



Los proveedores cloud están cada día más expuestos a las ciberamenazas

Alerta roja: los ciberataques ponen el ojo en el CPD

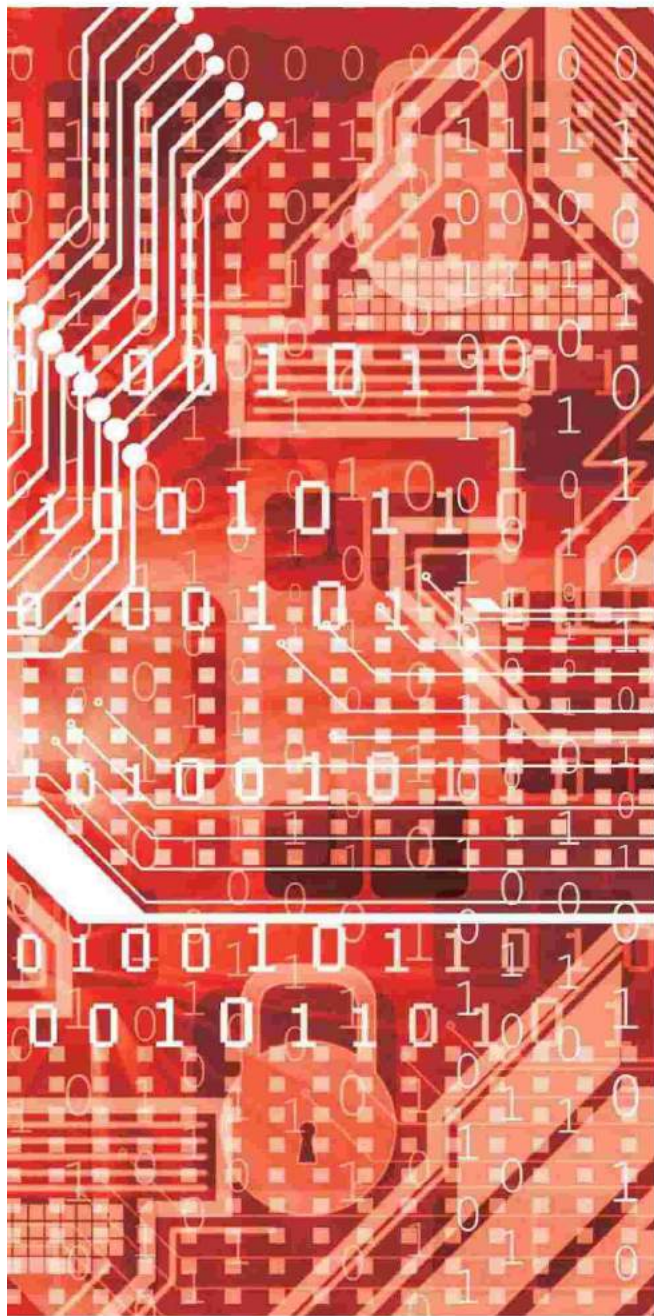
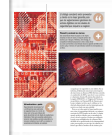
A medida que las empresas almacenan y migran cargas de trabajo a la nube (tanto pública como privada), aumentan las probabilidades de una gran ofensiva en estos entornos.



Cristina López Albarrán
✉ cristina.albarran@bps.com.es
🐦 [@DataCenterBPS](https://twitter.com/DataCenterBPS)
🌐 www.datacentermarket.es

El famoso WannaCry, que a mediados de mayo dejó en jaque a empresas públicas y privadas de multitud de países, ha puesto en el punto de mira la exigencia de tener al día un buen plan de ciberseguridad. Sobre todo en el entorno de los centros de datos. Ya el año pasado contá-

bamos que los ciberataques provocaban más del 20% de las caídas en el CPD. Un porcentaje nada despreciable, pero que podría ser todavía mayor. No en vano, para 2017 se espera que la nube esté en el punto de mira de los ciberataques. Así lo recoge una investigación realizada por Check Point en la que se constata que los proveedores cloud están cada día más expuestos a las ciberamenazas. La razón es clara, a medida que las empresas almacenan y migran cargas de trabajo a la nube (tanto pública como privada), aumentan las probabilidades de una gran ofensiva. Es por ello que un 93% de las organizaciones están pre-



