Mesa redonda

El CPD requiere una seguridad de 365º

Data Center Market ha realizado un desayuno de trabajo, en colaboración con Check Point y Rittal, para analizar la importancia de la protección del centro de datos. Daimler, Initec Plantas Industriales y Securitas Direct han participado en el debate.

Cristina López Albarrán
cristina.albarran@bps.com.es
@DataCenterBPS
www.datacentermarket.es

La seguridad del centro de procesamiento de datos es un reto permanente y debe abordarse desde una perspectiva holística. Para profundizar en este tema, Data Center Market ha organizado un desayuno de trabajo, en colaboración con Check Point y Rittal, en el que se ha analizado la importancia de la protección del CPD con una visión de 365 grados. Daimler, Initec Plantas Industriales (Grupo Técnicas Reunidas) y Securitas Direct han acudido al evento para exponer cómo están haciendo frente, desde sus respectivas compañías, a las últimas amenazas que están afectando a estas infraestructuras críticas y los retos que tienen ante sí.

Aunque bien es cierto que la seguridad física tiene muchos años de "rodaje" y ha llegado un punto en que tiende a verse en el sector como una commodity (algo que se da por hecho), no hay que dejarla de lado, sobre todo si hablamos de data centers que están expuestos a agentes externos que pudieran afectar a su correcto funcionamiento, como condiciones climatológicas adversas o ambientes con un alto riesgo de inundaciones, por ejemplo. Tal y como comenta Javier Albalat, DC & IT Sales Specialist de Rittal: "El CPD es un entorno muy protegido físicamente mediante equipos de control de accesos, sistemas anti incendios…, pero no está protegido de los eventos que se producen de fuera hacia dentro". Y añade: "Nos encontramos con clientes que ya han sufrido algún desastre y es a partir de ese momento cuando empiezan a considerar soluciones específicas que van más allá de la seguridad normal". En otras palabras: "buscan medidas de seguridad extra a las habituales".

Sin embargo, sin olvidar esta apartado, parece ser que la seguridad lógica de estas instalaciones (sistemas operativos, cortafuegos, dispositivos de red, aplicaciones, nube..) se impone como el gran desafío al que se enfrentan estos entornos. El hecho de que el mercado se mueva hacia soluciones híbridas

–CPD in house y externalizado para ciertas funciones– hace que las fronteras entre ambos mundos se difuminen y resulte cada vez más complicado mantener todo bajo control. "La propia dinámica del data center, que ya es mixto con parte de sus funciones en cloud, está animando a que se estén adoptando técnicas para conectar el centro de datos físico y lógico", indica Eusebio Nieva, director técnico para España y Portugal de Check Point.

Responsabilidad compartida

En este contexto el usuario es, a día de hoy, la principal amenaza. El recurrente "error humano" al que se alude cuando nos referimos a una buena operativa del centro de datos, destaca igualmente como factor de riesgo en el ámbito de la seguridad. Los usuarios son descuidados en demasiadas ocasiones, es algo en lo que coinciden con asistentes al encuentro. La responsabilidad de la seguridad del data center es cosa de todos. "Formamos un equipo, la seguridad somos todos y al final la responsabilidad es del dueño del dato", manifiesta David Matesanz Ureña, regional information security officer para Europa de Daimler. "El sheriff no puede tener la responsabilidad de todo", apunta.

"Somos todos responsables", interviene Carlos Asún, CISO de Intec Plantas Industriales (Grupo Técnicas Reunidas). Cuando ocurre un ataque lo primero es arrancar el protocolo, atacar la incidencia y resolverla. "Cubrirnos y luego hacer un análisis forense para saber qué ha pasado", detalla. Advierte de la importancia de cubrir el perímetro, el acceso… de la seguridad física (los equipos de limpieza, de mantenimiento…). Por eso insiste en que "hay que incidir en la concienciación y en la formación, que tiene un ROI incalculable". Argumenta que "cuantos más empleados tengas, más altos son los riesgos. Inviertes horas en formación, pero siempre va a haber algo, un porcentaje de fallo". De hecho, expone que una vez al año, como mínimo, en su empresa hacen pruebas de protocolos de seguridad y nunca obtienen un resultado cero por culpa de algún usuario.

