REPORTE OFICIAL | OCTUBRE DE 2014

Amenazas persistentes avanzadas: la defensa desde adentro hacia afuera

Russel Miller
CA Technologies, Administración de Seguridad

ca technologies

Tabla de contenidos

Resumen

Desafío

Proteger una organización constituye un desafío cada vez más arduo. Los ataques son cada vez más complejos, y el avance de las APT (amenazas persistentes avanzadas), un tipo de ataque dirigido a blancos específicos, ha hecho que las organizaciones tomen conciencia de su vulnerabilidad ante los ataques. Empresas, como RSA Security, Google o Northrup Grumman, han sido blanco de APT. El hecho de no haber sido víctima de una violación importante en el pasado no garantiza un avance en la seguridad, ya que las organizaciones que son blanco de las APT enfrentan dificultades que no suelen ver los administradores de seguridad, como el distanciamiento de las acciones en el transcurso de meses o años a los fines de evitar la detección. El daño causado por la violación también está en aumento, lo que hace este desafío completamente real para los ejecutivos sénior.

Oportunidad

No existe una solución fácil cuando se trata de defenderse contra las APT. Se deben emplear múltiples capas de protección que se combinen para reducir el potencial de una violación y mitigar el daño en caso de que ocurra una violación.

El enfoque inicial para defenderse contra los ataques a blancos específicos consiste en proteger el perímetro mediante firewalls y sistemas de detección de intrusión para detectar y bloquear conductas anómalas. Este enfoque puede ser eficaz en la defensa contra determinados tipos de ataques; no obstante, no protegen contra todos los vectores de ataque, como el “spear phishing” (ataque de suplantación de identidad dirigido) y la “ingeniería social”.

En tanto que ningún otro producto de seguridad de punto (basado en tecnología o de otro tipo) puede proteger completamente una organización contra las APT, la disponibilidad actual de las soluciones de seguridad multidominio puede ayudar a que las organizaciones se protejan del mejor modo posible. La administración de identidades con privilegios, la protección y el control de la información y la seguridad de la infraestructura interna son áreas que tradicionalmente se analizan en silos, pero que ahora es posible combinar para permitir que las organizaciones protejan sus infraestructuras de TI y centros de datos de maneras complementarias. CA Technologies lo denomina inteligencia de identidades y datos.

Beneficios

Comprendiendo las amenazas persistentes avanzadas y protegiéndose contra ellas, las organizaciones reducen el riesgo en el caso de que se conviertan en el blanco específico de un ataque. El riesgo que se reduce no es únicamente financiero, sino también operativo, legal, normativo y de reputación.

Mediante la adopción de una vista holística de la seguridad que se puede emplear contra las APT, una organización se protege igualmente de ataques menos avanzados, automatizados e incluso internos. Un enfoque integral de la seguridad posee varias otras ventajas, como la mejora del cumplimiento, la habilitación de servicios basados en la nube, la mejora de la seguridad de la virtualización y la generación de ahorros de costos.

Sección 1: Desafío

Amenazas persistentes avanzadas: no es el negocio de siempre

Las amenazas persistentes avanzadas plantean desafíos distintos a los de los riesgos de seguridad tradicionales. Las amenazas persistentes avanzadas se refieren a un ataque a largo plazo y sofisticado dirigido a una entidad específica. El atacante suele tener el patrocinio estatal y busca obtener inteligencia altamente valiosa de otros gobiernos, aunque también pueden realizarlos organizaciones privadas y dirigirlos a otras organizaciones privadas. Esta denominación fue utilizada por primera vez por la Fuerza Aérea de los Estados Unidos en 2006.[1] El NIST (Instituto Nacional de Normas y Tecnología) define las amenazas persistentes avanzadas (APT) de la siguiente manera:[2]

"La amenaza persistente avanzada es un adversario con niveles sofisticados de pericia o recursos considerables que le permiten, por medio del uso de múltiples vectores de ataque (p. ej., cibernético, físico y el engaño), generar oportunidades para alcanzar sus objetivos, que habitualmente son establecer y extender su posicionamiento dentro de la infraestructura de tecnología de la información de las organizaciones con fines de filtrar información hacia el exterior de manera continua o socavar o impedir aspectos importantes de una misión, un programa o una organización, o ubicarse en una posición que le permita hacerlo en el futuro. Además, la amenaza persistente avanzada persigue sus objetivos repetidamente durante un lapso extenso, adaptándose a las medidas de defensa del atacado, y con la determinación de mantener el nivel de interacción necesario para ejecutar sus objetivos".

