Especialistas en recuperación de datos, los 'salvadores' de la información

Dejamos atrás los meses de verano, tan tranquilos para algunos y verdaderas pesadillas para otros. Nos referimos a todos aquellos que, bien por trastear demasiado su PDA, bien por dejar el portátil en el coche a 48 grados de temperatura, bien porque se le ha caido la bebida en el móvil o bien porque sus instalaciones han sufrido una subida de tensión por la descompensación de energía –entre otros muchos ejemplos-, han perdido toda la información que tenían en su dispositivo electrónico. Parece que se acabe el mundo, pero aquí entran los "recuperadores de información", esos profesionales que, en la mayoría de las ocasiones, son capaces de hacer milagros.

La magnitud que está tomando la preocupación por el tratamiento y el almacenamiento de la información digitalizada, tanto en empresas como en nuestros hogares, es motivo más que razonable para plantearse qué ocurriría si uno se quedase de repente sin los datos que tiene en su agenda electrónica, en su ordenador o en su móvil. Red Seguridad enfocó, en esta ocasión, su desayuno de trabajo a la recuperación de datos, con el fin de aportar su granito de arena en la concienciación del valor que tiene, hoy día, la información.

Para ello, Manuel Ballester, director de la publicación, moderó un intenso debate fomentado por las opiniones de unos invitados doctos en la materia y con enriquecedoras visiones del asunto. Los protagonistas del encuentro fueron: Gianluca D'Antonio, director de Seguridad de la Información y Gestión de Riesgos de Fomento de Construcciones y Contratas (FCC) y presidente de ISMS Forum España; Carlos Cantero, experto en recuperación de datos de DataZenter; César Comas, representante de Jazztel; Gustavo San Felipe, responsable de Seguridad de Acens; Andrés Morales, responsable de Seguridad de Albatros; y Ramón Planas, director de Marketing de Spamina.

especial recuperación de datos

Antes de llegar a hablar de cualquier recuperación de datos, Gianluca D'Antonio, de FCC, abrió el turno de intervenciones recordando que el "indicador de madurez de las empresas para la información es que la hayan catalogado, porque no se puede proteger la información, si antes no se ha clasificado". Este directivo hacía esta puntuación refiriéndose a unas estadísticas americanas, en las que aseguraban que "las compañías sólo tienen un 20 por ciento de información en la empresa que es comprometida, el 80 por ciento restante no comprometería el negocio", según palabras del contertulio.

Gianluca D'Antonio

DIRECTOR DE SEGURIDAD DE FCC

"Las compañías sólo tienen un 20 por ciento de información que les compromete"

Un paso que es clave para, luego, poder gestionar esa información y poder darle una protección.

Para Carlos Cantero, de DataZenter, las empresas no están concienciadas: "Saben el valor real de los datos cuando los pierden". Y distinguió cuatro niveles: desde la gran corporación, que posee su propio departamento TIC; las medianas empresas, que son la mayoría de los clientes de DataZenter y que "suelen solicitar los servicios una o dos veces, a lo sumo, por que después ponen remedio"; las pymes, que no tiene medios; y el usuario final, que "está perdiendo una serie de datos, sobre todo con la fotografía digital, que suponen un valor sentimental muy grande". Haciendo uso de un ejemplo de un cliente particular, Cantero describió que uno puede llegar a perder los últimos diez años de su vida metidos en imágenes en su ordenador.

César Comas, de Jazztel, comentó que es difícil dar con la persona adecuada para ofrecer servicios de salvaguarda de la información, ya que, en su opinión, "los canales que manejan la seguridad en las empresas son más proteccionistas y hay que dirigirse a la dirección o al propietario del negocio". Ese proteccionismo al que aludía Comas dejaba entrever la desconfianza que un responsable de seguridad TIC puede sentir cuando un proveedor de servicios de protección y almacenamiento de la información le argumenta cómo asegurar su trabajo. En cambio, contrastó esta opinión con la "total y absoluta autoridad de decisión que tiene el responsable de seguridad en Jazztel para participar en la visión del negocio".

