LIBRO ELECTRÓNICO

ANÁLISIS DE LA SEGURIDAD PARA ENDPOINTS UNA PERSPECTIVA DE DEFENSA EXHAUSTIVA CONTRA EL RANSOMWARE

INTRODUCCIÓN: RECONSIDERAR EL ENDPOINT

La nube ha erosionado el otrora bien definido perímetro de la red, exponiendo a su empresa a ciberataques cada vez más sofisticados y dañinos. Los ordenadores

de sobremesa, portátiles y servidores protegidos de forma inadecuada proporcionan puntos de entrada para que los atacantes roben datos y causen estragos. Esto se ve agravado por el hecho de que los usuarios finales están repartidos por múltiples oficinas (en casa) y zonas geográficas, así como por la variedad de dispositivos y aplicaciones en la nube que se necesitan para hacer su trabajo.

Los ataques de ransomware están en constante evolución y son más frecuentes que antes, interrumpiendo directamente la actividad empresarial y repercutiendo en la reputación al ocupar los titulares de la prensa. Junto con los costes de las demandas y multas, los ataques contra endpoints cuestan a las grandes empresas más de 9 millones de dólares. En una encuesta realizada por CyberArk a 1 000 responsables de la toma de decisiones en materia de TI, el 59 % incluyó el ransomware en su lista de mayores riesgos para la seguridad[2].

[1] 2019 State of Endpoint Security Risk, Ponemon Institute
[2] CyberArk Global Advanced Threat Landscape Report

Defensa a fondo

Es hora de reconsiderar el endpoint y adoptar un enfoque de defensa exhaustiva de la seguridad para endpoints, estableciendo una serie de controles de seguridad para protegerse contra el ransomware. Concebido originalmente por la Agencia Nacional de Seguridad de EE. UU., un enfoque de defensa exhaustiva emplea múltiples capas de seguridad para eliminar las brechas, reducir las superficies de ataque y contener los riesgos.

Este libro electrónico repasa los cinco elementos esenciales de una estrategia integral de seguridad para endpoints. Un plan de seguridad para endpoints de varias capas puede ayudarle a detectar vulnerabilidades, mejorar su posición en materia de seguridad y mitigar los riesgos.

El promedio de las pérdidas económicas de un ataque contra endpoints supera los 9 millones de dólares[1]

Un enfoque de defensa exhaustiva para la protección contra ransomware

Cinco elementos esenciales de la estrategia de seguridad para endpoints

- Detección y respuesta para endpoints (EDR)
- Antivirus y NGAV
- Gestión de privilegios
- CDR - Protección del correo electrónico
- Parcheado de aplicaciones y SO

ELEMENTO N.º 1

DETECCIÓN Y RESPUESTA PARA ENDPOINTS (EDR)

Las herramientas EDR le permiten identificar e investigar de forma proactiva la actividad sospechosa en los endpoints. Las soluciones EDR, que surgieron en 2013 para ofrecer una capa de seguridad adicional, supervisan, registran y analizan continuamente las actividades de los endpoints, ayudando a los profesionales de TI y de seguridad a detectar y mitigar las amenazas avanzadas de forma eficaz.

Muchas soluciones EDR utilizan análisis avanzados, analizando los eventos de los endpoints para detectar actividades maliciosas que, de lo contrario, podrían pasar desapercibidas. Las herramientas EDR ofrecen visibilidad del comportamiento sospechoso de los endpoints en tiempo real, ayudándole a detener las amenazas antes de que se afiancen y propaguen por toda la empresa.

Detección y respuesta ampliadas (XDR)

Para detectar más amenazas y proporcionar más contexto a sus análisis, las herramientas están evolucionando para incluir redes, nubes y endpoints con análisis y automatización más avanzados.

DETECCIÓN Y RESPUESTA PARA ENDPOINTS

Detecte y responda a los ataques activos avanzados en los endpoints

ANTIVIRUS/NGAV

Evite la infección de malware mediante una amplia gama de técnicas

ELEMENTO N.º 2

ANTIVIRUS Y NGAV

Los antivirus (AV) y las herramientas de protección antivirus de última generación (NGAV) le ayudan a detectar y eliminar diversas formas de malware. Las soluciones AV tradicionales identifican y bloquean los programas maliciosos mediante la inspección de archivos y la búsqueda de patrones de firma de virus conocidos. Estas herramientas, si bien eran eficaces cuando se introdujeron por primera vez, no detectan los tipos de amenazas más recientes como malware sin archivos y exploits de día cero. De hecho, en una encuesta del Ponemon Institute, el 62 % de los encuestados afirmó que sus soluciones antivirus tradicionales solo mitigan el 50 % o menos de los ataques[3].

