Texto Laura del Río
Fotografía Santiago Ojeda
Vídeo Jorge Pariente

LA SECURIZACIÓN NECESITA DE FORMACIÓN

Conocer las vulnerabilidades para hacerse fuerte

La tecnología ha avanzado a pasos de gigante durante los últimos años y la rueda no parece tener visos de frenarse. Que cada vez confiemos más en la tecnología para gestionar todos los ámbitos de nuestra vida, personal y empresarial, convierte al terreno digital en un campo de minas donde los ciberatacantes están al acecho de los que no protegen sus datos. Para saber en qué estamos fallando y en qué hemos acertado, Computing se ha reunido con los proveedores Check Point, HP, Micro Focus y T-Systems; así como con clientes de diversos sectores de actividad en Madrid.

Si bien es cierto que la sofisticación de los ataques ha aumentado, el problema no es tanto de complejidad, como de falta de protección al prescindir de herramientas que las compañías "ya no consideran útiles", hasta que las brechas de seguridad salen a relucir. "WannaCry se podía haber evitado con tecnología de hace diez años, por ejemplo"; por este motivo, más que adquirir muchas soluciones, "hay que hacer una labor de concienciación para que se utilicen las que ya están implantadas". No saber cómo utilizar estas herramientas o incluso desconocer que están a nuestra disposición, son razones de peso por las que la seguridad en las empresas, en ocasiones, se hace insuficiente.

A la hora de sacarle el máximo partido a la infraestructura que se posee es fundamental el 'mentoring' por parte del proveedor y, después, contar con el talento necesario para desplegar todas sus capacidades. Por este motivo, es vital elegir un proveedor o integrador que sepa acompañar a la empresa en el proceso. "Las grandes compañías dan el primer paso de adopción de herramientas y talento, pero luego no lo emplean; y las pymes, muchas veces, no pueden adoptar ni una cosa ni la otra". En este contexto, la conclusión que extrajo Juan Cobo, jefe del Departamento de Seguridad de la Información de Ferrovial, es que "la gestión

MARIO GARCÍA, DIRECTOR GENERAL DE CHECK POINT

"MUCHAS PYMES NO HAN DISEÑADO NI UN PLAN DE ACTUACIÓN ANTE LOS ATAQUES"

Aunque es difícil hacer una media, se podría decir que las grandes empresas sí han hecho sus deberes en lo que a GDPR se refiere, y lo han hecho, más que invirtiendo en tecnología, aprovechando los recursos que ya tenían y adaptándolos a los nuevos requerimientos. Las pymes son las que más atrás se han quedado en cuanto a su transformación. Muchas de ellas todavía no han diseñado ni siquiera un plan de actuación ante los ataques, ni una forma de contactar con los clientes para la gestión de sus datos, ni un método para llevar el registro de sus acciones.

Esta falta de innovación y actualización de los sistemas deja al descubierto sus brechas de seguridad y las convierte en un blanco fácil, no solo para los ciberatacantes, sino para los auditores y supervisores encargados de poner las sanciones. Sin embargo, las compañías que se han quedado atrás, ya sean grandes o pequeñas, aún están a tiempo de revertir su situación.

MELCHOR SANZ, TECHNOLOGY & PRESALES MANAGER DE HP

"HAY EMPRESAS QUE SOLO SE HAN QUEDADO EN LA PARTE DEL CONSENTIMIENTO DEL USUARIO"

En realidad, el Reglamento General de Protección de Datos ofrece una gran oportunidad para que los sistemas informáticos de las empresas, organismos e instituciones se pongan al día, y garanticen que la gestión de los datos se hace de una manera correcta y eficiente. Existen ciertos aspectos del reglamento que se han tenido en cuenta tarde, por lo que muchas entidades solo han desarrollado la parte del consentimiento de usuario para el uso de sus datos personales, pero no han profundizado en otros procesos igual de relevantes como el borrado seguro del carácter privado, -y cuando el usuario lo considere-, el seguimiento y acceso a la información por parte de los diferentes miembros de la organización o detectar las fugas de información, etcétera.

Desde HP se está haciendo una intensa labor de divulgación para explicar a las compañías cómo establecer estas pautas; por ejemplo, cómo activar la monitorización para la detección de brechas de seguridad o la recuperación automática del sistema.

de la seguridad aún tiene que madurar", y para ello hay que centrarse en "afinar la metodología y los procesos, y dar formación".

Sin embargo, contar con profesionales especializados en seguridad no exime al resto de la organización de conocer y aplicar las medidas pertinentes, "este es un trabajo coral y de nada sirve tener a la gente mejor preparada en un área si el resto de la empresa va por libre", explicó Carlos Asún, jefe de Seguridad de la Información de INITEC Plantas Industriales. Esta afirmación cobra mayor sentido en el mundo conectado en el que vivimos, en el que datos y sistemas están interrelacionados y una brecha de seguridad en un sistema se convierte en una puerta abierta para llegar al último rincón de la empresa.

