Papel blanco técnico

Seguridad empresarial con recursos de empresas pequeñas y medianas

Contenido

Panorama de amenazas actual

La guerra entre los criminales cibernéticos y las organizaciones ha crecido en intensidad en las últimas décadas, ya que han evolucionado las herramientas que ambos utilizan para ejecutar y repeler ataques, respectivamente. Puede ser fácil pensar que esto sigue siendo un problema exclusivamente para empresas grandes, pero estos desarrollos han tenido notables repercusiones para el resto del mundo de los negocios.t

58 % de las víctimas del cibercrimen en 2018 fueron empresas pequeñas

Al hacerse el cibercrimen progresivamente más común y automatizarse cada vez más las amenazas desencadenadas por los criminales cibernéticos, ha aumentado la capacidad de estos de apuntar a vastas franjas de empresas cualquiera sea su tamaño. Por otro lado, las políticas de seguridad y capacidades defensivas de las empresas grandes han avanzado de manera increíble. En consecuencia, los criminales cibernéticos están dirigiendo su mirada cada vez más a las empresas de tamaño pequeño y mediano, que aunque ofrezcan menor rentabilidad se consideran a menudo como blancos más fáciles. El resultado es que 58 % de las víctimas del cibercrimen en 2018 fueron empresas pequeñas.[1]

Los peligros de una vulneración de datos no deben tomarse a la ligera, ya que cada vulneración tiene para las empresas de tamaño pequeño y mediano un costo promedio de 120 000 dólares.[2] Es claro que las empresas más pequeñas necesitan hacer más para defenderse contra la creciente cantidad de amenazas, pero muchas se preguntarán cómo pueden igualar una seguridad de nivel empresarial sin recursos de nivel empresarial.

Aunque las soluciones de seguridad en la nube son cada vez más accesibles para las empresas pequeñas y medianas (gracias a su naturaleza escalable y la ausencia de gastos de capital anticipados en infraestructura), es poco probable que las empresas pequeñas puedan permitirse una variedad de soluciones. Pero ¿qué pasa si gran parte de la seguridad que usted necesita ha venido incorporada en los puntos finales mismos?

Este artículo explicará algunas de las maneras en las que aun las organizaciones más pequeñas pueden solidificar sus defensas contra las amenazas cibernéticas. Se considerará especialmente la manera en que los puntos finales avanzados de HP, en combinación con políticas y procedimientos específicos, pueden proporcionar una amplia base de defensa que no solo puede impedir que ocurran las vulneraciones sino también responder de manera efectiva en caso de que ocurra lo peor.

[1] Verizon, '2018 Data Breach Investigations Report', (2018)
[2] https://usa.kaspersky.com/blog/economics-report-2018/15445/?utm_source=pr-media&utm_medium=partner&utm_campaign=us_economics-report18_promo&utm_content=link&utm_term=us_pr-media_promo_link_partner_economics-report18

Actualizaciones y administración

Cuando se trata de administrar políticas y procedimientos de seguridad en toda una flota de dispositivos de los empleados, puede ser difícil para TI asegurar la consistencia. La administración de la configuración de seguridad, como lo demandan los requisitos de la empresa y un cambiante panorama de amenazas, puede implicar muchas horas de trabajo; y asegurar que todas las actualizaciones y revisiones se instalen enseguida después de su emisión puede resultar una tarea abrumadora. Para las empresas pequeñas, con muchos menos recursos de TI que los de sus homólogas mayores, estas responsabilidades suelen ser más desafiantes. Por eso, no es de extrañar que muchas empresas fallen en esos aspectos. En efecto, una encuesta determinó que el 57 % de las organizaciones que informaron sobre una vulneración declararon que se debió a una vulnerabilidad para la que había una revisión disponible pero que no se había aplicado.[3]

57 % de las organizaciones que informaron sobre una vulneración declararon que se debió a una vulnerabilidad para la que había una revisión disponible pero que no se había aplicado

Han surgido soluciones de administración de puntos finales para proporcionar a las organizaciones una plataforma central de administración de su flota completa de dispositivos. Sin embargo, estas soluciones solo están diseñadas para administrar el software y el sistema operativo de sus dispositivos sin tener en cuenta las diversas funciones que se ejecutan a nivel del hardware. Afortunadamente, HP ha incluido este tema.