Las herramientas NGAV utilizan análisis predictivos, inteligencia artificial (IA) y aprendizaje automático (AA) para defenderse contra ataques contemporáneos como el ransomware y el phishing avanzado, que pueden eludir los programas antivirus convencionales. A diferencia de las soluciones AV tradicionales que escanean los archivos en busca de patrones conocidos, las soluciones NGAV adoptan un enfoque holístico, examinando cada proceso que se ejecuta en un endpoint y utilizando la IA y el AA para detectar y bloquear de forma inteligente formas desconocidas de malware.

[3] 2018 State of Endpoint Security Risk, Ponemon Institute

ELEMENTO N.º 3

GESTIÓN DE PRIVILEGIOS

Las soluciones de gestión de privilegios le ayudan a contener los riesgos asociados con las cuentas con privilegios, como las cuentas de administrador de Windows o Mac. Las cuentas con privilegios se utilizan para controlar archivos, directorios, servicios y derechos de acceso de usuarios. En las manos equivocadas, se pueden usar para robar datos o interrumpir sistemas.

Los atacantes a menudo intentan obtener acceso no autorizado a las cuentas con privilegios a través de ataques de malware o phishing en el endpoint. Una vez que se infiltran, pueden atravesar la red en busca de objetivos de alto valor y utilizar privilegios elevados para robar información confidencial o interrumpir aplicaciones críticas. Forrester estima que al menos el 80 % de las filtraciones de datos guardan relación con credenciales con privilegios comprometidas[5].

Las soluciones ayudan a reducir la exposición al eliminar los derechos administrativos locales y controlar estrictamente los permisos de usuarios y aplicaciones en función de políticas. Al aplicar el principio del mínimo privilegio (otorgar a los usuarios el mínimo conjunto de privilegios necesarios para realizar su trabajo), puede evitar la propagación lateral y mejorar su posición en materia de seguridad, sin perjudicar la productividad de los usuarios ni afectar al rendimiento de la empresa.

GESTIÓN DE PRIVILEGIOS

Gestione los derechos locales de administración y el acceso a las aplicaciones a la vez que mantiene la productividad de los usuarios

Protección contra el ransomware basada en privilegios

Al establecer controles de aplicaciones, algunas soluciones le permiten evitar que se ejecuten aplicaciones maliciosas conocidas y limitar el funcionamiento de aplicaciones no autorizadas. Esto reduce significativamente el riesgo y la incertidumbre. Las funciones ampliadas incluyen la capacidad de detectar ransomware en aplicaciones no cubiertas (todavía) por políticas, el bloqueo de intentos de robo de credenciales y la detención proactiva de ataques en curso mediante componentes de privilegios engañosos, como cuentas fraudulentas de administrador local o contraseñas falsas.

[5] The Forrester Wave™: Privileged Identity Management, Q4 2018

CDR - Seguridad del correo electrónico

Proteja las cuentas de correo electrónico ante pérdidas, compromiso y acceso no autorizado

