Universidad de Costa Rica
Administración de bases de datos
Mario Quirós Luna – B76090
Tarea 7

EQUIFAX:

Equifax es una de las tres empresas de informes de crédito más importantes de Estados Unidos. En septiembre de 2017 anunció que había sido víctima de un hackeo que afectó a más de 140 millones de sus clientes en ese país.

Origen del incidente

Se exploto una vulnerabilidad en un ambiente de código abierto llamado Apache Struts, los datos que Equifax manejaba con este entorno eran, nombre de la persona, dirección, fecha de nacimiento, número de seguridad social, número de la licencia de manejo y más de doscientos mil números de tarjetas de crédito.

¿Cómo lo manejó la empresa? ¿Tuvo la situación un manejo adecuado?

Según lo mencionado por el CEO de Equifax, este problema se debió a un error humano al no aplicar un parche, junto a un error técnico cuando el escáner no detecto la vulnerabilidad como pendiente por resolver. Sin embargo, en la actualidad se conoce que esto no fue así, entre los aspectos que se han descubierto que afectaron a este incidente serían:

- Falta de monitoreo de la integridad de los archivos.
- Falta de segmentación de la red.
- No se logró identificar oportunamente el ataque entre otras cosas por falta de visibilidad.
- El reporte a las autoridades y a los clientes no fue oportuno.
- Mal manejo organizacional de la crisis.
- Falta de involucramiento de la alta dirección en temas de ciberseguridad.

¿Cuál fue el impacto de este incidente dentro y fuera de la organización?

Entre las consecuencias que provoco el incidente, estarían:

- Caída del valor de la acción.
- Pérdida de reputación de la empresa.
- Afectación a la ciudadanía.

- Efectos financieros, pues deberán tener un fondo de hasta $700 millones de dólares para compensar a los clientes.
    - Cada cliente que demuestre que fue afectado, es decir, que ha tenido que invertir tiempo o dinero para resolver la situación (cargos no reconocidos, gastos de abogados, etc.), podrá recibir $20,000 dólares.
    - Los clientes afectados podrán recibir servicios de monitoreo de su estatus crediticio durante 10 años; los primeros 4 años con cualquiera de las 3 empresas principales y los restantes 6 directamente con Equifax. Si el cliente ya tiene contratado el servicio de monitoreo crediticio, podrá optar por recibir $125 dólares como compensación.
- El director de TI y un ingeniero que construyó parte del portal Web involucrado en el incidente de seguridad, fueron sentenciados por este incidente, ya que tomaron ventaja vendiendo sus acciones antes de publicar el hecho.

Opinión sobre la página Web creada:

Me parece una buena manera de volver a generar confianza tanto en los clientes afectados como en nuevos clientes, porque este servicio brinda la opción de que se puede consultar en cualquier momento el estado de sus datos.

Soluciones y consideraciones ante incidentes similares:

Entre las consideraciones que se pueden ver están la necesidad de aplicar siempre las mejores prácticas que se puedan, entre temas de seguridad, patrones etc. A su vez se puede ver la importancia de estar en constante actualización y mantenimiento buscando siempre mejorar el producto que ya se tiene, más aún cuando se trata de una empresa donde se maneja temas de finanzas. Para esto se debe estar siempre a la vanguardia aplicando los mejores estándares y las mejores tecnologías en temas de seguridad. Y a su vez también se puede ver la necesidad de un plan de respuesta ante cualquier incidente, ya que, por más seguro que se crea un servicio siempre existirá la posibilidad de que sea vulnerado de cualquier manera.

Bibliografía:

Itil, M. C. P. (s. f.). *El ciberataque a Equifax como caso de estudio*. Magazcitum. https://www.magazcitum.com.mx/index.php/archivos/5222