El diálogo constante entre proveedor y cliente es la mejor garantía para que las organizaciones gestionen los activos digitales con los niveles de seguridad que requiere su negocio



WannaCry enciende las alarmas

Este ransomware infectó el pasado 12 de mayo a empresas de todo el mundo. En España saltaron las alarmas por el ataque a Telefónica. Sin embargo, la compañía de telecomunicaciones no fue la única afectada. Junto con Iberdrola o Gas Natural (otras dos grandes del IBEX 35 de nuestro país), el servicio de salud británico también vio encriptados sus archivos.



Infraestructura a punto

Especialización del personal, SLA y certificaciones son parámetros de seguridad clave en el centro de dato, pero no hay que olvidarse del punto de partida como el diseño de arquitecturas tolerantes a fallos para aquellas aplicaciones o servicios más sensibles, escalado automático de recursos mediante el uso de API y el empleo de arquitecturas distribuidas, por ejemplo.



ocupadas por la seguridad en este ámbito. En su informe, el fabricante menciona la interrupción de cinco horas en Amazon Web Services ocurrida en septiembre de 2015 y que afectó a sus servicios y a bastantes clientes. El sistema fue aislado en la región USEAST-1 en Virginia del Norte por un problema con DynamoDB de Amazon, por lo que cualquier servicio que lo utilizase se vio afectado, demostrando que las interrupciones de servicio en cloud eran una realidad.

Esto no es todo, según la firma israelita veremos cómo el ransomware infectará a un número creciente de CPD basados en la nube. Lo harán usando archivos cifrados que se extenderán de cloud a cloud o gracias a hackers que utilizarán la nube como multiplicador de volumen. Más del 80% de los profesionales de la ciberseguridad están preocupados por este tipo de software malicioso que cifra los archivos de la víctima y los



Blanco de ransomware

Las razones por las que los centros de datos basados en la nube son un objetivo principal para el ransomware son:



- 1. Contienen información muy importante y lucrativa. Atacar a los entornos en los que se almacenan los datos más sensibles y críticos permite extorsionar a las empresas y pedirles grandes sumas de dinero.
- 2. Los cibercriminales profesionales están constantemente buscando nuevos objetivos con los que lucrarse. Los hackers, como los que están detrás de Carbanak o Morpho/Butterfly, el grupo GameOver ZeuS y otros son perfectamente capaces de atacar con ransomware a centros de datos basados en la nube.
- 3. Las protecciones de seguridad tradicionales no se adaptan a la naturaleza dinámica de los centros de datos basados en la nube. La seguridad avanzada, que podría prevenir las infecciones, a menudo no se implementa. Además, el modelo de responsabilidad compartida que tienen los proveedores de cloud público da una falsa sensación de seguridad a los clientes.
- 4. El aumento del ransomware específico para atacar a centros de datos en la nube se convertirá en un riesgo añadido. Los secuestros de datos pasan a ser un desafío para los proveedores de seguridad en la nube.