César Comas

REPRESENTANTE DE JAZZTEL

"Los canales que manejan la seguridad en las empresas son proteccionistas"

Aunque no tan tajante, Gustavo San Felipe, de Acens, corroboró que, efectivamente, la situación está cambiando con respecto al peso que está tomando la figura del responsable de seguridad informática en las empresas. Asimismo, confirmó las anteriores opiniones de sus compañeros de mesa al decir que "lo primero y fundamental es saber qué información se quiere proteger". Sin embargo, San Felipe rompió una lanza por los usuarios –empresariales y residenciales-, alegando varias razones: "Para las empresas todo ha ido muy deprisa (normativa, certificación, implantación inmediata, etc.); por otro lado, el intrusismo en la profesión hace que la pyme hable con un canal equivocado que le puede orientar mal".

Gustavo San Felipe

RESPONSABLE DE SEGURIDAD DE ACENS

"El intrusismo en la profesión hace que la pyme hable con un canal equivocado"

El representante de Acens defendió que "a las pymes se les tendría que explicar el porqué de la normalización y de la legislación, porque les llega como una obligación, y no entienden que la información es importante porque tienen que asegurar la información para el tratamiento de los datos y la seguridad de su negocio". Y es que, según sus pala-

especial recuperación de datos

bras, "hay que hacer el esfuerzo de prepararse para lo que pueda venir, para lo que no está previsto".

Andrés Morales, de Albatros, puso el ejemplo de madurez de su compañía: "Nosotros estamos auditados por empresas americanas desde hace 15 años, y nos hemos puesto las pilas porque los propios clientes nos lo pedían". De hecho, esas exigencias americanas a las que se refería este especialista, que les hace cumplir todo "a raja tabla", así como la durabilidad de sus productos ("hasta 30 años", según él), les ha "salvado de muchas".

Andrés Morales

RESPONSABLE DE IT DE ALBATROS

"El departamento de IT está alejado del negocio, porque sólo se le pide continuidad"

En este sentido, Morales resaltó que, en general, los responsables de IT no saben qué es lo que importa del negocio: "El departamento de IT está alejado del negocio, porque sólo se le pide que dé continuidad". Una vez más, el portavoz de Albatros (empresa dedicada a la fabricación de material ferroviario) compartió su propia experiencia. "Una parada en los sistemas de información de cuatro o cinco días lleva a la quiebra, los sistemas de seguridad responden a muchas vidas que van en un ferrocarril", explicó, para añadir que tardó tres o cuatro años en sentarse en un Comité de Dirección".

También puso otros ejemplos de lo "penosos" que son los centros de información de las empresas, porque, según Morales, "los organismos públicos no han sido capaces de legislar".

Situaciones que, en pymes, son normales como ver un servidor debajo de una mesa; pero que en compañías medianas también ocurren, como la falta de control de acceso físico a los centros de datos, por ejemplo.

Ramón Planas

DIRECTOR DE MARKETING DE SPAMINA

"El correo electrónico se está convirtiendo en almacenamiento de datos"

Desde otra óptica, Ramón Planas, de Spamina, puso de relieve la importancia que tiene hoy en día la información que guardamos en nuestros correos electrónicos, para la que "todas las medidas de seguridad tomadas son pocas". Y es que, según argumenta este experto, "el correo se está convirtiendo en almacenamiento de datos, un escenario algo distinto de lo vivido hasta ahora, con lo que empiezan a aparecer amenazas, porque nuestro correo esta totalmente abierto".

Planas apuesta por "medidas de filtrado de correo y servicios de archiving y encripting, en las que las empresas tienen que trabajar porque son claves para el negocio".

Gustavo San Felipe manifestó su acuerdo con su compañero de mesa y expuso: "Las empresas tienen dependencia absoluta del correo electrónico y, por ello, son imprescindibles soluciones como las de Spamina; además, con la movilidad, es positiva la externalización del correo electrónico para protegerlo de amenazas físicas y digitales".

Y, como no podía ser de otra forma tratando el tema de recuperación de datos, Ramón Planas citó catástrofes como el incendio del Windsor o los atentados de las Torres Gemelas, para mantener que "las casualidades existen y que todo es imprevisible". Incluso lanzó una pregunta algo provocadora a sus contertulios: "¿Quién ha probado el backup y no le ha funcionado?".