Llegados a este punto, Pedro Pablo López, gerente de Seguridad, Privacidad y Continuidad Global de Rural Servicios Informáticos (RSI), apelaba a la resiliencia, ya que "nadie está exento de ser atacado ni de caer víctima de la ingeniería social". Lo que hace que una empresa esté bien protegida es su capacidad de reacción y recuperación ante los ataques. Tener un plan de reacción se sitúa al mismo nivel que tener uno de prevención, y este último pasa por "incluir la seguridad desde el primer boceto de cualquier plan o sistema, como una característica innata". Sin embargo, no se puede aplicar la seguridad por diseño a los sistemas de información "sin antes establecer una estrategia de gobernanza de datos".

Las tecnologías de la desconfianza

La cloud es una de las tecnologías más controvertidas a la hora de hablar de ciberseguridad. A pesar de que, durante algún tiempo, muchas

"En ocasiones, el CISO se encuentra delante de los directivos como los 300 contra el ejército de Jerjes"

JAVIER BARANDIARÁN, SECURITY RISK & GOVERNANCE PARTNER MANAGER DE MICRO FOCUS

"GDPR AÚN NO HA SUPUESTO UNA MEJORA PARA EL ÁMBITO 'DATA PRIVACY'"

Lamentablemente, las compañías españolas aún están lejos de poder decir que la entrada en vigor de GDPR ha supuesto una mejora en el ámbito de 'data privacy'. Si bien es cierto que durante 2018 arrancaron muchas iniciativas, -sobre todo en las fases iniciales de la privacidad como pueden ser el control de identidades y el análisis-, las medidas adoptadas para securizar la información son todavía insuficientes a la hora de cumplir con la normativa.

Micro Focus es una compañía que cuenta con una amplia gama de soluciones para apoyar las iniciativas tecnológicas del DPO, desde la identificación y el acceso a la información hasta el cifrado de la misma, y todo ello de una forma holística y coordinada dentro de la organización. La interoperabilidad entre departamentos y herramientas, en este caso, es fundamental.

A pesar de que muchas empresas se encuentren al principio del camino, estamos avanzando y realizando una gran labor de concienciación sobre la inclusión de la seguridad en la forma de trabajar para siempre.

JOSÉ ARIAS, DIRECTOR DE SEGURIDAD DE T–SYSTEMS

"LAS ORGANIZACIONES SE APOYAN EN PROVEEDORES CAPACITADOS PARA SECURIZAR SUS SISTEMAS"

Las grandes empresas son las que cuentan con una infraestructura más preparada para cumplir con los retos de la ciberseguridad. Estas medidas están siendo adoptadas de forma más paulatina por las pymes, ayudadas por compañías suministradoras como T-Systems. Y es que tanto las pequeñas y medianas empresas como las más grandes apoyan sus sistemas de información en nuestros servicios y soluciones. Para la pyme, no contar con los recursos y el expertise suficientes para securizar todos sus procesos son los principales factores que frenan sus planes de ciberseguridad, y las razones por las que acuden a proveedores capacitados para, por ejemplo, migrar sus plataformas a la cloud.

En este sentido, T-Systems es una organización con mentalidad europea, lo que supone una ventaja a la hora de trabajar acorde a los estándares del Reglamento General de Protección de Datos, y también a la hora de que otras compañías confíen en nuestras soluciones y nuestros servicios para proteger su negocio.

"Los proveedores cloud brindan una protección de datos a veces mayor que la de los propios data centers"

empresas se han resistido a subir a la nube por desconfianza, ahora es precisamente la seguridad la razón por la que muchas están alojando sus datos en ella. Los proveedores cloud brindan a las compañías una protección a los datos, en ocasiones, mucho mayor de la que estas pueden disponer en sus propios data center. El tsunami tecnológico al que han tenido que hacer frente las empresas, -que muchas veces las han conducido al caos organizativo y la falta de amortización-, también ha desacelerado la subida a la cloud; unido al "miedo a la compra de una nueva tecnología que muchos expertos TI aún no entendían del todo y a salir de su zona de confort", añadió Óscar Pastor, gerente de Seguridad de Sistemas de Isdefe. No obstante, a medida que todas las compañías empiecen a alojar su infraestructura prácticamente al 100% en la cloud, los ataques irán cada vez más dirigidos y especializados a la nube. "Las amenazas se van profesionalizando y van evolucionando de ataques masivos o generales a otros con objetivos de tecnologías y empresas más concretos".

