La crisis de la pandemia ha puesto de manifiesto la creciente necesidad de invertir en almacenamiento y seguridad para poder compartir información sensible, ya sea a la hora de hacer una operación de M&A o para protegerse de ciberataques cada vez más comunes. Prácticas como el phishing, ransomware, ataques internos o a proveedores afectaron a siete de cada diez pymes el año pasado en España con un coste medio de €105.000, superando la media mundial de €78.000. Encriptar la información, almacenar en cloud o utilizar el Virtual Data Room adecuado puede ser clave para evitar un desastre que no sólo es económico, también puede causar un daño reputacional irreparable.

"LA SEGURIDAD ES NUESTRA OBSESIÓN, TE PUEDEN ARRUINAR UNA TRANSACCIÓN ROBANDO DATOS Y ESO NO TIENE PRECIO"

// Los datos digitales están expuestos a cada vez mayores amenazas. ¿Qué prácticas deben adoptarse para proteger y controlar los datos?

Las pymes son las grandes perjudicadas en los ciberataques: un 44% de ellas sufrió uno en España el año pasado. Las pymes suelen ser el foco de los cibercriminales porque es más sencillo el robo de datos. Son muchas las que no tienen la suficiente seguridad para hacer frente a estos ataques y la mayoría cree que no van a ser objetivo de las ciberbandas y justo eso es lo que las hace más vulnerables. Para proteger los datos conviene tener en cuenta estas cinco prácticas: **Controlar el acceso a la información:** es muy importante que cada colaborador tenga acceso sólo a la información que necesita para el cumplimiento de sus funciones y que haya acuerdos de confidencialidad. **Necesidad de formación a los colaboradores:** Todos los colaboradores deben ser conscientes de la importancia de mantener los datos bajo protección. **Reducción del uso de dispositivos de almacenamiento**: el uso de pen drives y de discos externos es una gran amenaza a la seguridad, por lo que lo recomendable es utilizar almacenamiento en cloud seguros y hacer copias de seguridad constantes. **Tráfico de los datos encriptado:** ya que la información que viaja por la red hasta su destino, debe estar encriptada para evitar que personas no autorizadas puedan acceder a ella. Lo recomendable es una conexión TLS 1.3 con un tamaño de cifrado de 256 bits, ya que hace muy difícil su hakeo. **Y el cifrado de los datos:** el cifrado transforma los datos en un código que es ilegible a menos que se tenga la clave o contraseña para descifrar y acceder al contenido del archivo.

// Para eso habéis desarrollado Enigma desde Multipartner...

Así es, Enigma es una fuerte e innovadora capa criptográfica adicional que opera en nuestra plataforma de Virtual Data Room, fruto de un contrato de investigación con el Centro de Investigación de Ciber Inteligencia y Seguridad de la Información (CIS) de la Universidad Sapienza de Roma. Esta nueva capa criptográfica pretende ir más allá del cifrado de extremo a extremo (el llamado SSL) y se basa en el principio: "No confíen en nosotros, sino en ustedes mismos". Enigma ofrece la conveniencia económica de un sistema en la nube (SaaS) con la seguridad de una instalación local . Y hay otro aspecto también fundamental que es la eliminación definitiva de todos los datos una vez que finaliza la transacción o el proyecto. Gran parte de nuestros clientes nos preguntan qué es lo que sucede con su información una vez terminado el proceso, cerrado el VDR y recibido el soporte digital documental. Multipartner envía un certificado al cliente, declarando que toda la información y documentos que han sido adquiridos en nuestros archivos han sido borrados y/o destruidos permanentemente.

> "Lo que asusta a las empresas y organismos públicos ya no es sólo la petición de rescate, sino también la amenaza de que los datos robados se difundan por la red"

// ¿Qué herramientas ofrecéis desde Multipartner? ¿Cuál es vuestro valor añadido?

Desarrollamos internamente y ofrecemos a nivel mundial plataformas web basadas en SaaS (Software As a Service), para el intercambio seguro de documentos/proyectos y la gestión de los flujos procesos de trabajo, a través de: **VDR** para el intercambio y la gestión segura de datos y documentos confidenciales; **Virtual Workspace Data Room (WDR)** para compartir documentos de forma segura y **gestionar simultáneamente varios proyectos;** y **Virtual Workflow & VDR integrados** para la organización de actividades y flujos de trabajo en seguridad. Y nuestro valor añadido es lo que nos define: **accesibilidad, disponibilidad, adaptabilidad, seguridad y un precio asequible.** Nuestro objetivo es concienciar a las pymes de que el Virtual Data Room, no es una herramienta cuyo coste pueden permitirse solamente "el bolsillo" de las grandes corporaciones. Un negocio, transacción o proyecto te lo pueden arruinar al secuestrar y robar la información confidencial, y esto no tiene precio.

