Crece la concienciación de las empresas en torno a la protección de sus datos


# El *backup*: blindarse frente al *ransomware* en la era del Covid-19

**Aunque no han cambiado sustancialmente sus técnicas, los *hackers* han aprovechado la expansión de la pandemia del Covid-19 para intensificar sus ataques de *ransomware*. El despliegue masivo del teletrabajo y el aumento del consumo de aplicaciones y servicios en la nube, en muchos casos sin una adecuada política de protección, expandió, como el fuego, la superficie de ataque, lo que ha dejado al descubierto las carencias de las empresas españolas en el ámbito del *backup*. Sin embargo, las principales empresas que ofrecen este servicio reconocen que ha aumentado la concienciación.**

Marilés de Pedro

Antes del dramático mes de marzo, los ataques de *ransomware* ya habían aumentado un 12 % en el mes de febrero. Según el estudio Cyber Protect, que Acronis realiza de forma periódica, en el mes de marzo el 37% de las empresas españolas se mostraba muy preocupada por el riesgo del *ransomware* y el 43 % temía una violación de datos. Marzo y abril han detectado un enorme incremento de los ciberataques relacionados con el *phishing*, el *ransomware* y los *criptolocker*. Los ciberdelincuentes han utilizado como gancho el Covid 19 para conseguir el éxito de sus ataques.

"Los ficheros de *backup*, estén donde estén, son objetivo primordial de los atacantes"

El auge del teletrabajo, provocado por las medidas de confinamiento adoptadas para detener la

pandemia, exigió un despliegue de ordenadores portátiles y equipos de sobremesa corporativos en los hogares. Unos dispositivos, a los que había que dotar de una seguridad adecuada, en la que el *backup* debía ser una pieza esencial. "Un *backup* fácil, sencillo, sin intervención del empleado y que le permitiera trabajar con la garantía de recuperar toda la información si fuese necesario", explica José Manuel Petisco, director general de Veritas en España y Portugal.

Este despliegue masivo del teletrabajo ha estado acompañado de un uso intensivo de las herramientas de comunicación por parte de los trabajadores. Muchos de ellos, además, era la primera vez que hacían uso de ellas en un contexto profesional. "Algunas de estas herramientas de colaboración se han convertido en objetivos principales para los *hackers*, que intentan desplegar sus ataques de *ransomware*, tanto en las infraestructuras tecnológicas de las empresas como en los dispositivos de los usuarios", alerta Petisco.

Más usuarios conectados a la red, con un mayor tiempo de exposición y un uso intensivo de herramientas y equipos que no siempre exhibían adecuadas medidas de protección. Un panorama que se erigía en la tormenta perfecta para el despliegue de *ransomware*. "Este tipo de ataques es capaz de encriptar los discos remotos, los discos en la nube, los discos extraíbles y los *pendrives*. Los ficheros de *backup*, estén donde estén, son objetivo primordial de los atacantes", alerta José Manuel Arnaiz, CEO de Loozend. "Es imperativo disponer de una herramienta que impida totalmente el borrado de los ficheros históricos y, sin embargo, la mayoría sí lo permite", recomienda.