En tanto que otras definiciones varían, las tres palabras ayudan a clarificar en qué consiste una amenaza persistente avanzada:[3]

- **Avanzada:** el atacante posee considerables capacidades técnicas para ser capaz de explotar las vulnerabilidades del blanco. Ello puede incluir el acceso a grandes bases de datos de vulnerabilidades y habilidades de explotación y codificación, pero también la capacidad de revelar y aprovechar las vulnerabilidades previamente desconocidas.
- **Persistente:** las APT suelen producirse durante un plazo extendido. A diferencia de los ataques a corto plazo que aprovechan las oportunidades temporales, las APT pueden tener lugar en el transcurso de varios años. Se pueden utilizar múltiples vectores de ataque, desde los basados en Internet hasta la ingeniería social. Es posible que se combinen violaciones de seguridad de menor importancia durante un cierto tiempo para obtener acceso a datos más significativos.
- **Amenaza:** para que exista una amenaza debe haber un atacante con la motivación y la capacidad para realizar un ataque exitoso.

Las herramientas puramente automatizadas no se consideran una APT por sí mismas, aunque pueden ser utilizadas por un grupo coordinado y organizado como parte de un ataque de mayores dimensiones.

Etapas

Una amenaza persistente avanzada típica puede componerse de las cuatro etapas siguientes:

Ilustración A.

Cuatro etapas de una amenaza persistente avanzada

1. **Reconocimiento:** investigación de las vulnerabilidades de una organización. Esto puede incluir la investigación básica, incluidas consultas de dominio hasta análisis de puertos y vulnerabilidades.
2. **Entrada inicial:** explotación de las debilidades para conseguir una posición en la red del blanco de ataque. Esto se puede realizar mediante métodos técnicos sofisticados o con diversas técnicas, como los ataques de suplantación de identidad dirigidos, lo que genera que se obtenga el acceso de un usuario normal a un sistema individual. "Ingeniería social", o la explotación de personas, también constituye un método común para obtener acceso.
3. **Aumento de los privilegios y la expansión del control:** una vez que un atacante penetra en el perímetro de la red, intenta obtener más privilegios y control sobre sistemas importantes. Este paso puede involucrar la instalación de herramientas de "acceso indirecto" destinadas a simplificar el acceso futuro a la red.
4. **Explotación continua:** una vez que se establece el control, el atacante puede exportar continuamente datos confidenciales.

Las etapas tercera y cuarta pueden tener lugar a lo largo de años a fin de reducir el riesgo de detección.

¿Qué hace que las APT sean diferentes?

La diferencia principal entre las APT y las amenazas "normales" es que tienen una organización como blanco específico. Si bien la defensa del "perímetro" y el uso de controles de seguridad estándar pueden proteger una organización contra los ataques estándares, es posible que estas técnicas no sean suficientes al momento de enfrentar las APT. Los pacientes atacantes pueden esperar hasta que nuevas vulnerabilidades revelen una debilidad o pueden combinar vulnerabilidades aparentemente menores en un ataque a gran escala y perjudicial.

Cuando se enfrenta una amenaza semejante, las reglas habituales no rigen. En el pasado, numerosas organizaciones sencillamente necesitaban contar con una mejor seguridad que otras organizaciones y negocios conectados a Internet, ya que muchos atacantes elegirían los blancos más fáciles. No obstante, en vista de las APT, las organizaciones deben ser capaces de vencer a un enemigo motivado que se tomará el tiempo de buscar debilidades en lugar de dirigirse a otro blanco.

El plazo de las APT también contribuye a que la detección sea especialmente difícil. En una violación de seguridad estándar, es posible que se exporten cantidades significativas de datos en un período corto, lo que hace posible la detección de la violación por medio de los firewalls y los dispositivos de detección de intrusiones. Un atacante en una APT puede exportar datos específicos a lo largo de meses o incluso años, venciendo incluso sistemas con funciones completas y bien configurados.

Objetivos	Blancos
Debido a su naturaleza dirigida, los perpetradores de las APT poseen a menudo objetivos diferentes a los de los piratas informáticos de Internet comunes, y en lugar de un robo simple y daños recreativos, se enfocan más en los siguientes puntos: ▪ Manipulación política ▪ Espionaje militar ▪ Espionaje económico ▪ Espionaje técnico ▪ Extorsión financiera	Tipos específicos de organizaciones corren más riesgos de sufrir APT debido a la frecuente naturaleza política y favorecida por el Estado de la amenaza: ▪ Organismos gubernamentales ▪ Organizaciones de defensa y contratistas ▪ Sistemas de infraestructura importantes (p. ej., sistemas de servicios públicos, comunicaciones y transporte) ▪ Organizaciones políticas ▪ Instituciones financieras ▪ Empresas de tecnología

Ejemplos

RSA

En 2011, RSA Security anunció que había sido víctima de lo que se define como una APT.[4] Los atacantes obtuvieron la entrada inicial engañando a un usuario interno para abrir un correo electrónico que incluía un archivo adjunto con una hoja de cálculo que explotó una vulnerabilidad de día cero en Adobe Flash. A partir de allí, los atacantes fueron aumentando sus privilegios, instalaron accesos indirectos y obtuvieron el control de sistemas adicionales.

