

“Ante una contingencia es necesario saber que los sistemas de *backup* nos van a responder”

El imparable ascenso del *ransomware* asusta. Una amenaza en constante evolución que está sobrepasando todos los límites. Según un estudio llevado a cabo por Veritas, el 53 % de las empresas españolas que han participado en el mismo ha sufrido un ataque de este tipo en los últimos meses. Así lo confirma Juani Sánchez, *partner account manager* de la compañía, aunque lo que más llama la atención es que el 66 % de las organizaciones afectadas han pagado un rescate para recuperar sus datos, revela.

Inma Elizalde

Datos a los que hay que unir los que aporta Juan Carlos Garcia-Calvo, consultor de sistemas de Inetum (antes Gfi e IECISA): como posibles estimaciones se cree que cada 11 segundos se produce un ataque de *ransomware* en el mundo. El promedio del tiempo del rescate gira en torno a los 18 días, aunque el tiempo de recuperación puede alargarse mucho más en el tiempo. La asignación promedio demandada por cada una de estas acciones se cree que podría girar en torno a los 170.000 dólares en 2020 y que entre 2019 y 2020 los ciberdelincuentes habrían recaudado más de 1.000 millones de dólares con estos actos.

Atrás quedaron los tiempos en los que la sofisticación no existía y sus objetivos pasaban por el acceso a las credenciales personales o al robo de pequeñas cantidades de dinero a través del *phishing*. En la actualidad reinan las aplicaciones de ingeniería social, el acceso a dispositivos conectados al IoT o a las vulnerabilidades en el software de instalaciones o de la infraestructura de servicios críticos, reflexionan Juani Sánchez, y Juan Carlos Garcia-Calvo.



Juani Sánchez, partner account manager de Veritas

Los objetivos que mueven a los ciberdelincuentes son por un lado el económico y por otro el táctico. En el primero piden un rescate por los datos secuestrados. En los últimos tiempos sus miras están

puestas en organizaciones con un mayor poder adquisitivo, al tiempo que están acercando posiciones a universidades y al sector sanitario. En este último con el agravante de que ya se han producido muertes al no poder atender el sistema sanitario a los pacientes en el centro atacado, revela Juan Carlos Garcia-Calvo.

En el apartado táctico priman los fines ideológicos en los que pueden participar desde un grupo organizado a grupos subvencionados por terceros. Pueden ser estados o competencias a nivel industrial, que persiguen desprestigiar y hundir económica y públicamente a sus víctimas, independientemente de si se demanda o no el rescate.

Juani Sánchez lanza un mensaje claro en este sentido: "nunca hay que dar dinero a cambio de recuperar los datos porque muchas veces, ni a pesar del pago, la recuperación es total". En este sentido señala que las leyes intentan atajar esto y ya hay lugares en el mundo en el que un estado puede multar a quien paga.

Ransomware como servicio

La sofisticación ha llevado al *ransomware* a ofrecerse y consumirse también como servicio. Dos tercios de las campañas lanzadas el año pasado se llevaron a cabo de esta manera, representando el 65 % de los ataques. Juan Carlos Garcia-Calvo desvela que también ha crecido el número de grupos organizados. Cada grupo está especiali-

zado en explotar un tipo de vulnerabilidad o su especialización llega a un determinado tipo de herramienta de acceso a la información. La cooperación entre todos ellos es máxima y se ayudan para alcanzar el fin último.

¿Hacia dónde evoluciona? Hacia un tipo de espionaje industrial, responde. Espionaje que siempre se ha intentado hacer de forma silenciosa

para que la competencia no fuera consciente de que sus patentes habían sido extraídas y explotadas. Se sospecha que también hay organismos

A tener en cuenta

- La tecnología Inetum cuenta con herramientas de avanzada tecnología que les permite gestionar todo lo relacionado con el dato, su custodia y conocer, en cada momento, si ese dato de alguna manera se ha visto afectado.
- Veritas, aunque no se define como una empresa de seguridad, pone al dato en el centro para cubrir cualquier tipo de necesidad en torno al mismo, se encuentre donde se encuentre el mismo.
- Veritas e Inetum recomiendan tener tres copias de los datos, en dos medios físicos diferentes y uno de ellos fuera de las instalaciones principales.
- Veritas NetBackup ayuda en gran medida a Inetum a garantizar la inmutabilidad del dato.
- Es muy importante hablar no solo de recuperación, también hay que tener un plan B, b de *backup*.



