- **Procedimiento Nº: E/01714/2021**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Como consecuencia de la notificación a la División de Innovación Tecnológica de esta Agencia de una brecha de seguridad de datos personales por parte del Responsable del Tratamiento URBASER, S.A. (en adelante URBASER) con número de registro de entrada ******REGISTRO.1***, relativa a un incidente de seguridad con acceso no autorizado y extorsión para no publicar los datos personales, se ordena a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

SEGUNDO A la vista de la citada notificación de quiebra de seguridad de los datos personales, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, teniendo conocimiento de los siguientes extremos:

Resumen de la notificación:

El viernes ******FECHA.1*** a las 23:30 se detecta en el Centro de Control de Redes actividad sospechosa y se comprueba que hay un acceso indebido con encriptación de ficheros.
Ante las primeras comprobaciones deducen que los sistemas informáticos corporativos de URBASER han podido ser atacados de forma externa por el Ransomware DopplePaymer y la información se encuentra cifrada, imposibilitando la operativa normal y el acceso.

Indican que constatan que el atacante es el grupo hacker "******GRUPO.1***" de origen ruso, activo en el mundo del cibercrimen, solicitando un rescate en bitcoins. Se procede a interponer la correspondiente denuncia ante la Unidad Central de Ciberdelincuencia de la Policía Nacional.

Manifiestan que no pueden concretar el número aproximado de datos y afectados por la brecha pero estiman un alto número.

En una ampliación de información de la brecha, recibida en esta Agencia el 11/02/2021, se indica que tras la encriptación de la información, la compañía ha sido víctima de una extorsión bajo la amenaza de una posible publicación de información en la Dark Web. Manifiestan que los datos afectados son del tipo: datos básicos, identificativos, de contacto, credenciales de acceso, cuentas bancarias, de afiliación sindical, de salud y biométricos. Los datos son titularidad de clientes, empleados,

usuarios y proveedores, existiendo un total de unos 123.000 afectados y unos 738.000 registros de datos.

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

URBASER, S.A con CIF A79524054 con domicilio en ***DIRECCIÓN.1** (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Solicitada información a URBASER de la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.
URBASER es una Sociedad Anónima dedicada básicamente a la gestión medioambiental (limpieza viaria, recogida de residuos, limpieza de zonas verdes, etc.). Tiene un volumen de ventas de unos 740 millones de euros (dato de 2019), y con 12928 empleados según AXESOR.

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

Aportan “Informe de brecha notificada”, que enumera los principales hitos acontecidos en la gestión de la brecha. En él se lee:

*“El ***FECHA.2**, URBASER fue víctima de una campaña de phishing, genérica y no dirigida, a través de la cual los empleados de la Sociedad recibieron correos electrónicos con archivos adjuntos infectados con malware, desde el dominio de Mediterranean Shipping Company, S.A. (en adelante, MSC), compañía cliente de URBASER. Según los informes forenses, el malware fue descargado en al menos dos ordenadores portátiles y ejecutado en, al menos, uno de ellos.*

Como consecuencia de lo anterior, se producen dos manifestaciones principales de la brecha; (i) Brecha de disponibilidad a través del cifrado de la información de los servidores junto a un chantaje económico para su recuperación y, (ii) Brecha de confidencialidad mediante la publicación en dark web de información de URBASER ante la negativa de proceder al pago solicitado. El análisis de los apartados siguientes del presente informe tomará en consideración la segregación del impacto de la brecha que se acaba de indicar.

Para la gestión de la brecha, y con la máxima inmediatez que resultó posible, URBASER ha contado con un equipo dedicado expresamente a la gestión, control y mitigación de los efectos de la brecha a nivel interno, a través del Comité de Seguimiento y evaluación continua de la Brecha de Seguridad (en adelante el Comité de Seguimiento) constituido a estos efectos en base a lo dispuesto en la normativa interna de la compañía acerca del protocolo de gestión de brechas de seguridad de los datos personales, así como expertos externos a través de proveedores contratados al efecto, como Telefónica (ElevenPaths), PwC, Microsoft o Ecix Group.

