Foto & vídeo
Santiago Ojeda y Carlos Entrena

Texto
R. Contreras

ES CLAVE QUE LA DIRECCIÓN DE LAS COMPAÑÍAS SE IMPLIQUE A FONDO

Comunicar y gestionar una crisis de TI

<< ¿Están preparadas las compañías españolas ante un potencial ataque de ransomware o una caída del servicio por causas naturales o un apagón? ¿Cómo gestionan y comunican una crisis de TI? Estas y otras cuestiones abordan los invitados de Computing en el siguiente artículo.

Todo responsable de seguridad ha tenido pesadillas temiendo ese día fatídico, en el que los sistemas de su organización dejan de funcionar. ¿Puede tratarse de un ransomware que le ha cifrado la información y ha dejado inutilizados los archivos de los empleados? ¿Puede ser una caída del sistema por causas ambientales imprevistas? ¿Puede ser un corte de suministro eléctrico ahora que todo el planeta tiembla con ese 'apagón digital' que planea sobre nuestras cabezas? Todos estos escenarios no son de una película de Spielberg, son, por desgracia, moneda corriente en las organizaciones sin distinción de nacionalidad ni de sector de actividad. Por tales razones, la gestión de una crisis de TI es una tarea que deben plantearse las compañías ante esta creciente suma de riesgos potenciales. Y ha sido esta gestión de la crisis el hilo central del encuentro organizado por Computing con la participación de Everbridge (firma que nació después de los atentados del 11 S especializada en comunicación y gestión de crisis) y SIA (empresa de ciberseguridad del grupo Indra) que tienen mucho que decir en la continuidad de nego-

cio. Un grupo de responsables tecnológicos de grandes cuentas han puesto sobre la mesa su visión en torno a este asunto y cómo asumen estos riesgos desde el punto de vista estratégico de sus compañías.

Agencia Tributaria

La Agencia Tributaria es una institución que no puede permitirse veleidades en este ámbito. José Borja Tomé, director del Departamento de Informática Tributaria de la AEAT, es consciente de la necesidad de cubrir todos los flancos que conforman la organización. "Yo diría que en ciberseguridad hay que hacer todo lo que puedas, cubrir todos los huecos de la mejor manera posible mediante políticas de seguridad, procedimientos, personas y organización".

Como explica, nadie es inmune a las amenazas: "Hay un aumento de la complejidad de la tecnología, mayor exposición a los riesgos y una tendencia creciente de los ciberataques con independencia del teletrabajo". Según su opinión, hay que establecer mecanismos de respuesta ante las crisis, que son de carácter organizativos para determinar cómo actuar en este tipo de situaciones. No solo hay que mirar lo que viene de fuera sino analizar la parte interna de la organización, poniendo énfasis en una visión corporativa completa y no en una pieza concreta del puzle.

Bergé es una compañía comprometida con la seguridad, de hecho, cuenta con la figura de CISO independiente, pero alineado con la visión global de la organización. Como explica Rafael Abreu Padín, director de Proyectos Estratégicos: "Tratamos de sistematizar el trabajo, en continuidad de operaciones, ciberseguridad y en todo lo que ronde a este mundillo de la seguridad". La firma se rige bajo un plan director de dos años en virtud del cual se ha invertido en hardware, pero sobre todo "estamos invirtiendo en concienciación de la gente, formación, training de comunicación, prueba de procedimientos, simulacros de ataques…". Unas tareas que a veces resultan complicadas de poner en práctica por tratarse de una firma que presta servicios 24x7, y no siempre es fácil encontrar la ventana oportuna.

"Es un tema de cultura", así resume el problema José Miguel Gil, IT Manager Holdings Spain de ArcelorMittal. "En nuestra empresa siempre ha sido una prioridad cómo responder a una situación de crisis. La ciberseguridad se integra en el esquema de seguridad completa de la compañía. Estamos desarrollando procedimientos y trabajando con los usuarios sobre cómo enfrentarse a una situación inesperada o sospechosa".