Los atacantes pudieron obtener acceso a los sistemas de RSA que guardaban información relacionada con sus tokens de autenticación de dos factores, conocidos como SecurID. Esta información incluía potencialmente valores “semilla” que RSA utiliza con sus tokens para generar las contraseñas de un solo uso que cambian cada 60 segundos. Si se robara el código fuente, los atacantes podrían buscar vulnerabilidades en la implementación de SecurID o incluso en el mismo cifrado.

Operación Aurora

Operación Aurora fue una APT que apuntó a numerosas empresas de gran magnitud, como Google, Adobe, Rackspace y Juniper Networks. Los reportes de los medios sugieren que también tuvo como objetivo muchas otras empresas, como Yahoo, Northrup Grumman, Morgan Stanley, Symantec y Dow Chemical.[5] Se cree que el Buró Político de China dirigió los ataques como parte de una campaña coordinada y de gran escala contra los Estados Unidos y otros países occidentales.[6]

Sección 2: Oportunidad

Protección exhaustiva

Para protegerse contra amenazas persistentes avanzadas, la clave es la "protección exhaustiva". Si cuenta con el tiempo suficiente, un atacante determinado será capaz de generar una violación en la mayoría de los perímetros de red. Una defensa exitosa tendrá las siguientes características:

1. Hacer que la penetración inicial sea difícil.
2. Reducir el potencial para aumentar privilegios en el caso de que una cuenta esté comprometida.
3. Limitar el daño que se pueda realizar por una cuenta comprometida, aun si tiene privilegios.
4. Detectar las cuentas comprometidas y las actividades sospechosas en las etapas iniciales del proceso.
5. Reunir información útil para una investigación forense, a fin de poder determinar qué daño se produjo, cuándo, y quién lo realizó.

La protección del perímetro con firewalls y sistemas de detección de intrusión en la frontera de la red solo puede ayudar con la primera y cuarta defensa. Se requiere una estrategia de protección más activa.

Detección temprana

Las violaciones se suelen detectar después de que el atacante obtuvo acceso a una red interna y causó daños o robó grandes cantidades de datos. En este punto, la "defensa" contra la APT implica un proceso costoso de control de daños, limpieza y monitoreo constantes. La clave para una protección accesible y posible de administrar contra las APT yace en la detección de las amenazas con la mayor anticipación posible. En la fase inicial de un ataque, cuando el atacante puede dar el primer paso dentro de la red, una organización puede valerse de distintas técnicas para detectar una violación, como la desvinculación de la seguridad del sistema de la administración del sistema y su externalización, la prevención y la detección de intentos de aumento de privilegios y el uso no autorizado de privilegios, además de la auditoría y el registro de las actividades de usuarios fuera de registros del sistema operativo (ese tipo de auditoría y registro puede ser desconocido para el atacante).

La administración de identidades con privilegios y la protección y el control de la información y la infraestructura interna conforman el núcleo de una protección exhaustiva contra las APT, conjuntamente con la detección temprana. Estas técnicas se detallan en las secciones a continuación.

Administración de identidades con privilegios

Las herramientas de PIM (administración de identidades con privilegios) administran y monitorean las cuentas administrativas, como "Administrador" en Windows y "raíz" en UNIX y Linux. Sistemas de PIM:

- Implementan el principio de "privilegios mínimos", aun para cuentas administrativas.
- Administran el acceso a cuentas compartidas a través de las capacidades de administración de contraseñas de usuarios con privilegios.
- Realizan el seguimiento de las actividades de usuarios para ayudar a garantizar su responsabilidad y también para prestar colaboración en una investigación de violaciones de seguridad.

Acceso de privilegios mínimos

Todo el personal debería poseer los privilegios mínimos necesarios para realizar sus tareas. Si bien numerosas organizaciones comprenden este concepto, con frecuencia fallan al momento de ponerlo en práctica, especialmente en el caso de las cuentas administrativas. Las personas que requieren cierto nivel de acceso con privilegios habitualmente reciben la contraseña para la cuenta administrativa correspondiente, que es compartida por varias personas.