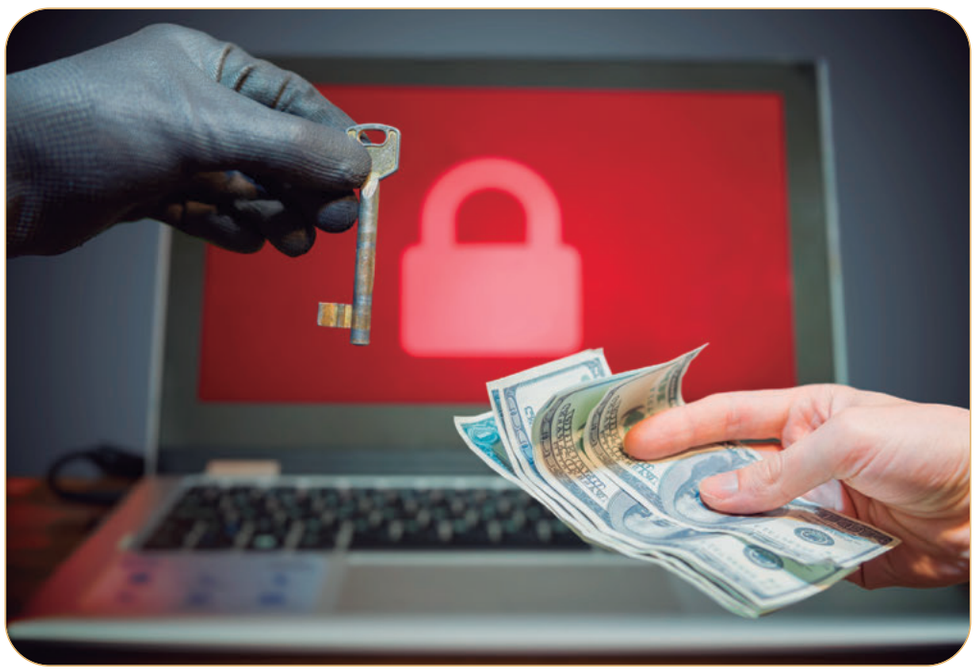
Unos ataques de *ransomware* que no conocen límites, ni sectores de actividad. "Incluso los hospitales están siendo víctimas de este tipo de ataques", recuerda Eulalia Flo, directora general de Commvault en España y Portugal. "No sólo se usa el *ransomware* para cifrar archivos, sino que se están pidiendo rescates para no desvelar datos confidenciales que han sido robados". Flo también alerta de otros problemas que se están observando, no ya de vulnerabilidades, sino de mala configuración por parte de los usuarios. "Las plataformas de videoconferencia, por ejemplo, están siendo configuradas de forma incorrecta, lo que está permitiendo que personas ajenas a las organizaciones puedan entrar en reuniones privadas y lanzar ataques de *phishing* o de *ransomware*". El mayor problema en todos estos casos "es que una gran parte de las organizaciones no tiene un plan de recuperación ante desastres. Por tanto, si son víctimas de un robo de datos o de un ataque de *ransomware*, no tienen forma de recuperarse cuando lo necesitan".

> "No sólo se usa el *ransomware* para cifrar archivos, sino que se están pidiendo rescates para no desvelar datos confidenciales que han sido robados"

## ¿Se hace bien el *backup*?

Uno de los principales problemas es que las empresas carecen, en muchos casos, de una verdadera estrategia de gestión y protección a lo largo del ciclo de vida del dato. "Algunas compañías siguen haciendo *backup* de los distintos silos de almacenamiento", alerta Eulalia Flo. La explosión del teletrabajo ha dejado en evidencia las carencias que existen en la protección de los puestos de trabajo. Aunque, como recuerda la máxima responsable de Commvault, los datos críticos deberían de estar en un repositorio corporativo y usarse escritorios virtuales, "la realidad es que muchos empleados trabajan en local y guardan datos críticos para la organización en sus propios dispositivos, lo que resulta muy peligroso ante un ataque de *ransomware*".

Algunas empresas cuentan con políticas de *backup* incompletas, que no incluyen una copia externalizada, como explica Javier Miquel, director general de Mast Storage. "No pueden acceder físicamente a su copia en local", insiste. Unas carencias que se hacen mucho más visibles en la actualidad, por el riesgo que supone el aumento del teletrabajo con conexiones poco o nada seguras, y porque los ataques de *ransomware* siguen creciendo cada día. "Aún hay empresas que no externalizan, o lo hacen con servicios que no están pensados para ello, con los riesgos que eso supone. Además, pocas empresas verifican periódicamente si se están haciendo bien las copias, y si los datos copiados son válidos y restaurables", completa.



Los ciberdelincuentes siguen haciendo uso del "tradicional" *phishing* como el método preferido para lanzar sus ataques de *ransomware*. Si lo hacen a través del correo electrónico, resulta más "sencillo" para el usuario comprobar la dirección antes de abrir un enlace, sin embargo, en los servicios de mensajería instantánea no se espera una intervención maliciosa y, como consecuencia, es más fácil que un *hacker* se haga pasar por alguien que no es. "En estos tiempos de confinamiento y teletrabajo un clic equivocado puede costarle a una compañía miles e, incluso, millones de euros", alerta José Manuel Petisco.

A su juicio, las soluciones de *backup* y de *appliances* específicos con capacidades de bastionado "deben ser prioridad".

