ActualTech MEDIA

Hewlett Packard Enterprise

Adelantarse a las amenazas de seguridad

Ed Tittel

ÍNDICE

EN ESTE INFORME

Este resumen técnico analiza cómo HPE y sus partners ayudan a las pequeñas y medianas empresas a alejarse de los problemas de seguridad. Estas operaciones deben poder identificar amenazas y vulnerabilidades que supongan riesgos potenciales, priorizarlas por gravedad y crear planes de acción y mitigación para solventarlos. Esto implica esfuerzos constantes y permanentes para enfrentarse a un paisaje de amenazas siempre cambiante.

Entre los aspectos más destacados se encuentran los siguientes:

- Alinear una estrategia de seguridad con objetivos empresariales
- Crear una cultura empresarial que priorice la seguridad
- Supervisar superficies de ataque y establecer remedos proactivamente antes de que los hackers puedan actuar

Cuando se trata de ciberseguridad, el dicho «Más vale prevenir que curar» se aplica a la perfección. Esto se debe a que los costes de una cura (poner remedio a las consecuencias de un incidente o brecha de seguridad) son lo suficientemente altos para que actualmente supongan una amenaza existencial para la mayoría de las empresas, sobre todo las que realizan operaciones más pequeñas.

Esto es lo que hace que entender y anticiparse a los peligros de las amenazas de seguridad y vulnerabilidades puede ser tan importante, o incluso primordial. Al fin y al cabo, se trata de la gestión de riesgos, que implica lo siguiente:

- A medida que se conocen las amenazas y vulnerabilidades, el primer paso es **identificar** las que suponen riesgos reales para la empresa y evaluar su impacto y consecuencias potenciales.
- En el caso de los elementos que impliquen un riesgo, es fundamental **priorizarlos** de forma que los que tengan un coste más alto o consecuencias más extremas se solventen en primer lugar y, sucesivamente, en orden decreciente.
- Para los elementos con riesgo suficiente para garantizar una respuesta, las empresas deberían establecer **planes de acción y mitigación de riesgos** para abordarlos.

A la práctica, sobre todo para las pequeñas empresas, implementar un equipo de seguridad interno, esto significa suscribirse a algún tipo de un servicio de solución e inteligencia de amenazas. De hecho, HPE y sus partners pueden ayudarte con estas cosas, incluyendo la identificación, priorización y solución de riesgos como parte de una oferta de servicios de seguridad completos.

La nube lo cambia todo... incluso la seguridad

A medida que las organizaciones llevan suscripciones y servicios de nube, también aparecerán nuevos vectores de amenazas nuevos y complejos en el panorama de la seguridad del negocio. Esto hace que sea primordial aumentar la seguridad y realizar pasos para mejorar la postura ante la seguridad y ciberresiliencia de la empresa. Se deberían realizar los siguientes ejercicios empresariales para ayudar a la empresa a alcanzar estos objetivos:

- **Alinear tu estrategia de seguridad con tus prioridades empresariales:** Entendiendo los vacíos entre las prioridades de la empresa y las de la ciberseguridad, los gestores y usuarios pueden empezar a alinear ambas estrategias para garantizar que las prioridades principales están establecidas y los recursos y presupuestos asignados en consecuencia. Es importante que los líderes empresariales alcancen un nivel de acuerdo sobre las prioridades y que los perfiles de riesgos se entiendan perfectamente.
- **Crear una cultura que priorice la seguridad:** Una cultura que priorice la seguridad es un paso importante para un mundo lleno de incertidumbres y riesgos. Proteger los activos vitales se convierte en asunto de todo el mundo. Es primordial invertir en formación de concienciación del personal dada su relevancia como fuente de ciberriesgo y porque un esfuerzo colectivo frente a las amenazar dará un mejor servicio a tu empresa.
- **Conocer tu superficie de ataque y solucionar las vulnerabilidades antes de que los hackers las encuentren:** Los análisis de cibervulnerabilidades, también denominados pruebas de seguridad o pruebas de penetración, son un proceso de pruebas para asesorar la postura de seguridad de la organización (consulta la **Figura 1**). Identifica vulnerabilidades antes de que un atacante las pueda explotar. Este proceso proporciona información de los riesgos a los que se enfrentan los activos de la organización, desde perspectivas externas e internas. También ayuda a identificar los vacíos de seguridad potenciales antes de realizar auditorías o evaluaciones de cumplimiento. Para mejorar la postura de seguridad de tu organización también es importante desarrollar planes de mitigación accionables. Con ese fin, implicar a partners con experiencia (como HPE y sus partners) puede construir puentes entre la falta de capacidades cibernéticas en tu empresa y mitigar vulnerabilidades.

Cuatro fases de pruebas de iniciación

Figura 1: Las cuatro fases de pruebas de penetración en inglés también se conoce como «pen testing»

Descripción de la terminología

Recuperación ante desastres: Describe servicios y sistemas que permiten que una empresa recupere el funcionamiento normal incluso frente a un desastre o una interrupción total de acceso y servicio.