Lo que las organizaciones deben comprender respecto de la prevalencia de las APT es que el acceso con privilegios no necesita ser una decisión a "todo o nada". Se pueden otorgar privilegios importantes a las personas para permitir que lleven a cabo únicamente una tarea muy específica. En el pasado, los sistemas UNIX y Linux lo realizaban utilizando la herramienta "sudo", pero las herramientas modernas de control de acceso pueden otorgar o denegar el acceso de forma centralizada tanto para sistemas UNIX como para Windows®.

Modelo de seguridad: desvinculación de la seguridad de la administración del sistema

Un sistema operativo típico cuenta con un modelo de seguridad de dos capas: usuarios con privilegios y usuarios comunes. No obstante, a los fines de la protección contra las APT, se necesita un modelo más sofisticado. Este modelo está basado en los principios de seguridad estándares de "privilegios mínimos" y "segregación de tareas". Como mínimo, se deben definir tres roles administrativos primarios:

- **Administrador del sistema:** el administrador del sistema en sí debe tener los privilegios requeridos para realizar las actualizaciones del software del servidor y los cambios de configuración necesarios e instalar el software. Los administradores del sistema no deben poder cambiar la configuración de seguridad importante ni visualizar registros relacionados con la seguridad.
- **Administrador de seguridad:** estos administradores deben poder actualizar y cambiar la configuración de seguridad y visualizar registros relacionados con la seguridad. Los administradores de seguridad no deben poder instalar software ni tener acceso a datos confidenciales de un sistema.
- **Auditor:** los auditores deben poder comprobar la configuración de seguridad y visualizar archivos de registro, pero no deberían tener la capacidad de realizar ningún cambio en el sistema. Si bien es posible que requieran tener acceso a archivos confidenciales, todos los accesos deberían ser de solo lectura.

Se deben crear tipos de administradores adicionales cuando sea apropiado, como administradores de bases de datos o para otras aplicaciones especialmente delicadas.

Por medio de un modelo de seguridad de múltiples niveles: se logran dos metas simultáneamente: proteger contra las amenazas internas de administradores internos limitando lo que cada persona puede hacer, y también hacer que sea mucho más difícil que los atacantes externos perpetren las ATP. En lugar de necesitar comprometer una cuenta de "superusuario", los atacantes ahora necesitarán obtener acceso a múltiples cuentas para poder tener acceso pleno a un sistema.

Controles específicos

Los controles específicos, aparte de ser una buena práctica de seguridad, son especialmente útiles en la mitigación de los daños causados por una APT. Una vez que los atacantes obtienen privilegios administrativos, suelen instalar "rootkits" de acceso indirecto y comienzan a exportar datos confidenciales. Con controles de acceso apropiados, un atacante aun con acceso con privilegios se ve limitado en lo que puede hacer, y es posible que se le impida tener acceso a archivos confidenciales, ejecutar comandos malintencionados, instalar programas, detener o iniciar servicios o cambiar archivos de registro. En un sistema donde se implementan controles específicos, es posible que un atacante se vea forzado a comprometer múltiples cuentas para poder realizar lo que antes era posible con una única cuenta.

La implementación de controles de acceso específicos también puede mitigar el riesgo que presenta la mayor debilidad de seguridad en una organización: su personal. Valiéndose de lo que se conoce como técnicas de "ingeniería social", los atacantes suelen engañar a empleados y otros agentes internos para que proporcionen información que puede utilizarse a fin de obtener acceso a sus cuentas o revelar otras debilidades de la seguridad. Mediante la limitación del acceso a sistemas y datos importantes de empleados, es posible disminuir el daño que puede realizar un atacante que obtenga acceso a las cuentas mediante ingeniería social.

Administración de cuentas compartidas

La administración de cuentas compartidas (o "administración de contraseñas de usuarios con privilegios") constituye una defensa clave contra las APT. La obtención del acceso a las identidades con privilegios (frecuentemente con el aumento de privilegios) es el paso intermedio clave en casi todos los ataques que logran su objetivo. Las herramientas de administración de contraseñas de usuarios con privilegios deberían servir para lo siguiente:

- Almacenar contraseñas cifradas de forma segura.
- Administrar la complejidad de las contraseñas y los cambios automatizados regulares de acuerdo con la política.
- Restringir el acceso a las cuentas administrativas exigiendo que todos los accesos atraviesen un portal centralizado.
- Usar la funcionalidad de "inicio de sesión automático" para prevenir que aun los usuarios autorizados conozcan las contraseñas de las cuentas con privilegios.
- Proporcionar acceso de emergencia a las cuentas, que posee controles adicionales y exige aprobaciones.
- Eliminar el uso de contraseñas integradas como parte del código en scripts (que suelen estar almacenadas en texto no cifrado y pueden ser robadas por un usuario malintencionado).

