Procedimiento Nº: E/05441/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante JOBS AND TALENT, S.L. (en lo sucesivo el reclamado), y en base a los siguientes:

HECHOS

PRIMERO: Con fecha de 07/07/2018 se recibe la notificación de una brecha de seguridad realizada en la entidad reclamada, en la que se ponen de manifiesto implicaciones transfronterizas que afectarían a Alemania, Gran Bretaña y Suecia.

SEGUNDO: A la vista de los hechos y de los documentos de los que ha tenido conocimiento esta Agencia, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, 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).

Según manifiestan los representantes de la entidad el 05/07/2018 fue detectado un ataque satisfactorio a la infraestructura del reclamado. El atacante consiguió acceder de forma no autorizada a una base de datos del reclamado y con base en las evidencias que manejamos existe probabilidad no confirmada de que el atacante haya extraído de la plataforma del reclamado registros de determinados campos de la tabla de usuarios. Se ha demostrado que para que el ataque sea posible el atacante necesitó acceso al código fuente privado del proyecto llamado *candidates*. No es posible para un atacante aleatorio ejecutar la secuencia de eventos sin conocer una clave secreta de 128 caracteres que se encontraba en el código y que es usada para validar las cookies de sesión.

Vector de ataque

El atacante tuvo acceso a la base de datos con el usuario y permisos de la aplicación web y en los registros se vieron peticiones normales, ejecutadas aparentemente a mano cómo se puede deducir de los errores de sintaxis. No hay signos de técnicas de *SQL Injection* ya que el rastro de ese tipo de peticiones es más ruidoso y las peticiones en el log tendrían un formato característico, distinto al que se ve. Por otro lado, tampoco hay traza de servidores comprometidos *vía ssh*, y no hay ningún otro servicio expuesto a internet distinto al del servicio web.

Durante el mismo periodo de tiempo del ataque saltaron las alarmas de comportamiento anómalo en un servicio. La petición que los generaba era un GET sin parámetros, y la URL a la que accede ****URL.1.*

Buscando en detalle en la traza de error, se pudo extraer los datos contenidos en la cookie, donde se comprobó que había una parte que había sido modificada desde un cliente con la forma de una línea de comandos inversa que permite abrir una vía de comunicación desde el servidor que la ejecuta hasta un servidor externo gestionado por el atacante (IP: 176.107.178.11 perteneciente a *DeltaHost*, un proveedor de servidores en Ucrania)

Para que un servidor del reclamado ejecute ese código necesita comprobar que la cookie que envía el cliente es válida. La cookie tiene un mecanismo de validación que consiste en un código hash de los datos en la cookie más un secreto que solo conoce el servidor. El atacante debe conocer el código secreto para crear un hash válido para el servidor y que la cookie sea ejecutada.

Medidas de seguridad previas al ataque

Las medidas de seguridad técnicas implementadas en el reclamado para proteger la información de sus usuarios están dentro del ciclo de evolución tecnológica de la compañía. El reclamado se apoya en los estándares en la industria para gestionar su seguridad y mantiene una política de implementación continua de mejoras para mitigar riesgos según aparecen o se tiene constancia en función de su impacto.

Las medidas de seguridad técnicas se distribuyen en todas las capas de la pila tecnológica. En función de la capa:

• Plataforma: el reclamado se basa en *Amazon Web Services* como proveedor de infraestructura en la nube, implementa las recomendaciones de seguridad que ofrece y se beneficia de sus características.

• Sistemas Operativos: El servicio se apoya en sistemas operativos modernos, Amazon Linux.

• Aplicación: el reclamado depende de software de terceros para realizar determinadas funciones o facilitar y simplificar el desarrollo de la funcionalidad del servicio.

Para gestionar este código el reclamado se apoya en *Github* como servicio de repositorio, seguimiento de código y sistema de control del cambio.

Github incorpora también un sistema de auditoría de vulnerabilidades en las dependencias de software de terceros en los que se basa el código del reclamado.

• Entornos: El desarrollo de la funcionalidad se realiza en entornos locales o de integración distintos pero estructuralmente iguales que el entorno de producción y con datos ficticios. Esto entornos replican la funcionalidad del reclamado sin necesidad de tener los datos del entorno real, simplificando así la gestión de la información.

• Gestión de secretos: La configuración de los servicios para que puedan funcionar correctamente incluye información sensible como

contraseñas de bases de datos y claves de servicios externos. El reclamado se apoya en *Hashicorp Vault* para poder gestionar de forma segura el acceso y propagación de esos secretos hacia las aplicaciones que los usen.

• Almacenamiento de credenciales de usuarios: Al recopilar y almacenar la contraseña de un usuario que se da de alta en la plataforma aplicamos un método de hash (algoritmo irreversible) a la contraseña antes de almacenarla en base de datos usando un algoritmo *shal* a través de *Devise*.

• Monitorización y alertas por anomalías. El sistema de monitorización está basado en *DataDog* para plataforma y *Rollbar* para aplicaciones. En ellos se apoyan las alarmas básicas de estado de plataforma y alarmas más avanzadas para detectar comportamientos anómalos tanto de servicios de JOBSANDTALENT como de los servicios de proveedores.