ELEMENTO N.º 4

CDR - SEGURIDAD DEL CORREO ELECTRÓNICO

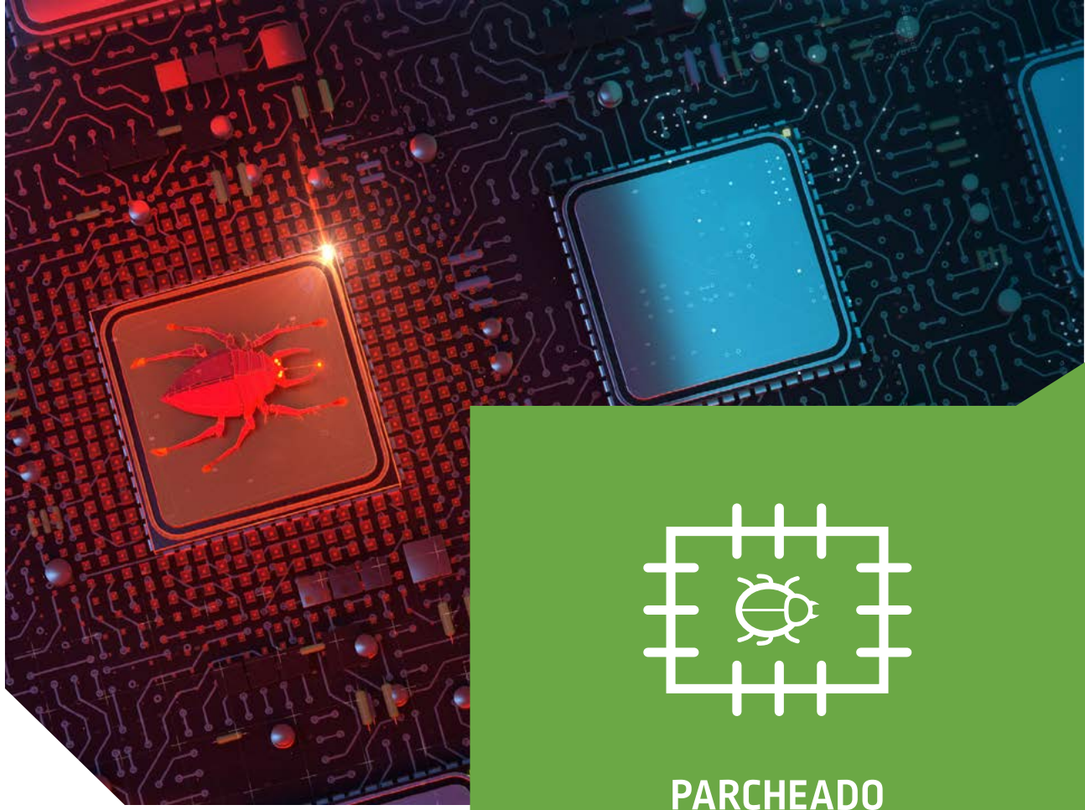
El 94 % de todo el malware se distribuye por correo electrónico y el phishing representa más del 80 % de los incidentes de ingeniería social notificados[4]. Mientras que la formación de concienciación del usuario final desempeña un papel importante a la hora de abordar estos problemas, las herramientas CDR (Content Disarm & Reconstruction) ofrecen una capa adicional de protección. Tradicionalmente, la tecnología CDR, a diferencia de la EDR, no detecta archivos maliciosos, sino que le permite eliminar los componentes no aprobados mediante reglas y políticas establecidas en una serie de fuentes, incluido el correo electrónico.

Las funciones de seguridad del correo electrónico incluyen protección contra correo no deseado, análisis de URL, espacios seguros para archivos adjuntos, filtrado dinámico de contenido y cifrado, además de archivado y copias de seguridad. Algunas soluciones están evolucionando para servirse de la IA y la información del usuario final en tiempo real para identificar y eliminar correos electrónicos maliciosos. Las consolas de administración permiten establecer políticas para usuarios, dominios y grupos de dominios, utilizar listas de permitidos/denegados y personalizar reglas de prevención de pérdida de datos (DLP).

[4] 2019 Data Breach Investigations Report, Verizon

ELEMENTO N.º 5

HERRAMIENTAS DE PARCHEADO



Las herramientas de parcheado le ayudan a realizar un seguimiento e implementar eficientemente las actualizaciones de software de los endpoints para reforzar su posición en materia de seguridad. Los habilidosos atacantes y ciberdelincuentes buscan constantemente vulnerabilidades de seguridad en las aplicaciones y los sistemas operativos para explotarlas. Los proveedores de software publican parches continuamente para solucionar vulnerabilidades conocidas[6]. En este juego continuo del gato y el ratón, las aplicaciones y los sistemas operativos deben mantenerse actualizados para mantenerse un paso por delante de los delincuentes.

Parcheado de aplicaciones

La gestión de las actualizaciones de las aplicaciones es un reto para muchas organizaciones. Según un estudio, una organización de TI típica tarda una media de 34 días en aplicar parches para vulnerabilidades de gravedad alta. Las soluciones de parcheado de aplicaciones le ayudan a eliminar procesos de gestión de parches manuales intensivos, propensos a errores y lentos, y a mejorar su preparación cibernética.