Considerando que en ningún momento ha habido una afectación a la normal continuidad del negocio, el impacto final que ha podido tener la brecha hasta la fecha, a nivel administrativo y de gestión interna, ha podido ser mitigado en gran parte en la medida que; (i) en relación a la brecha de disponibilidad se contaba, desde URBASER, con las copias de respaldo necesarias que han permitido el levantamiento de los sistemas recuperando, en un corto espacio de tiempo, la práctica totalidad de los procesos de gestión que lleva a cabo la compañía y que se habían visto afectados por el cifrado de los servidores y (ii) relativo a la brecha de confidencialidad, el volumen de documentación extraída y/o publicada (10 GB de información relativa a unos 3.500 interesados titulares de los datos personales), así como la tipología de dicha información no ha supuesto un alto impacto a causa de la información publicada, siendo gran parte de la misma contratos, poderes de representación y demás información tiene un impacto bajo para sus titulares."

Se resume a continuación la cronología de los hechos aportada:

- El 27 de enero de 2021 se introduce el malware dridex al abrir un usuario de la compañía un fichero Excel en el que se ocultaba. El fichero Excel fue recibido por correo electrónico en una campaña de phishing. El malware se dispersa y consigue acceso.

- El 28 de enero se produce la exfiltración de ficheros hacia direcciones IP sospechosas, ascendiendo la cantidad de información exfiltrada a 10 gigabytes.

- El 29 de enero inician el proceso de cifrado de todos los equipos a los que ha tenido acceso y se empiezan a recibir alarmas en los sistemas de seguridad a las 23:30h.

- El 30 de enero se escala el incidente hasta llegar al CEO de la entidad cumpliendo con el flujo de comunicación establecido en el protocolo interno de gestión de brechas. Se identifica el incidente en URBASER, se comunica y comienzan a llevarse a cabo acciones para conocer el alcance de los sistemas comprometidos y el impacto.

- El 1 de febrero se convoca el Comité de Seguimiento con objeto de realizar el seguimiento y gestión de la brecha de seguridad. Una vez detectados los problemas existentes, se dan instrucciones de apagado de todos los servidores de la Sociedad y se comienza a informar del alcance del ataque. Se acuerda interponer denuncia ante la unidad especial de ciberdelincuencia de la Dirección General de la Policía, se acuerda notificar a la AEPD y se acuerda organizar la notificación a afectados.

- El 3 de febrero se publican 8 ficheros que forman parte de la información sustraída durante el incidente.

- Días subsiguientes se aprueban diferentes medidas como la deshabilitación de los sistemas de acceso remoto permitiendo acceso únicamente a personal IT, el cierre perimetral para aislar la red de los servidores de copias de seguridad a fin de evitar su afectación y la atribución de capacidad ejecutiva al Director IT para adoptar medidas urgentes sin perjuicio de evaluación posterior. Se contratan expertos externos y se van recuperando diferentes sistemas de la compañía.

- Destaca del 3 de febrero al 3 de marzo: Se producen distintas subidas de ficheros en un dominio .onion, denominado "******DOMINIO.1***", destinada a publicar los ficheros sustraídos a empresas por el mismo ransomware del que URBASER ha sido víctima. En el apartado destinado a URBASER se identifican 147 archivos comprimidos, así como las maquinas comprometidas. Los representantes de la entidad manifiestan que se realiza una valoración preliminar de los documentos publicados y la tipología de datos que pudieran contener sin identificarse datos de especial protección ni datos que requiriesen/permitiesen del titular la adopción de medidas de autoprotección adicionales.

- El 17 de marzo, prosiguiendo con las actuaciones coordinadas tanto por los equipos internos, especialmente de sistemas, como por los refuerzos externos que se han ido incorporando al seguimiento y control del ataque, se recibe el informe de reporte encargado al equipo especializado de Eleven Paths indicando que no se han producido publicaciones adicionales a las del 03 de marzo, por lo que se acuerda dedicar los recursos a la valoración y estudio de cada uno de los archivos publicados, de forma exhaustiva.

Respecto de las causas que hicieron posible la brecha

Los representantes de URBASER han manifestado lo siguiente:

"El ataque se origina por medio de un phising, el vector de ataque utilizado fue el correo electrónico. Tras esto, el actor se movió lateralmente por la red hasta el día 30 de enero de 2021. Este día, el atacante cuenta con suficiente información sobre la red de la compañía y un amplio número de máquinas infectadas por Dridex como para comenzar a descargar y desplegar un componente nuevo conocido como DoppelPaymer. Este software tiene por objetivo secuestrar los datos mediante el cifrado de los mismos, siendo a día del presente informe inviable técnicamente su rescate sin las claves y/o certificados del secuestrador. Así queda constancia en los informes forenses presentados junto al presente informe a esta Agencia.