Ransomware: Un tipo de malware que deniega el acceso a sus empresas a sus sistemas y datos cifrándolo todo, para que nada funcione. Los criminales afirman que si se paga una rescate todo volverá al estado previo al ataque, pero el FBI recomienda que no se paguen rescates ya que las cosas no siempre salen bien.

Datos y aplicaciones contenedorizadas y virtualizadas: Aplicaciones y datos que se ejecutan en máquinas virtuales o contenedores a menudo en la nube, normalmente como parte de un modelo de computación basado en el consumo y en el uso.

Desde el extremo hasta la nube: Se refiere a los datos y recursos de computación que pueden residir en centros de datos o salas de servidores locales en el núcleo empresarial, en el borde de la red en ubicaciones remotas de campo, o en una o más plataformas de nube (por ejemplo, Amazon Web Services, Microsoft Azure, Google Cloud Platform).

Escenarios de nube híbrida y múltiple: Una nube híbrida implica la integración local y recursos de computación basada en la nube en un solo entorno par gestionar tareas de computación. Nube múltiple significa lo mismo, aunque implica dos o más plataformas de nube. Las empresas más modernas operan en entornos de nube híbrida y múltiple e intentan posicionar cargas de trabajo y datos donde tengan más sentido desde una perspectiva de coste, seguridad y rendimiento.

> **Es importante que los líderes empresariales alcancen un nivel de acuerdo sobre las prioridades y que los perfiles de riesgos se entiendan perfectamente.**

Cómo puede HPE (y sus partners) proteger la TI

Como un examen rápido lo verificará, las soluciones de ciberseguridad HPE son completas, innovadoras y fiables. Sus capacidades de seguridad empiezan a nivel de hardware y se amplían hasta los usuarios y sistemas en el extremo de la red. La tendencia general es recopilar y analizar inteligencia de seguridad para mantenerse actualizado en el paisaje de las amenazas, para mantener los sistemas y servicios de la empresa en uso, y para aconsejar (y dar asistencia) a sus clientes con la gestión y minimización de los riesgos de seguridad.

> **Las soluciones de ciberseguridad HPE son globales, innovadoras y fiables. Sus capacidades de seguridad empiezan a nivel de hardware y se amplían hasta los usuarios y sistemas en el extremo de la red.**

LA SEGURIDAD HPE EMPIEZA CON SUS SERVIDORES

HPE está reconocida como proveedor de los servidores estándar del sector más seguros. Su familia de servidores ProLiant ha recibido numerosos premios y elogios gracias a estas características concretas:

- **Proteger:** Los sistemas evitan la exposición a nivel de hardware y firmware a los ataques a través de una raíz de confianza de silicio, mejoras del módulo de plataforma de confianza (TPM), múltiples niveles de protección a prueba de alteraciones, e innovaciones HPE añadidas, como «Integrated Lights Out» firmware (iLO) para promover las capacidades de «priorizar la seguridad».
- **Detectar:** Un amplio conjunto de innovaciones que detecta y elude amenazas durante el tiempo de ejecución, que incluye comprobaciones de integridad de arranque, por las cuales iLO elimina códigos de firmware potencialmente pirateados (o realmente pirateados) y los sustituye con una copia válida conocida si es posible. En caso de que no se pueda producir la reparación, los sistemas no podrán arrancar (proporciona protección de prearranque frente a rootkits y otros ataques traicioneros basados en firmware).

- **Recuperar:** Capacidades fiables para restaurar y recuperar sistemas en sus últimos estados conocidos, correctos y que funcionen de forma rápida y fácil, gracias a sus mecanismos de restauración segura, copias de seguridad seguras y cifradas y a prueba de alteraciones.

Zerto

En 2021, HPE completó la adquisición de Zerto, una empresa que se especializa en recuperación ante desastres, recuperación de ransomware y soluciones de movilidad de nube múltiple. Ahora parte de HPE, Zerto ofrece protección de datos continua y recuperación de datos y aplicaciones contenedorizadas y virtualizadas desde el extremo hasta la nube. Con Zerto, las organizaciones pueden recuperar en minutos un estado unos segundos previos al ataque, eliminando largas y costosas pérdidas de datos y disrupciones. Zerto aporta más disponibilidad y menos gastos generales administrativos que la solución de protección de datos antiguos. Además, la gestión de datos escalable, automatizada y unificada de Zerto hace que la movilidad de datos y carga de trabajo entre nubes sea inmediata. Zerto también ofrece protección de datos continuos para organizaciones que emplean una estrategia para la nube híbrida e incluye Recuperación ante desastres como servicio (DRaaS) con una red de más de 350 proveedores de servicios gestionados. Visita la página HPE/Zerto para conocer como tu empresa puede evitar pérdidas de datos y tiempo de inactividad tan cerca de cero como la tecnología puede alcanzar.