// Hablando del mercado de M&A, involucráis al comprador, al vendedor y también a los asesores, ¿qué pasa si finalmente no se llega a un acuerdo?

Como proveedor, nos distinguimos por nuestra estrategia no sólo comercial sino también de atención al cliente para satisfacer las necesidades de cada uno de ellos. Tenemos varias opciones convenientes a los requisitos de abrir/cerrar/interrumpir durante un periodo. No sólo la plataforma está hecha a medida sino también la parte contractual dada la exigencia de digitalizarse. Entre otras alternativas tenemos Preliminary Time Gratis, que da acceso al data room sin coste hasta la apertura oficial a los usuarios externos. Y también ofrecemos la opción **Descarga, Elimina y Reutiliza** que permite eliminar parte/todo el contenido de un VDR -para poder reutilizar el espacio liberado en nuevos archivos y proyectos, **sin ningún coste adicional.**

// Imagino que la protección de los datos está más que garantizada...

Imaginas bien, la seguridad es nuestra misión y obsesión. Desde Multipartner utilizamos tanto la anonimización como el cifrado (Enigma) cuando los datos están "en reposo", mientras que cuando los datos están "en tránsito" adoptamos un nivel de cifrado como TLS 1.3. Además, en el caso de las soluciones ofrecidas en la nube, sugiero preguntar siempre al proveedor de la nube dónde se encuentra la granja de servidores de referencia, en relación con la cuestión de la soberanía digital sobre los datos, vinculada a la mayor protección de los datos en la UE. Cualquier solución de un proveedor externo debe garantizar a la organización que ella misma no es vulnerable a los ataques. En el caso de las soluciones SaaS (Software as a Service) como es la de Multipartner, son los proveedores de la nube los que se encargan de la protección de la infraestructura, con continuas auditorías internas y de terceros, comprobaciones periódicas de la infraestructura, así como de parches continuos. Sugerimos verificar también la adopción de algoritmos de detección de cryptolockers en las fases de carga documental y preguntarse si el proveedor VDR hace una vigilancia continua para prevenir ataques.

// Venimos de dos años difíciles de pandemia, en los que muchas empresas quieren reducir costes. ¿Cómo convencerles de que es una inversión?

La importancia de la inversión en almacenamiento en la nube se ha visto reforzada por la pandemia de COVID-19, que nos ha puesto a todos muchas trabas, pero también nos ha enseñado, que lo digital es una oportunidad que hay que aprovechar. Muchos empresarios siguen siendo reacios a sacar los datos fuera de los límites físicos de la empresa por miedo a perder el control sobre ellos, lo que hay que cambiar es precisamente la forma de pensar en los datos como algo que reside en una ubicación física bien definida. La nube permite romper estos límites al introducir un nuevo concepto de distribución y redundancia de datos, reduciendo así el riesgo. La mayoría de ataques que sufren las empresas se realizan a través del email corporativo, que con el aumento del teletrabajo se ha convertido en la primera vía de entrada, junto con los ataques a los servidores en la nube, a los servidores corporativos y a los móviles, tanto personales como de empresa. No sólo eso, sino que los riesgos también evolucionan: lo que asusta a las empresas y organismos públicos ya no es sólo la petición de rescate, sino también la amenaza de que los datos robados se difundan por la red. Los efectos de un ataque son importantes tanto en términos de costes como de daños de imagen y pueden ser tan devastadores que una empresa no pueda recuperarse.

// ¿Los fondos Next Generation de la UE pueden ayudar a este proceso? ¿qué otras ayudas hay?

La digitalización en España para pequeñas y medianas empresas es un reto mayúsculo. Según el Índice de la Economía y la Sociedad Digitales (DESI) supervisado por la Comisión Europea,

Mª del Mar García Rodero
Manager Spain & Latam de
Multipartner

España está en el puesto 16 de los 27 de la UE, y ligeramente por debajo de la media. Y para muchas pymes afrontar ese coste es muy complicado tras la Covid19, por lo que los fondos 'Next Generation UE', conllevan una gran ayuda para este tipo de empresas. En España, estos fondos europeos se ven canalizados a través del programa Kit Digital, dotado con más de €3.000M para la digitalización de autónomos y pymes de entre uno y 49 empleados. A finales del mes de Julio se anunció el Programa RETECH, que invierte €530M del Plan de Recuperación en 2022 y 2023 para desplegar redes de proyectos tecnológicos y transformadores en el área digital. La exigencia del mercado y de los consumidores están cambiando las reglas de juego. Por lo que la innovación digital ya es una exigencia y no una posibilidad. Adaptarse, renovarse y actualizarse es un requerimiento y no una opción para tener viabilidad y poder competir. &