Cybersecurity SummIT

Organizado por

Patrocinado por

Junio 2019

La cuarta edición del Digital Enterprise Show ha vuelto a tener récord de visitantes. Se consolida como el evento de referencia en transformación digital y sigue innovando con nuevas propuestas, como Cybersecurity SummIT, un evento dentro del evento, un espacio coorganizado por IT Digital Media Group, a través de sus cabeceras IT User y IT Digital Security, y el propio DES, y que este año ha estado patrocinado por T-Systems.

Cybersecurity SummIT ha sido un espacio de reflexión en torno a los retos a los que se enfrentan los responsables de seguridad de las empresas. Y es que en un momento en que las tecnologías se suceden prometiendo mejoras en productividad, en disponibilidad, en eficiencia…, cada una de ellas conlleva un riesgo, un impacto en la arquitectura de seguridad de las empresas. Ese Big Data que tanto éxito promete, ¿accede de manera adecuada a los datos que debe analizar? El cloud, ¿es amigo o enemigo?; el IoT, que asegura poder revolucionar empresas y ciudades, ¿es seguro?; la Inteligencia Artificial, ¿añade mejoras en la seguridad? Añadamos el cloud, la realidad aumentada y virtual, blockchain, los microservicios… y tenemos un cóctel listo para ser tratado con mucha precaución.

Los retos del CISO se han abordado desde tres perspectivas. Por un lado a través de una ponencia de Dr. Andrew Hutchison, Cybersecurity Specialist at T-Systems Switzerland, y experto en asesorar a los clientes en su estrategia de seguridad, hoja de ruta y soluciones, tras la cual un grupo de CISOs debatieron sobre cómo mantener la seguridad en una era sin perímetro y con tecnologías que avanzan a gran velocidad. Al finalizar la misma se tuvo la oportunidad de realizar una entrevista a Ángel Otermin responsable de Ciberseguridad de T-Systems, a quien preguntamos, entre otras cosas, por el papel del CISO en la era de la Transformación Digital.

Liderando la digitalización con ciberseguridad

En su avance hacia un mundo cada vez más digital todo está plagado de nuevas experiencias y los CISOs deben hacer frente a muchas de ellas. La digitalización transforma las industrias, dota de inteligencia a la logística, se apuesta por la analítica predictiva, por el Smart data, por el IoT o porque los servicios financieros estén tan al alcance de la mano como el móvil.

Así arrancaba su ponencia Dr. Andrew Hutchison, especialista de seguridad de T-Systems Switzerland, durante el Cybersecurity SummIT celebrado en el marco del DES 2019.

Explicaba Hutchison que ahora todo está cada vez más conectado, tanto como para que los fabricantes de coches se planteen cómo asegurar la conectividad o los servicios de entretenimiento, “porque lo creamos o no, los componentes del coche no están securizados de manera predeterminada, y esa es una de las cosas que tenemos que plantearnos: la seguridad por diseño”.

La digitalización está impactando en las industrias de manera muy profunda, decía también Hutchinson, afirmando que la seguridad es una parte importante de esa transformación digital. Uno de los ejemplos tiene que ver con la economía compartida y, de manera más concreta, con el vehículo compartido. Una de las claves del éxito de este sistema es que “cualquiera puede desbloquear un coche” para su uso a través de un lector colocado en el sal-

LIDERANDO LA DIGITALIZACIÓN CON CIBERSEGURIDAD

CLICAR PARA VER EL VÍDEO

picadero, y parece claro que la seguridad, que entre otras cosas sólo permite que acceda al coche quien pueda, se convierte en un habilitador de este modelo de economía digitalizada.

Lo mismo ocurre con las plataformas o las APIs abiertas, que permiten que diferentes actores interactúen con los clientes. Si no hay una seguridad que impida que el resto de los sistemas de esa economía digitalizada quede comprometida, no se puede avanzar. “No digitalization without Security”, aseguraba Dr. Andrew Hutchison, añadiendo que la seguridad debe ser uno de los pilares de una propuesta de valor.