Juan Carlos Garcia-Calvo, consultor de sistemas de Inetum

Proteger, detectar, recuperar

¿Cómo ayudan Veritas e Inetum a proteger, detectar y recuperar? En la consultora tecnológica hacen suya la estrategia de Veritas denominada Enterprise Data Services Platform, que consiste en tener claro que para proteger, detectar y recuperar no siempre hay que tener una misma línea de producto, sino que puede complementarse con diferentes soluciones. A la hora de detectar posibles intrusiones, Juan Carlos Garcia-Calvo señala que con los *appliances* se puede llevar a cabo un análisis estático de código para comprobar si hay algún tipo de variación en el código del software de gestión, ya que esto podría ser indicativo de algún tipo de ataque.

Es muy importante que el sistema operativo en el que se basa la gestión de estos sistemas de *appliance* esté basado en Linux, subraya, pero es un subsistema de Linux no público en el que de alguna manera se han

capado ciertos accesos y solo se ha conservado aquello que es intrínsecamente necesario para gestionar la plataforma y el almacenamiento. Una gestión de autenticación basada en roles.

Por su parte, NetBackup permite hacer un traslado de los datos de *backup* en capas o en modelos de almacenamiento de primer y segundo nivel, con otro tipo de *appliances* y replicar esas imágenes de *backup* desde un *appliance* a otro en diferentes condiciones físicas o en la nube, con los sistemas de réplica que tiene el propio producto.

Para Juani Sánchez es importante recordar que todos los productos de Veritas son agnósticos. “Nos adaptamos a cualquier sistema operativo que tenga el cliente en su CPD. No hacemos que lo cambie. Lo adaptamos y vamos con ellos a todos los entornos físicos, a los entornos virtuales y a las diferentes nubes”, explica.

y estados que subvencionan este tipo de actividades porque es la manera más rápida y fácil de adquirir tecnología, conocimiento e información. “Datos críticos que afectan no solo a la privacidad de las personas, sino que además es un ensayo de la capacidad de respuesta y ataque de un entor-

no contra otro, para, llegado el caso, tener armas de tipo social, económico y político a la hora de presionar a organizaciones y al propio estado”, dice. Y por otro lado para revenderlos a terceros, aunque aquí entran en juego las leyes de protección de datos.

Para Juani Sánchez en el momento actual de migración a la nube, las empresas tienen que adaptarse a la mezcla de infraestructura (parte en casa del cliente, parte en la nube) y no concentrarse en un único producto para combatir el *ransomware*.

La importancia de contar con un buen *backup*

Desde Veritas recuerdan que ante los nuevos tipos de ataques ninguna empresa está a salvo y las organizaciones necesitan un plan B para estar a salvo, B de *backup*. ¿Qué características definen a un buen *backup*? La principal es que tiene que ser recuperable, admite Juani Sánchez, sobre todo dentro del entorno del *ransomware*. En este sentido, Veritas trabaja en que esa recuperación sea cada vez más rápida y segura. “Trabajamos mucho en la inmutabilidad del

dato”, asegura, “porque es muy importante que cuando ese dato se recupere, sea el dato original. Que nadie, ni por un error humano ni un ciberdelincuente, lo haya alterado”.

Juan Carlos Garcia-Calvo señala que para Inetum, como integrador, es fundamental contar con herramientas de *backup* multidisciplinares que abarquen la mayor parte de los sistemas y que permitan la evolución continua de las aplicaciones para una continua protección. En este sentido señala que Veritas siempre ha estado ahí con sus productos: al pasar del entorno de sistemas

operativos físicos a entornos virtuales, al ir a entornos de contenedores, al usar la nube como herramienta accesoria de salvaguarda, etc. Por ello, recuerda la importancia de contar con herramientas que permitan garantizar a los clientes que, ante una contingencia, sus sistemas de *backup* les van a responder.

¿Cómo consiguen la inmutabilidad del dato? Haciendo que la gestión de identidad del usuario y los roles en los que está basado este acceso estén totalmente controlados.

Los datos tienen que estar protegidos, por lo que hay que encriptar los mismos en origen para que viajen de manera segura a través de las comunicaciones hacia el repositorio local. Y si esto no es posible, hay que añadir una segunda opción de seguridad. Que esa encriptación sea también completa y segura en el destino. Por último, la plataforma de destino tiene que estar protegida. Para ello hay que hacerla lo más agnóstica posible a la hora de trasladar la información y las imágenes de un lugar a otro.



En este sentido Veritas cuenta con Open Storage Technology, que permite que los repositorios de *backup* sean compatibles a la hora de almacenarse en diferentes entornos de disco y una línea puntera de *appliances* que basan su diseño en una política de contenedor en la que existe una tecnología intrínseca para la utilidad del dato.

