DELL Technologies

Protección de terminales en medio de nuevas amenazas

Brindar a los empleados la flexibilidad para ser plenamente productivos mientras trabajan de manera remota hace que sea crítico que las empresas tengan implementadas medidas de seguridad de terminales, a fin de prevenir y detectar el creciente panorama de amenazas, así como responder ante él, a la vez que ofrece a los empleados dicha flexibilidad con el propósito de trabajar de forma remota.

A medida que los líderes de TI analizan el futuro en busca de señales del fin de la pandemia de la COVID-19, muchos están planificando en función de una nueva normalidad con un número mucho más alto de trabajadores remotos que nunca antes. Si bien muchas empresas y sus empleados se beneficiarán debido a una mayor productividad y un estilo de trabajo más flexible, se debe pagar un precio en términos de protección. El aumento repentino del trabajo remoto debido a la COVID-19 ha hecho que defender los terminales sea más complejo: el 84 % de los líderes de TI señala que proteger a una fuerza de trabajo remota es más difícil[1]. Una de las posibles explicaciones es el aumento del 148 % en los ataques de ransomware a organizaciones globales en medio del brote de la pandemia[2]. Esta es una estadística preocupante, ya que los trabajadores de oficina en el hogar dependen del correo electrónico como su principal medio de comunicación empresarial, lo que ha provocado un aumento del 350 % en los ataques de phishing[3].

Tendencias continuas de seguridad cibernética

El cambio repentino al trabajo remoto se lleva a cabo en un contexto de muchas inquietudes preocupantes de seguridad cibernética, que están sometiendo a prueba la experiencia de los profesionales de seguridad cibernética. Estos incluyen:

1. Ataques a nivel del BIOS: vulnerabilidades explotadas en hardware o silicio. Cuando el BIOS se ve comprometido, el atacante a menudo permanece oculto, mientras que el dispositivo tiene acceso con credenciales a la red y a los datos. El 63 % de las empresas ha sufrido una vulneración o infracción de datos debido a dichos ataques[4].
2. APT (Amenazas persistentes avanzadas): amenazas sofisticadas que a menudo acechan silenciosamente mientras recopilan información de comportamiento como un preludio para extraer datos valiosos. Es posible que las víctimas no se den cuenta de que ha ocurrido un ataque silencioso durante mucho tiempo (108 días en promedio[5]).
3. Malware basado en archivos y sin archivos
   - Malware basado en archivos: por lo general, se aplica a tipos de archivos con extensiones conocidas, como .DOCX y .PDF, la clase de archivos que los empleados necesitan para realizar su trabajo. Cuando un usuario abre el archivo, se ejecuta un código malicioso integrado.
   - Malware sin archivos: generalmente, es un programa legítimo que infecta a una computadora. Cuando el usuario inicia dicho programa desde un correo electrónico, el malware sin archivos infecta la computadora y, potencialmente, la red, de modo que elude con éxito muchas de las tecnologías de seguridad.
4. Ataques basados en estados-nación: por lo general, provienen de China, Corea del Norte, Rusia e Irán. Dado que cuentan con la experiencia tecnológica y el respaldo financiero de dichos estados-nación, los ataques a menudo son sofisticados y muy dañinos. Sin embargo, muchos de estos ataques aprovechan los sistemas que carecen de las actualizaciones y los parches más recientes. La unidad CISA (Cyber and Infrastructure Security Agency) del FBI envía asesorías periódicamente.

El cambio repentino al trabajo remoto se lleva a cabo en un contexto de muchas inquietudes preocupantes de seguridad cibernética, que están sometiendo a prueba la experiencia de los profesionales de seguridad cibernética.

1. "The State of DLP 2020", Tessian.
2. Blog de VMware Carbon Black, Patrick Upatham y Jim Treinen, 15 de abril de 2020.
3. Informe de Google, como se citó en PCMAG.com, 30 de marzo de 2020.
4. "Match Present-Day Security Threats with BIOS-Level Control", un documento de liderazgo del pensamiento de Forrester Consulting encargado por Dell, junio de 2019.
5. The 2018 U.S. State of Cybercrime Survey.

