UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERIAS
DEPARTAMENTO DE CIENCIAS COMPUTACIONALES

MATERIA:
SEGURIDAD DE LA INFORMACION

MAESTRO:
FRANCO LOPEZ VELARDE, EMMANUEL

TITULO DE INVESTIGACIÓN:
ACTIVIDAD DE APRENDIZAJE NÚMERO 4: ESPANOL

FECHA ENTREGA:
LUNES 10 DE SEPTIEMBRE 2018

ALUMNO:
FELIPE DE JESUS RUIZ GARCIA

CODIGO:
214522077

CARRERA: INGENIERIA INFORMATICA (INNI)

SECCION: D02

CALIFICACIÓN Y OBSERVACIONES:

PREVENCION A LA FUGA DE INFORMACION

Las bases de datos son dinero, cuanto vale toda la informacion de una empresa ? Si bien, el mal uso de la informacion por si mismo puede darle a la empresa un dolor de cabeza, ahora imaginemos en las manos incorrectas ... un secuestro de informacion podria ser fatal. Por ello, debemos tomarnos en serio el control y politicas para el trato y resguardo de la informacion.

Lo de hoy es la nube: Podriamos pensar que guardar nuestra informacion en un sitio como dropbox or google drive nos garantiza la disponibilidad e integridad de la informacion pero; Por cuantos sitios pasa nuestra informacion antes de llegar a los servidores del prestador de servicio ? Y que pasa si el prestador de servicio es vulnerado ? O nuestras cuentas son robadas ?
Eh aqui la importancia de saber definir politicas y normas a lujo de detalle, de acuerdo al giro de la empresa, modelo de negocio y su infrestructura.

Por cierto, infrestructura, Podria pensar que en cierto departamento se asegura la integridad de la informacion, fuera de fugaz y copias no autorizadas, pero esta al ser requerida en otro departamento puede ser robada y alterada por por personal no autorizado o incluso por alguien fuera de la organizacion. Por ello se debe tomar en cuenta todo ello en infrestructura, porque suele ser ahi donde pueden abundar las fugaz y vulnerabilidades.

Lo que se comparte a internet, vivira para siempre:
Eliminar informacion no significa que no se pueda recuperar :o
El desechar incorrectamente informacion puede ser un hueco en la fuga de informacion puesto que existen algoritmos y software capaces de recuperar grandes porcetajes de informacion en dispositivos formateados. Con la seguridad nunca se exagera. No me pareceria para nada exagerado usar como norma el formateo militar, o escribir varias veces en 0 todo el almacenamiento de un dispotivo.
Vamos a poner un ejemplo de como todo lo anterior es

fundamental para evitar la fuga de informacion:

1. Un despacho de abogados quiere automatizar sus procesos para el facil manejo de su informacion y hacer disponible alguna informacion via internet para dispositvos modernos como smartphones.
2. El despacho de abogados actualmente emplea todos sus procesos mediante papeles y quiere migrar todo ello a medios digitales.
3. El despacho de abogados desea compartir por internet alguna informacion de uso sensible a personas especificas (clientes).

Para el punto 1 primero deberia estudiarse todo el proceso del despacho de abogados: como es procesada la informacion, las fuentes de esta, su rubro y prestar especial atencion en aquello que se desea compartir.
Algun departamento dentro del despacho requiere informacion procesada por otro despacho. Y aqui comienza el diseno de una buena infrestructura, en el analisis. Asegurar que solo se comparte entre un departamento y otro solo la informacion requerida a las personas requeridas. Como sera enviada la informacion ? Todo proceso local no deberia involucrar nada con internet.
Para el punto 2 se deberia restringir el acceso al papeleo del negocio, incluso tomar en cuenta contratos legales para las personas que capturaran la informacion, que no usaran esta para fines no establecidos. Tambien establecer como y donde se guardaran. Aqui tambien entra en juego el diseno de la infrestructura. Guardar la informacion en base de datos normalizada en un servidor local podria ser una buena opcion, donde para ingresarla los capturistas solo llenan formularios y no tienen contacto directo con todas las tablas de la DB ni pueden ejecutar querys sobre ella. Aun no involucramos a internet para nada.
Para el punto 3 se debera garantizar la fiabilidad de la informacion, inalterable por un tercero. Aqui tiene un peso muy