Estas capacidades no solo evitan que se compartan estas contraseñas, también previenen el robo de contraseñas desde archivos de contraseñas personales o mediante el registro de pulsaciones de teclas. Exigiendo que todos los inicios de sesión de cuentas con privilegios atraviesen un proxy central, una organización puede hacer el seguimiento de todos los inicios de sesión y las actividades en el caso de una violación, lo que ayuda a las medidas de investigación y potencialmente a mitigar el daño.

Generación de reportes de las actividades del usuario

Comprender cuáles acciones realizan las cuentas con privilegios resulta un componente clave para detectar las APT y mitigar el daño en un evento de un ataque inicial exitoso. Por su naturaleza, las APT suelen implicar la exportación de grandes cantidades de datos, lo que puede detectarse con las herramientas correctas. Los registros de actividades de usuarios prueban qué sistema y qué actividades de usuario están ocurriendo en un sistema o dispositivo de red y pueden servir para identificar violaciones de las políticas e investigar violaciones de seguridad.

Normas, como la HIPAA (Ley de Responsabilidad y Portabilidad del Seguro Médico) y el proyecto de Ley 1386 de California, y numerosas leyes estatales de notificación de violaciones exigen que una organización revele la violación de seguridad a la persona u organización afectada. Los registros de las actividades de usuarios se pueden utilizar para investigar la violación de seguridad a los fines de descubrir no sólo quién la cometió sino también cómo sucedió, de modo que se puedan corregir los controles internos y mejorar los procesos.

Las herramientas de generación de reportes de actividades de usuarios deberían poder efectuar estas tareas:

- Seguimiento de lo siguiente:
  - Todos los inicios de sesión, especialmente los de las cuentas compartidas y con privilegios, incluido el IP (protocolo de Internet) de origen, el id. del usuario original que tiene acceso a una cuenta compartida, y la fecha y la hora tanto del inicio como del cierre de sesión.
  - Todas las actividades de las cuentas compartidas hasta llegar al id. de usuario original.
  - Todos los comandos, ingresados por la línea de comandos o escritos en la GUI.

- Detección de comportamientos anómalos:
    - Identificar actividades sospechosas y generar alertas.
    - Proporcionar la capacidad de correlación de registros, con el foco en la conexión entre la actividad del usuario y la persona que lo llevó a cabo, por medio de un análisis de patrones complejos de registros de auditoría.
- Investigación de violaciones:
    - Comprobar "quién hizo qué" en un entorno de cuenta compartida.
    - Entregar herramientas visuales de análisis de registro con capacidades de obtención de detalles que puedan acelerar la investigación de actividades de usuarios y recursos, además de la identificación de violaciones a políticas.

En el evento de una violación, estas capacidades ayudarán a que una organización comprenda lo siguiente:

- El modo en que el atacante pudo obtener acceso a una cuenta.
- Lo que pudo llevar a cabo mientras utilizó esa cuenta y el daño que produjo.
- Cómo prevenir futuros ataques por medio del mismo método o métodos similares.
- Quién fue el atacante, potencialmente, y de dónde provino.
- Qué información se debe reportar a los organismos regulatorios.

Resulta fundamental recordar que los registros deben estar protegidos de los administradores. Los usuarios con privilegios pueden determinar dónde están almacenados localmente los registros en los sistemas y pueden detectar cuáles políticas de auditoría se utilizan en la organización. Pueden cubrir su propio rastro por medio de la eliminación de registros dentro de los archivos de registro locales, gracias a que poseen acceso completo a los sistemas (si es que no están implementados controles específicos apropiados). Las organizaciones deberían almacenar los registros en una ubicación remota a la que puedan tener acceso esos usuarios con privilegios y, además, monitorear si se realizan intentos de eliminar los archivos de registro local en los sistemas.

Control y protección de la información

En una APT, la meta final del ataque es robar información confidencial, de modo que tener control sobre los datos resulta un componente esencial en una defensa exitosa. Para proteger datos confidenciales contra una APT, una organización debería proteger y controlar los datos en cuatro estados:

- **Datos en el acceso.** Intento de tener acceso a información confidencial por parte de una persona en una función que no le corresponde.
- **Datos en uso.** Información confidencial que se maneja en la estación de trabajo local o en un equipo portátil.
- **Datos en movimiento.** Información confidencial que se transmite a través de la red.
- **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 inadecuado a los datos o un uso incorrecto de estos. Una vez que se produce una violación de políticas (como intentar el acceso a propiedad intelectual, copiar la información a una unidad USB [bus serie universal] 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 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.