Al invertir en la serie de laptops HP EliteBook 360, las organizaciones tendrán acceso al kit de integración de gestión de HP. Este kit posibilita la gestión remota del BIOS, seguridad, hardware y software preinstalado. Está diseñado para integrarse con el Microsoft System Center Configuration Manager o la consola de administración de clientes que usted elija, para permitirle administrar las funciones mencionadas en este artículo, y muchas más, desde una ubicación individual remota. Con una visión general de su flota de puntos finales, puede otorgarse o rescindirse la autoridad según sea necesario, pueden aplicarse las reglas de política de grupo en toda la compañía y pueden implementarse las actualizaciones por oleadas. Al utilizarlo en colaboración con su consola de administración de clientes, usted puede elegir franjas horarias para implementar oleadas de actualizaciones y por lo tanto minimizar todo posible tiempo inactivo que afecte a sus empleados. Estas soluciones reducirán finalmente la carga de trabajo de su equipo de TI, mejorarán la velocidad de implementación y minimizarán la perturbación de los empleados.

[3] ServiceNow, 'Today's State of Vulnerability Response: Patch Work Demands Attention', (2018)

Navegación segura por la web

Para muchas empresas, sus navegadores web son el punto de entrada más vulnerable. Los empleados trabajan cada vez más en entornos de navegadores, por lo que pueden acceder de manera accidental a sitios web o correos electrónicos no seguros.

EL software antivirus tradicional puede eliminar el malware conocido, y los firewalls pueden bloquear código sospechoso; sin duda alguna, ambos deben implementarse en su red. Sin embargo, estas soluciones por sí solas no son una garantía de seguridad. Las amenazas flamantes que todavía deben identificarse pueden eludir las soluciones de seguridad tradicionales, ya que los hackers trabajan constantemente en el desarrollo de nuevas formas de evadir las soluciones de seguridad.

Otra opción es la creación de listas blancas o listas negras. Si bien la realización de una lista blanca que contenga solo direcciones de correo electrónico y sitios web aprobados puede garantizar seguridad, es probable que resulte un enorme obstáculo para sus empleados. Por otra parte, una lista negra está lejos de ser una solución completa, ya que solo abarcará un pequeño porcentaje de los dominios peligrosos. Además de esto, ambas opciones requieren amplias cantidades de tiempo para configurarse y mantenerse.

Pero ¿qué ocurre si usted pudiera garantizar que los empleados puedan navegar libremente por Internet y tengan acceso a todos los archivos que necesiten sin poner nunca su empresa en riesgo?

La laptop HP EliteBook x360 viene con soluciones incorporadas que pueden hacer que esto se haga realidad. HP Sure Click fortalece su seguridad al abrir todo sitio no confiable en un contenedor virtual aislado. Esta micromáquina virtual engaña al malware para que crea que está ejecutándose en su dispositivo, cuando en realidad se lo está atrapando y evitando que acceda y se disemine a cualquier otra parte de su dispositivo o incluso la red. Esta capa extra de defensa puede utilizarse sin limitar el acceso de los empleados ni su funcionalidad.

HP Sure Click fortalece su seguridad al abrir todo sitio no confiable en un contenedor virtual aislado

Esta protección puede extenderse incluso a los archivos descargados como los PDF, Microsoft Word, Microsoft Excel y Microsoft PowerPoint, que han sido reconocidos como los más propensos a contener código malintencionado.[4] Los archivos desconocidos pueden abrirse y examinarse en un entorno seguro, con lo que se garantiza a los usuarios que no liberarán accidentalmente malware en el sistema. Esta solución viene preinstalada, no require capacitación y es aplicada por hardware; esto garantiza que no puede deshabilitarse si el sistema sufre un ataque.