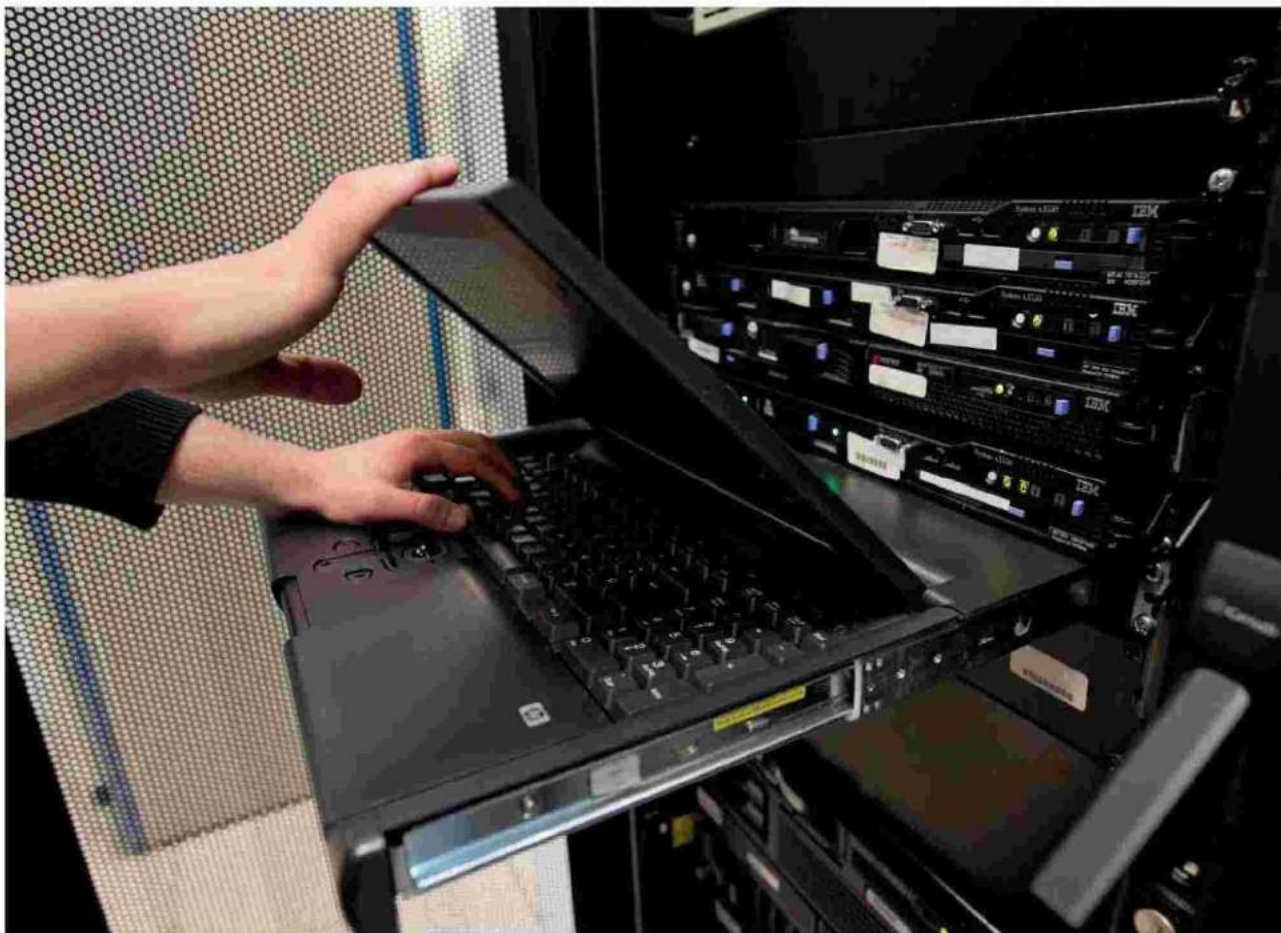
Fuente: Check Point.

secuestra hasta que ésta pague un rescate, normalmente en bitcoins. Ha surgido como una amenaza potente y cada vez más común en la red. “Pero muchos usuarios de Internet no son conscientes de que este malware también puede hacerse fácilmente con el control de los archivos almacenados en los servicios cloud. Las empresas suelen tener un antivirus en su servidor, pero es insuficiente”, alertan.

Medidas para mitigar las ciberamenazas

Ante este hecho, nos preguntamos ¿qué medidas se están llevando a cabo para mitigarlos? O planteado de otra manera, ¿qué se puede hacer para proteger los datos corporativos en la nube? Para Check Point una buena estrategia para luchar contra este tipo de vulnerabilidades, al igual que para hacer frente a interrupciones de servicio, es realizar copias de seguridad de los datos, tener un plan de recuperación ante desastres (DRP) e implementar soluciones de prevención contra ataques avanzados en los entornos cloud.