La motivación de la confiabilidad del correo recibido por parte del usuario que ejecutó el archivo que contenía el malware se deriva de que (i) el emisor del correo es cliente de la compañía al que se le proporciona un servicio regular y (ii) la inclusión de dicho emisor en la lista blanca de recepción de correos, en la que se engloban interlocutores habituales y de confianza de la compañía."

Respecto de los datos afectados.

Con relación a los afectados ha de segregarse entre; (i) La brecha de disponibilidad que pudo afectar a cerca de 123.000 personas físicas de las cuales se disponía de datos personales en los servidores afectados por el cifrado objeto de esta brecha y, (ii) en cuanto a la brecha de confidencialidad, los datos publicados en *dark web* pudieron afectar a 3.500 personas físicas, la gran mayoría representantes legales de sociedades firmantes de los contratos publicados. Adicionalmente, los servidores de la URBASER alojaban un volumen residual de información de una filial de la entidad en Finlandia, datos los cuales se vieron afectados únicamente por el apartado de la brecha relativa a la disponibilidad durante el tiempo que éste tuvo lugar.

La tipología de los datos afectados es:

-Brecha de disponibilidad: datos básicos, datos de contacto, DNI, algunos datos de salud (relativos a RRHH), credenciales de acceso (las del usuario afectado por el phishing), datos económicos y financieros así como datos de cuenta bancaria en el programa de gestión de nóminas, datos de afiliación sindical en el apartado de gestión de nóminas, y biométricos (para el acceso a determinadas instalaciones).

-Brecha de confidencialidad: datos básicos, datos de contacto, DNI (presentes principalmente en los algo más de 300 contratos públicos ordinarios, 100 avales societarios, 17 patrocinios, 54 formaciones, 35 apoderados de URBASER, 48 escrituras mercantiles, etc.).

Los representantes de la entidad manifiestan que no se aprecia, en base a lo anteriormente expuesto posibilidad de consecuencias relevantes para los afectados, por cuanto; (i) En cuanto a la brecha de disponibilidad, las copias de seguridad solventaron cualquier impacto a medio/largo plazo que hubiera podido suponer el cifrado de los servidores y, (ii) En relación a la brecha de confidencialidad, tanto la volumetría de los datos como la tipología de los mismos suponen un bajo impacto para los titulares de los mismos, por cuanto URBASER por la naturaleza de su actividad, sólo ha visto publicado información mercantil y organizativa de la entidad, sin llegar a afectar a clientes persona física, credenciales de acceso a servicios de cliente persona física, datos de especial protección de estos, etc. por lo que no resulta posible, por parte del interesado la adopción de medidas de autoprotección adicionales a las puestas por URBASER. Adicionalmente, no consta ni se ha hallado evidencia de la indexación de los contenidos publicados en *dark web* en motores de búsqueda, lo cual minimiza la exposición, así como no se tiene constancia de la utilización por parte de terceros de la información, compraventa de la misma, utilización con fines delictivos o de ser objeto de un ataque colateral, etc. Por todo ello, las evidencias recabadas hasta la fecha no permiten concluir que pudiera haber consecuencias de alto impacto para los usuarios afectados.

En el informe de la brecha indican que, adicionalmente, los servidores de URBASER alojaban un volumen residual de información de una filial de la entidad en Finlandia, datos los cuales se vieron afectados únicamente por el apartado de la brecha relativa a la disponibilidad durante el tiempo que éste tuvo lugar.

Indican que no se ha recibido reclamación o evidencia, por parte de personas físicas, de la utilización de sus datos y que los informes de vigilancia en redes indican que no se ha hallado evidencia, hasta la fecha, de la indexación en motores de búsqueda de la información publicada en *dark web*, así como tampoco se ha identificado utilización de ningún tipo de la misma por parte de terceros.

Notificaciones a afectados.

Una vez constatada el grado de afectación de la brecha, URBASER resolvió comunicar su ocurrencia a aquellas personas afectadas por la misma, tal y como se evidencia en el acta de reunión del Comité de Seguimiento y evaluación continua de Brecha de Seguridad aportada, de fecha 01/02/2021.

