GUÍA PARA REDEFINIR LA SEGURIDAD DE SU ENTORNO DE TI

Responder al desafío de la seguridad en un panorama de TI cambiante

Definición de la era de la transformación digital

Si se observa el auge de empresas que han nacido en el mundo digital, como Uber y Airbnb, vemos que, en estas empresas, la tecnología actúa como factor diferenciador respecto a la competencia. Uber, por ejemplo, se ha convertido en el servicio de taxis más importante del mundo sin tener ningún vehículo; y Airbnb es la mayor empresa de alojamiento del mundo sin tener ninguna propiedad inmobiliaria.

Transformación de las empresas tradicionales

También podemos observar que la tecnología está trasformando las empresas tradicionales más consolidadas. Las empresas de fabricación, por ejemplo, se están dando cuenta de que es esencial usar software para mejorar la eficiencia y productividad de sus operaciones. Jeff Immelt, presidente y director ejecutivo de General Electric, lo resume de este modo: «Hemos constatado que si uno empieza siendo una empresa industrial, acaba convirtiéndose en una empresa de software». Lo que General Electric y otras empresas están aprendiendo es que para competir en el entorno empresarial actual hay que ser una empresa digital.

Evaluación del desafío de seguridad

Junto a la rápida transformación digital, estamos asistiendo a un crecimiento masivo y continuo del número de usuarios finales con dispositivos digitales, así como del volumen de aplicaciones y datos que es preciso gestionar. Se trata de un fenómeno que ha generado una tormenta perfecta de amenazas de seguridad para las organizaciones de TI. Los centros de datos que antes estaban seguros en las instalaciones de la empresa han evolucionado hacia entornos multicloud públicos y privados muy dinámicos. Y los usuarios que antes trabajaban desde estaciones de trabajo de la empresa ahora están en constante movimiento, fuera del lugar de trabajo, y esperan acceder a las redes corporativas desde sus dispositivos personales, e incluso a través del Internet de las cosas (IoT).

Un número de riesgos cada vez mayor

Todos estos factores hacen que la exposición a riesgos sea cada vez mayor. Y atacantes sofisticados buscan aprovecharse de estas vulnerabilidades del centro de datos. En un estudio reciente que evaluaba la seguridad de TI global de las empresas, el 75 % de los encuestados admitieron que seguramente se verían obligados a combatir un ciberataque en 2016.[1] Además, las organizaciones de TI se enfrentan cada vez más a exigencias relativas al cumplimiento normativo. En realidad, las responsabilidades de cumplimiento representan hasta un 20 % del tiempo de un empleado de TI.[2]

En este panorama de TI cambiante, los desafíos de seguridad resultantes son claros, aunque no sencillos de resolver: ¿Cómo protegemos las interacciones entre usuarios, aplicaciones y datos?

SUMA DEL IMPACTO GLOBAL

- El coste medio de una interrupción no planificada del centro de datos aumentó hasta 740 357 dólares en 2016.[3]
- Si se suman los costes asociados al robo de propiedad intelectual, el ciberespionaje global llega a costar a las empresas hasta 1 billón de dólares al año en todo el mundo.[4]
- En 2016, el coste medio de una vulneración de datos aumentó a 4 millones de dólares (o 158 dólares por registro robado o perdido).[5]

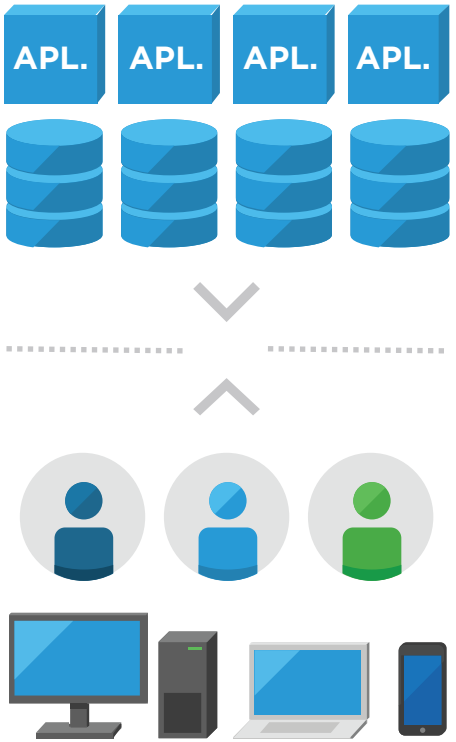


Figura 1. «La transformación digital afecta al personal de TI y a la seguridad».

[1] State of Cybersecurity: Implications for 2016, ISACA, 2016.
[2] Cost of Data Center Outages, Ponemon Institute, enero de 2016 (http://datacenterfrontier.com/white-paper/cost-data-center-outages/).
[3] Cost of Data Center Outages, Ponemon Institute, enero de 2016.
[4] Https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/.
[5] 2016 Cost of Data Breach Study: Global Analysis, Ponemon Institute, junio de 2016.