Seguridad de la infraestructura interna

Mientras que la protección del perímetro de la red y las identidades con privilegios y los datos son componentes fundamentales de una defensa exhaustiva contra las APT, también resulta importante proteger la infraestructura de TI interna. Además de una apropiada arquitectura y segmentación de red, ello implica configurar y proteger adecuadamente los servidores y dispositivos individuales, así como sus entornos.

Seguridad imprevista y externalizada

Los atacantes elaboran estrategias y emplean tácticas contra las defensas de seguridad conocidas. Igualmente, utilizan comandos, funciones y utilidades comunes del sistema operativo para reunir información, monitorear el sistema y tomar medidas para expandir su control. Los profesionales de la seguridad pueden utilizar las suposiciones básicas de los atacantes en su contra incorporando elementos inesperados a un sistema. Por ejemplo, archivos y comandos que en apariencia no están protegidos ni monitoreados por los registros del sistema pueden estar, efectivamente, protegidos y monitoreados por una herramienta externa. De hecho, los permisos que un atacante visualiza no son necesariamente los permisos que están siendo aplicados. Esto hace posible que una organización detecte a un atacante que verifica los permisos del sistema operativo y viola políticas externas cuando prueba los límites de los permisos.

Este es el motivo fundamental por el cual la administración de seguridad debe externalizarse y separarse de la administración del sistema operativo. Luego de obtener el acceso inicial a un sistema, el atacante típico intentará aumentar sus privilegios a los fines de eludir los controles del sistema operativo. Con este acceso, asumen que podrán anular los mecanismos de seguridad y “ocultar sus huellas” eficazmente. Con una función de seguridad externa, suele ser posible detectar y contener a los atacantes mucho más temprano en el proceso de la APT: cuando un atacante intenta aumentar sus privilegios, cambiar los controles de seguridad de los sistemas o ejercer privilegios que no se han otorgado. Si bien un atacante puede eludir exitosamente los controles y registros del nivel del sistema operativo tradicionales, los procesos de detección externa pueden tomarlos por sorpresa. Básicamente, una organización puede implementar una directiva de control de acceso en la trastienda, de un modo potente e inesperado.

Además, se pueden cambiar y modificar los comandos estándares del sistema. Si los administradores vuelven a nombrar las funciones, como “sudo”, todos los intentos de utilizar el comando sudo original pueden activar un alerta y conducir a la detección temprana de una violación.

Refuerzo del servidor

Todos los servidores que alojan información confidencial se deben configurar de modo que se minimice el potencial de compromiso y difusión de datos en el evento de que efectivamente se produzca un compromiso. Ello incluye lo siguiente:

- Utilizar un firewall de software para controlar las comunicaciones entrantes y salientes, restringir los paquetes mediante IP de origen, protocolo (p. ej., SSH, TELNET, etc.) y puerto TCP; bloquear los protocolos inseguros (p. ej., servicios no cifrados, como los FTP)
- Bloquear todas las ejecuciones e instalaciones de aplicaciones salvo que estén especificadas explícitamente ("lista blanca de aplicaciones"), lo que previene las explotaciones de la ejecución del código y la instalación de software indirecto.
- "Confinamiento" de aplicaciones. Definir y permitir acciones aceptadas para aplicaciones de alto riesgo y restringir cualquier conducta que exceda estos límites. Por ejemplo, se puede elaborar una ACL (lista de control de acceso) basada en un id. lógico que posee procesos y servicios de Oracle®, de modo que su conducta confinada le prohíbe realizar cualquier acción aparte de iniciar los servicios de Oracle DBMS.
- Prevenir cambios en los archivos de registro.
- Habilitar el monitoreo de integridad de los archivos para detectar cambios en archivos clave, como los que realizan los "rootkits".
- Controlar el acceso a los archivos de directorio de aplicaciones confidenciales (p. ej., únicamente la aplicación de nómina de pago puede abrir archivos de nómina de pago).
- Detectar cambios de archivos confidenciales en tiempo real.

Seguridad unificada

Un problema común en la computación distribuida es la variación de capacidades y disponibilidad de los controles de seguridad en las plataformas (p. ej., los controles de los archivos y los directorios de UNIX son considerablemente diferentes de los de Windows). Esto puede provocar una serie de problemas susceptibles de explotación:

- Las políticas de seguridad dirigidas a un modelo de sistema, en lugar de a un modelo de seguridad del negocio.
- Las políticas de seguridad deben adaptarse a las limitaciones de los sistemas.
- La complejidad adicional de la administración de la seguridad genera errores y omisiones.