Por su parte, Lorea Revilla, directora de Operaciones en [Arsys](#), reconoce que la securización de los servicios IT siempre ha sido una cuestión determinante para los proveedores cloud, pero





El papel de los SOC

Los SOC (del inglés, Security & Network Operation Center) son centros especializados en la seguridad que para los usuarios proporcionan un valor importante adquirido mediante la experiencia obtenida a diario con múltiples clientes y desde múltiples fuentes de información. Sus funciones están encaminadas a garantizar la seguridad, confidencialidad y disponibilidad de la información de la empresa, unas tareas que hace años solían depender de los departamentos de sistemas y que a medida que las TIC han ganado peso en las organizaciones ha llevado al nacimiento de esta nueva figura.



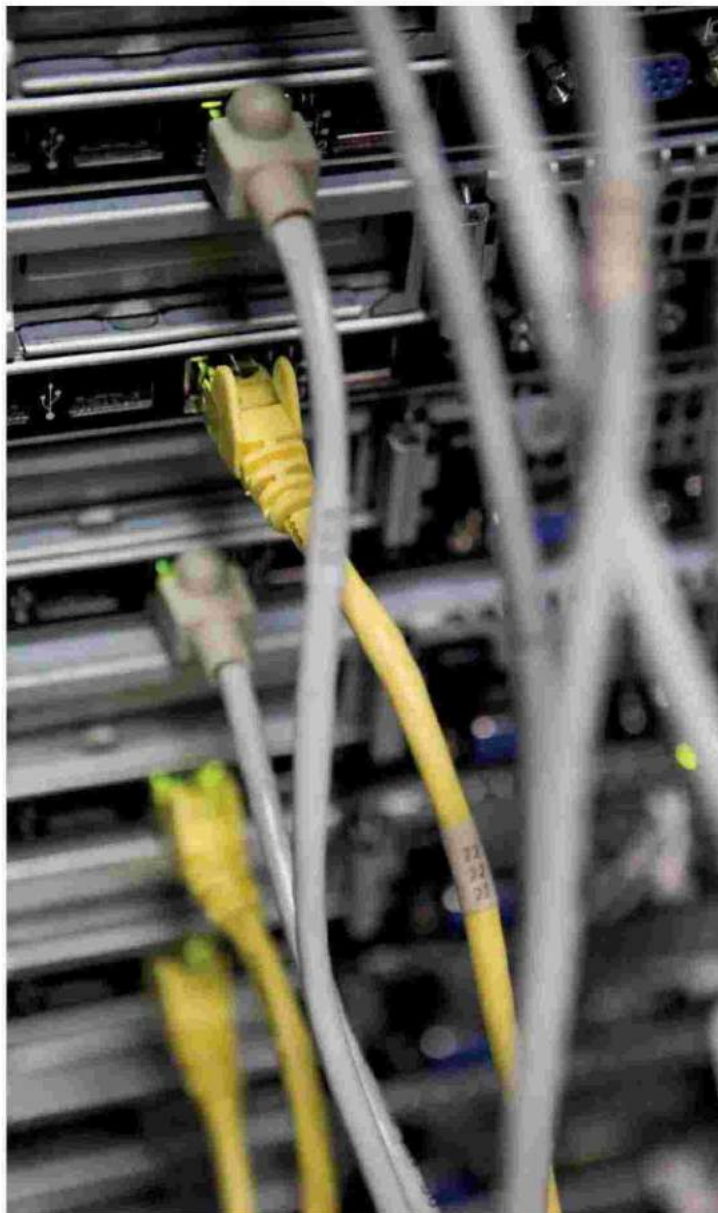
"La prevención y monitorización, claves para proteger el CPD"

de que se produzca un riesgo de disponibilidad. Y en esta tarea de prevención, el papel más determinante es desempeñado por el personal que está detrás 24x7, gestionando y monitorizando la infraestructura y aplicando su experiencia a los datos que nos proporcionan los sistemas", confirma.