Restringir la protección a únicamente la información de los servidores es otro problema recurrente. "Las tecnologías tradicionales de *backup* son muy poco prácticas y costosas para proteger los PC individuales", cree José Manuel Arnaiz. "Sin embargo, es evidente que muchos de los usuarios siguen teniendo información relevante en sus discos locales", reconoce. "Es injusto culparles por ello; por lo que es mucho mejor seleccionar tecnologías más modernas que den cobertura a esta información. Es el caso, por ejemplo, de certificados digitales, ficheros grandes, temporales de Office, la papelera de reciclaje, configuraciones, favoritos..., por no mencionar el software y las licencias. Por tanto, es necesario proteger esa información que está ubicada en los equipos de los usuarios".

> "Aún hay empresas que no externalizan, o lo hacen con servicios que no están pensados para ello, con los riesgos que eso supone"

¿La mejor ley para aplicar un *backup*? La que siempre ha regido el mercado (3-2-1): las empresas deben contar con tres copias de sus datos, dos de las cuales están en diferentes medios de almacenamiento y la tercera debe estar ubicada en un repositorio externo.

Javier Miquel insiste, de cualquier modo, que no se trata solo de comprar un determinado software. "Es básico entender la problemática del *backup* y planificar una estrategia que defina la manera de llevar a cabo esta tarea", insiste. "La pregunta clave que debe hacerse la empresa es qué plan de contingencia tiene para proteger su *backup*. Tan importante es la metodología del *backup* como la tecnología". Una filosofía que debe incluir un análisis del *backup* y de las necesidades del cliente. "Hay que planificar una estrategia en la que se definan los plazos para hacer la copia, los dispositivos y las máquinas virtuales objeto de la misma, etc.".

## La subida a la nube

Lógicamente, la nube no es ajena a este panorama. Se calcula que el negocio *cloud* se habrá triplicado en 2023 y en 2019 alcanzó un crecimiento de más de un 25 %. "Se está evolucionando desde las licencias tradicionales a una tecnología basada en nube", recuerda Alessandro Perotti, *channel manager* para Italia e Iberia de Acronis. "La copia de seguridad de datos es una pieza importante en la estrategia general para proteger todos los aspectos de los datos, aplicaciones y sistemas en cuanto a seguridad, accesibilidad, privacidad, autenticidad y seguridad (SAPAS)".

La nube es uno de los principales impulsores de la aceleración de los negocios digitales modernos y a medida que aumenta la dependencia hacia los entornos *cloud* se requiere que las organizaciones empleen estrategias de gestión y protección de datos que sean sólidas, que estén de acuerdo a las diferentes regulaciones y que a su vez sean lo suficientemente flexibles para agilizar la continua transformación, al tiempo que mitigan los riesgos por la posible pérdida de esa información o incumplimiento regulatorio. "Sin embargo, son muchas las empresas a las que el Covid-19 les ha pillado de improviso en este aspecto", alerta Petisco. "En las últimas semanas se ha realizado un gran despliegue para ayudar a las empresas a poder adaptarse a los entornos *cloud* y, por tanto, a la necesidad de realización de *backups* de las cargas de trabajo que realizan en las diferentes nubes y sus

servicios, con el fin de proteger toda la información que tienen en estos entornos".

Se trata, como apunta José Manuel Arnaiz, de protegerse, entre otras variantes de ataques, de los *ransomcloud*. "Un concepto nuevo, pero desgraciadamente muy real, que atacan directamente la información en la nube, encriptándola, y pidiendo un rescate", explica. La nube, expone, no es tan segura como mucha gente piensa. "Lo ideal en un caso de uso exhaustivo de la nube es sincronizar en local, y proteger en otro sitio también la información local, de manera que haya siempre las tres copias", insiste.

## ¿Más concienciación?

Los fabricantes, a pesar de esta complicada situación, reconocen que ha aumentado la concienciación en las empresas. "Esta crisis ha sacado a la luz la necesidad de una tecnología fiable", apunta Perotti. "La copia de seguridad ya no solo es un valor añadido, sino una clara necesidad de seguir siendo relevante en el negocio. Más que sólo respaldo, la protección cibernética es como la quinta necesidad humana esencial después del aire, la comida, el sueño y el refugio".