importante pensar en layers, niveles, capas : como cebollas.
Los documentos que se desean compartir por internet para personas especificas son el resultado de cierto proceso, por cual su alteracion no deberia ser posible y deberian ser emitidos como finales, solo personal autorizado podria tener acceso de modificacion y expidicion de estos.
De igual manera las cuentas de acceso a los servicios y servidor donde se alojaran dichos documentos.
Entonces podemos pensar que dentro de la organizacion deberia haber solo una red para el acceso local sobre la cual la infrestructura sera montada y otra para el acceso a internet, donde se haran disponibles los documentos.
Nunca combinar estas. Si tenemos

El ejemplo anterior ataca muchos de los casos, de fuga de informacion. Ahora, el uso de buenas practicas con la implementacion de un DLP podria ser bastante mas efectivo.

Hacker Leaked - Snapchat Source Code On GitHub

https://thehackernews.com/2018/08/snapchat-hack-source-code.html

August 07, 2018

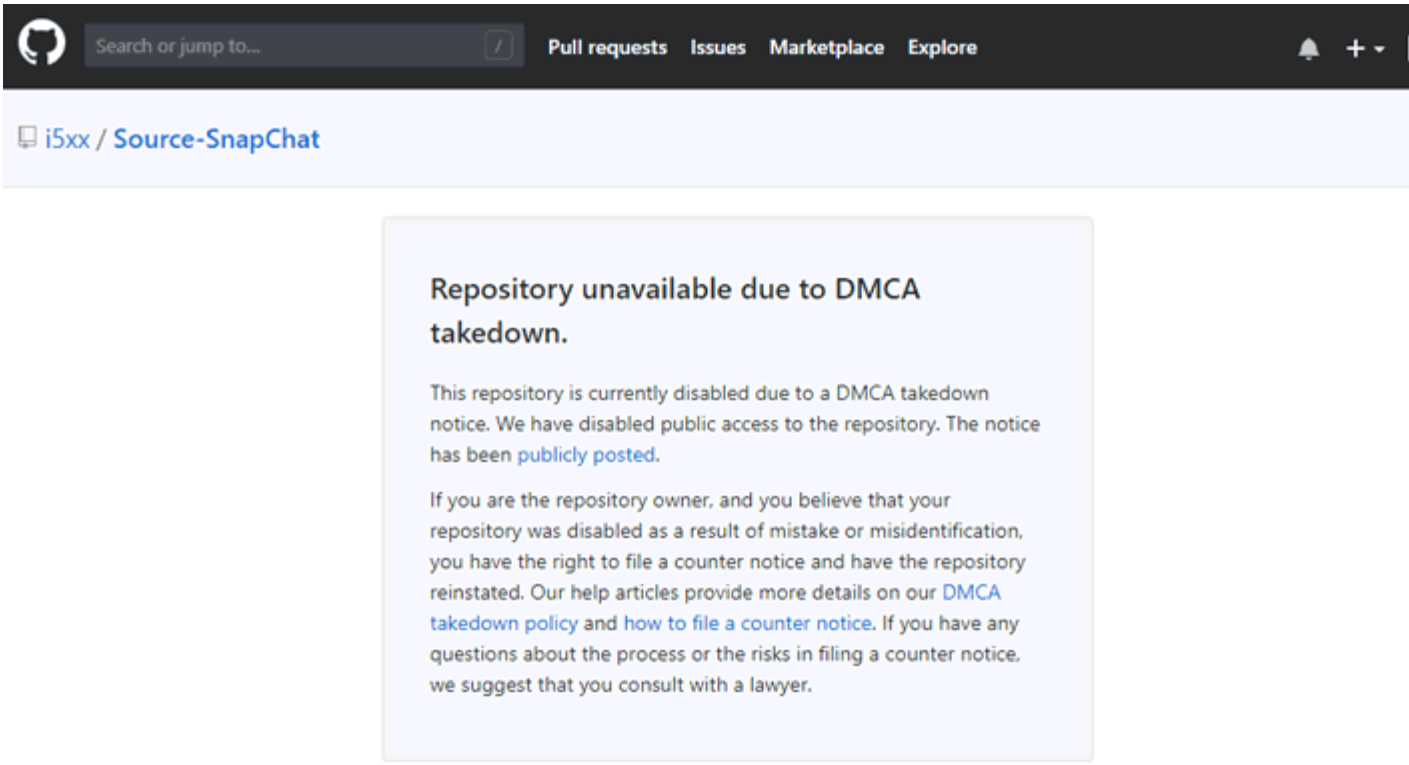
The source code of the popular social media app Snapchat was recently surfaced online after a hacker leaked and posted it on the Microsoft-owned code repository GitHub.

