo tiempo, la confianza innecesaria conlleva riesgos innecesarios. Por ejemplo, las personas en las que más se confía, es decir, los usuarios con privilegios de una organización, pueden causar el mayor daño. Por lo general, estos administradores tienen los privilegios para realizar prácticamente cualquier operación en sistemas clave, y los usuarios suelen tener acumulados más derechos de los que necesitan para su función laboral actual. Otro riesgo innecesario asociado con las identidades con privilegios es el uso de cuentas compartidas. Varias personas con acceso a la misma cuenta generan una falta de responsabilidad.

Administrar el elemento humano es el aspecto más difícil de la administración de amenazas internas. Varias personas sienten la necesidad de creer que su empresa confía en ellos, y se sienten menospreciados ante nuevos controles que les quiten el acceso a información a la que antes tenían acceso. Además, con frecuencia, se piensa en el acceso como una forma de estatus, en especial, entre los administradores de TI, y el intento de controlar el acceso, por lo general, ocasiona resistencia.

Ejemplos de infracciones de seguridad internas

Muchas infracciones de seguridad cometidas por usuarios internos nunca se hacen públicas. Las organizaciones prefieren dejar estas infracciones en el ámbito privado para evitar los daños a la reputación y las posibles inquietudes de los clientes respecto de su seguridad. Sin embargo, se han divulgado varias infracciones internas que han ocasionado grandes daños. A continuación, se incluyen algunas de las más conocidas:

Infracciones de seguridad internas ampliamente conocidas

Agencia Nacional de Seguridad	San Francisco	Motorola
Edward Snowden, mientras trabajaba para Booz Allen Hamilton como contratista para NSA, les proporcionó a periodistas documentos altamente clasificados sobre programas denominados “Prism” y “Boundless Informant”. La información que brindó Snowden exponía detalles sobre el almacenamiento y procesamiento de las comunicaciones de NSA, incluidos llamados telefónicos y correos electrónicos.[5]	Un empleado insatisfecho de San Francisco bloqueó la red FiberWAN de la ciudad, que contenía documentos confidenciales, como expedientes policiales. Aun más grave fue que no era posible acceder al correo electrónico y no se pudieron emitir los cheques de la nómina de pagos. La ciudad gastó más de un millón de dólares en un intento fallido de obtener acceso a la red.[6]	A Hanjuan Jin, un ingeniero de software en Motorola durante nueve años, lo atraparon los funcionarios de la aduana de los EE. UU. mientras embarcaba un avión a Beijing con $30 000 en efectivo, junto con más de 1000 documentos que indicaban que era “información confidencial y de propiedad exclusiva”, lo que representaba un total de $10 a $15 millones de dólares en secretos comerciales. Jin fue declarado culpable por robar secretos profesionales en un Tribunal Federal de los EE. UU., y fue sentenciado a cuatro años de prisión.[7]

Sección 2:

Oportunidad

Las organizaciones deben reconocer que los ataques internos no solo son una amenaza importante, sino que su complejidad es cada vez mayor. Dado que gran parte de los activos y la información de una organización está disponible en línea, las organizaciones deben adoptar un enfoque proactivo para defenderse contra el ataque interno. Este enfoque debe incluir una serie de soluciones que aborden la administración de identidades y accesos, y la protección de la información. Nada puede evitar por completo todos los ataques internos, pero aquellos que adoptan un enfoque proactivo firme pueden ayudar a reducir el riesgo, mejorar el cumplimiento y permitir que la organización de TI respalde las iniciativas de negocio con más eficacia.

Cómo encontrar un equilibrio

Las herramientas para administrar identidades, accesos y datos pueden permitirle a una organización encontrar el equilibrio adecuado entre las habilitaciones, y el uso compartido de información confidencial, y los controles necesarios para reducir los riesgos de infracciones de seguridad internas. Las organizaciones pueden reducir el riesgo de los tres tipos de amenazas internas (usuario malintencionado, explotado y descuidado) si habilitan la responsabilidad, implementan el acceso con privilegios mínimos y controlan los datos confidenciales. La responsabilidad hará que los usuarios internos malintencionados lo piensen dos veces antes de actuar, ayudará a identificar a los usuarios internos explotados y hará que los usuarios sean más cuidadosos con sus acciones. El acceso con privilegios mínimos denegará acciones y limitará el daño ocasionado por todos los tipos de ataques internos, incluidas las acciones involuntarias, pero dañinas. Controlando los datos confidenciales directamente, las empresas pueden prevenir que se los exporte fuera de la red con herramientas como unidades USB o, incluso, mensajes de correo electrónico.

