Instituto Tecnológico Superior Ibarra

Desarrollo de Software

REVISIÓN A LA HISTORIA

Autores:

Santiago Rosales Andrade.;

Santiago Andrade Alvarez.;

Directores:

Santiago Rosales Andrade.;

Santiago Andrade Alvarez.;

Ibarra – Ecuador

2024

REVISIÓN A LA HISTORIA

1. ***Sony Pictures (2014)***
    - **Tipo de ataque:** Ataque de malware (wiper) y exfiltración de datos.
    - **Vector de ataque:** Los atacantes ingresaron a la red a través de phishing y el uso de malware sofisticado que se infiltró en los sistemas de Sony.
    - **Objetivos:** Robar y publicar datos confidenciales, como correos electrónicos internos, películas no estrenadas, y datos personales de empleados.
    - **Fecha y hora:** Noviembre de 2014.
    - **Duración:** El ataque duró varias semanas, con efectos que se sintieron durante meses.
    - **Alcance:** Miles de empleados y sistemas internos de Sony Pictures fueron afectados.
    - **Daños causados:** Pérdida masiva de datos, interrupción de operaciones, daño severo a la reputación de la empresa, y pérdidas financieras significativas.
    - **Costos:** Se estima que el costo fue de hasta $100 millones, incluyendo la restauración de sistemas y los costos legales.

    Lecciones Aprendidas:

    - **Vulnerabilidades:** Falta de segmentación en la red y protección insuficiente de datos sensibles.
    - **Fallos en los procesos:** Inadecuada monitorización de la red y una respuesta tardía al incidente.
    - **Recomendaciones:** Implementar segmentación de la red, mejorar las prácticas de seguridad interna, y realizar simulacros de ciberataques para preparar al personal.

2. ***Yahoo (2013-2014)***
    - **Tipo de ataque:** Brecha de datos (Data Breach).
    - **Vector de ataque:** Los atacantes explotaron una vulnerabilidad en el sistema de gestión de cookies de Yahoo, lo que les permitió falsificar cookies para acceder a las cuentas de los usuarios sin necesidad de contraseñas.

- **Objetivos:** Los atacantes buscaban acceso a cuentas de usuario, incluyendo información personal como nombres, direcciones de correo electrónico, fechas de nacimiento, contraseñas cifradas y preguntas de seguridad.
- **Fecha y hora:** Los ataques ocurrieron en 2013 y 2014, pero fueron revelados al público en 2016.
- **Duración:** Aunque los ataques individuales pudieron haber sido breves, la brecha en la seguridad duró más de un año.
- **Alcance:** Aproximadamente 3,000 millones de cuentas de usuario fueron comprometidas, lo que representa la mayor brecha de datos en la historia.
- **Daños causados:** Pérdida masiva de datos personales, daños significativos a la reputación de Yahoo, y una reducción en el valor de mercado de la compañía. Además, el acuerdo de adquisición de Yahoo por Verizon se renegoció, reduciendo el precio de compra en $350 millones.
- **Costos:** Yahoo estimó que el costo directo de la violación de datos fue de al menos $350 millones, sin contar los costos de litigios, multas y otras sanciones.

Lecciones Aprendidas:

- **Vulnerabilidades:** La falta de actualización y parcheo de sistemas críticos permitió la explotación de vulnerabilidades conocidas. Además, la gestión inadecuada de las cookies creó un punto de acceso para los atacantes.
- **Fallos en los procesos:** La respuesta lenta de Yahoo para identificar, informar y resolver la brecha fue uno de los mayores fallos. La compañía tardó años en reconocer y comunicar públicamente la magnitud del ataque.
- **Recomendaciones:** Es crucial implementar políticas de seguridad más rigurosas, incluyendo la actualización continua de sistemas, la monitorización activa de redes para detectar comportamientos sospechosos y la mejora de la gestión de autenticación, como la implementación de autenticación multifactor (MFA).

3. Uber (2016)

- **Tipo de ataque:** Exfiltración de datos.
- **Vector de ataque:** Acceso no autorizado a través de credenciales comprometidas en un repositorio de código público.

- **Objetivos:** Robar información personal, incluyendo datos de conductores y usuarios.
- **Fecha y hora:** Octubre de 2016.
- **Duración:** El ataque fue descubierto un año después de que ocurriera.
- **Alcance:** 57 millones de cuentas de usuarios y conductores fueron afectadas.
- **Daños causados:** Pérdida de confianza y reputación, multas por ocultar el ataque a las autoridades y a los usuarios.
- **Costos:** Uber pagó $148 millones en multas y enfrentó otras penalizaciones legales.

Lecciones Aprendidas:

- **Vulnerabilidades:** Gestión deficiente de las credenciales y acceso no controlado a repositorios de código.
- **Fallos en los procesos:** Falta de notificación a los usuarios y reguladores tras descubrir el ataque, lo que agravó la situación.
- **Recomendaciones:** Implementar mejores prácticas de gestión de credenciales, controles de acceso estrictos, y políticas de divulgación rápida ante incidentes de seguridad.

4. ***Cambridge (2018)***
    - **Tipo de ataque:** Explotación indebida de datos (Data Exploitation).
    - **Vector de ataque:** Cambridge Analytica obtuvo acceso a los datos personales de millones de usuarios de Facebook a través de una aplicación de terceros, que recolectó información bajo el pretexto de un test de personalidad.
    - **Objetivos:** El objetivo principal era recopilar datos personales para influir en el comportamiento de los votantes en diversas elecciones, incluido el referéndum del Brexit y las elecciones presidenciales de Estados Unidos en 2016.
    - **Fecha y hora:** La explotación de datos ocurrió entre 2014 y 2015, pero el escándalo fue revelado en 2018.
    - **Duración:** La recolección de datos se llevó a cabo durante varios meses. Sin embargo, la explotación de estos datos para campañas de desinformación y publicidad dirigida duró varios años.