A los fines de proveer una defensa integral contra APT, las configuraciones de seguridad deben aplicarse con la mayor equidad posible en todas las plataformas. Se deben comprender y seguir todas las limitaciones y contradicciones.

Esta es otra razón por la que las organizaciones no deberían confiar exclusivamente en la seguridad de su sistema operativo. Las herramientas externas pueden ofrecer una plataforma universal para aplicar un paradigma de seguridad en todos los entornos, lo que permite un enfoque de seguridad centralizado, dinamizado y específico del negocio.

Seguridad de la virtualización

La cantidad de sistemas virtualizados aumentó explosivamente, lo que convierte a los entornos virtuales en un blanco clave de APT para los atacantes. El hipervisor también constituye un blanco importante debido al nivel de acceso que puede representar. Si un atacante compromete el hipervisor, puede obtener prácticamente acceso completo a todas las máquinas virtuales que se ejecutan en ese hipervisor. En tanto que la seguridad del sistema operativo puede evitar inicios de sesión directos y el cifrado puede proteger los datos confidenciales, estas medidas no resisten a un atacante insistente. Alguien con el control administrativo de un hipervisor puede copiar máquinas virtuales completas en un

entorno externo, como así también eludir la seguridad basada en host utilizando métodos de fuerza bruta o bien sobrescribiendo archivos clave.

A los fines de proteger los entornos virtuales, las organizaciones deben concentrar su atención, una vez más, en los administradores y aplicar el principio de privilegios mínimos. En primer lugar, se debe controlar estrictamente el acceso a las cuentas con privilegios del hipervisor con monitoreo y registro de todas las acciones. En segundo lugar, del mismo modo que se hace en los entornos físicos, se debe restringir a las identidades con privilegios del hipervisor para que lleven a cabo únicamente las acciones requeridas. Por ejemplo, un administrador de finanzas debe poder tener acceso solo a las máquinas virtuales que pertenezcan al departamento de finanzas y no a los sistemas de recursos humanos.

Síntesis

Ninguna herramienta de seguridad protegerá una organización contra una APT perpetrada por un atacante determinado, capaz, persistente y con abundantes recursos. La meta de cualquier estrategia de defensa contra una APT yace en dificultar al máximo posible la penetración en la red (limitando la cantidad de daño que se puede realizar y la cantidad de información que se puede robar en el caso de una violación que logre su objetivo) y en detectar una violación con la mayor celeridad posible.

En tanto que la seguridad perimetral es un componente obligatorio en la prevención de la violación inicial, de ningún modo resulta suficiente y tampoco sirve para reducir el daño una vez que se produjo la violación. La clave para la mitigación se encuentra en la combinación inteligente de administración de identidades con privilegios, clasificación y control de datos, y la seguridad de la infraestructura.

Las herramientas estándar de administración de identidades con privilegios pueden restringir u otorgar el acceso basadas en un conjunto de reglas. Si bien esta capacidad puede proporcionar una segregación de tareas adecuada, no es una solución rígida por naturaleza. Los privilegios se pueden modificar con el tiempo a medida que cambian las funciones, pero se trata de una solución esencialmente pasiva.

Se necesita de una función “basada en el contenido” para incorporar una nueva generación de defensa activa contra las APT. Esto quiere decir integrar la inteligencia de datos en cada decisión que se tome cuando se determine si aprobar o no una solicitud. Esa integración se debe realizar por medio del reconocimiento y la comprensión de patrones de accesos y usos de datos. Por ejemplo, se deberían tener en cuenta los siguientes puntos:

- **Cambios en el acceso a tipos de datos.** Un administrador que de modo continuo tiene acceso a datos de un tipo específico (p. ej., registros operativos) luego solicita el acceso a información financiera confidencial o datos de clientes.
- **Cambios en el uso de los datos.** Un administrador habitualmente tiene acceso a datos confidenciales por medio de una aplicación específica con solicitudes de acceso de solo de lectura para exportar datos a un disco duro externo, unidad USB o enviarlos por correo electrónico.
- **Cambios en la cantidad de los datos.** Un administrador tiene acceso a 100 MB de datos confidenciales por semana y solicita acceso a 500 GB en un período similar.
- **Cambios en la frecuencia de acceso a los datos.** Un administrador tiene acceso a datos altamente confidenciales una vez por mes y, repentinamente, tiene acceso a esos mismos datos, diariamente.