“Confianza” no significa darles a los empleados acceso sin restricciones a la información que no es relevante para sus trabajos. Las organizaciones depositan un nivel de confianza en cualquier empleado que tenga acceso a sistemas o datos confidenciales. Otorgar acceso más allá del requerido es un riesgo innecesario que no significa que una organización no confía en sus empleados. Simplemente es una acción inteligente.

Para sustentar los nuevos controles de seguridad, es fundamental establecer una norma cultural en cuanto al acceso de privilegios mínimos mediante la aplicación de controles de manera estándar en toda la organización. A partir de esta acción, los individuos perciben la seguridad de los datos como una prioridad de la organización y no como una falta de confianza en una persona específica. Esto reduce los sentimientos negativos asociados con un enfoque de control cuidadoso al acceso a los datos.

Un enfoque detallado para mitigar las amenazas internas

Las capacidades de seguridad de la actualidad pueden reducir el daño de una infracción de seguridad interna, identificar una infracción después del hecho para permitir una respuesta efectiva o, incluso, evitar una infracción en primer lugar. Las funcionalidades más importantes son las siguientes:

Administración de identidades con privilegios

La administración de identidades con privilegios se encuentra en el centro de cualquier ciberdefensa contra las amenazas internas. Las cuentas con privilegios tienen el acceso necesario para ver y robar la información más confidencial de una organización, o para provocar el mayor daño posible en los sistemas de TI fundamentales. Generalmente, también se comparten entre varias personas que tienen acceso a las mismas cuentas y contraseñas, lo que conlleva a la falta de responsabilidad.

Administrar las identidades con privilegios requiere de un enfoque multifacético. Además de administrar las cuentas compartidas, los controles adicionales hacen posible la responsabilidad de usuarios internos y pueden limitar el daño realizado por un atacante externo que obtiene acceso a una cuenta administrativa.

56 % "Porcentaje de ejecutivos que afirman que su fraude más grave se debió a un usuario con privilegios".[8]

– Pricewaterhouse Coopers

"Si no implementa los controles adecuados para los usuarios con privilegios, corre el riesgo de que se produzca la degradación del nivel de servicio, de pagar costos de resolución de auditorías, de que los desarrolladores accedan a datos de producción (confidenciales) y de que empleados insatisfechos derriben su infraestructura o lo mantengan como rehén".[9]

– Forrester Research, Inc.

Capacidad clave	Necesidad	Descripción	Beneficio
Administración de contraseñas de cuentas compartidas	Las cuentas con privilegios, como las cuentas 'raíz' en UNIX y de 'Administrador' en Windows, se suelen compartir, lo cual reduce la responsabilidad.	Controla el acceso a las cuentas administrativas con privilegios con el almacenamiento de contraseñas y capacidades de inicio de sesión automático. Este es el punto de partida para la mayoría de las soluciones de administración de identidades con privilegios.	Disminuye el riesgo de que usuarios no autorizados obtengan acceso a cuentas con privilegios. Evita que se compartan contraseñas.
Controles de acceso específicos	El acceso a las cuentas con privilegios suele ser "todo o nada", un riesgo de seguridad innecesario que genera usuarios con más privilegios de los que necesitan.	Administra el acceso de usuarios con privilegios después del inicio de sesión. Controla en qué acceso los usuarios basaron su identidad individual, incluso, cuando se utiliza una cuenta administrativa compartida.	Reduce el riesgo, ya que otorga a los administradores únicamente los privilegios mínimos que necesitan para realizar sus tareas.
Reportes de actividades del usuario/grabación de sesiones de video	Realizar el seguimiento de todas las acciones de usuarios para poder determinar lo que ocurrió y "quién hizo qué" en una investigación. No se graban todas las actividades del usuario, y muchas aplicaciones no generan registros, lo cual reduce la responsabilidad y dificulta las investigaciones forenses.	Registra todas las acciones del usuario, realiza el seguimiento de todos los registros por persona, aun cuando se utiliza una cuenta compartida. Idealmente, realiza el seguimiento de un sistema de TI en un formato tipo video.	Hace más simple averiguar "quién hizo qué" en una investigación forense, gracias al uso de un video comprensible en lugar de una búsqueda a través de archivos de registro ininteligibles. Hace posible la responsabilidad de los usuarios de sistemas de TI. Crea registros para las aplicaciones que no los generan de forma nativa.
Seguridad de la virtualización	La virtualización agrega una nueva capa de infraestructura que se debe proteger: el hipervisor.	Administra los usuarios con privilegios en VMware, en tanto que proporciona una automatización compatible con virtualización de los controles de seguridad en las máquinas virtuales.	Reduce los riesgos de la virtualización, abarcando desde los administradores de VMware hasta las máquinas virtuales.
Puente de autenticación de UNIX	La administración de las cuentas y el acceso de usuarios en los servidores individuales UNIX y Linux suponen una carga administrativa que puede devenir en errores y negligencias.	Autentica a los usuarios en sistemas UNIX y Linux para Microsoft Active Directory.	Consolida la información de autenticación y de cuenta contenida en Active Directory, en lugar de administrar las credenciales de UNIX de forma local, en cada sistema. Disminuye los gastos generales administrativos.