Según José Manuel Armada, director de ingeniería de clientes de Interoute Iberia, la migración al cloud no debería provocar cambios significativos en las políticas de seguridad, ya que éstas pueden replicarse en casi todos los casos y mejorarse en la práctica. "La filosofía es bastante

con la irrupción de un nuevo modelo de usuario, permanentemente conectado, multidispositivo y en movilidad, la situación se ha vuelto más importante que nunca. "Ahora los proveedores de servicios y soluciones en la nube tenemos que abordar las cuestiones de seguridad desde un doble punto de vista: desde dentro y desde fuera". La directiva explica que de un lado implementan las habituales medidas de seguridad internas. Es decir, "los sistemas de redundancia, monitorización, segregación y aislamiento que implantamos sobre las cinco capas que componen todo proyecto cloud: software, capacidad de computación, almacenamiento, redes y data centers". En otras palabras, habla de firewalls, anti-malware, sistemas de detección y prevención de intrusos, acceso biométrico o CCTV, entre otros. "Y desde fuera, por el conocimiento de nuestros clientes, sus prioridades y proyectos, lo que nos permite incorporar las medidas adicionales de seguridad que requieren y poder ofrecerles un servicio de infraestructura IT a su medida, basado en soluciones tan flexibles que permiten añadir medidas específicas principalmente encaminadas a la prevención y a la detección de vulnerabilidades, que continúa siendo la mejor manera de evitar incidentes no deseados", menciona. Se trata de desplegar, también dentro del modelo "as a service", sistemas de monitorización y alerta temprana a todos los niveles, cortafuegos de red y de aplicación, protección frente a intrusiones, ataques DDoS, código malicioso y, por supuesto, copias de seguridad.

"Y algo que no podemos olvidar. Por muchas medidas que tomemos, la más importante de todas continúa siendo la prevención y monitorización. Por ese motivo, contamos con diferentes tecnologías que nos permiten actuar incluso antes





simple: el proveedor se centra en mantener la seguridad de la infraestructura subyacente que soporta el cloud y el cliente puede concentrarse en la seguridad de sus aplicaciones y puede además contar con la experiencia del proveedor adquirida en la práctica diaria y beneficiarse de sus especialistas". Además, detalla que existen servicios como la mitigación de ataques de denegación de servicio, que son inherentes a la red y que esencialmente han de detener las amenazas antes de que alcancen la infraestructura del cliente. "Para esto, es esencial disponer de un proveedor que gestione también las redes de comunicaciones que soportan las aplicaciones, porque son la vía desde donde llegan las amenazas", puntualiza.