Cinco áreas donde redefinir la seguridad del entorno de TI

Como hemos visto, aunque el gasto en seguridad de TI ascendiera a 80 000 millones de dólares solo en 2016[6], el antiguo enfoque de la seguridad de TI no es suficiente para hacer frente al incremento de los niveles de amenaza. Teniendo esto presente, hay cinco consideraciones que le ayudarán a redefinir su enfoque de seguridad del entorno de TI:

1. Cambiar el modelo de seguridad
   Los sistemas de seguridad de TI tradicionales, que utilizan soluciones puntuales añadidas, equipos autónomos o productos de software, son complejos y están mal coordinados. Se necesita un modelo integral que proporcione seguridad de un modo sencillo y efectivo.
2. Implementación de una capa de software omnipresente
   Con una capa de software omnipresente en la infraestructura de aplicaciones y los terminales, es posible separar la infraestructura de las aplicaciones que se ejecutan en ella. Esto le permite aplicar seguridad de un modo sencillo y efectivo en todo el centro de datos.
3. Máxima visibilidad y contexto
   Al separar la infraestructura de las aplicaciones, logrará visibilidad de los flujos de datos de aplicaciones y todo el contexto de las interacciones entre usuarios, aplicaciones y datos.
4. Adaptación de los controles y las políticas de seguridad a las aplicaciones
   Con las ventajas de máxima visibilidad y contexto, puede empezar a adaptar sus controles y políticas de seguridad a las aplicaciones que intenta proteger.
5. Inserción de servicios de seguridad de terceros
   Al adaptar los controles y las políticas de seguridad a las aplicaciones, puede empezar a introducir servicios de seguridad de terceros para tener más capas de protección inteligente.

[6] «Gartner Says Worldwide Information Security Spending Will Grow 7.9 Percent to Reach $81.6 Billion in 2016», Gartner Inc., agosto de 2016.

NUEVAS REGLAS DE SEGURIDAD PARA LAS REDES

Las antiguas reglas básicas de seguridad de las redes han dejado de ser válidas y los equipos de TI deben ponerse al día:

- **Cambios en la infraestructura:** la infraestructura está evolucionando, al pasar de los entornos locales a respaldar la cloud y las aplicaciones distribuidas.
- **Mayor movilidad:** el departamento de TI debe ampliar sus políticas de seguridad para respaldar la avalancha de nuevos dispositivos y modelos.
- **Nuevos requisitos de cumplimiento normativo:** Las empresas se enfrentan a nuevos requisitos de cumplimiento normativo.

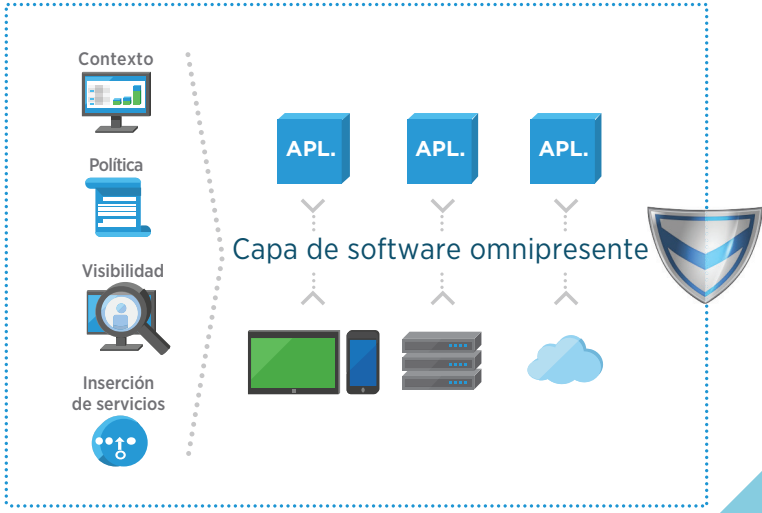


Figura 2. Una capa de software omnipresente significa que la seguridad está en todas partes.

Adopción de un enfoque triple de la seguridad de TI

Transformar su entorno de seguridad para abordar los actuales desafíos esenciales de seguridad requiere un enfoque triple.

Protección del centro de datos: redefina la gestión y la seguridad de su centro de datos

Necesita tener los medios adecuados para compartimentar mejor la información confidencial, adaptar mejor los controles de seguridad a estos recursos, y obtener mayor visibilidad y control para poder detectar posibles amenazas y responder adecuadamente.