Otras tecnologías punteras, como Internet de las Cosas (IoT), pueden convertirse en un foco para la fuga de información debido a su interconexión y los datos que se distribuyen entre los distintos dispositivos. Además, cuando las exigencias del negocio aprietan, "se prioriza el cumplimiento de los plazos a crear un producto correctamente securizado", lamentó Javier Tobal, director de Seguridad Informática de Fintonic.

Tecnologías, privacidad, compliance, normativa, etcétera. Son tantos los frentes que las

Banco Inversis,
Manuel Fernández

Ferrovial,
Juan Cobo

Fintonic,
Javier Tobal

organizaciones tiene abiertos, que en ocasiones no pueden abarcarlos todos. "Valorar la criticidad de cada proceso e invertir en mayores recursos evitará que nos sintamos sobrepasados", afirmó Ramón Ortiz, responsable de Seguridad de Mediaset. Así, los CISO se encuentran con dos vertientes: "Por un lado, la protección de los activos, -cuyas medidas pueden ser iguales en muchos sectores en el caso de las amenazas globales, o específicas en el caso de servicios concretos como los cajeros o la banca online-; y por el otro, la de incluir la ciberseguridad en los proyectos tecnológicos y de negocio desde el inicio", indicó Fernando Vega, SCF Global CISO de Santander Consumer Finance.

No obstante, cada vez es más difícil establecer un modelo de seguridad igual para todo tipo de empresas, ya que "cada una tiene una casuística y debe considerar lo que más le conviene". En esta línea, una adecuada asignación de recursos se torna fundamental, y tener en cuenta que, aunque la tarea de divulgación se tiene que extender a toda la organización, son los "empleados que operan con información más sensible o confidencial los que deben tener una formación adicional", puntualizó Alejandro Adalid, Information Security Officer de Siemens Rail Automation.

Recursos, ¿insuficientes o mal empleados?

Atribuir un valor o un potencial impacto económico o reputacional a los activos de la empresa, es clave para hacer entender al CEO la importancia de invertir en securizar ciertos aspectos. "En ocasiones, el CISO se encuentra delante de los directivos como los 300 contra el ejército de Jerjes", comparó Óscar Pastor. Esta cuestión es especialmente significativa a la hora de conseguir inversión por parte de la administración pública, donde toda adquisición está sujeta a unos presupuestos y debe pasar por unos procesos de aprobación más lentos y jerarquizados. Que en ocasiones la AAPP compre únicamente infraestructura que no necesita simplemente para justificar que están invirtiendo en TI, -por ejemplo, ordenadores-; en lugar de trazar un verdadero plan de digitalización, fue una de las causas de queja en el encuentro. Sin embargo, por otra parte, reconocieron que la Administración española está a la cabeza de Europa en cuestiones como la protección de datos, gracias al cumplimiento de la estricta Ley Orgánica de Protección de Datos (LOPD), que le preparó en gran medida para el posterior Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés); a diferencia de lo ocurrido en otros países.

Tras mucho debatir sobre los recursos, David Moreno, director de Seguridad de Sistemas de TI de Tendam, sintetizó que "lo primordial no es contar con recursos infinitos para alcanzar la excelencia, sino contar con los recursos suficientes para realizar lo necesario". Al fin y al cabo, la mala repartición de recursos hace que una misma figura acabe ejerciendo de CIO, CISO, consultor, audi-

Haya Real Estate,
Javier Sánchez Salas

INITEC Plantas Industriales,
Carlos Asún

Isdefe,
Óscar Pastor

Mediaset,
Ramón Ortiz

RSI,
Pedro Pablo López

Santander Consumer Finance,
Fernando Vega

Siemens Rail Automation,
Alejandro Adalid

Tendam,
David Moreno

tor, … "y hasta psicólogo"; y todo ello con la responsabilidad que conlleva, "y que las empresas deben saber reconocer en el perfil de responsable de TI y de seguridad".

"Entender los recursos y los datos de la compañía como propios de cada empleado es el quid de la cuestión", dijo Manuel Fernández, CISO de Banco Inversis, "ya que nadie valora de la misma manera sus bienes personales que los ajenos". Esto explica, en parte, que "las entidades reaccionen más ante medidas coercitivas, -como multas y sanciones-, por las que sufren una pérdida económica; que por respeto a la norma", añadió Javier Sánchez, CISO de Haya Real Estate. "Resiliencia, cultura y cadena de suministro" son los tres drivers que hay que mirar de cerca en el terreno de la ciberseguridad, según el CISO.

En lo que todos coincidieron durante el debate es que en el camino a la madurez digital nos hemos topado con un nuevo reto: la ciberseguridad, el cual estamos consiguiendo pasar a base de prueba-error, la única forma válida de aprender, y la que nos está ayudando a dejar de ser 'salvajes digitales'. ■