Administración y gobernanza de identidades

La asignación de derechos incorrecta representa una causa importante de las infracciones de seguridad. Esto puede deberse a la configuración incorrecta de los derechos de acceso iniciales, la acumulación de derechos a través del tiempo o, incluso, la asignación de derechos de acceso intencionalmente incorrecta a un usuario por parte de un administrador colaborador no autorizado. La acumulación de derechos puede darse como resultado de una falta de mantenimiento cuando un empleado cambia de puesto y mantiene todos sus derechos de acceso anteriores. Mientras que los derechos de usuario incorrectos son el factor principal del aumento de las amenazas internas, los agentes externos también pueden obtener acceso a esas cuentas o descubrir cuentas no utilizadas que les permiten ocultar más fácilmente sus actividades. Una equivocación frecuente que cometen muchas organizaciones es despedir administradores y no desaprovisionar inmediatamente sus cuentas, ni eliminar todos los derechos de acceso.

Una solución obtenida de las mejores prácticas es el proceso integral y continuo que consiste en comprender qué usuarios deben tener acceso a qué recursos y, luego, verificar periódicamente que cada usuario tenga los derechos de acceso correspondientes. La gobernanza de identidades (dividida en Administración de Funciones y Cumplimiento de Identidad en los niveles altos) implica diversos procesos relacionados con la identidad, como la verificación y la limpieza de los derechos de usuario existentes, la construcción de modelos adecuados de funciones y la aprobación de políticas y procesos que ayuden a garantizar la asignación apropiada de privilegios a los usuarios. Las soluciones de gobernanza de identidades pueden entregar una gran variedad de beneficios, que incluyen los siguientes:

- Mayor seguridad mediante la automatización de los procesos necesarios para pasar las auditorías de cumplimiento y mediante el establecimiento de políticas de seguridad de identidades entre sistemas.
- Menores costos de administración de identidades mediante la simplificación de los pasos incluidos en los proyectos, como la detección de funciones, la organización de los privilegios y la certificación.
- Mejor tiempo de posicionamiento en el mercado de la IAM y cumplimiento de la política mediante la entrega más rápida de una base precisa y coherente de seguridad y funciones.

Controles de datos

La meta final de todos los ciberataques es robar información confidencial o provocar daños, de modo que tener control sobre los datos resulta un componente esencial de una defensa exitosa. De forma similar, muchas infracciones de seguridad internas son la consecuencia de que un empleado descargue valiosos datos de propiedad intelectual (como los códigos fuente). Para proteger los datos confidenciales, una organización debería proteger y controlar los datos en cuatro estados:

1. **Datos en el acceso.** Intento de tener acceso a información confidencial por parte de una persona en una función que no le corresponde.
2. **Datos en uso.** Información confidencial que se maneja en la estación de trabajo local o en un equipo portátil.
3. **Datos en movimiento.** Información confidencial que se transmite a través de la red.
4. **Datos en reposo.** Información confidencial almacenada en repositorios, como bases de datos, servidores de archivos o sistemas de colaboración.

Para lograrlo, las organizaciones deben definir políticas que apliquen el control si se detecta un acceso o uso inadecuado de los datos. Una vez que se produce una violación de políticas (como intentar el acceso a propiedad intelectual, copiar la información a una unidad USB o intentar enviarla por correo electrónico), la solución debe mitigar el compromiso y, al mismo tiempo, generar una alarma.