El procedimiento de notificación a interesados se discutió y trato en una reunión específica del Comité, de acuerdo con lo recogido en el acta aportada de fecha 04/02/2021, y se desarrolló entre los días 5 y 8 de febrero, consistiendo en el envío de comunicaciones específicas en función del perfil del interesado afectado. El día 5 de febrero se aprobó el texto de publicación de información en la página web, de acuerdo con lo señalado en el acta aportada de fecha 05/02/2021.

Adjuntan diversos documentos reflejando el contenido de los avisos remitidos a cada clase de afectado, así como el aviso exhibido en la página web de URBASER. Adicionalmente, aportan un compendio de fotografías que con la exhibición de los avisos informativos en las oficinas.

El procedimiento de notificación a los interesados ha sido objeto de seguimiento por parte del Comité, de acuerdo con lo reflejado en el acta aportada de fecha 11/02/2021.

Respecto de las medidas de seguridad implantadas

Con anterioridad a la brecha.

Aportan “Informe sobre medidas de seguridad”, que ofrece un análisis y resumen a alto nivel respecto de las medidas de seguridad adoptadas con anterioridad a suceder el incidente. Aportan también Informe forense realizado por PricewaterhouseCoopers en relación con el mismo, en el que entre otros aspectos se aborda el estado de situación en términos de medidas de seguridad con anterioridad a la sucesión de la brecha sufrida. Aportan a su vez, relación documental de 47 evidencias para sustentar el citado estado de situación.

Se verifica que en informe forense consta que: *“…hemos realizado un análisis comparativo entre las recomendaciones técnicas (en adelante, Recomendaciones) que proporciona el Instituto Nacional de Seguridad (en adelante, INCIBE) para evitar sufrir ataques de tipo ransomware y los controles y medidas implantadas por URBASER antes del Incidente. El resultado del citado ejercicio nos permite concluir que la Sociedad cumplía con la mayoría de las Recomendaciones del INCIBE y en los casos en los que no cumplía en su totalidad, hemos obtenido evidencias de que existía trabajo en curso, encaminado a la implantación de controles y medidas de remediación.”*

Aportan también copia del Informe del Análisis de Riesgo que ha conllevado la implantación de las citadas medidas de seguridad.

Con posterioridad a la brecha.

Aportan copia del “informe incidente URBASER”, elaborado por ElevenPaths Incident Response Team y Telefónica Cybersecurity Tech que describe detalladamente en su apartado 6 las medidas técnicas y organizativas propuestas para el corto, medio y largo plazo, a fin de evitar incidencias similares en el futuro. También en el apartado 5 del mismo informe se enumeran extensamente las medidas para la fase de contención y erradicación durante el incidente tales como: la deshabilitación de los sistemas de acceso remoto y VPNs, permitiendo únicamente acceso al personal de IT con doble

factor de autenticación (2FA), alta de todas las direcciones IP maliciosas incluidas en los listados en el conjunto de firewalls, el EDR y demás sistemas colaterales, la aplicación de restricciones de ejecución, revisión de la seguridad asociada al correo electrónico, minimización del número de usuarios con privilegios, reinicios de contraseñas, etc.

En el informe forense realizado por PricewaterhouseCoopers también se describen con detalle las medidas de seguridad adoptadas para la mitigación y erradicación de la brecha (apartado 4.3. del informe). También consta un informe interno de recomendaciones, de 14 páginas, adjunto a la contestación como documento número 8, que detalla recomendaciones a seguir a corto, medio y largo plazo.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante quiebra de seguridad) como “todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.” En el presente caso, consta que se produjo una quiebra de seguridad de datos personales en las circunstancias arriba indicadas, categorizada inicialmente como brecha de disponibilidad y posteriormente también de confidencialidad.