A GitHub account under the name Khaled Alshehri with the handle i5xx, who claimed to be from Pakistan, created a GitHub repository called **Source-Snapchat** with a description "**Source Code for SnapChat**," publishing the code of what purported to be Snapchat's iOS app.

The underlying code could potentially expose the company's extremely confidential information, like the entire design of the hugely-successful messaging app, how the app works and what future features are planned for the app.

Snapchat's parent company, Snap Inc., responded to the leaked source code by filing a copyright act request under the Digital Millennium Copyright Act (DMCA), helping it takedown the online repository hosting the Snapchat source code.

SnapChat Hack: Github Took Down Repository After DMCA Notice



Though it is not clear precisely what secret information the leaked SnapChat source code contained, the company's panic can be seen in the DMCA request (written in all-caps) which suggests the contents of the repository were legitimate.

> "I AM [private] AT SNAP INC., OWNER OF THE LEAKED SOURCE CODE," a reply from a Snap employee, whose name is redacted, on the DMCA notice reads.

Upon asking "Please provide a detailed description of the original copyrighted work that has allegedly been infringed. If possible, include a URL to where it is posted online," the Snap employee responded:

> "SNAPCHAT SOURCE CODE. IT WAS LEAKED AND A USER HAS PUT IT IN THIS GITHUB REPO. THERE IS NO URL TO POINT TO BECAUSE SNAP INC. DOESN'T PUBLISH IT PUBLICLY."
>
> "WE WOULD APPRECIATE YOU TAKE DOWN THE WHOLE THING."

Snap told several online news outlets that an iOS update in May exposed a "small amount" of its iOS source code.

Although the company identified and rectified the mistake immediately, it discovered that some of the exposed source code had been posted online.

However, Snap did confirm that the code has been subsequently removed and that the event did not compromise its application and had no impact on its community.

Pakistani Hacker Threatens to Re-Upload Snapchat's Source Code

It appears that the online user behind the source code leak created the Github account with the sole purpose of sharing the Snapchat source code as nothing else was posted on the account before or after the Snapchat leak.

Moreover, some posts on Twitter by at least two individuals (one based in Pakistan and another in France) who appear to be behind the i5xx GitHub account suggest that they tried contacting Snapchat about the source code and expecting a bug bounty reward.

But when they did not get any response from the company, the account threatened to re-upload the source code until they get a reply from Snapchat.

The Snapchat source code has now been taken down by GitHub after the DMCA request, and will not be restored unless the original publisher comes up with a legal counterclaim proving he/she is the owner of the source code.

However, this does not rectify the issue completely. Since the Snapchat source code is still in the hands of outsiders, they could re-publish it on other online forums, or could use it for individual profit.

MY FEEDBACK
Fuga de informacion ? donde NO ?

Una vez mas, se aprecia como todo el esfuerzo de una empresa o el departamento de esta puede parecer un desperdicio y perder lo mas valioso que tiene, y peor aun, sin saber como fue que lo esto llego a pasar... que estaban haciendo mal ? Como pueden estar seguros de que no volvera a pasar ? Y si reincide que haran para que esto no sea critico.

Afortunadamente la empresa pudo recurrir por el lado legal y asi conseguir el blockeo de dicho repositorio en github.

Como pudo alguien tener todo el codigo de la aplicacion ? Esto es una burla para todo el departamento de seguridad de la empresa.

Personamente el caso de snapchat creo que tiene que ver con seguridad fisica, mas que con logica...
Quiza algun ex empleado resentido ...