Perotti explica que en este periodo muchas empresas han migrado temporalmente sus servidores a servicios *cloud* para poder seguir dando servicio a sus clientes o para permitir que sus trabajadores pudieran seguir trabajando, lo que va a permitir que "las empresas que todavía estaban reticentes, prueben esta tecnología, y vean que sus datos están seguros en esos almacenamientos *cloud*. Tras esto, es obligatorio el *backup*, por lo que se incrementarán las ventas en este tipo de producto".

Se trata, como apunta Javier Miquel, no solo de *backup* y de protección de datos, sino de continuidad de negocio. "Tras un ataque de *ransomware*, el coste que supone recuperar los datos es, como mínimo, de 1 o 2 bitcoins, lo que significa entre 6.000 y 12.000 euros", alerta.

"Sin embargo, puede ser muy superior. Conocemos empresas a las que se les ha pedido 200.000 euros de rescate", desvela. Su esperanza es que aumente la concienciación de la necesidad de realizar un *backup* con garantías de restauración.


La incorrecta sensación de seguridad de las empresas es otro problema que debe mejorar. "Muchas organizaciones piensan que están preparadas para hacer frente a una crisis, pero la verdad es que no lo están. Y no lo saben porque no han hecho las pruebas necesarias", alerta Eulalia Flo.

Incrementar la resiliencia y la agilidad tomarán mayor protagonismo a la hora de reevaluar las iniciativas y revisar prioridades. "La definición de escenarios de recuperación en función de la criticidad de los entornos llevará a una revisión de las estrategias de gestión y protección de los datos", explica. "Hay que crear políticas de recuperación frente a distintos escenarios y además probar su efectividad". La directiva de Commvault desvela que las empresas están contratando seguros frente al *ransomware*. "Sin embargo, en caso de que sea necesario recuperar el entorno, no será posible si no existen copias de seguridad de la información que se ha perdido o si éstas copias son dispersas y resulta imposible saber en qué orden hay que recuperar los archivos para volver a operar con normalidad".

> "En estos tiempos de confinamiento y teletrabajo un clic equivocado puede costarle a una compañía miles e, incluso, millones de euros"

José Manuel Arnaiz cree que se ha incrementado muchísimo el valor de los activos digitales y también la necesidad de protegerlos. "En la era de inteligencia artificial, el Internet de las Cosas y el *big data*, tener toda nuestra información bien resguardada es un derecho, pero también una obligación ineludible. No hacerlo es una grave irresponsabilidad individual y de las empresas".

## ¿En qué se ha crecido?

Las empresas han notado un incremento de sus ventas. En el caso concreto de Mast Storage, se ha incrementado un 15 % el número de peticiones de empresas que necesitan un servicio de *backup online* durante el confinamiento por no poder acceder físicamente a cambiar discos o cintas de sus sistemas de *backup* local.

Durante el mes de abril, observando la situación tan complicada que estaban atravesando muchas empresas, la marca decidió no cobrar el servicio Mast Backup Online. "Es una medida extraordinaria que alcanzar tanto a los clientes actuales como a nuevos clientes que puedan necesitar esta solución durante el confinamiento", explica Javier Miquel.

## Las pymes

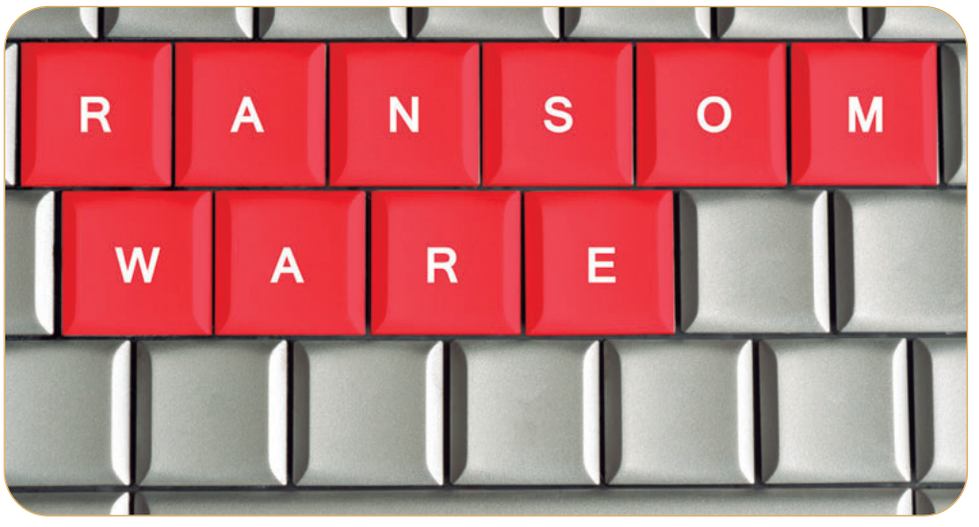
Tras un ataque, los riesgos que se abren para las empresas son enormes. Según calcula Acronis, el 50 % de las empresas que recibe un ciberataque acaba cerrando. "Muchas pymes no tienen una percepción muy clara de dónde tienen almacenados sus datos y cómo están protegidos", opina Perotti. "Todas las organizaciones deben tener un plan claro de recuperación ante desastres", aconseja. "Las pymes deberían realizar un ejercicio de emergencia y probar si pueden restaurar con éxito todos los datos requeridos y cuánto tiempo les lleva hacerlo. Un ejercicio que, sin duda, les puede aportar información valiosa sobre su nivel de resiliencia".