El centro de cualquier iniciativa de seguridad de los datos es la clasificación de la información. Sin comprender la información en contexto, como qué es la información y dónde está ubicada, es imposible implementar un programa de protección de datos integral. Una organización debe detectar y clasificar con precisión la información confidencial sobre la base de su nivel de confidencialidad para la organización. Esto incluye la propiedad intelectual y también la información de identificación personal, la información privada de salud y otra información no pública.

Después de clasificar adecuadamente la información, definir políticas e implementar controles, una organización puede proceder a monitorear y controlar el acceso y el manejo de toda la información confidencial. Esto abarca acciones de usuarios como el simple intento de acceso y lectura de datos confidenciales, la copia de datos en un dispositivo extraíble o su impresión, su envío fuera de la red por correo electrónico, hasta la detección de datos almacenados en un repositorio, como SharePoint.

"Solo los aficionados seleccionan máquinas como objetivo; los profesionales seleccionan personas".[10]

– Bruce Schneier

Autenticación avanzada

A pesar de que, generalmente, no se consideran los métodos de autenticación cuando se analizan las amenazas internas, estos son muy relevantes en el caso en que un agente externo explote a un usuario interno para que le proporcione sus credenciales. Las contraseñas no proporcionan una seguridad adecuada para la información y las aplicaciones importantes de la actualidad. Cuando los atacantes se autentican en el sistema, existen factores contextuales que, si se reconocen, pueden servir como advertencia acerca de la validez de la autenticación. Por ejemplo, si una persona del Departamento de Finanzas que trabaja en Nueva York de repente inicia sesión en Rusia, o bien, si una persona inicia sesión desde Roma dos horas después de cerrar sesión en Nueva York, es obvio que se está realizando una autenticación fraudulenta.

La autenticación basada en el riesgo proporciona una calificación de riesgo para cada intento de autenticación, lo cual ayuda a determinar si se está ejecutando un intento de infracción. En estos casos, se podrían utilizar métodos de "autenticación incremental" adicionales, se podría rechazar, simplemente, el intento, o bien, se podría activar una alarma.

Seguridad de la virtualización

El potencial para el daño provocado por las amenazas internas aumentó recientemente gracias a las enormes cantidades de datos confidenciales y a las herramientas de administración más potentes. El auge de la virtualización, en particular, dio lugar al surgimiento de nuevos riesgos. En primer lugar, existe una nueva clase de administradores en el hipervisor que se debe administrar, monitorear y controlar. En segundo lugar, esos administradores del hipervisor pueden cambiar, copiar o eliminar decenas de máquinas virtuales mediante unos pocos clics del mouse, lo cual hace que el robo y los daños sean más simples y más rápidos de conseguir, más perjudiciales, y más difíciles de detectar que nunca.

Para superar los desafíos de seguridad en un entorno virtualizado, las organizaciones deben adoptar un enfoque proactivo en lugar de reactivo para impedir las amenazas y las negligencias. Para empezar, se podrían aplicar las bases de la seguridad que ya están incorporadas en una infraestructura tradicional en la capa del hipervisor.

Estas acciones permiten establecer una base de seguridad sólida, pero por sí solas no pueden abordar todos los cambios dinámicos que hacen que los servidores virtuales sean menos seguros que los servidores físicos. La infraestructura virtual debe asegurarse aún más con la implementación adicional de capacidades que sean específicas de la virtualización. La automatización compatible con virtualización ofrece funcionalidades sin precedentes para administrar los riesgos asociados con la seguridad del hipervisor. Esto, utilizado junto con los elementos fundamentales de la seguridad, salvaguarda su entorno virtual mientras soporta las demandas rápidas de su negocio.

Sección 3: Beneficios

Control para habilitación

Con el uso de controles de seguridad basados en datos e identidades, las organizaciones no solo reducen los riesgos de infracciones internas, sino que mejoran los programas de cumplimiento. Las capacidades automatizadas y administradas de forma central ayudan a reducir costos, al mismo tiempo que fortalecen los controles de seguridad de TI. Con las auditorías estrictas, los desafíos de cumplimiento parecen menos intimidantes, ya que permiten a las organizaciones proporcionar pruebas de los controles y demostrarles a los auditores el funcionamiento eficaz de los controles de seguridad establecidos.

Defenderse contra los usuarios internos de cualquier tipo es un problema fundamentalmente desafiante. El flujo de información es fundamental para el funcionamiento de un negocio. Las restricciones pueden ocasionar problemas operativos o evitar que los empleados tengan acceso a la información que necesitan para ser eficaces e innovadores.

