

ABENET SOLUCIONES

«LAS CIBERAMENAZAS CADA VEZ SON MÁS INTELIGENTES»

César de la Hoz, director de Desarrollo de Negocio de la firma experta en transformación tecnológica

Extras. Con vocación de ayudar a las empresas a prepararse, protegerse y reaccionar, por ejemplo, ante posibles incidentes de seguridad que pudieran dañar la capacidad operativa o hacer peligrar la continuidad del negocio, Abenet Soluciones se presenta como un socio tecnológico preferente para hacer despegar un negocio. En la Dirección de Desarrollo de Negocio está César de la Hoz.

—¿Qué retos plantea en los próximos años la seguridad digital?

—Cada vez más facetas de la vida de las empresas están afectadas por la tecnología, son numerosos los retos a los que nos tendremos que enfrentar en un futuro reciente. La transformación digital de las empresas va íntimamente ligada a la industria 4.0. Se trata de la irrupción de las tecnologías digitales en los procesos de producción de las organizaciones, la digitalización de estos procesos es una realidad que las distintas empresas y organizaciones están llevando a cabo. Términos como 'big data', robótica o realidad aumentada son algunos de los retos de industria a corto y medio plazo. La industria tradicional siempre ha buscado proteger a las personas de posibles daños físicos, al trabajar y operar con máquinas. Pero la industria 4.0 se sostiene, principalmente, en el mundo tecnológico-digital, esto obliga a un replanteo en materia de seguridad donde se proteja a las personas y a los sistemas tecnológicos. Este es uno de los motivos por los que la ciberseguridad es tan necesaria actualmente.

—También queda sobre la mesa el fenómeno de la hiperconectividad.

—El aumento constante de interconexión entre personas y empresas, el uso masivo de dispositivos móviles y el internet de las cosas está dando lugar a un mundo totalmente interconectado. Gartner prevé que para el próximo año 2020 haya cerca de 20.000 millones de dispositivos conectados. SophosLabs realizó un reciente estudio, en el que se analizaron más de 10 millones de muestras de Android cedidas por los usuarios, desveló que existían 3,5 millones de aplicaciones consideradas potencialmente sospechosas o maliciosas, y de ellas, el 77% eran 'malware'. Todo esto unido exige una mayor y más profunda atención a la ciberseguridad ya que las



César de la Hoz, en las instalaciones de Abenet Soluciones en el Parque Tecnológico de Paterna. DAVID GIMÉNEZ

ciberamezanas cada vez son más inteligentes, autónomas y complejas de detectar que nunca.

—¿A qué tipo de ciberamenazas de nueva generación estamos expuestos?

—En estos últimos años se han visto muchos desastres de ciberseguridad, desde fallos de seguridad en miles de millones de microchips, hasta ataques más elaborados con 'software' malicioso —'ransomware'—. Es precisamente el 'ransomware', la ciberamenaza más de moda a día de hoy. Los ciberdelincuentes están recurriendo a ataques dirigidos de 'ransomware' premeditados con los que están obteniendo millones de dólares en rescates, y donde el modus operandi es bloquear —cifrar— los datos de los sistemas informáticos hasta que la víctima paga un rescate, generalmente con una criptomoneda imposible de rastrear. Un reciente informe de ciberamenazas de Sophos indica que se ha visto un aumento en el número de ataques de 'ransomware' dirigido, que si bien han sido menos numerosos que los ataques masivos del año anterior, son más peligrosos.

—¿Qué es lo que más preocupa a las empresas alrededor de la seguridad digital?

—Lo vemos cada día en nuestros clientes, la ciberseguridad es una de las preocupaciones más importantes que tienen muchos gestores de empresas ya que el robo de datos de una empresa puede suponer un gran trastorno en la gestión diaria de la misma, además de un importante desembolso económico para poder volver a recu-

«La vulnerabilidad de los datos es un problema que afecta a todos los sectores»

perarlos —y sin ninguna garantía de recuperación—. Los avances tecnológicos y el uso masivo de dispositivos hacen que los ciberataques se produzcan cada vez con mayor frecuencia y donde el objetivo es la sustracción de información confidencial para venta a terceros o chantajes a empresas. A estos puntos se une la mayor complejidad y elaboración de estas ciberamenazas que hacen que los recursos de las organizaciones requieran cada vez más especialización, algo que resulta complicado para los departamentos de IT. Por ello, colaborar y confiar en socios tecnológicos como Abenet Soluciones y en soluciones de ciberseguridad completa como las ofrecidas por Sophos es cada día más habitual para las organizaciones.