- **Alcance:** Se estima que los datos de aproximadamente 87 millones de usuarios de Facebook fueron explotados sin su consentimiento explícito.
- **Daños causados:** Daño significativo a la confianza del público en Facebook y Cambridge Analytica. Facebook fue multado con $5,000 millones por la Comisión Federal de Comercio (FTC) de Estados Unidos. Además, el escándalo desencadenó un debate global sobre la privacidad de los datos y la ética en la manipulación de la información.
- **Costos:** Los costos incluyeron multas millonarias, pérdidas en el valor de las acciones de Facebook, y gastos legales. La reputación de Facebook se vio gravemente afectada, lo que llevó a cambios en sus políticas de privacidad.

Lecciones Aprendidas:

- **Vulnerabilidades:** La laxitud en las políticas de privacidad de Facebook y la falta de supervisión sobre cómo los datos de los usuarios eran utilizados por terceros permitió que Cambridge Analytica explotara esta información.
- **Fallos en los procesos:** La incapacidad de Facebook para monitorear y regular adecuadamente las aplicaciones de terceros fue un fallo crítico. También hubo una falta de transparencia en la comunicación con los usuarios sobre cómo se manejaban sus datos.
- **Recomendaciones:** Se debe reforzar la supervisión de aplicaciones de terceros y mejorar las políticas de privacidad y transparencia. Las plataformas deben ser proactivas en la protección de datos y asegurar que los usuarios tengan un control más efectivo sobre cómo se utilizan sus datos.

5. ***Dropbox (2012)***

- **Tipo de ataque:** Exfiltración de datos.
- **Vector de ataque:** Los atacantes obtuvieron credenciales de un empleado de Dropbox, lo que les permitió acceder a una base de datos de usuarios.
- **Objetivos:** Obtener direcciones de correo electrónico y contraseñas de los usuarios.
- **Fecha y hora:** Julio de 2012.
- **Duración:** El ataque no fue detectado de inmediato, permitiendo a los atacantes acceso durante semanas.

- **Alcance:** 68 millones de usuarios de Dropbox fueron afectados.
- **Daños causados:** Pérdida de datos personales, daño a la reputación y confianza de los usuarios, y la necesidad de implementar nuevas medidas de seguridad.
- **Costos:** Aunque no se revelaron cifras exactas, el ataque llevó a Dropbox a mejorar significativamente su seguridad y gestionar las contraseñas comprometidas.

  Lecciones Aprendidas:
- **Vulnerabilidades:** Gestión inadecuada de credenciales y seguridad insuficiente en el almacenamiento de contraseñas.
- **Fallos en los procesos:** No se detectó el ataque de inmediato, lo que permitió a los atacantes tener acceso prolongado a los sistemas.
- **Recomendaciones:** Implementar autenticación de dos factores, monitorización constante de actividad sospechosa, y auditorías regulares de seguridad.

6. ***Stuxnet (2010)***
   - **Tipo de ataque:** Gusano informático (Worm) diseñado específicamente para sabotaje industrial.
   - **Vector de ataque:** Stuxnet se introdujo inicialmente a través de unidades USB infectadas y luego se propagó por las redes internas de las instalaciones industriales.
   - **Objetivos:** El objetivo principal fue sabotear las centrífugas utilizadas en el programa nuclear de Irán, específicamente en la planta de enriquecimiento de uranio en Natanz.
   - **Fecha y hora:** Stuxnet fue descubierto en 2010, aunque se cree que su desarrollo comenzó varios años antes y estuvo activo durante al menos un año antes de ser detectado.
   - **Duración:** El ataque duró varios meses, desde la infección inicial hasta la interrupción significativa del programa nuclear iraní.
   - **Alcance:** Afectó principalmente las instalaciones de Natanz en Irán, pero Stuxnet también se propagó a otras instalaciones industriales en todo el mundo, aunque sin causar daños significativos fuera de Irán.
   - **Daños causados:** Stuxnet causó el daño físico de aproximadamente 1,000 centrifugadoras, retrasando el programa nuclear iraní. Este ataque es considerado uno de los primeros ejemplos de una "ciberguerra" dirigida a destruir infraestructura crítica.

- **Costos:** Aunque el costo exacto del ataque no se conoce, el impacto en el programa nuclear iraní fue significativo. Los costos para desarrollar, desplegar y contrarrestar este ataque probablemente ascendieron a millones de dólares.

Lecciones Aprendidas:

- **Vulnerabilidades:** La dependencia de sistemas de control industrial vulnerables y la falta de segmentación de redes críticas permitió la propagación de Stuxnet. El uso de dispositivos USB como vector de ataque mostró la necesidad de controles más estrictos sobre los dispositivos portátiles en entornos sensibles.
- **Fallos en los procesos:** La falta de detección temprana y la capacidad limitada para responder a un ataque tan sofisticado fueron fallos críticos. Además, la confianza excesiva en la seguridad física sin medidas de ciberseguridad adecuadas facilitó el éxito del ataque.
- **Recomendaciones:** Es crucial implementar una ciberseguridad robusta en infraestructuras críticas, incluyendo la segmentación de redes, la detección avanzada de amenazas y la limitación del uso de dispositivos externos. También se recomienda la adopción de medidas proactivas para protegerse contra ataques dirigidos, incluyendo la actualización constante de sistemas y la realización de pruebas de penetración regulares.