El trabajo de educar sigue, pues, vigente. "Lo que más temo es un usuario "tonto", porque es más fácil hacer un ataque a través de un descuido de un empleado que crear una línea de código. Por tanto, la formación y concienciación del usuario es fundamental", corrobora Eusebio Nieva, de Check Point. El directivo menciona el "síndrome de Casandra" que padecen los expertos en seguridad, que advierten de posibles y probables amenazas que acaban ocurriendo. "A la gente hay que darle herramientas tanto físicas, como tecnológicas y mentales para hacer frente a las amenazas. Si a los usuarios les explicas los peligros, reduces muchísimo la posibilidad de que ocurra un incidente". Ahora, puntualiza "si después de darle toda la información se produce un incidente, tiene que tener una responsabilidad por ello. Un gran poder conlleva una gran responsabilidad".

En este sentido, César Romo, director de explotación de sistemas IT de Securitas Direct, sostiene que es muy importante el apoyo de la dirección al departamento de seguridad. "Nos ven como unos paranoicos". Es decir, la concienciación tiene que darse a todos los niveles, tanto horizontal como verticalmente.

El sector de la seguridad está en constante movimiento, ya que cada vez hay más amenazas y resulta difícil pararlas. Para ello, hay que estar al día

Estar al día

Aunque existe en el mercado tecnología al alcance para mantener a raya la protección del centro de datos -protocolos, segmentación entre servicios y redes, etcétera- y muchos profesionales, lo cierto es que los métodos para hacerse con la información cada vez son más creativos. Hay que tomar medidas para responder a las nuevas amenazas, que son cambiantes, pero teniendo en cuenta que la seguridad va a interferir con la velocidad del negocio. Si ocurre un ataque lo primero es ver cómo se va a poder contener, intentando no interrumpir el funcionamiento de la compañía y asegurando una buena resiliencia. La prevención entraría en juego después, pero siempre con un papel relevante. Los proveedores de seguridad se afanan por enriquecer la forma de detectar y de prevenir, porque hacer que la tecnología sea preventiva es la forma de evitar que entren los ataques. Eso sí, el paciente cero ya no es válido, ahora hay que pararlo desde el principio.

Podríamos decir que en la actualidad los peligros más habituales son el ransomware, los ataques a costa de los usuarios (minería de bitcoins) y vulnerabilidades a móviles, sobre todo Android, que se producen a través de las descargas de aplicaciones que están afectando a consumo pero que, en breve, llegará también al ámbito empresarial.

"Durante la crisis se notó una falta de inversión en nueva construcción, y tan sólo había adecuaciones de centros de datos ya existentes. Pero actualmente la Administración ha empezado a mover ficha y vuelven a surgir proyectos"

"La normativa va por detrás de la tecnología"

"Sí se puede. Solemos ser muy pesimistas acerca de que no hay seguridad absoluta, pero tenemos herramientas para afrontar los ataques que vayan surgiendo"

Eusebio Nieva, director técnico para España y Portugal de Check Point.

"El principal reto es llegar a ese balance seguridad/negocio"

David Matesanz Ureña, regional information security officer para Europa de Daimler.

"Tenemos muchas normativas, fabricantes, asociaciones, consultorías... pero hay que mejorar, debemos concienciar y formar"

Carlos Asún, CISO de Initec Plantas Industriales (Grupo Técnicas Reunidas)

"La seguridad es un reto permanente, las medidas de prevención son las llaves para poder asegurar la continuidad del negocio"

Javier Albalat, DC & IT Sales Specialist de Rittal.

"La seguridad somos todos, es responsabilidad de todos y requiere la colaboración de todos"

César Romo, director de explotación de sistemas IT de Securitas Direct.