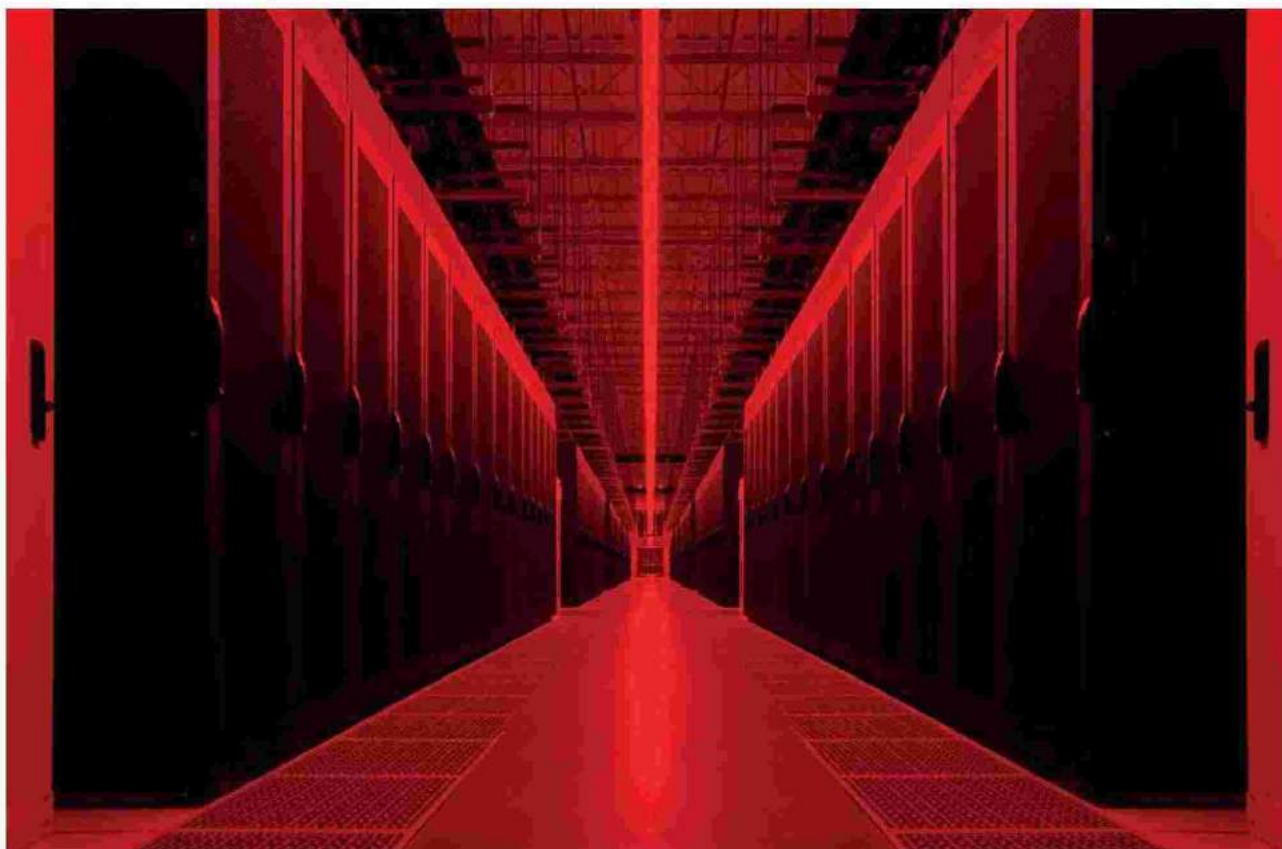
Especialización y profesionalización

Aunque los ciberataques cada vez son más frecuentes y persistentes, el error humano continúa

gestión de infraestructuras eléctricas y mecánicas, con dedicación exclusiva y formación continua" –añade-. "Además, deben establecerse protocolos documentados de actuación y herramientas de gestión adecuadas".

"Las medidas para minimizar el error humano en los centros de datos son la formación y la correcta organización y documentación, que no es otra cosa que buscar la excelencia en la operación y el mantenimiento", declara Isidro Ramos, socio director de AEON Ingeniería.

Por su parte, la directiva de [Arsys](#) coincide en esta percepción: la especialización de los equipos técnicos y el establecimiento de unos procedimientos que contemplen la máxima seguridad pero tampoco afecten a la funcionalidad de las soluciones. "Resulta determinante que nuestros equipos cuenten con experiencia y formación certificada en la gestión de las plataformas IT y



figurando como el principal peligro en un centro de datos. La mejor manera de prevenirlo es mediante la experiencia en las operaciones de los empleados: "Principalmente a través de la especialización del personal, es decir, disponer de un equipo formado, coordinado y preparado", indica Robert Assink, director general de Interxion España. "El personal a cargo del CPD debe estar compuesto por profesionales con experiencia en la

**"Un ciberataque
contra los
proveedores cloud
afectaría a los datos de
sus clientes"**

que cualquier intervención en el centro de datos esté previamente planificada, siguiendo estándares que abarquen de una manera integral la gestión de la seguridad de la información, como la certificación ISO 27001, que garantiza que los datos alojados se gestionen adecuadamente en cuanto a su confidencialidad, integridad y disponibili-



dad". Eso sí, insiste en que por muchas medidas que adopten los proveedores, también los clientes han de tomar sus propios protocolos de seguridad en su día a día. "Por muy rigurosos que sean los Acuerdos de Nivel de Servicio de su hoster o las numerosas medidas técnicas y humanas que éste pueda adoptar, ante esas vulnerabilidades poco podrá hacer".