Se preguntaba en el escenario Hutchinson cómo estamos afrontando la ciberseguridad actualmente, y mencionaba algunos de los estándares que establecen la mayoría de las compañías, empezando por la autenticación como una manera de saber quién crea y envía los datos; el control de acceso, o quién tiene acceso a qué datos; la confidencialidad nos permite estar seguros de que nadie puede ver la información, para lo que se aplica el cifrado; la integridad de los datos, que no sean alterados, es también un elemento importante, así como la disponibilidad, o acceso a los sistemas.

> Si no hay una seguridad que impida que el resto de los sistemas de esa economía digitalizada quede comprometida, no se puede avanzar

Como no podía ser de otra manera el CISO juega un papel “absolutamente fundamental” en el proceso de transformación digital, un proceso que le lleva de proteger activos a proteger ecosistemas o de gestionar y verificar la identidad a proteger la privacidad. Todo empieza identificando lo que es estratégico para cada compañía, qué parte necesito tener más segura y escoger al partner adecuado para complementar las necesidades.

De manera más concreta, identificaba Hutchinson algunas de las preguntas que deberían que hacerse los responsables de seguridad de las empresa:

- **¿Cuánto debe hacer internamente vs. externamente?**
- **¿Realmente necesito tener mi propio SOC?**
- **¿Visión global y centralizada o un enfoque federado?**
- **¿Pequeño partner local de seguridad o un partner global?**
- **¿Plataformas SIEM específicas o plataformas de Big Data?**
- **Integración de los entornos de IT y OT o enfoque específico de dominio**
- **¿Visibilidad en las plataformas Cloud o plataformas abiertas?**

Por último, establecía el experto de seguridad de T-Systems tres tipo de personas y, por extensión, de CISOs: los que ven que las cosas pasan; los que hacen que las cosas pasen, o los que se preguntan qué ha pasado. “Espero que todos ustedes sean del segundo tipo”, concluía Dr. Andrew Hutchison.

Nuevos retos del CISO frente a nuevas amenazas

Las tecnologías se suceden prometiendo mejoras en productividad, en disponibilidad, en eficiencia…, pero cada una de ellas conlleva un riesgo, un impacto en la arquitectura de seguridad de las empresas. Ese Big Data que tanto éxito promete, esa Transformación Digital e imparable, ¿cómo está impactando en las empresas? Las amenazas internas, consecuencia de descuidos o mala praxis, que se multiplican con el número de servicios y endpoints desde los que acceder a ellos, pueden controlarse?

A la cantidad de nuevas tecnologías que irrumpen en el mercado, que hay que adoptar de un modo seguro, se suma el número de productos y soluciones de seguridad disponibles, los nuevos vectores de ataque, la escasez de profesionales, casi imposibles de retener, presupuestos contenidos que a veces no cubren todas las necesidades y una industria, la de las ciberdelincuencia, cada vez más innovadora y rentable.

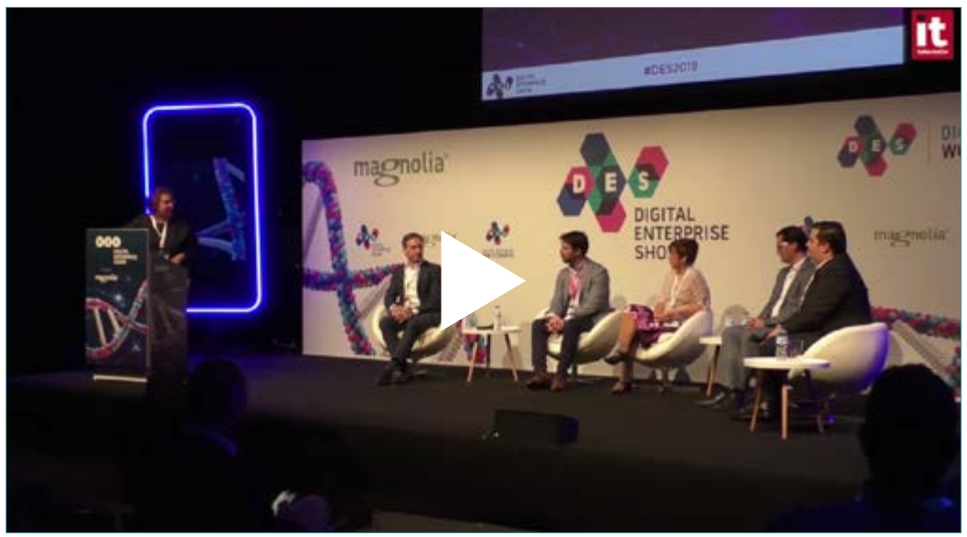
Los retos del CISO fue el tema central de una mesa redonda organizada en el marco del Cybersecurity SummIT, dentro de DES 2019, y patrocinada por T-Systems, y en la que participaron Daniel Zapico, CISO de Globalia; Ángel Otermin, responsable de Cibersecurity de T-Systems Iberia; Mónica de la Huerga Ayuso, CISO de Sopra Steria; José Antonio Rubio Blanco, CISO de la Universidad Rey Juan Carlos y Javier Sánchez Salas, CISO de Haya Real Estate.