SOLUCIONES DE SEGURIDAD HPE

Las herramientas de seguridad, herramientas, tecnologías y soluciones HPE utilizan las tres aproximaciones a través de su diseño, desarrollo, fabricación y mantenimiento. Su mejor descripción es la siguiente:

- **Seguridad centrada en los datos:** Las medidas de seguridad buscan proteger primero los datos y especialmente, los datos con algún grado de confidencialidad (información identificable personalmente o PII; cuentas y contraseñas, datos financieros, de salud o protegidos legalmente de otra forma, etcétera). Esto conecta directamente con la siguiente aproximación, que se centra en quién obtiene acceso a sistemas y datos, y con qué fines.

> **Contratar a partners con experiencia (como HPE y sus partners) puede abarcar lagunas de capacidades cibernéticas en tu empresa y mitigar vulnerabilidades.**

- **Seguridad de confianza cero:** El Instituto Nacional de Estándares y Tecnología (NIST) describe confianza cero (ZT) con el epigrama: «No confíes nunca, verifica siempre.» ZT se centra en la protección de datos y servicios pero también debería incluir todos los activos (dispositivos, elementos de la infraestructura, aplicaciones y recursos virtuales y en la nube) y sujetos (usuarios, aplicaciones, servicios y sistemas). Básicamente, ZT asume que los atacantes siempre están presentes y activos. Por eso, no confía en nadie y siempre analiza y evalúa riesgos para las funciones y activos empresariales. Verificar la identidad de todos los accesos solicitados es una estrategia fundamental, como lo es aplicar el «Principio de menos privilegio» (también conocido como PLP), que significa no dar más privilegios de los necesarios a los sujetos de los que necesitan para realizar sus trabajos.
- **DevSecOps:** Para explicarlo simplemente, es una extensión de la idea de DevOps, que pone a desarrolladores (y personal de soporte como testadores, documentadores y formadores) con personal de operaciones (administradores, soporte técnico y técnicos de campo o solucionadores de problemas) en una sola organización con objetivos compartidos. DevSecOPs va un paso más allá e integra al equipo de seguridad a través de todo el ciclo de vida de desarrollo, de forma que la seguridad se tiene en cuenta durante las fases de diseño, construcción, pruebas, mantenimiento y retirada en las operaciones de TI empresariales.

MÁS ALLÁ DE LAS SOLUCIONES: AYUDA DE CONSULTORÍA EXPERTA

HPE Pointnext Services puede ayudar a pequeñas y medianas empresas a asesorar, definir y redefinir sus estrategias de seguridad. Pointnext ofrece asistencia experta en la formulación de políticas de seguridad y en el cumplimiento de los requisitos de privacidad, confidencialidad y protección de datos. También pueden ayudar a empresas con limitación de recursos o conocimientos a integrar soluciones asequibles y efectivas para la continuidad del negocio y la recuperación ante desastres. De hecho, Pointnext se especializa en ayudar a las empresas a preparar proyectos

de seguridad para diseños e implementaciones de seguridad desde cero teniendo en cuenta la realidad (y dentro de las restricciones presupuestarias). También pueden proporcionar asistencia global a través de implementaciones de pruebas, pilotos y producciones. Por último, Pointnext ayuda a las empresas a garantizar que la seguridad esté integrada en toda la organización: trabajadores remotos, en el extremo, local y en entornos híbridos y de múltiples nubes.

Garantizar la cadena de suministros

Para atender a las necesidades de los clientes con unos requisitos de seguridad más altos de lo normal y escenarios de uso altamente seguros, HPE trabaja con una cadena de suministro de confianza (TSC). Clientes destascados de esta cadena de suministro incluyen el gobierno de EE. UU. y organizaciones y agencias del sector público que deben adquirir productos fabricados en los EE. UU. con garantía de producto verificable. La tecnología está presente en el TSC de dos formas importantes. En primer lugar, los productos incluyen características de seguridad reforzadas para que sean resistentes a las alteraciones o incluso a prueba de alteraciones. En segundo lugar, HPE supervisa toda la cadena de suministros, y da la aprobación a todas las piezas, observa el montaje y mantiene los bienes embalados de forma segura (y libre de alteraciones) hasta que el cliente acepta la entrega.

El Proyecto Aurora ofrece una arquitectura de seguridad completa con nuevas soluciones de seguridad integradas desde la capa de silicio.. Descubre cómo el Proyecto Aurora arranca en la cadena de suministro y establece una cadena de confianza inmutable a través de la infraestructura, el sistema operativo, la plataforma de software y las cargas de trabajo, sin necesidad de firmas, pérdidas significativas del rendimiento ni bloqueos.

Las herramientas de seguridad, herramientas, tecnologías y soluciones HPE utilizan las tres aproximaciones a través de su diseño, desarrollo, fabricación y mantenimiento.

HPE y sus partners ofrecen una amplia variedad de soluciones de seguridad cuidadosamente diseñadas para ayudar a pequeñas y medianas empresas a gestionar los riesgos, proteger sus sistemas y datos y afrontar el panorama de seguridad actual complejo y prohibitivo. Visita la página Soluciones de TI para pequeñas y medianas empresas HPE para obtener todos los detalles. Ten en cuenta que HPE y sus partners también pueden ofrecer coaching, consultoría, asistencia y servicios para ayudar a las empresas más pequeñas a estar seguras a través de su organización de servicios Pointnext.