A tenor de lo expuesto en la mesa, el concepto de ciberseguridad está madurando. Como explica, Javier Sánchez Salas, CISO de Haya Real State: "En nuestro caso no somos regulados, pero nuestros clientes son bancos, con lo cual tenemos una doble 'regulación'. Llevamos tiempo yendo a máximos en la gestión de crisis y en estos dos últimos años hemos dado un paso adelante explicando a los usuarios que la continuidad de negocio depende de toda la empresa, creando conciencia de grupo e invitándoles a participar activamente". Sánchez Salas destaca que en los entrenamientos que realizan cuentan con el apoyo de la dirección: "en todos los comités de crisis, el primer convocado es el CEO y esto ayuda a una alta participación".

El caso del BBVA

En una entidad como el BBVA se trabaja intensivamente desde la prevención del personal. "Es fundamental que las personas estén preparadas y hacemos continuamente simulacros de phishing para entrenarlas y sepan identificar un vector de entrada como es la ingeniería social. También trabajamos en la gestión y la respuesta ante incidentes. Con la alta dirección hacemos ciberejercicios, poniéndola en situaciones reales para reaccionar de una forma adecuada ante situaciones como el fraude del CEO, ataques a la cadena de suministro o cartera de proveedores. Ponemos énfasis en la concienciación de las personas que tienen capacidad de hacer pagos para que utilicen procedimientos de doble check y conozcan bien estos fraudes", relata Laura del Pino, responsable de Seguridad Corporativa de Ingeniería de BBVA.

Sin ser un sector tan regulado, la educación es uno de los principales objetivos del cibercrimen. Así lo constata Carlos Garriga, CIO de IE University, "las universidades públicas han sufrido un gran volumen de ataques, me consta que colegas CISO y responsables de TI han pasado por verdaderos problemas. No se trata de un tema puntual ni localizado en nuestro país, habernos abierto a la educación online ha generado un mayor número de vectores de ataques. Antes la formación por Internet era marginal, ahora ha aumentado el atractivo para los cibercriminales".

El sector industrial es el que más puede temer una caída de servicio por sus consecuencias

> **"No solo hay que mirar lo que viene de fuera sino analizar la parte interna de la organización"**

ÁNGEL GONZÁLEZ DEL RÍO, HEAD OF BUSINESS CONTINUITY DE SIA (GRUPO INDRA)

"NO SOLO ES IMPORTANTE TENER UN BUEN PLAN, SINO TENERLO PROBADO"

En los últimos tiempos los vectores de riesgo a los que se enfrentan las compañías están cambiando. El número de ciberataques es cada vez mayor y la especialización de los atacantes es más sofisticada, lo que provoca que los daños sean más impactantes. Todo ello obliga a que las compañías tengan que reestructurar sus planes de continuidad de negocio, incorporando estos factores comentados. No solo es importante tener un buen plan, sino tenerlo probado. Igualmente, cuando abordamos una situación de indisponibilidad es importante tener definido un buen proceso de crisis. Una gestión de crisis que nos va a garantizar que el impacto sea el mínimo y en el menor tiempo posible. A ello se une que las compañías son cada vez más diversas: ya son multipaís, con la información repartida en diferentes CPD, con algunos procesos externalizados y se enfrentan a infraestructuras en la nube. Hay que evitar los procesos manuales y tenemos el reto de poder automatizarlos. Hay que tener un plan de crisis probado y automatizado para optimizar la continuidad de negocio y ahí es donde SIA puede ayudar a las empresas.

JOSÉ MANUEL VILLANUEVA, COUNTRY MANAGER DE EVERBRIDGE EN ESPAÑA Y PORTUGAL

"RESPONDEMOS CON CONOCIMIENTO Y PRECISIÓN ANTE CUALQUIER EVENTO CRÍTICO"

Con la llegada de Internet, los smartphones y las tabletas, la informática ha ido llegando a muchos más usuarios. Cada día las empresas desarrollan soluciones y servicios que hacen que nuestra vida sea mucho más fácil. Pero al otro lado, están los departamentos de TI de las organizaciones, donde su actividad se ha complicado porque han tenido que desarrollar aplicaciones e integrarlas y los sistemas son mucho más frágiles y complejos. Con el añadido de los ciberdelincuentes, que nos atacan con insistencia con malware y ransomware. Por todo esto, es necesario adoptar estrategias e implementar herramientas para poder tener una gestión de crisis perfectamente diseñada, para que cuando se produzca una caída de sistema e interrupción del servicio, sea capaz de tener una comunicación eficaz por diferentes canales para poder desarrollar planes de gestión de crisis y poder mitigar ese impacto. En Everbridge hemos desarrollado una plataforma que permite a nuestros clientes poder responder con conocimiento, confianza y precisión ante cualquier evento crítico (caída del servicio, deficiencia de este o una interrupción), que se le pueda presentar.