De la documentación aportada por la investigada, entre otra, Informe de incidente Urbaser de fecha 18/02/2021, Informe técnico independiente de fecha 25/03/2021, Análisis de riesgos de fecha 01/2/2021 y una síntesis de éstos, contenido en el informe de medidas de seguridad, se constata que previamente a la brecha, se encontraba en el proceso de elaboración de un PDS basado en la serie ISO/IEC 27000, que comprende también la implantación de un sistema de gestión de seguridad de la información. Asimismo y tal como se afirma en el informe de fecha 25/03/2021, la investigada cumplía con la mayoría de las recomendaciones del INCIBE para evitar los ataques de rasomware y en los casos en que no se cumplía, existía trabajo en curso para implantar controles y medidas de remediación. De todo ello se desprende que, con anterioridad a producirse la brecha, la entidad investigada disponía de medidas de seguridad razonables en función de los riesgos estimados.

La brecha fue posible a través phishing usando un correo electrónico, supuestamente proveniente del dominio de un cliente de la entidad, por lo que pasó desapercibido y

fue difícil de evitar, en el que se adjuntaba un fichero Excel conteniendo el malware, que al ejecutarse provocó la extensión de la infección.

Tras conocerse el incidente, se actúa con diligencia convocando al Comité de Seguridad que rápidamente decide la contratación de una consultora tecnológica especializada en ciberseguridad, la cual despliega un equipo especializado en Digital Forensics & Incident Response, que fue el encargado de liderar las actuaciones para la contención y erradicación de la brecha, entre las medidas adoptadas destacan: la deshabilitación de los sistemas de acceso remoto y VPNs, permitiendo únicamente acceso al personal de IT con doble factor de autenticación (2FA), alta de todas las direcciones IP maliciosas incluidas en los listados en el conjunto de firewalls, el EDR y demás sistemas colaterales, la aplicación de restricciones de ejecución, revisión de la seguridad asociada al correo electrónico, minimización del número de usuarios con privilegios y reinicios de contraseñas.

Asimismo se procedió a aislar la red de los servidores de backup, de la red de infraestructura y al apagado de la plataforma cliente para posteriormente realizar el análisis y limpieza. Aparte de estas medidas se procedió a contratar un servicio que consta de dos ingenieros para dar soporte al incidente, uno especializado en Directorio Activo y el otro en correo electrónico

En lo referente al impacto, se han visto afectados, por la brecha de disponibilidad fundamentalmente datos personales, datos básicos, datos de contacto y DNI, de 123.000 personas físicas, no obstante las consecuencias han sido mínimas, ya que ésta fue solventada con las copias de seguridad.

En lo referente a la brecha de confidencialidad, han sido afectados datos básicos, datos de contacto y DNI de 3500 personas, la gran mayoría representantes legales de las empresas firmantes de los contratos publicados, siendo el resto de la información exfiltrada, fundamentalmente información mercantil y organizativa de la investigada, sin llegar a afectar a clientes persona física, a credenciales de acceso a servicios de cliente persona física ni a datos de especial protección de estos, por lo que el impacto es considerado por la investigada como bajo. Adicionalmente, no consta, ni se ha hallado evidencia, de la indexación de los contenidos publicados en la *dark web* en motores de búsqueda, lo cual minimiza la exposición, ni tampoco se tiene constancia de la utilización por parte de terceros de la información.

Para evitar que estos hechos se repitan, la investigada propone establecer una serie de medidas a corto, medio y largo plazo, tanto de ámbito técnico como organizativo, entre ellas, aplicación del principio aislar y conectar a EDR para los clientes, monitorización de las conexiones que van haciendo los servidores, revisión diaria de alertas y ficheros de LOG, minimizar el número de usuarios privilegiados , en el medio plazo podemos destacar la intención de establecer como obligatoria la política de doble factor de autenticación para cualquier infraestructura expuesta públicamente, así como la creación de un playbook para respuesta a incidentes y simular anualmente los escenarios de ataque.

En consecuencia, consta que disponía de medidas técnicas y organizativas razonables para evitar este tipo de incidencia, no obstante y una vez detectada ésta, se produce una diligente reacción al objeto de mitigar los efectos, notificar a la AEPD, interponer

denuncia ante la unidad especial de ciberdelincuencia de la Dirección General de la Policía y organizar la comunicación a afectados.

Por último, se recomienda elaborar un Informe Final sobre la trazabilidad del suceso y su análisis valorativo, en particular, en cuanto al impacto final. Este Informe es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos y servirá para prevenir la reiteración de una brecha de similares características como la analizada.

III

Por lo tanto, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a URBASER, S.A con CIF A79524054

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-0419

Mar España Martí
Directora de la Agencia Española de Protección de Datos