Ninguno de estos cambios indica por su mera aparición que se ha producido una violación; no obstante, sí representan un cambio en la conducta. Un sistema que controle de forma inteligente el acceso de usuarios con privilegios debería tomar en cuenta todos estos factores cuando revise una solicitud de acceso. Esta inteligencia de datos puede utilizarse para denegar el acceso a recursos en tiempo real o bien para permitir el acceso, pero crear también una alerta que señala actividad sospechosa.

Sección 3: Beneficios

Reduzca los riesgos

Las organizaciones que son blanco de una amenaza persistente avanzada enfrentan múltiples tipos de daños. Es posible que los atacantes roben propiedad intelectual y documentos estratégicos, y afecten así posiblemente la competitividad. El robo de datos de clientes puede provocar la reacción negativa de clientes, daño a la reputación y el inicio de acciones legales. El robo de información privada de salud o registros financieros puede generar problemas de cumplimiento normativo.

Un beneficio secundario de un programa holístico de defensa contra las amenazas persistentes avanzadas es que ayuda a proteger una organización de otras amenazas, como los ataques externos automatizados o las amenazas internas. Muchas de las técnicas empleadas para mitigar el daño de las APT limitan también el acceso que se otorga a las cuentas internas, incluso las de administradores. Limitando el acceso y segregando las tareas aun para los usuarios con privilegios, una organización se protege a sí misma contra un administrador no autorizado u otro usuario interno malintencionado.

Otro aspecto único de este enfoque es que no requiere de conocimiento específico de vulnerabilidades y nuevas explotaciones, y que no depende de la defensa perimetral. Con el uso de estas técnicas, las organizaciones pueden aplicar un modelo de seguridad y permitir o denegar acciones basándose en reglas empresariales, confidencialidad de los datos o conducta anómala. Como este modelo se puede aplicar uniformemente en todas las plataformas y se puede separar de la seguridad del sistema operativo, puede brindar un medio eficaz para defender contra las APT y detectar los ataques en las etapas iniciales del proceso.

Sección 4:

Conclusiones

La preponderancia de los ataques a blancos específicos es cada vez mayor. Las violaciones a empresas, como RSA, han recibido gran difusión en los medios y tendrán consecuencias a largo plazo, tanto para la reputación como para las ganancias.

La idea de protección exhaustiva no es nueva. Se trata de un aspecto fundamental de cualquier programa de seguridad. Lo que sí es nuevo es el enfoque en la protección de las identidades internas con privilegios a los fines de prevenir el daño realizado por agentes externos. Dado que el perímetro de la red ya no es el bastión de la seguridad que solía ser, la identidad se torna un aspecto todavía más importante. Básicamente “la identidad es el nuevo perímetro”.

Cuando se utiliza la identidad para protegerse contra amenazas internas y externas, como las APT, el “conocimiento de contenido” debería ser un requisito clave. Por medio del uso de inteligencia de datos como parte de cada decisión de acceso, las organizaciones actuales pueden comprender mejor los riesgos asociados con cada una de las acciones que realiza un usuario. Las solicitudes de acceso a datos confidenciales se pueden analizar y comprender en un contexto muchísimo más amplio que en el pasado. En lugar de depender de reglas fijas para permitir o bloquear ciertas acciones, los datos se pueden usar para generar un panorama más claro de las actividades de usuarios.

Para ayudar a que su organización se anticipe a la jugada en lo que respecta a la defensa contra ataques a blancos específicos, adopte la administración de identidades con privilegios y el conocimiento de contenido como las piedras angulares de su programa de seguridad.

Sección 5:

Referencias

1 http://taosecurity.blogspot.com/2010/01/what-is-apt-and-what-does-it-want.html

2 Publicación especial del Instituto Nacional de Normas y Tecnología 800-30, revisión 1, Guide for Conducting Risk Assessments (Guía para realizar evaluaciones de riesgo), http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf

3 "Advanced Persistent Threat" (Amenaza persistente avanzada), Wikipedia, http://en.wikipedia.org/wiki/Advanced_persistent_threat

4 http://www.rsa.com/node.aspx?id=3872

5 http://en.wikipedia.org/wiki/Operation_Aurora

6 http://www.nytimes.com/2010/11/29/world/29cables.html?_r=2&hp

Sección 6:

Acerca del autor

Russell Miller trabaja, desde hace más de ocho 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 Productos en CA Technologies, y se centra en la administración de identidades con privilegios y la protección de los datos. Russell tiene una licenciatura en Informática de la universidad Middlebury College y una maestría en Administración Empresarial de la Escuela de Administración y Dirección de Empresas del MIT (Instituto Tecnológico de Massachusetts).