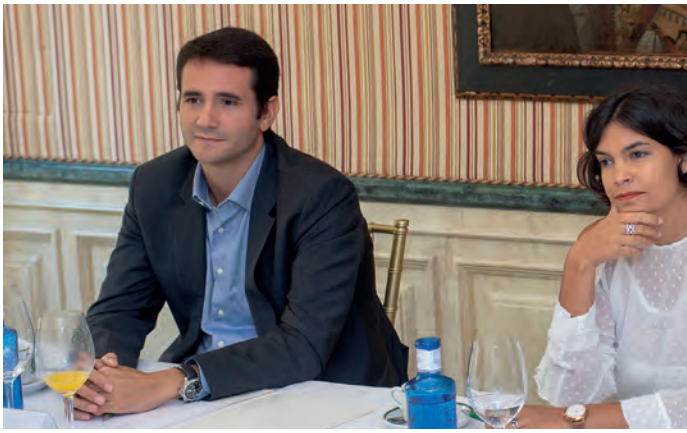
"El machine learning se aplicará como medida preventiva de seguridad"

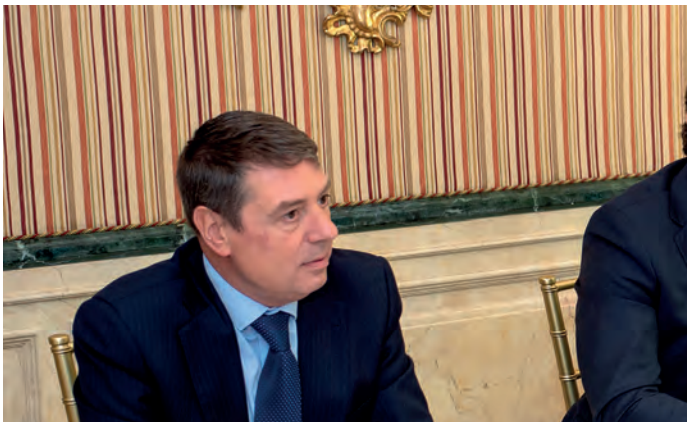
Sobre este particular, Javier Albalat, de Rittal, recalca que cada organización es un mundo y que se suelen encontrar con un interlocutor diferente en cada caso. Es más, observa que en muchas ocasiones no hay una figura definida como responsable de seguridad, concretamente esto suele ocurrir en pymes. "A mayor tamaño de la compañía es normal que haya un cargo específico en seguridad".

Dispositivos conectados

Una de las razones de que el usuario sea una puerta de entrada de vulnerabilidades radica en los dispositivos que lleva consigo. La Internet de las Cosas, que dibuja un futuro hiperconectado, hace saltar la voz de alerta. Como afirman desde Initec, es en la parte de dispositivos donde el nivel de riesgo es más alto y donde, por lo tanto, hay que poner más foco.

"Somos una empresa IoT desde el inicio de los tiempos", declara sobre este debate el portavoz de Securitas Direct. "Tenemos gente constantemente en la calle con dispositivos conectados y aunque no es nuevo para nosotros, tenemos que estar evo-

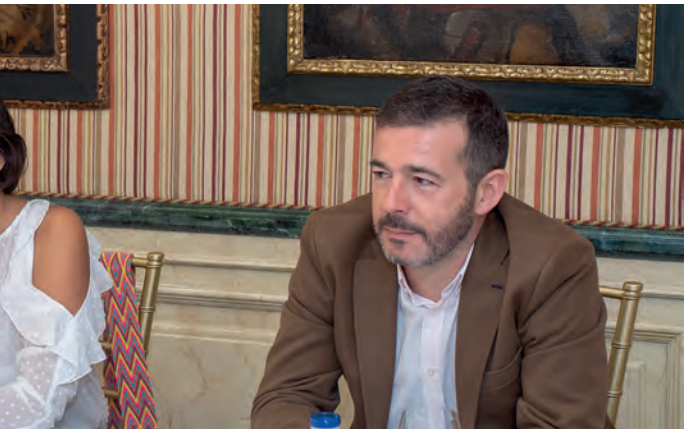


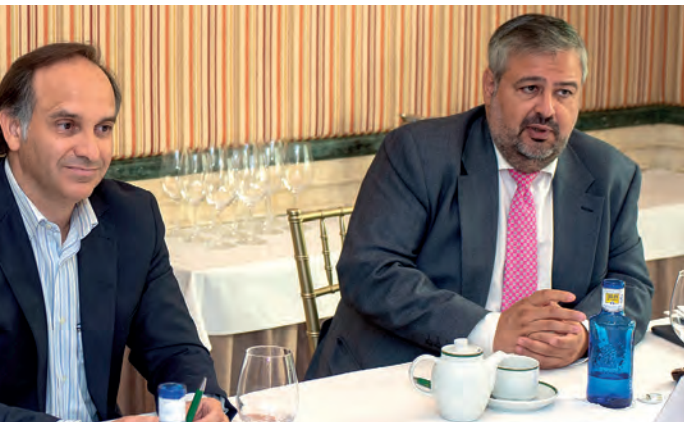


"La seguridad va a interferir con la velocidad del negocio"

lucionando constantemente, porque el desafío que plantea la Internet de las Cosas es su expansión. Aunque en el mercado hay herramientas para tener bajo control estos accesos –como acuerdos con los carriers (implementando VPN)– nadie está libre de un ataque".

