SIN SEGURIDAD NO HAY PRIVACIDAD

PRESENTADO A:
RAFAEL MARTINEZ RANERA

AUTORES:
ANDRÉS FELIPE LEAL MORA
JUAN DAVID ESCOBAR ESCOBAR
JUAN MANUEL BAUTISTA CORREA
WILLIAM RAMIRO RIOS HENAO

UNIVERSIDAD INTERNACIONAL DE LA RIOJA
MÁSTER EN VISUALIZACION Y PROCESAMIENTO DE DATOS MASIVOS
GOBIERNO DEL DATO Y TOMA DE DECISIONES
JULIO, 2022

1. Profundización del caso

1.1. Cómo se materializó el ataque

El día 20 de julio del año 2015 un grupo de hackers que se hizo llamar The Impact Team sacó un comunicado en el que se atribuían un ataque contra Ashley Madison, una aplicación que facilitaba citas discretas entre personas casadas para engañar a sus parejas. De acuerdo con los autores del hackeo la compañía dueña de la aplicación estaba engañando a sus usuarios ya que les exigía el pago de un monto de dinero para borrar los perfiles a modo de chantaje. Por eso en su momento el grupo The Impact Team exigió que se borraran todos los sitios web asociados a The Impact Team. Ashley Madison no cedió ante las amenazas y los datos de 32 millones de usuarios fueron revelados en internet, junto con información interna de la compañía. Dentro de los datos revelados se encuentran correos electrónicos, perfiles (incluyendo contraseñas, direcciones y teléfonos) y hasta transacciones de tarjetas de crédito (Enter, 2015).

El total de datos publicados fue un paquete de 9.7 gigabytes mediante la web oscura utilizando una dirección de Onion accesible sólo a través del navegador Tor. Los archivos incluyen detalles de cuentas e inicios de sesión usuarios del sitio de redes sociales, siete años de tarjetas de crédito y otros detalles de transacciones de pago también forman parte de la base de datos del portal de citas (Wired, 2015).

Algunos de los datos sensibles como las contraseñas publicadas en el lote de datos fueron codificadas mediante el algoritmo "***bycypt***" de PHP el cual a pesar de ser una de las formas más seguras para almacenar contraseñas, no es un gran desafío para los hackers informáticos lograr descifrar los hash o códigos cifrados mediante el algoritmo, lo cual pone en peligro información privada asociada a las cuentas de usuario de la plataforma web o aplicación. Cabe mencionar que otros portales en algunas ocasiones nunca se molestan o implementan algún control de seguridad de cifrado de información sensible o confidencial como las contraseñas (Wired, 2015).

¿Qué motivó a los hackers?

En la nota de rescate inicial, el Equipo de Impacto sugirió que las prácticas comerciales indecorosas en ALM, por ejemplo, una política de cobrar a los usuarios por eliminar sus cuentas en Ashley Madison y luego continuar almacenando la información personal de los usuarios salientes en servidores internos, habían provocado la ira de los piratas informáticos. y justificó su ataque. Pero la divulgación masiva de datos privados, para señalar el maltrato de datos privados, no puede haberle parecido a nadie una razón muy coherente para hacer todo esto (The Guardian, 2016).

1.2. Por qué tuvo éxito

El portal de Ashley Madison ofrece la posibilidad de agendar citas para parejas infieles y citas matrimoniales, su eslogan describe la frase “La vida es corta tenga una aventura hoy en Ashley Madison”, lo cual hace atractivo a miles de esposos y esposas infieles alrededor del mundo, razón por la cual los afectados no tenían gran autoridad moral para reclamar sin ser juzgados ellos mismos sus derechos a la privacidad de datos personales. Al tratarse de un portal de la índole inmoral descrita en el párrafo anterior, no se podría esperar garantías de seguridad y medidas de control para cuidar la información de las cuentas suscritas, por lo cual el portal se convirtió en un blanco llamativo para los piratas informáticos y sacar provecho del chantaje y beneficio financiero a costa de la vergüenza, divorcios, suicidios y otros lamentables hechos sucedidos debido a las publicaciones de información sensible, íntima y comprometedora. “*Cualquiera que haga algo en línea”, me dijeron, “debería asumir que no es seguro*” (The Guardian, 2016).