[4] Cisco, '2018 Annual Cybersecurity Report', (2018)

Protección por contraseña

81 % de las vulneraciones relacionadas con hackeo se valen de contraseñas robadas o débiles

Las contraseñas juegan sin duda un rol importante en la seguridad de la empresa, pero la aplicación de la protección por contraseña únicamente no suele ser suficiente para mantener segura su empresa. En efecto, Verizon determinó que el 81 % de las vulneraciones relacionadas con hackeo se valen de contraseñas robadas o débiles.[5] El paso siguiente es a menudo requerir contraseñas o frases de contraseña complejas, la renovación frecuente de estas contraseñas e incluso la introducción de múltiples respuestas (como una contraseña más una pregunta de seguridad). Aunque esto puede conducir a contar con defensas más resistentes, existen a menudo varios efectos secundarios no deseados que normalmente se pasan por alto.

Con el uso de una cantidad constantemente creciente de sistemas digitales en nuestra vida profesional y personal, se espera que los empleados recuerden una multitud de complicadas contraseñas de múltiples caracteres que deben cambiar periódicamente. Los estudios muestran que el 56 % de los empleados tienen que llevar cuenta de dos a cinco contraseñas diferentes para archivos y aplicaciones requeridas en su trabajo.[6] Algunos empleados pueden aceptar este desafío, pero otros pueden responder siguiendo prácticas potencialmente peligrosas, desde anotar sus contraseñas a reformular entradas anteriores e incluso elegir frases comunes u obvias. Alternativamente, la productividad de los empleados puede entorpecerse por los frecuentes bloqueos y solicitudes de renovación de contraseñas, todo ello debido al olvido de contraseñas.

La implementación de capacitación del personal y el respaldo a la importancia vital de las prácticas de contraseñas seguras es una táctica esencial para combatir estos problemas, pero no es la única herramienta a su disposición. La autenticación multifactor, que utiliza varios factores de identificación diferentes, asegura que en caso de que un atacante obtenga acceso a un tipo de información, su sistema permanecerá seguro. Estos sistemas pueden utilizar una amplia variedad de factores, como algo que el usuario conoce (contraseñas), algo que el usuario tiene (tarjetas inteligentes) y algo que el usuario es (reconocimiento facial) para ofrecer una protección que supera ampliamente los enfoques tradicionales.

Muchos servicios basados en la nube ofrecen la autenticación multifactor, a menudo con un segundo paso a través de una aplicación o un correo electrónico de seguimiento, pero es esencial que las empresas examinen su uso en asegurar sus puntos finales también. Con una elección apropiada del dispositivo, las organizaciones pueden evitar la inversión en un sistema de terceros extra para la administración de credenciales. La HP EliteBook x360 ofrece hasta tres niveles de autenticación que incluyen el uso de una cámara IR, un sensor de huellas digitales y un lector de tarjetas inteligentes, todos los cuales interactúan con el proceso existente del sistema operativo a fin de crear una experiencia de inicio de sesión sin problemas para los usuarios. Así, usted puede garantizar que no solo la seguridad de su acceso ha mejorado exponencialmente sino también que sus empleados pueden continuar trabajando sin obstáculos.