Veritas puso el foco en el *ransomware* mucho antes de que estuviera de moda, declara Juani Sánchez, por lo que cuidaron en gran medida que sus *appliances* estuvieran protegidos y en ningún momento han sufrido ataques en los mismos. Algo que pueden demostrar sus clientes.

Peligros que se ciernen sobre el *backup*

Los ciberdelincuentes, conscientes de la importancia que está adquiriendo el *backup*, han puesto sus miras en el mismo. Juan Carlos Garcia-Calvo considera que es un objetivo en sí mismo, de igual importancia que los datos alojados en los entornos productivos de determinadas empresas, porque es la manera que tiene el atacante

Optimizando costes con Aptare

Una herramienta complementaria a Veritas NetBackup, como núcleo de protección es Aptare. Permite identificar y gestionar la validez de la salvaguarda de los datos que estamos llevando a cabo con nuestras herramientas de *backup*. “Una manera de discriminar las políticas de *backup* que no son satisfactorias y mejorarlas para asegurarnos que todos los *backup* que generamos son recuperables”, asegura Juan Carlos Garcia-Calvo.

Indica anomalías tanto en duración de los trabajos de *backup* como en el tamaño de las imágenes propias del mismo, que deberían esperarse para esas políticas. Permite el análisis de mitigación de riesgos y fuentes de datos, así como de posibles fallos a nivel de aplicación.

Aptare ayuda a optimizar costes. Y es que tal y como Juani Sánchez comenta, “podemos ayudar al cliente demostrándole qué es lo que tiene, cómo lo tiene y cómo lo está utilizando. Aptare es un motor de análisis muy potente para dar esta información y a partir de ahí poder tomar las acciones necesarias dentro de la infraestructura para dar solución a lo que pueda ser mejorable”.

de garantizar que no tiene línea de defensa y de recuperación el cliente ante la extorsión. Por ello recuerda que es muy importante proteger no solo los accesos a sus principales entornos productivos, también su entorno de recuperación.

En este sentido sostiene que es imprescindible saber qué datos son críticos y contar con herramientas complementarias como las que tiene Veritas, no solo de *backup*, también de análisis, monitorización y gestión del dato.

Juani Sánchez añade que tan importante es poner el foco en la parte de la recuperación como en la de detección, análisis y respuesta frente a cualquier ataque. “Entre las soluciones que tenemos en Veritas también contamos con la parte de detección para conocer si este dato está sufriendo una fuga, un ataque malicioso o si puede haber un error humano detrás”, confirma. “Con estas herramientas podemos con-

trolar que el dato está siendo bien tratado o que no hay nadie intentando acceder a sitios donde no debe, con los permisos necesarios para cada usuario dentro de una determinada plataforma”.

Al lado del CIO

Su aproximación al CIO es total. Y en esta aproximación tiene que responder a cuál es la disponibi-

lidad de sus datos, cuál es su grado de protección y si sabe qué tipo de datos tiene.

El CIO tiene que disponer de herramientas para categorizar los datos críticos y confidenciales para establecer políticas y controles específicos, apunta Juan Carlos Garcia-Calvo. Tiene que huir de soluciones de nicho y contar con soluciones multiplataforma tanto en hardware como en software y multicanal tanto en *on-premise* como en la nube. Contar con un *backup* fácilmente gestionable y un sistema que garantice la información.

Juani Sánchez comenta que están viendo un gran interés por parte del CIO por quién es el propietario de los datos en entornos como Office 365, ya que se están dando cuenta de que el encargado de hacer el *backup* no es la herramienta de Office. En Veritas cuentan con Veritas NetBackup SaaS Protection para poder hacer el *backup* de esos datos. O Veritas NetBackup CloudPoint que permite hacer copias utilizando tecnología tipo *container* y *cloud* nativo para desarrollar acuerdos con entornos de nube.

Veritas-Inetum, combinación perfecta en la prevención empresarial

Cinco son las premisas que van a permitir que una organización siga funcionando: identificar, proteger, detectar, responder y recuperar. Inetum, como integrador, necesita el aval y el cumplimiento de soluciones que gestionen la protección y detección de posibles intrusiones en el dato. En este sentido, Veritas es importante al proporcionarles un *portfolio* de soluciones que han utilizado a lo largo de una estrecha relación que les ha convertido en los *partners* preferentes con mayor certificación de Veritas y el único *platinum* en España.

Veritas trabaja poniendo el dato en el centro, creando soluciones alrededor del dato. Y dentro de esa gestión necesitan *partners* como Inetum para dar un servicio completo al cliente.