Asociación de Internautas

¿Sabes dónde están tus datos?

¿Sabes dónde están tus datos?

Propiedad intelectual e industrial, datos de caracter personal, datos bancarios, directorios de proveedores y clientes, comunicaciones interpersonales... Hoy en día los datos son unos de los activos mas importantes en nuestras organizaciones e incluso en nuestras vidas privadas.

El pasado año 2017 lo cerramos con importantes filtraciones de datos que aún están recientes en nuestra memoria.

Tenemos el intento de encubrimiento por parte de UBER de datos sobre 57 millones de usuarios, Equifax y su filtración de datos sobre 145.5 millones de usuarios, bases de datos de foros de temática policial y de la web de la Comunidad de Madrid por parte de Anonymous...

Esta filtraciones se producen por fallos en la infraestructura que estamos usando, como los problemas de los Western Digital 'My Cloud' que comenta mi colega Claudio en la Asociación de Internautas o los "buckets" en Amazon que tenía la NSA.

En otras ocasiones existe una intrusión mas en profundidad en la organización, con intereses mas que bien definidos.

Por ejemplo, hoy por hoy, ya hay casos de "Ransomware" que lo que hacen es contactar con la entidad vulnerada e informarles de que sus datos han sido robados, cifrados y publicados en internet a disposición de todo el mundo.

¿Si no se paga lo solicitado?

Se publica la clave para descifrar los datos. Y que sea lo que Dios quiera...

En la actualidad hemos de ser concientes que vivimos en un mundo que es mas que probable acabar comprometido de una o de otra manera, y mas según mas grande y compleja sea la organización.

Lo importante yo resaltaría es que una vez vulnerados: Ser resiliente, tener una respuesta ágil y eficaz, así como, añadir este conocimiento a nuestro bagaje y compartirlo con otros actores de la seguridad defensiva.

¡Y pensar en como ponérselo lo mas difícil a los "malos" para sacar la información de nuestra casa!

La exfiltración de información va mas allá que "tostar un CD", copiar los datos a un pincho o sacar kilos de papel por las impresoras...

Algunos métodos clásicos son:

- Enviar los datos mediante una conexión HTTPS a un servidor del atacante.
- Usar servidores de la nube como Pastebin

- Usando conexiones de SMTP o de FTP.
- Usando paquetes TCP o ICMP

Voy a citar algunos de los métodos que se conocer mas curiosos desde mi punto de vista:

- Tweets cifrados con la información robada.
- Subir la información dentro de un vídeo de Youtube, una imagen en Flickr o un documento en Linkedin, mediante el uso dee esteganografía.
- Consultas a un DNS del atacante, haciendo consultas de nombres de subdominios al mismo... Cuando en realidad lo que está enviando es la información sustraída y cifrada.
- Usando Skype u otros servicios de mensajería (p.e. IRC).
- Creando redes wireless con distintos ESSIDs, cuyos nombres en realidad son la información que se está robando...

Con esta enumeración tan simplona, lo que queiero conseguir es concienciar un poco al lector de este artículo.

El uso de tecnología DLP (Data Loss Prevention) no debe residir unicamente en inspección el tráfico SSL, si no en una estrategia de defensa en profundidad y gestión documental.

> "Los datos son el nuevo petróleo"

Artículo de Antonio Fernandes en Linkedin