"Tenemos que ser capaces de adaptarnos para responder a los nuevos retos", decía Javier Sánchez Salas cuando se planteó qué impacto está teniendo la transformación digital en la seguridad de las empresas. Añadía después del directivo de Haya Real Estate que "la tecnología nos está ayudando a cambiar, debemos ser habilitadores y acompañantes de la transformación digital", una

transformación digital que “en la administración pública va más despacio”, aseguraba José Antonio Rubio Blanco, para después decir que, a pesar de ello, la inversión en seguridad está subiendo y eso es porque la alta dirección está viendo que sin tecnología ningún negocio crece “y la seguridad tiene que acompañar a esa tecnología”.

Para Mónica de la Huerga Ayuso el impacto de la digitalización está relacionado a que se ha pasado de un modelo reactivo a uno proactivo, “a tener identificados un mapa de riesgo para poder ver las tendencias y adaptarnos a los nuevos negocios que están viniendo de la mano de la transformación digital”. Aseguraba Ángel Otermin que la seguridad es uno de los cuatro pilares estratégicos de T-Systems y que la digitalización no sólo ha sido un reto, “sino una oportunidad”. Ponía el ejemplo de la red mundial de honeypost de la compañía “para poder saber cómo atacan los hackers y poder aprender de ellos, y eso es una manera de convertir un reto en una oportunidad”.

También para Daniel Zapico la Transformación Digital es una oportunidad que “facilita más la vida”. Pone como ejemplo que los dispositivos móviles, la mayoría de los cuales incorporan tecnología biométricas, facilitan los dobles factores de autenticación, o que el cloud ya no es un inconveniente “porque está relegando una parte importante de la seguridad. Lo veo como una ventaja”.



NUEVOS RETOS DEL CISO FRENTE A NUEVAS AMENAZAS — **CLICAR PARA VER EL VÍDEO**

GDPR, un año después

Un año ha pasado desde que el reglamento general de protección de datos, o GDPR, sea de obligado cumplimiento. Para muchos supuso sangre, sudor y lágrimas, otros muchos estaban preparados gracias a nuestra LOPD, y algunos sigue en ello…

“Mi experiencia me dice que casi nadie está adaptado”, decía Daniel Zapico. Para Ángel Otermin tanto las posibles multas como el tema reputacional en caso de brecha de seguridad son drivers de la adopción, y aseguraba que en T-Systems hay un framework interno que aglutina los controles de diferentes normativas y se aplican diariamente con programa de Awareness, “lo que transmite confianza a nuestros clientes”.

Apuntaba la CISO de Sopra Steria que GDPR “nos ha servido a los CISOs para incentivar y poner sobre la mesa medidas de seguridad relacionadas con datos y sistemas, y aprovechar la confusión entre el rol del DPO y del CISO para poner un poco más en valor nuestro trabajo”.