La HP EliteBook x360 ofrece hasta tres niveles de autenticación que incluyen el uso de una cámara IR, un sensor de huellas digitales y un lector de tarjetas inteligentes

[5] Verizon, '2017 Data Breach Investigations Report', (2017)
[6] https://businessinsights.bitdefender.com/security-impacts-productivity

Reacción y recuperación

En 2018, en el continente americano, las empresas demoraron una mediana de 71 días para descubrir una vulneración

Las organizaciones se han apoyado tradicionalmente en las estrategias de prevenir y proteger para mantener la propia seguridad; sin embargo, la alta sofisticación y el volumen de los ataques actuales indican que usted nunca puede garantizar que no sufrirá una vulneración. Como se indicó anteriormente, las ramificaciones de una vulneración pueden ser increíblemente costosas para las empresas, por lo que cuanto más se tarde en reconocer que ha ocurrido una vulneración y reaccionar a ella, mayor será el costo para la empresa. Sin embargo, el tiempo que les lleva a las organizaciones el descubrimiento de una vulneración sigue siendo alarmantemente alto. En 2018, en el continente americano, las empresas demoraron una mediana de 71 días para descubrir una vulneración.[7] En consecuencia, es vital que las empresas tengan implantadas estrategias de detección y de respuesta que las habiliten a actuar rápidamente en la identificación y la mitigación del daño de una vulneración cuando ocurre.

El antivirus y el software de detección de amenazas serán su primera línea de defensa en caso de que sus otras soluciones no puedan prevenir una intrusión. Estas soluciones deben monitorear continuamente su entorno y poner en cuarentena cualquier actividad sospechosa. Sin embargo, las soluciones de seguridad tradicionales a veces no logran identificar un malware o incluso son socavadas por las mismas amenazas que tratan de remediar. Esto puede ocurrir porque algún malware esté diseñado para destruir servicios y aplicaciones de seguridad críticas, y por lo tanto continúe oculto dentro de su red.

Afortunadamente, la HP EliteBook x360 viene con funciones aplicadas por hardware que pueden proteger sus dispositivos y datos en caso de que su seguridad tradicional falle. HP Sure Run está diseñada para proteger las aplicaciones y procesos críticos en todo el sistema operativo (OS). Monitorea aplicaciones, procesos, configuración de directivas y funcionalidad del OS en busca de cualquier cambio inusual, como un proceso que termina, un archivo que se borra o una configuración de registro crítica que cambia. Si ocurre una instancia de este tipo, automáticamente se reinicia el proceso o se restaura la configuración de ajuste mientras se notifica el incidente al usuario y a TI. De este modo, usted puede garantizar que ninguna de sus defensas se deshabilite, y como el agente es aplicado por hardware y se ejecuta fuera del dominio del sistema operativo, es invulnerable a las amenazas que pueden deshabilitar sus soluciones de seguridad basadas en software.

En caso de que se detecte una vulneración, usted probablemente necesitará restablecer la imagen inicial de su dispositivo o incluso de su flota completa, y restaurar sus datos con copia de seguridad. Desafortunadamente, este proceso puede ser increíblemente largo, y el tiempo inactivo resultante puede conducir a una pérdida importante de productividad. Asimismo, inevitablemente se perderán algunos datos vitales. La cantidad, sin embargo, depende de la periodicidad de las copias de seguridad.

Las organizaciones deben entonces priorizar la realización de copias de seguridad periódicas de los datos críticos para la empresa en una ubicación fuera del sitio, ya sea que tenga una infraestructura propia u opte por utilizar alguna de las diversas alternativas basadas en la nube. Muchas soluciones pueden incluso automatizar las copias de seguridad para que se realicen en momentos establecidos fuera del horario laboral, con lo que se libera a TI de la laboriosa tarea y se evita perturbar a los empleados.

[7] FireEye, 'M-Trends 2019 Report', (2019)

HP Image Assistant le ayudará a mantener con facilidad imágenes actualizadas de sus dispositivos y HP Sure Recover le permitirá restaurar de manera simple y rápida la última imagen, en caso de que la necesite

Antes de poder restaurar los datos con copia de seguridad, usted necesitará restablecer la imagen inicial de sus puntos finales para asegurar la erradicación de cualquier código malintencionado. HP Image Assistant le ayudará a mantener con facilidad imágenes actualizadas de sus dispositivos y HP Sure Recover le permitirá restaurar de manera simple y rápida la última imagen, en caso de que la necesite. Si se sospecha que la vulneración ha impactado en múltiples dispositivos, usted puede incluso restablecer la imagen inicial de su flota completa, de manera remota y en un solo paso. Aun si no mantiene y almacena su propia imagen de software, HP Sure Recover puede ayudar. El sistema extraerá la última versión del OS directamente de HP.

