Procedimiento Nº: E/07213/2019
940-0419

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: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de violación de seguridad de datos personales (en adelante quiebra de seguridad) remitido por GRUPO QUIRONSALUD (en adelante QUIRONSALUD) en el que informan a la Agencia Española de Protección de Datos que se ha detectado virus en la red provocando indisponibilidad parcial de servicios. No se percibe pérdida, ni integridad de información pero si la indisponibilidad mencionada.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Fecha de notificación de quiebra: 26 de junio de 2019

ENTIDADES INVESTIGADAS

GRUPO QUIRONSALUD con NIF 08028829N con domicilio en ZURBARAN, NUM 28 - 28010 MADRID (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1 Con fecha 6 de septiembre de 2019 se requiere información a QUIRÓNSALUD y de la respuesta recibida con fecha 20 de septiembre de 2019 se desprende:

1.1. QUIRONSALUD realiza la comunicación inicial a la Agencia dentro de las 72 horas marcadas por la normativa por un deterioro en los servicios de autenticación de una serie de usuarios y la detección de un malware en la infraestructura.

1.2. No hay ninguna evidencia de que se hayan visto afectados datos de carácter personal y por tanto ninguna actividad de tratamiento.

1.3. En la resolución del incidente han estado involucrados además de QUIRONSALUD, Telefónica como proveedor de infraestructura (CPDs: Tier IV de Alcalá de Henares redundado con CPD Julián Camarillo) y como equipos de Respuesta ante incidentes, Microsoft y McAfee.

El martes 25 de junio de 2019 a las 14.30 horas las consolas de monitorización de los servicios antivirus empiezan a detectar en los equipos un malware tipo troyano.

Inicialmente sólo se aprecian reinicios en algunos de los equipos, no obstante, alrededor de las 21 horas se detecta un tráfico anómalo a una serie de IPs externas de un número elevado de orígenes distintos dentro de la red interna de QUIRÓNSALUD. Inmediatamente se bloquean estas IPs en los firewalls de QUIRÓNSALUD.

Sobre las 5.00 horas de la mañana se despliegan los parches de McAfee que permiten la eliminación del virus y parece que la incidencia queda solucionada.

Se realiza un análisis interno y se comprueba que no ha existido accesos indebidos a las bases de datos, ni exfiltración de datos de carácter personal, ni deterioro de los servicios.

El 26 de junio de 2019 sobre las 14.30 horas, se detecta una incidencia con reinicios inesperados en puestos de trabajo, servidores y controladores de dominio que provocaban deterioro en servicios de IT que afectan parcialmente a la operativa en los centros hospitalarios; en concreto en la autenticación, no existiendo afectación en las actividades de tratamiento de carácter personal. Inmediatamente se redirige la autenticación a los controladores no afectados y se activan los protocolos de contingencia en los hospitales. Se analizan los equipos afectados y se identifica que han sido infectados con un malware.

En la misma fecha aproximadamente a las 16.30 horas, se activa el procedimiento de respuesta a incidentes de seguridad coordinado por un Comité de Crisis liderado por QUIRÓNSALUD, con apoyo de colaboradores externos.

Se acuerda llevar a cabo las siguientes acciones de forma inmediata:

- Desconexión inmediata de internet • Reseteo y eliminación de cuentas privilegiadas,
- Análisis de equipos infectados, recogida de muestras y logs.
- Limpieza del malware y/o reinstalación de los equipos infectados.
- Bloquear accesos remotos (vpn)

El protocolo de comunicación incluye el aviso a diferentes Comités de QUIRÓNSALUD, a las Fuerzas y Cuerpos de Seguridad del Estado (Delitos telemáticos de la Guardia Civil) y a la Agencia Española de Protección de Datos.

Una vez finalizado el análisis forense (12 Julio) se determina que la propagación del malware se hizo con dos cuentas con permisos de administración. El resultado del análisis forense no muestra ninguna evidencia de que datos de carácter personal hubieran sido afectados de ninguna forma (acceso, modificación, deterioro o exfiltración).

Se procede a la apertura de internet y conexiones vpn de forma controlada.

Del 1 de agosto al 12 de septiembre se realiza un proyecto junto con Microsoft de recuperación y securización de cuentas administrativas.

1.4. Respecto de las causas que han hecho posible la incidencia

El malware en esa fecha no era detectado por el antivirus principal instalado y además en su funcionamiento realizaba una conexión a una IP's externas desde donde se descargaba otro archivo malicioso enmascarado lo que permitía su instalación sin ser detectado. La instalación forzaba el reinicio en las máquinas infectadas.

La infección de malware que ha sido difundida por la infraestructura corporativa de QUIRÓNSALUD a través de dos cuentas privilegiadas de IT. Estas cuentas fueron comprometidas mediante otras técnicas fraudulentas.

1.5. Respecto del número de clientes afectados por la incidencia

No hay datos afectados.

1.6. Respecto de las acciones tomadas con objeto de minimizar los efectos adversos

25 de junio a las 14.30

- Bloqueo de IPs maliciosas en el Firewall.
- Reseteo y eliminación de cuentas privilegiadas
- Análisis activo de equipos infectados, recogida de muestras y logs.

26 de junio a las 16:30

- Desconexión inmediata de internet.
- Bloquear accesos remotos (vpn)
- Activación de los protocolos de contingencia de los hospitales.
- Activación Comité de crisis liderado por QUIRONSALUD

  - Informar órganos de Dirección de QUIRONSALUD.
  - Informar a la Agencia Española de Protección de Datos y a la Unidad de Delitos Telemáticos de la Guardia Civil.
  - Informes diarios de situación

26 de junio al 12 de Julio

- Limpieza del malware y/o reinstalación de los equipos infectados.
- Incremento monitorización e informes diarios de situación
- Análisis forense

1.7. Respecto de las acciones realizadas para la resolución final de la incidencia

Para la resolución final de la incidencia de seguridad del 1 de agosto al 12 de septiembre se ejecutaron las siguientes acciones:

- Ejecución de un proyecto junto con Microsoft de recuperación y securización de cuentas administrativas
- Implementación de la autenticación multifactor en las VPN.
- Implantación de los FW de análisis en tiempo real.

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 como brecha de disponibilidad como consecuencia de la instalación de un malware que había superado los análisis de los antivirus instalados.

No obstante, también consta que QUIRÓNSALUD, a través del servicio de Informática, disponía de medidas técnicas y organizativas para afrontar un incidente como el ahora analizado, lo que ha permitido la identificación, análisis y clasificación de la brecha de seguridad de datos personales así como la diligente reacción ante la misma al objeto de notificar y minimizar el impacto e implementar las medias razonables oportunas para evitar que se repita en el futuro a través de la puesta en marcha de un plan de actuación previamente definido por las figuras implicadas del responsable del tratamiento.

No consta que la confidencialidad e integridad de los datos personales obrantes en el sistema de información hayan sido comprometidas

También debe valorase la adopción de medidas técnicas y de gestión, como es la comprobación de todos los sistemas de información similares y la denuncia de los hechos ante las Fuerzas y Cuerpos de Seguridad del Estado, al objeto de comprobar y en su caso mejorar la calidad y seguridad de las aplicaciones de gestión de datos personales.

El informe final tras el seguimiento y cierre sobre la brecha y su impacto es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos futuros. El uso de esta información servirá para prevenir la reiteración del impacto de una brecha.

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 ***GRUPO QUIRONSALUD*** con NIF ***08028829N*** y con domicilio en ***calle ZURBARÁN, NUM 28 - 28010 MADRID (MADRID)***

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