> "Tenemos que ser capaces de adaptarnos para responder a los nuevos retos"
>
> Javier Sánchez Salas,
> CISO Haya Real Estate

"GDPR nos ha servido a los CISOs para incentivar y poner sobre la mesa medidas de seguridad relacionadas con datos y sistemas"

Mónica de la Huerga Ayuso, CISO Sopra Steria

José Antonio Rubio Blanco volvió a dar la visión de la administración pública asegurando que a pesar de que se estaba preparado gracias a la LOPD, GDPR "ha sido un cambio radical" al actuar como impulsor de que la seguridad tome más protagonismo y sea un habilitador del negocio. "Sinceramente, el miedo nos ha venido bien a todos", sentenciaba Javier Sánchez Salas, CISO de Haya Real Estate, añadiendo que GDPR ha servido también "para aumentar presupuesto".

Amenazas internas

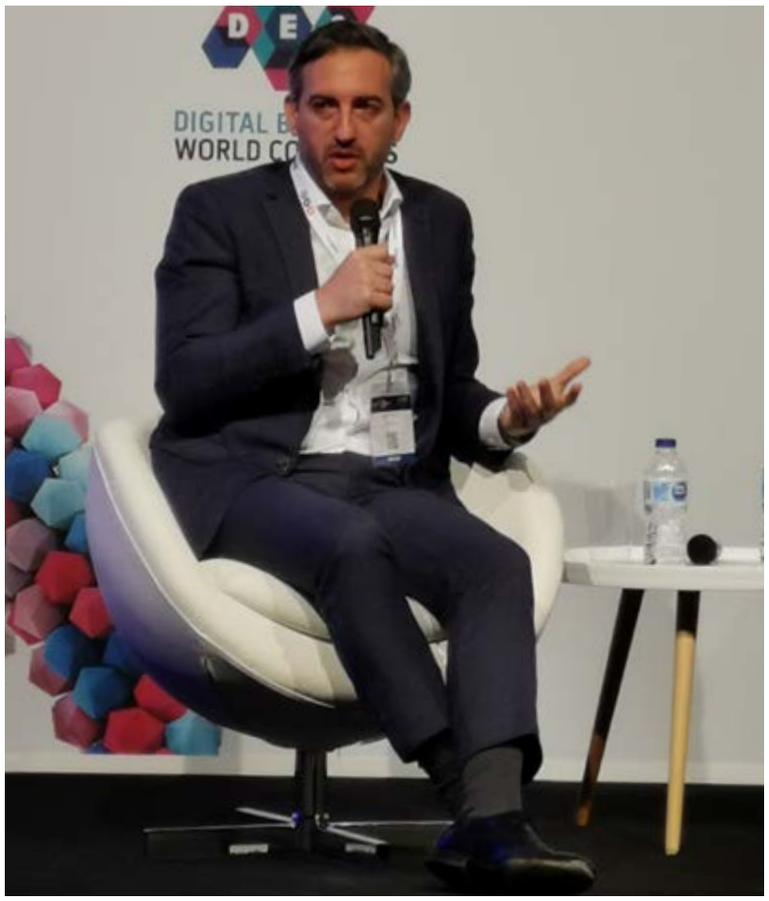
Las amenazas internas se han convertido en un verdadero peligro. ¿Cómo gestionar la conducta de miles de empleados?, ¿de cientos de colaboradores? ¿cómo prevenir un error, una conducta inadecuada?

Javier Sánchez tiene claro que todo lo que un empleado pueda tocar o acceder, es un riesgo, sobre todo "porque los usuarios no tienen por qué saber lo que están haciendo o si están haciéndolo mal, y lo que tenemos que hacer siempre es educarles".

Para el CISO de la Universidad Rey Juan Carlos, "hay que ver las cosas a medio plazo y ser creativos", y explicaba que no basta con dar un curso al año y poner un póster, que hay que ser más proactivos para concienciar y que la gente lo entienda. Mencionaba Mónica de la Huerga Ayuso que el ser humano es impredecible y lo que se puede hacer es "educarles, sensibilizarles con formación, con-

"La alta dirección está viendo que sin tecnología ningún negocio crece "y la seguridad tiene que acompañar a esa tecnología"

José Antonio Rubio Blanco, CISO Universidad Rey Juan Carlos



"Cuando a alguien le das la posibilidad de hacerlo mal, lo va a hacer mal por mucho que se lo expliques"

Daniel Zapico, CISO de Globalia

cienciación, hacer campañas de phishing, eventos como este que permitan a los gerentes y colaboradores saber qué es lo que están haciendo y ser capaces de cumplir con una serie de medidas que no es un capricho del CISO de turno, sino que son buenas para mantener nuestro negocio".