Por su lado David Matesanz, de Daimler, reconoce que en lo que atañe a su sector, "mi opinión personal es que para la seguridad del coche conectado los desarrollos se están haciendo con mucho cuidado". Bien es cierto, como reflexiona el director técnico para Iberia de Check Point, que siempre que afecta a la vida de las personas existe una mayor concienciación sobre la seguridad, y ahí es cuando se ponen encima de la mesa los riesgos. "Eso no ocurre con los smartphones" y no hay que olvidar lo peligrosos que resultan los dispositivos que puede introducir un usuario en un CPD. ¿Quién ha vigilado el teléfono, tablet, ordenador portátil o smartwatch que lleva un operario en un centro de datos? Ahí está la clave. "En el data center la amenaza más grave es tener una buena seguridad física. Un único punto de entrada para el data center es fundamental", comenta. No obstante, Eusebio Nieva continúa con su reflexión y medita que no ve un problema grave en la Internet de las Cosas si los dispositivos no están conectados a la red. Eso sí, hay que controlar quién y con qué accede a nuestras redes. La identidad del usuario toma más relevancia en los data center, concluye.





Modelo combinado

¿Cómo están combatiendo Securitas Direct, Daimler e Initec Plantas Industriales la seguridad de sus centros de datos y que desafíos se les plantean en el camino? César Romo, director de explotación de sistemas IT de Securitas Direct, menciona que dan operación a ocho países separados entre sí, lo que hace que haya puntos de amenazas dispersos y traten la seguridad a nivel de grupo. Cuentan con un CPD propio con una escala de seguridad muy alta, similar a la que posee su Central Receptora de Alarmas (CRA), aunque también trabajan con empresas de colocation y diferentes fabricantes. Con su core de negocio totalmente interno, actualmente están inmersos en iniciativas para montar data center europeos, ya que tienen estructurada la compañía en dos cluster: norte y sur. "Como empresa de seguridad no podemos permitirnos un incidente a nivel reputacional", matiza. De ahí que estén focalizados en la gestión de identidades, sigan un 'roadmap' de seguridad con auto consultorías semestrales y cumplan las normativas vigentes. "Tenemos una gran amenaza en el propio regulador porque la normativa va por detrás de la tecnología", denuncia.

Por su parte, David Matesanz Ureña, regional Information Security Officer para Europa de Daimler, observa que están llevando a cabo un proyecto importante de regionalizar los CPD de los países europeos. En este proyecto los principales retos de Seguridad los encontramos en tres flancos: la seguridad física (que con las certificaciones que hay en vigor corroboran que está en orden), lógica (con múltiples tecnologías que permiten luchar contra los peligros en un mundo híbrido en el que el dato está repartido por muchos sitios) y el outsourcing, "el flanco más difícil pues debes analizar cómo gestionar a estos proveedores externos", de ahí que lleven a cabo medidas contractuales con ellos".

Finalmente, Carlos Asún, CISO de Initec Plantas Industriales (Grupo Técnicas Reunidas), ingeniería especializada en refinería de petróleo y gas, explica que hace un par de años construyeron un nuevo data center y que poseen otro de respaldo en Madrid. Además, cuentan con micro CPD en casi todas las filiales del mundo en las que están presentes y junto a ellos disponen de micro CPD temporales que ubican en lugares remotos o de orografía difícil, como desiertos. Están muy pendientes de la seguridad, tanto física como lógica. Responden a los parámetros de legislación exigidos, hacen test continuos y hacking ético para someter a pruebas sus instalaciones y son muy estrictos con los proveedores a nivel de seguridad.

Se difuminan las fronteras del centro de datos, imponiéndose un mundo híbrido en el que el dato está repartido por muchos sitios