En la actualidad los riesgos no detectados o detectados pero aún no corregidos se tratan a través de un protocolo donde se discuten las causas, se validan los datos y se proponen cambios para evitar o minimizar impacto en caso de que vuelva a pasar.

Medidas de seguridad adoptadas tras el incidente

En cuanto el ataque fue confirmado las siguientes medidas fueron tomadas para minimizar riesgos:

• Restringir la ip del atacante en la plataforma de modo que se evita el riesgo de que el atacante vuelva a intentar el ataque desde el único origen que ha usado para perpetrar todos los intentos mientras aplicamos las demás medidas.

• Rotar el secreto conocido por el atacante, usado para crear la cookie con el código malicioso de este modo se anula el vector de ataque al evitar que el atacante conozca el secreto que usa el servicio para validar las cookies en el que se basa el ataque. Con esta medida también se invalidan las cookies y, por lo tanto, las sesiones de todos los usuarios del servicio web, obligándoles a introducir de nuevo su usuario y contraseña.

• Rotar preventivamente secretos disponibles en los servidores comprometidos, como claves de servicios externos usados por la aplicación para funcionar de modo que se reducen los riesgos de que el atacante aproveche posible conocimiento ganado durante el ataque para elaborar nuevos ataques en base a esos nuevos secretos potencialmente conocidos.

Con estas medidas ya no es posible un ataque con los secretos comprometidos, pero además se han añadido más capas de seguridad en la plataforma:

• Filtrado de conexiones salientes: Las conexiones de salida hacia internet son bloqueadas para no permitir extracción de información no controlada.

• Ampliar la monitorización por comportamiento: Inclusión de una alarma de monitorización de anomalías de tráfico de salida en la base de datos. Las alarmas disponibles hasta este momento permitieron detectar el ataque por un comportamiento anómalo en la aplicación atacada. Con esta alarma añadimos el punto de vista de la base de datos en la detección de patrones de comportamiento anómalo en el tráfico de salida mejorando la visibilidad en

caso de un ataque similar.

• Eliminar cualquier secreto del código fuente y lo gestionarlos mediante variables de entorno almacenadas en un sistema de gestión de secretos (*Hashicorp Vault*).

• Cambio del hash de las contraseñas de usuarios almacenadas en la base de datos con el objetivo de hacer inviable atacar por fuerza bruta para ello los usuarios debieron cambiar sus contraseñas al acceder a la plataforma.

Conclusión

Más allá de las medidas de seguridad disponibles antes y después del incidente, no hay ni ha habido ninguna vulnerabilidad conocida en la infraestructura que haya podido ser usada para un ataque directo. El ataque recibido solo pudo ser posible con un acceso al código fuente donde estaba almacenado el secreto de 128 caracteres con el que poder firmar cookies que los servidores admitan como válidas.

El secreto involucrado ya ha sido rotado y eliminado del código al sistema de gestión de secretos haciendo que una nueva fuga del código fuente no pueda ser usada para un nuevo ataque. En esta línea también se ha auditado el código fuente para eliminar cualquier otro secreto, eliminando así la posibilidad de un vector de ataque similar.

Suponiendo que pudiera ocurrir un nuevo ataque que consiguiera explotar una vulnerabilidad no conocida se han implementado nuevas medidas de seguridad que extreman la dificultad para la extracción de información hacia fuera de la plataforma así como sistemas de monitorización extra que exponen estos intentos de forma más precisa.

El número aproximado de ciudadanos de cada país cuyos datos han sido comprometidos:

- Gran Bretaña: 347.200
- Alemania: 5.950
- Suecia: 700

Ningún encargado del tratamiento se ha visto afectado por el ataque.

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 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (en lo

sucesivo RGPD) define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

También hay que señalar, que la notificación de una quiebra de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

En el artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control, determinando lo siguiente:

“1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene

lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

Y el artículo 34 del Reglamento mencionado indica cuando es necesario informar de una violación de la seguridad de los datos personales al interesado, señalando lo siguiente:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales

afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

En este mismo sentido se señala en los *Considerandos* 85 y 86 del RGPD:

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados,

mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

En el presente caso, de la documentación obrante en el expediente se ofrecen indicios evidentes que de la brecha de seguridad producida en los sistemas del reclamado ha vulnerado el artículo 32 del RGPD, *Seguridad del tratamiento*, permitiendo potencialmente que el atacante consiguiera acceder de forma no autorizada a una base de datos del reclamado y existiendo la probabilidad no confirmada de que el atacante hubiera extraído registros de determinados campos de la tabla de usuarios.

No obstante, el reclamado notificó a esta autoridad de control la quiebra de seguridad detectada en sus sistemas de manera diligente, dentro del plazo de notificación establecido en el artículo 33 del RGPD. Además, hay que señalar que el reclamado tenía implementadas medidas de seguridad que, en principio, eran las adecuadas para garantizar que los datos personales no fueran accesibles por terceros y, como consta en los hechos, en cuanto el ataque fue detectado y confirmado por la entidad se adoptaron de manera inmediata una serie de medidas de seguridad adicionales con el fin de minimizar los riesgos y extremando las dificultades para el acceso y extracción de la información.

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:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente resolución a **JOBS AND TALENT, S.L.** con NIF ***B85384808.***

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.

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