Ángel Otermin afirmaba por su parte que "lleva tiempo adquirir cultura de seguridad" una cultura que se consigue "realizando programas de sensibilidad y formación". A pesar de estar de acuerdo en que la formación y concienciación son importantes, Daniel Zapico, CISO de Globalia, asegura que no funcionan; "cuando hablamos de amenazas internas no sólo hablamos de empleados, hablamos también de clientes. Y cuando a alguien le das la posibilidad de hacerlo mal, lo va a hacer mal, seguro, por mucho que se lo expliques".

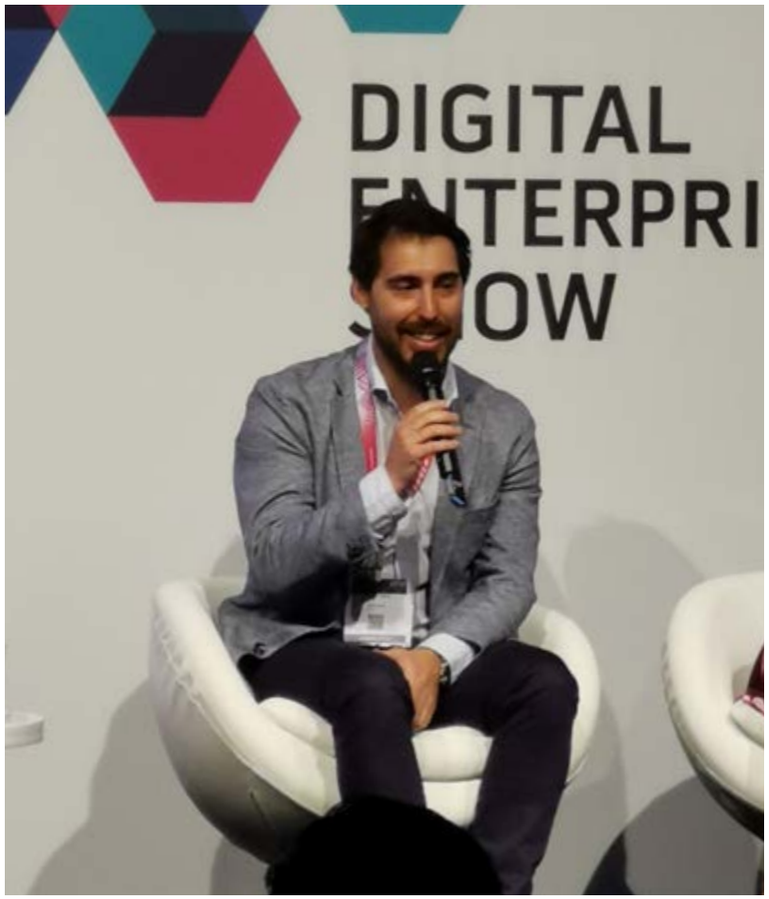
CISO, de stopper a habilitador

¿Cuál es el papel del CISO dentro de las empresas? ¿Cómo se siente tratado? "Yo me siento bastante escuchado, pero no es ni mucho menos lo ha-

Participantes del Cybersecuty SummIT. De izquierda a derecha José Antonio Rubio Blanco, CISO de la Universidad Rey Juan Carlos; Dr. Andrew Hutchison, Cybersecurity Specialist at T-Systems Switzerland; Ángel Otermin, responsable de Cibersecurity de T-Systems Iberia; Daniel Zapico, CISO de Globalia; Mónica de la Huerga Ayuso, CISO de Sopra Steria; Javier Sánchez Salas, CISO de Haya Real Estate y Rosalía Arroyo, directora de IT Digital Security, que actuó como moderadora del evento.