Morales continuó en su línea "gráfica" y le contestó con una experiencia que él hizo en Albatros. "Propuse al Comité de Dirección hacer un simulacro, provocar un desastre; se hizo a las dos de la madrugada y fallamos en una cosa muy simple: el personal de mantenimiento no está de noche".

especial recuperación de datos

Tras esta experiencia, Andrés Morales afirma que el plan de contingencia hay que testearlo un par de veces al año, porque además puede haber cambios de personal, y "estas pruebas son muy buenas para que la Dirección se dé cuenta de lo que vale; después una inversión en seguridad será más apoyada por todos".

San Felipe agregó que "las pruebas de los planes de contingencia de los negocios ya son obligatorias en la normativa 27001, con el fin de comprobar teléfonos que han cambiado, sistemas de backup defectuosos…". De ahí que desde Acens vean un incremento en la demanda de servicios de backup remoto por parte de sus clientes.

Este profesional explicó que para Acens el error humano es uno de los aspectos que más influye en la pérdida de la información y que, por eso, en su compañía cubren los tres niveles de seguridad: la física (incendios, rotura de discos…), la lógica (malware, virus…) y la que llaman "político-corporativa" (cumplimiento legislativo…).

Como portavoz de un operador, César Comas, garantizó que Jazztel vive ahora un "momento de consolidación", ya que "aumenta el diálogo entre las distintas áreas de la empresa".

Retomando de nuevo el papel del director de IT, Andrés Morales bautizó a esta figura como "el hermanito pobre de la organización". "Somos tecnólogos y no tenemos preparación para estar en un Comité de Dirección donde hablan de estrategia", dijo, haciendo autocrítica. Una reprobación que aplaudió Gianluca D'Antonio pero desde otro enfoque: "La Dirección sí está preocupada por la seguridad; es la seguridad la que no está preocupada por la Dirección, ya que alinear IT al negocio es ofrecer soluciones para que el negocio sea rentable". Así pues, para D'Antonio, lo que se le requiere a un directivo de IT es comunicación, porque "debe hablar de lo que va a ganar la empresa en dinero si implanta medidas de seguridad, ya que esta gente entiende el símbolo del euro".

Según Comas, "una vulnerabilidad equivale a mala planificación en el desarrollo y en el diseño del proyecto, y eso, al final, también explota debido al control del presupuesto que tienen los directores de TIC". Para él, la única solución para solventar esta situación es "cultura, información, documentación de planes de contingencia y probar, probar, probar... porque falla".

Carlos Cantero

EXPERTO EN RECUPERACIÓN DE DATOS DE DATAZENTER

"Cuando alguien llama pidiendo socorro, nosotros somos los bomberos"

Ahondando más en la recuperación de datos, pura y dura, Carlos Cantero expresó: "Cuando alguien pide socorro, nosotros somos los bomberos". Y es que, desde la experiencia de DataZenter, les llegan muchas y variadas causas por las que la gente acude a que "les apeguen el fuego". Según Cantero, en primer lugar, están las pérdidas de información por catástrofes (incendios, inundaciones…) y por problemas eléctricos (subidas de tensión, tormentas eléctricas). En otro nivel, los discos duros, que fallan "porque no son la panacea". Un tercer motivo es la temperatura, sobre todo en los meses de verano, "época alta de las empresas de recuperación de datos". También "acusó" al fallo humano, a veces, de los que supuestamente debería ser los más especializados: "La gente de IT en servidores son nuestros grande aliados o el técnico de la casa, que suelen meter la pata hasta el fondo". Y, en otro grupo, series de productos defectuosos; los discos de mucha capacidad -1 TR-, porque sufren más calentamiento; malas medidas de ventilación, lugares o salas inadecuadas; suciedad; o "el enteraillo que "intenta" arreglar el dispositivo antes de mandarlo a una empresa especializada".

Para intentar evitar los problemas que pueden hacer que una empresa pierda información, es fundamental que exista formación de seguridad en toda la organización, así como cierta disciplina. "En nuestro centro de datos no entra la señora de la limpieza, porque no hay estándar para limpiar el CPD". ☒

especial recuperación de datos