Proteger la red

Visto lo visto, la seguridad ocupa un lugar destacado en estas infraestructuras de misión crítica, y como los propios centros de datos también ha evolucionado, en su caso, hacia la ciberprotección y hacia la focalización de esfuerzos en las redes, en la conectividad. De esta manera, en un primer momento se trasladaron las arquitecturas y polí-

"El ransomware infectará a un número creciente de CPD basados en la nube"

ticas de seguridad que el cliente mantenía en sus instalaciones, al centro de datos externo. Sin embargo, en la actualidad se está observando un avance en este terreno al aplicar las economías de escala del cloud y las redes también a la seguridad. Y es que, la externalización de los servicios a la nube (gracias a la flexibilidad y eficiencia que aporta) se está articulando como una de las mejores vías para alcanzar los niveles de protección que realmente requieren las organizaciones hoy en día.

Además, se está tomando conciencia de la interrelación entre las redes y el CPD, por ejemplo, en lo que se refiere a la mitigación de ataques de denegación de servicio y el uso de cortafuegos de última generación. Asimismo, ya se está traba-

Ataques más habituales en el CPD

- **Ataques contra aplicaciones web.** Los ataques contra las aplicaciones web son comunes. De hecho, según el 2016 Data Breach Incident Response Report, los ataques contra aplicaciones web fueron responsables de la mayoría de las vulneraciones de datos durante el pasado ejercicio. Aunque las aplicaciones web no están dentro del centro de datos, son sin duda puertas de entrada a este para los delincuentes. Los ataques habituales incluyen las inyecciones de SQL, infracciones de la autenticación, y scripts de sitios, entre otros.
- **Ataques de ransomware.** Estos ataques se han vuelto frecuentes durante los últimos años. En los ataques de ransomware, el malware se desliza clandestinamente en el sistema y cifra sus datos. El impacto en el rendimiento y la disponibilidad puede ser brutal para los centros de datos. Las empresas pueden tener que cerrar, y denegar el acceso a las aplicaciones y los datos. El atacante exige un pago de algún tipo a cambio de restaurar los datos al estado anterior.
- **Ataques de autenticación.** Cuando se habla de ataques de autenticación, a menudo se piensa en el robo de nombres de usuario y contraseñas de sitios web, o tal vez en el descubrimiento de contraseñas mediante fuerza bruta. Desde luego, estos son ataques de autenticación, aunque también lo son los llevados a cabo sobre sistemas que se han quedado con un nombre de usuario y contraseña por defecto, o credenciales descubiertas por fuerza bruta, y las credenciales robadas y utilizadas para adentrarse más en el centro de datos. Asimismo, según el informe Data Breach Investigations Report, el 63% de los ataques han utilizado credenciales robadas durante un ataque en algún momento del incidente.
- **Ataques de amenazas persistentes avanzadas, malware y ataques personalizados multivector.** Los atacantes avanzados, una vez que se introducen en el centro de datos, explotan cualquier vulnerabilidad a su alcance para hacer prosperar su ataque. Utilizarán software de ataque para espiar el tráfico de la red. Sembrarán malware, rootkits y exploits que les ayuden a garantizarles un acceso continuo al centro de datos y a los sistemas de nube.

Fuente: Bitdefender



Ya se está trabajando en asegurar la red de monitorización de los dispositivos

jando en securizar la red de monitorización de los dispositivos y personalizar los elementos de seguridad como los de acceso a los equipos de los usuarios o de determinados protocolos y su integración en las plataformas de gestión del cliente. ●