5. Ataques basados en la nube: aumentan a medida que las aplicaciones de productividad y colaboración basadas en la nube reemplazan a las aplicaciones de escritorio. En vista de que la empresa promedio usa más de 2400 servicios de nube, el 93 % de las organizaciones está moderadamente o muy preocupada por la seguridad en la nube[6]. La protección debe incluir la DLP (prevención de pérdida de datos) y la protección contra amenazas en los servicios en la nube. Además, la autenticación del usuario debe estar protegida contra la suplantación, y los datos deben estar cifrados desde y hacia los servicios en la nube.
6. Normativas de cumplimiento: destinadas a proteger la PII (información de identificación personal). A fin de evitar que la PII caiga en las manos equivocadas y, en última instancia, se utilice para el robo de identidad, algunas industrias han adoptado normativas estrictas que implican sanciones severas. Entre estas se incluyen la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) en la atención médica, las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI-DSS) en los servicios financieros y el comercio minorista, y el Reglamento General de Protección de Datos (RGPD) para empresas que realizan negocios con ciudadanos europeos.
7. Riesgo abrumador: generado por US$6 billones en pérdidas por delitos cibernéticos previstos en 2021, lo que corresponde a un aumento de US$3 billones en comparación con el año 2015. Las pérdidas se deben a daños y destrucción de datos, robo de fondos, pérdida de productividad, robo de propiedad intelectual, robo de datos personales y financieros, interrupciones posteriores a un ataque, daño a la reputación y más, de acuerdo con Cybersecurity Ventures[7].

Replanteamiento de la seguridad de terminales

Seguridad de terminales: parte de la seguridad empresarial
En vista de que hay una población de trabajadores remotos más grande que nunca, muchos de los cuales deben manejar información confidencial para hacer su trabajo, los líderes de TI deben evaluar el estado actual de la seguridad de los terminales en sus organizaciones. Sin embargo, en lugar de considerar la seguridad de los terminales por separado, deben considerarla como una parte integral de la seguridad empresarial a fin de implementar una protección en profundidad, y deben mirar más allá de los terminales para incluir el almacenamiento, las redes y los servicios basados en la nube. Un enfoque integral para crear "dispositivos de confianza" dentro de la empresa debe tener en cuenta estos factores:

Seguridad integrada
En lugar de depender exclusivamente del software a fin de proteger los terminales, un enfoque integral requiere el uso de dispositivos de confianza: dispositivos de computación para el usuario final que incorporan la seguridad dentro de ellos. Estos dispositivos protegen la PII y desempeñan un rol importante en lo que respecta al cumplimiento normativo en caso de que se produzca la pérdida o el robo de un dispositivo. Los dispositivos de usuario final también deben incluir la tecnología de pantalla de privacidad, que limita la capacidad de los compañeros de trabajo y los visitantes de la oficina para ver la información confidencial en la pantalla de una computadora.

Los líderes de TI deben considerar la seguridad de los terminales como una parte integral de la seguridad empresarial.

6. Cybersecurity Insiders Cloud Security Reports, 2018, 2019.
7. Cybersecurity Ventures, 2020.

Protección sobre y bajo el SO

Sobre el SO. TI necesita visibilidad, monitoreo y seguridad de datos, además de prevención, detección y corrección de amenazas. El cifrado en el dispositivo también es muy importante para cumplir con los requisitos de cumplimiento de normas; sin embargo, no debe ralentizar el rendimiento de una manera que degrade la productividad del usuario.

Bajo el SO. TI necesita protección de BIOS, además de autenticación de chips debido a la frecuencia de los ataques en el firmware y el hardware. Un BIOS comprometido puede dar a los atacantes acceso a todos los datos de un terminal, incluidas las credenciales, lo que permite que se muevan dentro de la red de una organización y ataquen la infraestructura de TI en un nivel más amplio.

IA y ML

Con los ataques cada vez más sofisticados de hoy en día, el uso de la inteligencia artificial y el aprendizaje automático en la detección y la corrección es fundamental para la protección de terminales. Cuando observan los patrones de comportamiento, los algoritmos de IA y ML (aprendizaje automático) pueden detectar una actividad inusual que podría señalar y evitar una infracción.

Cadena de suministro segura

En el proceso de fabricación, es posible que agentes maliciosos implanten componentes comprometidos para permitir un ataque de puerta trasera. Una vez integrados en un producto fabricado, dichos componentes pueden permitir que se produzca una infracción que podría ser extremadamente perjudicial y difícil de detectar. Por lo tanto, es crítico que tanto los proveedores como los fabricantes implementen medidas de seguridad estrictas en los puntos críticos en la cadena de suministro.