La experiencia de Mast Storage en este campo de la pyme se extiende más de dos décadas y en la actualidad gestionan el *backup* diario de más de 6.000 empresas en España, siempre a través de su canal. Miquel explica que durante los últimos años han comprobado que muchas pymes cuentan con un departamento de informática pero no con un responsable encargado de gestionar exclusivamente la política de *backup*. Para "remediarlo", el fabricante cuenta con un equipo técnico propio que supervisa las copias diarias de los clientes, notifica cualquier incidencia y asesora sobre cómo resolverla. "Formamos el tándem perfecto con el distribuidor o la casa de software y el responsable TI de la empresa".

José Manuel Arnaiz asegura que el tejido empresarial español muestra idéntica vulnerabilidad que la de cualquier otro país. "Cada ordenador del mundo recibe de media más de 6 ataques de *ransomware* al año y en España recibimos nuestra ración", contabiliza. El CEO de Loozend reconoce que es fundamental que las empresas mantengan actualizados los sistemas operativos y las aplicaciones, así como el uso de un antivirus para detectar la presencia de un ataque. "Ahora bien, es vital disponer de un *backup* de toda la información y que éste esté bien protegido. Es la única garantía para no perder información".

> "Tras un ataque de *ransomware*, el coste que supone recuperar los datos es, como mínimo, de 1 o 2 bitcoins, lo que significa entre 6.000 y 12.000 euros"

Eulalia Flo explica que han notado que algunos proyectos se han acelerado. "Muchas organizaciones han tenido que adaptar sus sistemas de forma rápida para dar servicio al incremento de demanda *online* e incluso han tenido que dotar de más infraestructura y adaptar las propias aplicaciones para satisfacer nuevas exigencias". La directiva recuerda que hay que ir más allá del *backup* y pensar en los escenarios de recuperación. "Estamos ampliando el concepto a la gestión inteligente de los datos que incluye entender qué datos tenemos, dónde están y quién tiene acceso a ellos para gestionar su ciclo de vida". La marca está organizando una serie de seminarios *online* en los que dan información para acelerar los proyectos en la nube, cómo proteger el puesto de trabajo o el entorno ante un ataque de *ransomware*, cómo migrar el *backup* tradicional a la nube de forma segura y efectiva, o cómo hacer frente a una recuperación ante desastres.




En el caso de Loozend, cuya andadura en el mercado es joven, el crecimiento es relevante. "El crecimiento del teletrabajo, basado en muchos casos en infraestructura doméstica, nos hace mucho más vulnerables a los ataques y, por tanto, a las pérdidas accidentales", recuerda Arnaiz. "En muchos casos se trata de ordenadores que no están diseñados para estar encendidos todo el día, con una antigüedad que conlleva un riesgo de averías en los discos duros, los sistemas operativos y las aplicaciones, que en muchos casos están desactualizadas; también el uso de *routers* no profesionales y aunque las comunicaciones sean encriptadas en VPN, nos hacen más vulnerables; por lo que es más necesario protegerse".

En el caso de Veritas, una de sus principales apuestas es la última versión de su producto estrella, NetBackup 8.2., que ha puesto especial atención al entorno de la nube, con más de 60 conectores. La marca asegura que la copia de seguridad, el almacenamiento y la deduplicación sean sencillos, todo en un solo dispositivo.