negativas para la sociedad en general. Raquel Martínez, responsable de Continuidad de Negocio de Red Eléctrica, explica que su empresa tiene experiencia en la puesta en marcha de simulacros, especialmente en la parte industrial. "Con la pandemia, el perímetro se ha abierto y hemos trabajado en los procedimientos. Lo básico es entrenar los roles y, dependiendo de las funciones, poner en marcha la comunicación sin perder de vista la parte regulatoria". Hay que dejar bien definido a quién comunicar en caso de incidente grave y escalar para completar la gestión de la crisis. Raquel Martínez incide en la importancia de la comunicación externa, pues de ella dependerá el impacto en la reputación de la compañía.

En este aspecto de la comunicación trabajan desde RTVE, según relata Pere Vila, director de Estrategia Tecnológica e Innovación Digital: "Hacemos cursos para directivos de cómo hacer un mensaje estructurado, con grabaciones en las que intervienen asesores especialis-

ASISTENTES

1 José Borja Tomé, AEAT | **2** Juan Miguel Gil, ArcelorMittal | **3** Antonio Crespo, Asociación Española contra el Cáncer | **4** Laura del Pino, BBVA España | **5** Rafael Abreu Padín, Bergé y Compañía | **6** Javier Sánchez Salas, Haya Real Estate | **7** Carlos Garriga Gamarra, IE University | **8** Jesús Garrido, INTA | **9** Francisco Alonso Batuecas, Ministerio del Interior | **10** Raquel Martínez, Red Eléctrica | **11** Pere Vila, RTVE

tas. Somos una infraestructura crítica y esto condiciona nuestros procedimientos externos. Nuestro director de Seguridad está en contacto con el CNI". La complejidad del ente es que tanto los servidores y las redes de TVE son diferentes de las de RNE, son sistemas aislados cada cual con sus propios protocolos.

En la AAPP no hay tantos recursos como en el sector de la gran cuenta privada, esa es al menos la sensación de Jesús Garrido, CIO del Instituto Nacional de Técnica Aeroespacial (INTA). "No somos una empresa como un banco, que comparte servidores, estamos en 17 comunidades autónomas y 300 organismos, cada uno con diferente presupuestos y particularidades. Lo que sucedió al SEPE es una gota de agua de lo que puede venir". Garrido opina que el Esquema Nacional de Seguridad se ha quedado obsoleto con las nuevas ciberamenazas y que los equipos de trabajo están desbordados y muchos de ellos no han podido ni redactar sus planes de continuidad.

Ministerio del Interior

El Ministerio del Interior tiene un doble papel: "Investigar a los malos y protegernos de lo que hacen los malos, un doble trabajo que se retroalimenta", afirma Francisco Alonso, jefe del Área de Infraestructura y Seguridad. El experto siente que la "ciberseguridad es una sensación. El reto es encontrar el equilibrio para interactuar en el metaverso de una forma segura". En Interior protegen sus infraestructuras críticas y prestan servicios a todos los cuerpos de seguridad, cualquier caída les puede impedir trabajar y esto toca con la ciberseguridad ciudadana. "Dotar de herramientas al ciberpolicía es difícil, pero, aun así, se hacen cosas. La gestión de crisis la llevamos trabajando desde 2005, tenemos 'callo' para afrontar procesos como puedan ser unas elecciones, pero nunca hay que bajar la guardia".

Una gran verdad es que el peligro es constante y no distingue entre sus víctimas. Antonio Crespo, director de Tecnología, Data e Innovación Digital de la Asociación Española contra el Cáncer, se lamenta del "mal gusto" de estos atacantes que no discriminan ni con asociaciones benéficas ni hospitales. "En el área de seguridad estamos creciendo cada vez más, pero nunca estamos lo suficientemente seguros. Subes al siguiente escalón en una carrera sin fin que hay que aguantar. El problema es que hemos ampliado los perímetros de nuestros educadores, que se cuentan por miles, y nuestros profesionales tienen un alto grado de gestión de datos sensibles, algo que nos preocupa". ■