Dell Trusted Devices

Dell incorpora seguridad en cada PC con estas tecnologías:

SafeBIOS con indicadores de ataque del BIOS (IoA): proporciona visibilidad de los cambios del BIOS para evitar la manipulación. Dell mantiene una imagen protegida fuera del host para verificar la integridad del BIOS. SafeBIOS ahora está integrado en VMware Carbon Black Audit and Remediation, lo que aumenta la visibilidad de los ataques mediante la generación de informes automatizados y permite el acceso remoto para solucionar daños en el BIOS.

SafeID: proporciona autenticación basada en chips. La información de identificación de los usuarios finales se verifica mediante un chip de seguridad exclusivo, en lugar de depender del software que es menos seguro.

SafeScreen: protege las pantallas que podrían exponer información confidencial a compañeros de trabajo de oficina, visitantes, trabajadores de mantenimiento u otras personas no autorizadas.

SafeGuard and Response. El portafolio de Dell, impulsado por las tecnologías de VMware Carbon Black y Secureworks, incluye lo que se indica a continuación:

VMware Carbon Black: una plataforma de protección de terminales nativa de la nube que combina el reforzamiento inteligente del sistema y la prevención del comportamiento necesarios para mantener las amenazas emergentes al margen mediante un solo agente ligero y una consola fácil de usar.

Los dispositivos de confianza protegen la PII y desempeñan un rol importante en lo que respecta al cumplimiento normativo en caso de que se produzca la pérdida o el robo de un dispositivo.

Servicios administrados de Secureworks: recopila y correlaciona la telemetría de la nube, la red y los terminales para identificar amenazas en toda la empresa. Los servicios administrados de Secureworks se integran en la plataforma VMware Carbon Black, además de muchas otras plataformas, y proporcionan una respuesta ante incidentes líder en la industria.

SafeData. La colaboración, que siempre es un sello distintivo de las organizaciones exitosas, adquiere mayor importancia en la era de un trabajo remoto intensificado. La colaboración de la fuerza de trabajo actual requiere seguridad de datos, tanto en el dispositivo como en la nube, de modo que no ralentice al usuario final. Dell se asocia con Netskope y Absolute para brindar seguridad holística de terminales.

Netskope. Dado que adopta un enfoque centrado en los datos, la tecnología de Netskope protege los datos creados y expuestos en la nube. Gracias a que le proporciona a TI visibilidad en tiempo real, acceso a la nube, monitoreo y prevención de pérdida de datos, Netskope redefine la nube, la red y la seguridad de datos. Los equipos cuentan con el equilibrio adecuado de protección y velocidad, lo que les permite proteger el recorrido de transformación digital de su organización.

Absolute. Dell incorpora la tecnología de Absolute en el firmware de todos los dispositivos, lo que le otorga a cada terminal un enlace de autorreparación al panel de Absolute basado en la nube. Esto permite que los administradores rastreen, administren y protejan los terminales y los datos contenidos en ellos, incluso cuando están fuera de la red. Tecnología de Absolute:

- Localiza y administra los dispositivos.
- Proporciona persistencia del software de seguridad y VPN.
- Implementa una solución aislada para permitir la recuperación de los ataques.
- Incluye soluciones de protección de datos de múltiples nubes que pueden estar definidas por software o basadas en dispositivos.

La colaboración de la fuerza de trabajo actual requiere seguridad de datos, tanto en el dispositivo como en la nube, de modo que no ralentice al usuario final.

Conclusión

El aumento repentino en el trabajo remoto debido a la pandemia de la COVID-19 incrementa el peligro en un panorama de seguridad cibernética que ya está lleno de amenazas. Se necesita un enfoque nuevo e integral para la protección de terminales. El replanteamiento de la protección de terminales comienza con dispositivos de confianza que estén protegidos sobre y bajo el SO. Dicha estrategia también va más allá de los terminales en sí para adoptar una visión empresarial de la seguridad cibernética, que incluye servidores, redes, servicios basados en la nube y cumplimiento normativo. El portafolio de dispositivos de confianza de Dell incorpora un enfoque así de integral. La protección de terminales de Dell abarca la empresa a fin de incluir soluciones de protección de datos de múltiples nubes, que se pueden ofrecer como soluciones definidas por software o basadas en dispositivos. Principalmente, los dispositivos de confianza de Dell permiten a los usuarios seguir siendo altamente productivos y frustrar ataques cada vez más sofisticados en el nuevo paradigma de trabajo remoto.

Para obtener más información, visite:
https://www.delltechnologies.com/es-mx/endpoint-security/index.htm