—¿Cualquier empresa está expuesta a un ataque informático?

—Por supuesto, en las organizaciones empresariales los ciberataques son una realidad a la que ninguna empresa es inmune, por lo que acotar su impacto, responder de forma rápida, recuperar y reanudar la operativa en el menor tiempo posible son objetivos que todas las organizaciones deben tener presente y hacer frente. La seguridad de los datos sigue siendo un problema que afecta a las em-

«Las empresas españolas viven una falsa sensación de seguridad»

presas de todos los tamaños y sectores. No existe un sector concreto al que se le ataque más. El sector de las finanzas está a la cabeza como foco de ataque pero, por otro lado, suele ser el más preparado con diferencia. Compañías de seguros o bancos emplean equipos informáticos de primer nivel, ¿eso significa que no les atacan? No, les atacan todos los días. Las pymes, por desgracia son de las más atacadas y vulnerables, y en muchas ocasiones, es la menor inversión en seguridad que hacen, un factor clave para que no estén tan preparados a la hora de afrontar los retos. Las empresas españolas viven una falsa sensación de seguridad, donde estudios muestran que, a pesar de que el 91,46% tienen algún sistema de seguridad instalado, más del 60% han reconocido haber sufrido algún problema de seguridad informática. Esto no significa que grandes empresas no sean atacadas a pesar de su inversión en seguridad, como hemos podido ver en casos como: Yahoo!, Renault, Tesla o Facebook.

—¿Qué deben hacer las empresas para sentirse más seguras?

—En nuestras reuniones con los directivos y gerentes de las empresas, ellos saben que deben pro-

tegerse, pero no siempre están preparados para maximizar la efectividad de sus sistemas de protección. No se trata de que hacer para que se sientan más seguros, sino de ser y estar realmente más seguros y protegidos ante los ciberataques. Las empresas son cada vez más conscientes de la necesidad de invertir en su ciberseguridad y los datos demuestran la apuesta de las organizaciones por mejorar esta parcela aunque aún hay mucho camino por recorrer. IDC prevé un aumento de más del 7% de la inversión este año en ciberseguridad y un crecimiento sostenido similar hasta 2020. No obstante, la piedra angular de la ciberseguridad son las personas-usuarios porque son el eslabón más débil. Eso también lo saben los malos y por ello dirigen un buen número de ataques a los empleados. El 'phishing', el 'ransomware' o el 'adware' son algunos ejemplos. Los delincuentes saben cómo aprovechar esas debilidades mediante la ingeniería social y otras técnicas de suplantación. Es fundamental que los trabajadores reciban la formación adecuada y la concienciación en seguridad digital, que hagan un uso seguro de la información y de las herramientas que pone a su disposición la organización. Sin embargo, contar con las medidas de protección adecuadas en el entorno digital es una carrera de fondo que requiere una evolución constante y donde la elección del proveedor tecnológico es fundamental. En Abenet Soluciones contamos con un portfolio completo de soluciones y servicios, con los profesionales, la experiencia y el conocimiento para hacer frente a la ciberdelincuencia, y todo ello de la mano del único fabricante líder en los cuadrantes mágicos de Gartner de protección de puestos y redes: Sophos.

—¿Cómo pueden protegerse para asegurar su continuidad?

—Debemos tener presente, que la seguridad al 100% no existe. Desde Abenet Soluciones, hemos establecido una red de alianzas para cooperar con los principales fabricantes y concretamente en el ámbito de la seguridad y con un fabricante especializado como Sophos, líder en seguridad de redes y 'endpoint' de próxima generación y pionero de la seguridad sincronizada, de forma que podamos ofrecer un amplio abanico de soluciones que permiten proteger y optimizar el acceso a los centros de datos, controlar la navegación web, facilitar la entrega de aplicaciones, gestionar los dispositivos móviles y el acceso a puestos de trabajo virtuales y todo ello sin olvidar al propio usuario con herramientas y soluciones de concienciación, formación mediante ataques simulados, etcétera.