Protección del BIOS

La mayoría de las soluciones de seguridad del arsenal de una empresa están diseñadas para proteger la red, el software y los sistemas operativos de los dispositivos. Sin embargo, algunos ataques pueden apuntar a dispositivos a nivel de hardware, lo que elude completamente las defensas tradicionales que usted haya implementado. Los BIOS de sus dispositivos están específicamente en riesgo, ya que si los infecta un atacante podría robar datos valiosos, instalar ransomware o inutilizar su PC. Para empeorar las cosas, la mayoría del software antivirus no analiza su BIOS, por lo que si resulta infectado es probable que usted solo descubra el problema cuando sea demasiado tarde. Un BIOS que está dañado o infectado es increíblemente difícil de reparar, y puede originar un tiempo inactivo prolongado o un costoso reemplazo.

Afortunadamente, la HP EliteBook x360 viene como estándar con HP BIOSphere, un ecosistema de firmware que proporciona una protección automatizada y una gestionabilidad simple para los equipos de TI. Esto asegura que su dispositivo se inicie con un BIOS genuino cada vez que se arranca y que todas las actualizaciones son auténticas y firmadas digitalmente por HP.

La HP EliteBook x360 viene como estándar con HP BIOSphere, un ecosistema de firmware que proporciona una protección automatizada y una gestionabilidad simple para los equipos de TI

Por otro lado, HP Sure Start proporciona una recuperación automática ante una infección del BIOS. Esto funciona mediante la detección de cualquier cambio en el BIOS y restablece de manera automática la versión más reciente no afectada. Dado que esta función responde a cualquier cambio no autorizado en lugar de reconocer un malware conocido, puede proteger contra cualquier nueva amenaza. Aparte de esto, la solución es aplicada por hardware, lo que garantiza que no puede resultar dañada.

Para quienes cuentan con recursos de TI limitados, HP BIOSphere simplifica la administración de la configuración de BIOS de los dispositivos de su flota. Los equipos de TI pueden configurar y actualizar parámetros de manera centralizada para todos los dispositivos en unos pocos minutos, y las actualizaciones del BIOS pueden preconfigurarse para ocurrir a intervalos establecidos. Por otra parte, HP Sure Start viene habilitada de manera predeterminada y notifica automáticamente, tanto al usuario como a TI, cuando ocurre un evento. Esto simplifica más la carga de trabajo de TI.

Seguridad física

En el entorno de trabajo móvil de 24 horas al día y 7 días a la semana (24/7) es inevitable que los empleados necesiten trabajar fuera de la seguridad de las instalaciones de su empresa. En estas instancias, sus empleados y los dispositivos propios de ellos corren el mayor riesgo de robo, hackeo visual e intrusión física. En efecto: un 11 % de las vulneraciones implican una acción física por parte de un atacante.[8] La mejor defensa contra estos peligros es una capacitación completa de sensibilización en materia de seguridad, en la que los empleados tomen conciencia de los peligros físicos que acechan fuera de la oficina. Sin embargo, hasta el empleado más consciente de la seguridad puede dejar caer sus defensas en algún momento. En estas instancias, los equipos de TI pueden garantizar que los datos de la compañía permanezcan a salvo asegurando que los empleados estén equipados con los dispositivos apropiados. La HP EliteBook x360 viene con una cantidad de características que pueden reducir drásticamente la probabilidad de un robo de datos o un acceso no autorizado cuando los empleados están fuera de la oficina.