1.3. Cuáles fueron las fueron las consecuencias sobre los afectados

El mayor riesgo presente es que las personas que los usuarios conocen puedan buscar en los vertederos de información pública para ver si tienen amigos, compañeros de trabajo o cónyuges entre los usuarios del sitio. El uso del sitio también podría volver a perjudicar a los consumidores, por ejemplo, en procesos de divorcio o custodia, "Todo es aprovechable por la persona adecuada que busca lo correcto" (Nbc News, 2015).

Los hackers, que operaban con impunidad, comenzaron a avergonzar y exprimir a los expuestos. En Alabama, los editores de un periódico decidieron imprimir en sus páginas todos los nombres de las personas de la región que aparecían en la base de datos de Ashley Madison. Después de algunas renuncias de alto perfil en toda América del Norte, la gente se preguntaba si no habría riesgo de repercusiones más trágicas. Brian Krebs, con cierta presciencia, escribió un blog en el que aconsejaba sensibilidad: “Existe una posibilidad muy real de que la gente reaccione de forma exagerada”, escribió. “No me sorprendería si viéramos a personas quitarse la vida por esto”.

Se informó de un pequeño número de suicidios, entre ellos un sacerdote en Luisiana. En declaraciones a los medios de comunicación después de su muerte, la esposa del sacerdote dijo que había descubierto que su nombre estaba entre los de la lista antes de suicidarse. Ella dijo que habría perdonado a su esposo y que Dios también lo habría hecho. “La gracia de Dios en medio de la vergüenza es el centro de la historia para nosotros, no el truco. Mi esposo conocía esa gracia, pero de alguna manera olvidó que era suya cuando se quitó la vida”.

Durante las primeras semanas de la crisis, ALM, la compañía detrás de Ashley Madison dejó de responder de manera adecuada a las llamadas y correos electrónicos de sus aterrorizados clientes. Innumerables matrimonios estaban en riesgo, la gente se tambaleaba ante decisiones atroces y, mientras tanto, ALM publicaba enérgicos comunicados de prensa, uno de los cuales anunciaba la partida del director ejecutivo Noel Biderman. Hizo ajustes superficiales en el frente de su sitio web, y en algún momento decidió eliminar el gráfico que describía a Ashley Madison como "100% discreta" (The Guardian, 2016).

2. **Justificación de una posible violación de seguridad tal y como se define en el RGPD**

"Violación de la seguridad de los datos personales": toda violación de la seguridad que ocasione 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» (art. 4.12, RGPD). La violación también puede ser referida como brecha de seguridad. De acuerdo con los hechos sucedidos el portal web fue atacado por piratas informáticos, que lograron tener accesos a información confidencial de 32 millones de usuarios, lo cual indica claramente una o varias brechas de seguridad, ya que además de lograr acceder, robar y publicar información confidencial, los piratas informáticos lograron descifrar contraseñas que se encontraban encriptadas mediante algoritmos de cifrado "seguros".

El portal vulnerable fue un blanco perfecto para ser atacado ya que probablemente quien lo hizo sabía muy bien de la falta de controles de seguridad que tenía el sitio web, al ofrecer un servicio relacionado a un tema inmoral y sin ética alguna, lo más factible es que los empleados informático tuvieran acceso a la información lo cual los hace principales sospechosos y tal vez la compañía no contaba con controles de seguridad, monitoreo y auditoría como el más básico acceso basado en roles y responsabilidades, probablemente tampoco se contaba con una segmentación de ambientes donde se aloja el sitio web y los datos (desarrollo calidad y producción), con la finalidad de que los roles informáticos solo tengan acceso a los dos primeros ambientes para soportar, desarrollar y ejecutar pruebas de calidad con información anonimizada y no la real, la cual debe reposar en repositorios de almacenamiento en un ambiente productivo donde solo personal autorizado y responsable tiene ciertos accesos de acuerdo a su responsabilidad puntual y que cuente con un monitoreo estricto y controles adicionales para auditar las acciones, logs y consultas efectuadas sobre los datos por cada uno de los usuarios con acceso al portal.