La mayoría de las soluciones de parcheado de aplicaciones ofrecen:

- IEscáneres de inventario para detectar todas las aplicaciones distribuidas por toda la empresa.
- Paneles de control de estado e informes para identificar aplicaciones vulnerables y corregidas.
- Herramientas para automatizar los procesos de aprobación, distribución e instalación de parches.

PARCHEADO

Implemente las actualizaciones para abordar problemas de seguridad y correcciones de errores

[6] Security Report for In-Production Web Applications, tCell by Rapid7

ELEMENTO N.º 5

Parcheado del SO

Al igual que las actualizaciones de las aplicaciones, debe estar atento a las actualizaciones del SO de los endpoints. Puede reducir las vulnerabilidades de seguridad estableciendo actualizaciones automáticas del sistema operativo o implementando otros sistemas y prácticas para garantizar que todos los ordenadores de sobremesa, portátiles y servidores de la empresa cuenten con las versiones más recientes.

Cada proveedor tiene su propio enfoque a la hora de emitir los parches del sistema operativo y debe ser considerado de forma individual. Microsoft publica **actualizaciones de seguridad** para servidores y escritorios Windows el segundo martes de cada mes. Estos parches se pueden instalar de forma automática desde Windows Update. Si desea probar las actualizaciones antes de desplegarlas en producción, puede utilizar Windows Server Update Services (WSUS) o una herramienta de parcheado de aplicaciones de terceros para distribuir e implementar las actualizaciones del SO en el horario que estime conveniente.

Apple publica software para macOS de forma periódica (que puede incluir actualizaciones de seguridad). Puede **configurar un Mac** para instalar las actualizaciones de macOS de forma manual o automática.

RESUMEN

Los endpoints suponen riesgos de seguridad significativos. Los habilidosos delincuentes pueden explotar las vulnerabilidades de los endpoints para robar información confidencial o interrumpir los servicios de TI, lo que conlleva una pérdida de ingresos y cuantiosos acuerdos legales y multas por incumplimiento de la normativa. Al adoptar un enfoque de defensa exhaustiva contra el ransomware —estableciendo una amplia gama de controles de seguridad para endpoints—, puede reforzar su posición en materia de seguridad y reducir la exposición.

La gestión de privilegios es un componente fundamental de una estrategia de seguridad para endpoints eficaz y a menudo se pasa por alto. Los usuarios internos maliciosos o los atacantes externos explotan las cuentas de administrador de los endpoints para afianzarse en una red, y luego se desplazan lateralmente para penetrar o alterar los objetivos de mayor valor.

Las soluciones de gestión de privilegios restringen el acceso con privilegios e imponen el control de aplicaciones, lo que permite a los usuarios disponer de los derechos mínimos necesarios para realizar su trabajo y reforzar la seguridad sin afectar a la productividad de los usuarios. Esto mitiga las amenazas en el endpoint de entrada, evita la propagación lateral y la propagación de malware, lo que en última instancia le ayuda a reducir la exposición y evitar el cifrado del ransomware.

04.21. Doc. 236307

Acerca de CyberArk

Como líder consolidado en la gestión del acceso con privilegios, CyberArk ofrece el conjunto más completo y flexible de capacidades de protección de la identidad para aplicar privilegios y permitir el acceso mediante cualquier dispositivo, en cualquier lugar y en el momento adecuado. La plataforma de Seguridad de la Identidad de CyberArk, basada en el comportamiento de IA y el análisis de riesgos, ofrece protección continua y acceso Just-In-Time para cualquier identidad, ya sea humana o de máquina, a medida que admite una plantilla distribuida, adopta la nube y nuevas tecnologías de la nube, y ofrece experiencias de cliente basadas en la confianza.

Con CyberArk, añade una línea de defensa crítica contra los ataques de ransomware al eliminar los derechos de administrador local y proporcionar acceso Just-In-Time a los privilegios cuando sea necesario. En combinación con las funciones de control de aplicaciones, bloqueo de robo de credenciales y privilegios engañosos, CyberArk ofrece una solución completa para la protección contra ransomware.

Las integraciones preinstaladas y las que se realizan a través del Marketplace de CyberArk respaldan nuestro enfoque de defensa exhaustiva.

Las funciones ampliadas abarcan la información sobre amenazas, datos de activos y otros indicadores del estado de seguridad de los endpoints.

MÁS INFORMACIÓN