bitual", dice Daniel Zapico, que en su empresa tiene una posición muy alta, "el reporte es al más alto que se puede tener en una compañía, es paralelo al CIO y estoy involucrado en todos y cada uno de los procesos de la compañía". Menciona Ángel Otermin el papel que tiene el CISO no sólo en la protección de la empresa a la que sirve, sino como "una figura que está dentro del negocio para decir cómo un producto o servicio que va a lanzar la compañía puede ser más seguro"; en T-Systems, asegura, "no concebimos la digitalización sin seguridad".

"Que se nos deje de ver como asuntos internos", reclamaba la CISO de Sopra Steria, reivindicando



el papel del responsable de seguridad como una figura de confianza a la que acudir en busca de ayuda. José Antonio Rubio Blanco visualizaba la figura del CISO "como alguien que estaba en una mazmorra, en un sótano, que jamás hablaba con negocio", pero que gracias al Esquema Nacional de Seguridad y a GDPR su papel ha cambiado; "quizá no reporta al más alto nivel, pero sí a un nivel medio, cosa que antes no ocurría".

Javier Sánchez tiene claro el rol del CISO: "Es verdad que cada vez estamos más cerca de negocio, los acompañamos, intentamos ayudarles en la medida de lo posible, pero seguimos siendo stoppers y tenemos que serlo", asegurando que hay que poner pies de plomo y saber en todo momento "a qué problemas de seguridad nos enfrentamos".

Servicios de Seguridad Gestionados

Una de las cosas que ha traído la transformación digital es una oferta mucho más amplia y variada. Ha multiplicado las propuestas, y por tanto dificultado la toma de decisiones, a lo que se suma la escasez

"También hay que ver al CISO como una figura que está dentro del negocio para decir cómo un producto o servicio que va a lanzar la compañía puede ser más seguro"

Ángel Otermin, responsable de Cibersecurity de T-Systems Iberia

de expertos. Los Servicios de Seguridad Gestionados se convierten en una solución a esta situación "aunque entre en juego el riesgo del proveedor", apuntaba el responsable de seguridad de la Universidad Rey Juan Carlos, quién además recordaba que es importante saber dónde se invierte y lo que se necesita internamente.

Mónica de la Huerga Ayuso recodaba en su intervención el problema de falta de profesionales y la necesidad de saber hasta dónde se puede llegar para tomar una decisión lo más correcta y alineada con las necesidades que se tienen.

"Sí a los servicios gestionados", decía Ángel Otermin. Explicaba el directivo de T-Systems que si bien la parte del gobierno de la seguridad debe estar en la empresa "no tiene sentido que lo esté la parte operativa", añadiendo que la seguridad como servicio "es un tema de confianza. Es cuestión de romper la barrera, de racionalizar, y el secreto es conseguir un partner de confianza".

"Tiene sentido hacer outsourcing de muchos procesos, en particular porque suele ser complicado encontrar el conocimiento específico, profesionales", apuntaba Daniel Zapico, coincidiendo con sus colegas.

Adopción de nuevas tecnologías

Llevamos hablando de cloud muchísimo tiempo y hemos terminado afrontando tanto el cloud. Se habla muchísimos ahora de inteligencia artificial, de machine learning, de analítica... Se pregunta a los expertos si realmente se están adoptando este tipo de tecnologías para la seguridad, o por el momento se habla sin que se estén dando pasos.

Decía el CISO de Globalia que sí se adoptan, pero en productos, y no en las compañías, algo que confirma Ángel Otermin al señalar que T-Systems ya está trabajando esas tecnologías en productos para sus clientes. Mónica de la Huerga Ayuso apuntaba que se están aplicando en todos los servicios gestionados, pero que "a nivel de empresas no se está poniendo en marcha ni machine learning ni inteligencia artificial salvo que sea parte de su negocio".