Los datos fueron tomados por personas inescrupulosas sin ética de manera ilícita, dicha información fue publicada, se utilizó como material de chantaje para sacar beneficio económico (dinero sucio), adicional la publicación de los datos generó grandes desastres a nivel psicológicos, divorcios, económicos, sociales, reputacionales, entre otros. Sin embargo, estos datos puede ser solicitados por entes legales, puede darse el caso en el que se esté materializado un divorcio y existan pruebas y sospechas de que un miembro de una pareja infiel tenga una suscripción y tenga algún tipo de relación extramarital, la cual está afectando psicológicamente y emocionalmente a la pareja, adicional de un divorcio esta información confidencial también puede ser solicitada de manera especial por entes legales para hacer seguimiento a casos judiciales.

La compañía o el dueño del portal estaba en el deber de contar con un responsable del tratamiento (RT) quien, ante una situación de violación de la seguridad, deba demostrar la improbabilidad de que dicha violación entrañe riesgo para los derechos y libertades de las personas físicas. Exigir esta responsabilidad tiene por objeto garantizar los derechos de los afectados (considerando 85, RGPD). La compañía tampoco se molestó en generar una notificación temprana (plazo de 72 horas) a los usuarios afectados luego de la publicación de varios datos confidenciales, por lo cual muy posiblemente la compañía podría ser sancionada económicamente.

3. Evaluación de la notificación

Notificaciones de violaciones de seguridad de los datos personales a la autoridad de control

El reglamento establece como medida de seguridad adicional y de transparencia la obligación para los responsables de tratamiento de notificar a la autoridad de control que le corresponda la violación de seguridad en un plazo de 72 horas. En el caso de que no se efectúe esta notificación en el plazo establecido por un retraso, deberá argumentarse los motivos del retraso (hay que recordar que la autoridad de control se determina en virtud de la aplicación del artículo 55).

3.1. ¿Piensas que los afectados habrían podido protegerse del impacto negativo de la divulgación de la información?

Al tratarse de un caso de violación de datos una notificación temprana y responsable puede ayudar a que los afectados tomen acciones preventivas, por ejemplo, algunos datos eran tarjetas de crédito, las cuales pueden ser bloqueadas para evitar compras en línea por parte de los atacantes o quienes posean dicha información. Otra posible medida es generar denuncias por violación de los derechos de privacidad de datos personales, aun así, muchos de ellos no tenían su conciencia tranquila y autoridad moral, ya que estaban

comprometidos con sus parejas, familias, reputación y trabajos profesionales en las compañías. Datos como el teléfono pueden ser cambiados por seguridad y evitar chantajes, otro dato como la dirección hace que las personas implementen medidas de seguridad como implementar sistemas de seguridad en sus hogares, el simple cambio de llave de acceso, o hasta el cambio de vivienda. El correo electrónico también podría ser actualizado y eliminar la cuenta actual para evitar chantajes y contacto con los delincuentes.

Bibliografía

Enter. (21 de Agosto de 2015). *Enter.co*. Obtenido de https://www.enter.co/cultura-digital/el-popurri/el-hackeo-de-ashley-madison-vuelve-la-inquisicion-opinion/

Nbc News. (20 de Julio de 2015). Obtenido de https://www.nbcnews.com/tech/internet/should-ashley-madison-users-worry-about-blackmail-n395291

The Guardian. (28 de Febrero de 2016). Obtenido de https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked

Wired. (18 de Agosto de 2015). Obtenido de https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/

Tabla de valoración individual

	Sí	**No**	**A veces**
Todos los miembros se han integrado al trabajo del grupo	X		
Todos los miembros participan activamente	X		
Todos los miembros respetan otras ideas aportadas	X		
Todos los miembros participan en la elaboración del informe	X		
Me he preocupado por realizar un trabajo cooperativo con mis compañeros	X		
Señala si consideras que algún aspecto del trabajo en grupo no ha sido adecuado		X	