Texto
Andrea Gómez

SESIÓN SOBRE CIBERSEGURIDAD Y REPUTACIÓN CORPORATIVA

"Los vectores tradicionales son los principales focos de riesgo"

"Estamos obligados a tener un modelo integral de gestión y una visión global del riesgo"

Un año más, la Asociación @aslan abrió sus puertas en el Palacio Municipal de Congresos de Madrid de IFEMA, con la intención de informar y presentar las nuevas tecnologías que van a acelerar la transformación digital de las compañías, preparándolas así para la nueva economía digital. El evento, como es habitual, se iba a dividir en dos jornadas pero, siguiendo las recomendaciones anunciadas por el Gobierno y el Ministerio de Salud, que decretaban la suspensión de todos los eventos culturales, de ocio y similares con una asistencia superior a las 1.000 personas en las zonas con una transmisión alta, se tuvo que cancelar la segunda de ellas.

En la primera jornada del foro ASLAN 2020 se puso el foco en las soluciones y herramientas capaces de acelerar la transformación digital de las compañías. El evento contaba con 7.000 visitantes inscritos, más de 120 stands y 150 ponentes, que centraron sus charlas en temáticas variadas como la seguridad, el almacenamiento cloud, la movilidad y redes, los centros de datos, las nuevas tendencias en IoT, y en un inesperado pero conveniente protagonista, el puesto de trabajo digital y remoto para favorecer el teletrabajo, claramente propulsado por el virus.

Computing se encargó de moderar distintas charlas. La primera del día, 'La ciberseguridad y la reputación corporativa', fue conducida por Ambrosio Rodríguez, director de Computing, y en ella participaron Iván Sanchez, director de Seguridad de la Información de Sanitas; Juan Cobo, Global Ciso de Ferrovial; Ramón Ortiz, Ciso de Mediaset; y Alberto López, director de Sistemas de Información y Ciberseguridad del Grupo Comar.

Antes de dar comienzo al debate, Pedro Martinez, business development manager de Aruba, quiso hacer una pequeña introducción sobre el tema. "Para Aruba, es primordial en materia de ciberseguridad tener una alta visibilidad de los dispositivos y usuarios conectados a la red, ya que eso nos permite adaptar las medidas de pro-

tección a las necesidades de cada caso concreto, anticiparnos a los problemas y dar respuestas más rápidas". Sacando a colación el tema del día, "con el coronavirus, la ciberseguridad tiene más relevancia que nunca, ya que el teletrabajo va a forzar el diseño de planes de seguridad para que esta no se vea comprometida".

Planes de actuación

Entonces, ¿cuáles son los planes concretos que tienen las compañías en estas áreas? "Para la gran empresa española, la ciberseguridad es siempre una prioridad de primer nivel", contaba Juan Cobo, de Ferrovial. "Nuestra aproximación es global, tenemos presencia y operaciones en muchos países distintos, lo que nos obliga a disponer de un modelo global de gestión y una visión global del riesgo". En sus palabras, "hoy en día no se puede vivir dando la espalda a la ciberseguridad, el pensamiento no es 'esto me puede pasar', sino, 'esto me va a pasar y tengo que estar preparado para responder cuando pase".

"En Sanitas acometimos el camino hacia la digitalización hace unos años, y una de las claves a la hora de gestionar la transformación fue la seguridad de la información", explicaba Iván Sanchez. "Hicimos un plan a 3 años, que el consejo acogió muy bien porque era consciente del riesgo. Nuestro sector tiene datos muy sensibles y una regulación muy alta, por lo que se decidió que proteger esto era un valor. Dentro de la organización estamos todos de acuerdo con que el riesgo existe".

"La regulación en el sector del juego es también muy alta y estricta, ya que nosotros tratamos con muchos datos personales desde el momento que una persona entra al casino", coincidía Alberto López, por parte del Grupo Comar. "Antes la seguridad se regía por un modelo tradicional que cubría el endpoint y el perímetro, pero eso ha quedado obsoleto, por lo que nuestra visión es ahora 360, cubriendo la seguridad desde todas las áreas, y desde dentro. Ya no nos planteamos si vamos a ser atacados, sino cómo resolverlo cuando lo seamos".

Por su parte, Ramón Ortiz, desde Mediaset, indicaba que cualquier compañía, "independientemente del tamaño, con experiencia en la gestión del riesgo ciber, tiene un plan trazado desde hace ya tiempo; la cuestión es seguir realizando continuamente revisiones sobre dicho plan".

La conversación sobre el ciberriesgo ha evolucionado mucho a lo largo de los años, parece ser que ya casi todas las compañías son conscientes de la amenaza que supone, pero ¿han

evolucionado también los riesgos? "Las amenazas han ido variando y creciendo a lo largo del tiempo, pero lo curioso o lamentable es que los vectores de entrada son los mismos que los de hace años. El correo electrónico es la primera fuente de entrada y es una vulnerabilidad conocida por todos desde hace mucho tiempo, pero que sigue siendo explotada porque continúa siendo rentable", narraba Juan Cobo. En esta misma línea, Iván Sánchez subrayaba que "los ataques a los correos electrónicos siguen funcionando bien porque van por volumen, todos usamos las mismas tecnologías, por lo que esa homogeneidad muchas veces nos pone a todos a la vez en el foco del riesgo".

"Siguen existiendo fallos en las medidas clásicas de prevención y contención contra el riesgo", coincidía Ramón Ortiz, "ocuparse de las prácticas clásicas sigue absorbiendo mucho tiempo, por eso es fundamental que los empleados y directivos conozcan y sepan lidiar con los riesgos que están en sus manos, para ello la formación y la concienciación son primordiales".

"A nivel de infraestructura puedes gastarte millones en nuevas tecnologías predictivas, pero al final las personas siguen siendo el gran foco de riesgo", afirmaba también el representante de Grupo Comar, Alberto López.

Como conclusión, quedó claro que la ciberseguridad se encuentra en el primer nivel de prioridades de la mayoría de las organizaciones, pero a la vez, la creciente digitalización aumenta también el riesgo, puesto que no todos los puntos que conforman esa nueva red son capaces de ser gestionados, pero esto es un trabajo que se tendrá que hacer de forma unida, y sobre todo, concienciada. ■

"Es fundamental que los empleados y directivos conozcan y sepan lidiar con los riesgos que están en sus manos"