El CISO de Haya Real Estate coincidía en que "esa analítica e inteligencia artificial está a nivel de producto", mientras que Javier Sánchez asegura que sí se está utilizando. "Yo ya la tengo", decía Javier Sánchez, aunque no desde el punto de vista de seguridad, sino en temas de marketing y orientado a modelos predictivos.

“No creemos en la cultura del miedo”

Ángel Otermin, T-Systems

Transformación Digital sí o sí. Quizá sea complicado, pero no hacerlo es peor. Hace tiempo que la mayoría de las empresas iniciaron su ‘digital journey’, un viaje que aún no ha terminado y que ha impactado en todas las áreas del negocio, incluida la encargada de mantener la empresa segura, o cibersegura.

La nube, la movilidad, los modelos as-a-service, terminaron por difuminar ese perímetro que intentaron crear los firewalls hace una década. Los responsables de seguridad, los CISOs, no sólo se enfrentan a nuevas tecnologías, sino a una gran cantidad, y variedad de endpoints, a servicios que se acceden desde cualquier sitio, en cualquier momento y por diferentes perfiles.

Sobre los retos del CISO hablamos con Ángel Otermin, responsable de Ciberseguridad de T-Systems, durante el Cibersecurity SummIT, un evento celebrado en el marco de DES 2019. Asegura Otermin que los retos del CISO son muchos. Habla de la Transformación Digital como una oportunidad que obliga a ser muchos más innovadores; “tenemos que tener en cuenta muchos servicios que hay que securizar” y aplicar “el security by desing” que permita partir con cierto grado de garantías. Asegura el directivo que “con T-Systems siempre procuramos que todos los productos y servicios se securicen por defecto y por diseño”.

Stoppers, así han calificados a muchos responsables de seguridad que veían alarmados cómo algunos servicios que venían de la mano de la transformación digital les hacían perder el control. Ahora vienen a ser los habilitadores. ¿Cómo se ha producido ese cambio? Dice Ángel Otermin en la entrevista que el cambio “se ha producido por la propia tecnología”. Asegura que “la digitalización lo ha invadi-

“NO CREEMOS EN LA CULTURA DEL MIEDO” ÁNGEL OTERMIN, T-SYSTEMS

CLICAR PARA VER EL VÍDEO

do todo” y que ahora se ve como valor añadido que los productos y servicios incorporen seguridad, “que haya un doble factor de autenticación, por ejemplo, que las comunicaciones sean cifradas”. Es ahora cuando “negocio se acerca a nosotros para ver cómo podemos enriquecer esos productos”.

Teniendo entonces en cuenta que la digitalización lo ha invadido todo, que cada vez son más las tecnologías a tener en cuenta, las soluciones que poder implementar, ¿qué papel juegan los servicios gestionados? Para el responsable de ciberseguridad de T-Systems los servicios gestionados son “una herramienta que nos permite tener una ayuda externa” en medio de restricciones presupuestarias, de equipos limitados y falta de skills; “este tipo de servicios nos permiten tener un personal especializado y que las empresas se dediquen a lo que se tienen que dedicar, que es a su negocio”.

Son muchos los estudios que recogen que actualmente la mayoría de las amenazas de seguridad no llegan a las empresas desde fuera, ni siquiera a través de malware, sino de dentro, tanto de los empleados como de los socios. A veces por errores y en ocasiones por conductas delictivas. Nos explica Ángel Otermin que desde T-Systems de hace frente a esta situación de dos formas. Por un lado mediante la educación y concienciación, “porque no creemos en la cultura del miedo sino que las personas entiendan la problemática, se les eduque y poco a poco se vaya creando una cultura segura que termine calando”. Y luego con medidas tecnológicas que faciliten que las personas puedan actuar de la manera más segura y fácil.

> "Es ahora cuando "negocio se acerca a nosotros para ver cómo podemos enriquecer nuestra oferta con seguridad"
>
> Ángel Otermin, responsable de Ciberseguridad de T-Systems

Enlaces de interés...

- Toda la cobertura del DES a tu alcance
- #DES2019: T-Systems destaca la importancia de la seguridad TI en la era digital
- Reyes Maroto muestra la apuesta del Gobierno por la digitalización de las empresas en #DES2019