Tener los controles ***adecuados,*** sin embargo, puede permitirle a una organización compartir información con una gran variedad de personas. Estos controles le permiten a una organización operar con ***confianza limitada.*** Al no estar restringidas a otorgar únicamente privilegios de "todo o nada", las organizaciones pueden compartir información específica con personas a las que antes se les habría denegado ese acceso. Las organizaciones que usan los controles de esta manera hacen de la seguridad una herramienta para habilitar el negocio.

Las organizaciones también deben tener en cuenta que al protegerse de las amenazas internas, también se están protegiendo de los atacantes externos. Las partes externas generalmente usan las identidades, incluidas las identidades con privilegios, después de que el atacante violó el perímetro de la red. Al emplear una base sólida de controles de seguridad interna, una organización sienta las bases para prevenir o reducir los daños de ataques externos.

Sección 4:

Conclusiones

Las amenazas internas son reales y están en aumento. Las organizaciones deben enfrentar la realidad de que las amenazas internas ya no son un concepto abstracto, sino algo que podría ocurrir en cualquier momento. Pero en lugar de adoptar una mentalidad defensiva y aceptar la inevitabilidad de dichos ataques internos, las organizaciones deben adoptar una postura más activa para combatir las amenazas internas. Una parte central de esta actitud agresiva debe ser la administración de identidades y accesos, junto a la prevención de fuga de datos.

Las amenazas internas nunca podrán eliminarse de forma permanente, pero los controles basados en la identidad son los elementos estructurales sobre los cuales debe basarse un programa exitoso de prevención de amenazas internas. Las organizaciones que toman en serio la lucha contra las amenazas internas deben implementar algunas o todas estas capacidades, ya que hacerlo es un mecanismo eficiente y comprobado para controlar los ataques internos.

Sección 5:

Referencias

1 El Ponemon Institute, “The Risk of Insider Fraud: Second Annual Study” (El riesgo del fraude interno: segundo estudio anual), febrero de 2013

2 El Ponemon Institute, “The Risk of Insider Fraud: Second Annual Study” (El riesgo del fraude interno: segundo estudio anual), febrero de 2013

3 bigstory.ap.org/article/sentencing-set-corporate-espionage-suspect

4 cert.org/insider_threat

5 newyorker.com/online/blogs/closeread/2013/06/edward-snowden-the-nsa-leaker-comes-forward

6 slate.com/articles/technology/future_tense/2013/02/fiberwan_terry_childs_gavin_newsom_on_why_governments_should_outsource_technology.single

7 articles.chicagotribune.com/2012-08-31/business/ct-biz-0830-moto-theft--20120831_1_trade-secret-case-hanjuan-jin-trade-secrets

8 online.wsj.com/article/SB10001424052970203753704577255723326557672

9 Forrester Research Inc., “Assess Your Identity And Access Management Maturity” (Evalúe su nivel de madurez en la administración del acceso y las identidades), 26 de septiembre de 2012

10 schneier.com/crypto-gram-0010

Sección 6:

Información sobre los autores

Russell Miller trabaja, desde hace más de seis años, en el área de seguridad de red, y ha desempeñado distintas funciones, que comprenden desde ataques informáticos éticos a marketing de productos. Actualmente, es director de Marketing de Soluciones en CA Technologies, y se centra en la administración de identidades con privilegios y la seguridad de la virtualización. Russell tiene una licenciatura en Informática de la universidad Middlebury College y una maestría en Administración de Negocios de la Escuela de Administración y Dirección de Empresas del MIT (Instituto Tecnológico de Massachusetts).

Merritt Maxim tiene 15 años de experiencia en el marketing y la administración de productos en la industria de seguridad de la información, además de realizar tareas para RSA Security, Netegrity y CA Technologies. En su actual función en CA Technologies, Merritt maneja el marketing de los productos para la administración de identidades y las iniciativas de seguridad en la nube de CA. Coautor de "Wireless Security" (Seguridad inalámbrica), Merritt hace comentarios sobre una variedad de temas acerca de la seguridad de TI y se lo puede seguir en www.twitter.com/merrittmaxim. Merritt obtuvo su BA con honores en Colgate University y su MBA en MIT Sloan School of Management, y es el autor de Wireless Security (Seguridad inalámbrica).