Un 11 % de las vulneraciones implican una acción física por parte de un atacante

El hackeo visual, en el que una persona ve físicamente la información en una pantalla cercana, es una de las maneras más simples y efectivas para que los aspirantes a hackers tengan acceso a datos confidenciales. Un experimento realizado para probar la eficacia de las técnicas de hackeo visual determinó que en 91 % de las instancias el hackeo visual fue exitoso, y el instigador pudo capturar información vital como credenciales de inicio de sesión e información financiera.

Para reducir la probabilidad de que se produzca el hackeo visual, HP introdujo Sure View en sus dispositivos. Esta nueva tecnología previene este tipo de ataque, simplemente haciendo que la pantalla sea visible a quienes estén directamente frente a ella. Con el toque de un botón se activa una pantalla privada integrada; esto significa que quien intente ver la pantalla desde la periferia se encontrará con un espacio en blanco.

Su preocupación siguiente es que una persona logre el acceso físico a un dispositivo sin vigilancia. En estas instancias, esa persona puede quitar datos a través de un puerto USB o cargar malware en el punto de conexión. Estos tipos de ataque son altamente efectivos a causa de la velocidad con la que ocurren. Los informes indican que se producen alrededor de 113.8 millones de este tipo de incidentes por año en todo el mundo. Sudamérica se destaca específicamente como una región propensa a estos tipos de ataque.[9] Los puertos USB pueden deshabilitarse, pero esto está lejos de ser una solución práctica. En cambio, HP Device Access Manager protege su sistema de estas amenazas al requerir la autenticación del usuario cuando se conecta cualquier dispositivo extraíble al dispositivo. Esto bloquea de inmediato una de las vulnerabilidades más peligrosas de su dispositivo.

[8] Verizon, '2018 Data Breach Investigations Report', (2018)
[9] https://securelist.com/usb-threats-from-malware-to-miners/87989/

A pesar de sus mejores esfuerzos, los empleados pueden terminar perdiendo o sufriendo el robo de un dispositivo. De hecho, más de la mitad de las empresas ha tenido datos expuestos debido a la pérdida de dispositivos por parte de empleados.[10] Por más completa que sea la forma en que usted haya asegurado los datos en un dispositivo, si alguien logra el acceso físico a su unidad de disco duro es muy poco lo que su seguridad puede hacer para impedirle el acceso a los datos. Esto ocurre a menos que la unidad de disco duro esté cifrada. Las laptops de HP tienen unidades con autocifrado que pueden configurarse fácilmente para garantizar que los datos permanezcan seguros. A diferencia del software de cifrado de terceros, el cifrado de HP funciona a nivel de hardware y por lo tanto no tiene impacto sobre el desempeño del sistema. Finalmente, cuando su dispositivo llegue al fin de su vida útil usted puede asegurar que todo dato confidencial que contenga la unidad de disco duro no caiga en las manos equivocadas, mediante el uso de HP Secure Erase. Esta solución destruye de manera permanente todos los datos, por lo que usted puede eliminar sus dispositivos sin trabas.

Conclusión

Con las nuevas amenazas que surgen cada año, las empresas de tamaño pequeño y mediano necesitan ser vigilantes como nunca antes. Sin embargo, la defensa de su empresa y sus empleados sin los recursos de una empresa más grande puede parecer una tarea abrumadora. Afortunadamente, existen nuevas soluciones que finalmente hacen factible para las empresas más pequeñas contar con una seguridad completa. La HP EliteBook x360, la PC más segura y manejable del mundo, ofrece incomparables capacidades defensivas que no requieren la capacitación de los empleados y permiten un manejo fácil por parte de TI. Una inversión en las HP EliteBooks le proporciona más que solo laptops: le garantiza que el futuro de su empresa es seguro.

La HP EliteBook x360 es las pc más seguras y manejables del mundo

[10] https://www.kaspersky.com/blog/the-human-factor-in-it-security/