Protección del terminal: redefina la gestión y la seguridad de la infraestructura de usuarios

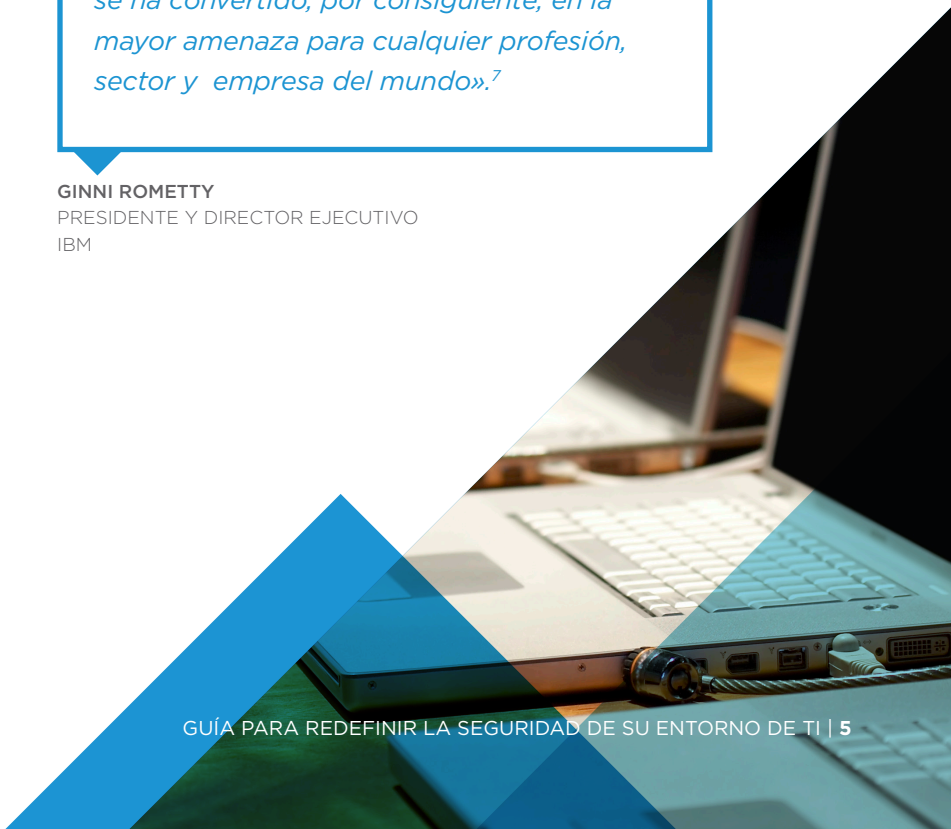
Con la proliferación de dispositivos móviles y sistemas operativos, no existe una estructura uniforme para la infraestructura de usuarios. Fuera hay un mundo complejo y heterogéneo. Necesita visibilidad y control, no solo desde el punto de vista de la infraestructura, sino también desde una perspectiva centrada en las aplicaciones, sin dañar la experiencia que se ofrece al usuario.

Protección del usuario: redefina los controles de usuario y acceso

El acceso de los usuarios es fundamental para potenciar el trabajo de sus empleados. Necesita un enfoque que le ayude a reducir la superficie de ataque, a mejorar la visibilidad de las interacciones de los usuarios y a dar una respuesta eficaz a las inevitables amenazas de seguridad.

«Creemos que los datos son el fenómeno de nuestro tiempo. Son el nuevo recurso natural, la nueva base para las ventajas competitivas, y están transformando todos los sectores y profesiones. Si todo esto es cierto, incluso inevitable, la ciberdelincuencia se ha convertido, por consiguiente, en la mayor amenaza para cualquier profesión, sector y empresa del mundo».[7]

GINNI ROMETTY
PRESIDENTE Y DIRECTOR EJECUTIVO
IBM



[7] Declaraciones del director ejecutivo de IBM sobre los hackers: «La ciberdelincuencia es la mayor amenaza para cualquier empresa del mundo». Forbes. 24 de noviembre de 2015.

Conclusión

La transformación digital representa una gran oportunidad para su empresa. Pero esta oportunidad conlleva riesgos y un gran desafío: proteger el número creciente de interacciones entre usuarios, aplicaciones y datos.

Para enfrentarse a esta amenaza de seguridad actual, debe redefinir el enfoque de seguridad de su entorno de TI. Transformar su estrategia de seguridad empieza por crear una capa de software omnipresente en la infraestructura de aplicaciones y los terminales. Esta capa de software le proporcionará una amplia visibilidad de las interacciones que desea proteger y el contexto que necesita para entender su significado.

Permítenos apoyarte para una solución acorde a tus necesidades.

EMPIECE HOY MISMO

Obtenga ayuda para redefinir el enfoque de seguridad de su entorno de TI

MÁS INFORMACIÓN >

For more information contact: Grupo Intego, Luis Silva
ventas@grupointego.com.mx
+01(55) 5171 1130
www.grupointego.com.mx

vmware®

GRUPO intego® TECHNOLOGIES
Integración de Tecnología para tu Negocio

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 EE. UU. Tel. +1 877-486-9273 Fax +1 650-427-5001
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.es