¿Qué debes saber para establecer el nivel imprescindible de seguridad en aplicaciones de eventos, sitios web y soluciones de registro?

por **eventscase**

¿Cómo de inseguros son los entornos en los que estamos trabajando ahora?

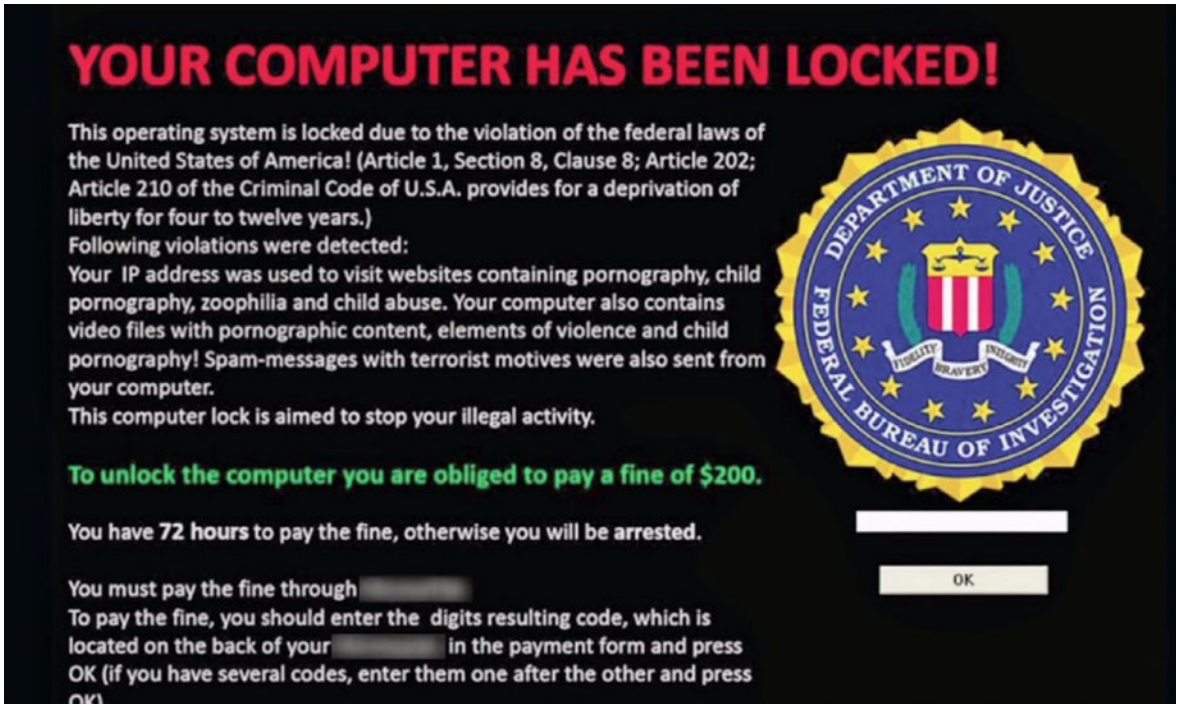
¿Crees que tu ordenador es seguro?

La seguridad se puede entender como una competición continua entre nosotros y el "lado oscuro" (los hackers). Lo primero que tenemos que tener claro es que es imposible estar 100% seguro porque los sistemas siempre dependen de varios factores, como el sistema operativo, el tipo de procesador que usa tu servidor o la forma en que funciona Internet. Los bugs y fallas de seguridad aparecen en todas partes y debes estar siempre actualizado y listo para enfrentarte a ellos.

Un error muy común es creer que teniendo un antivirus estamos protegidos, lo cierto es que no es del todo así. Un antivirus siempre te va a dar protección contra virus y operaciones lógicas de las que se conoce su comportamiento, pero ese no es el mayor de los peligros. Hay un refrán que dice que el 99% de los problemas informáticos, y sobre todo de los problemas de seguridad, se encuentran entre el teclado y la silla y es que por mucho que tengamos sistemas que intentan protegernos, al final somos nosotros quienes tenemos la última palabra para dar acceso a un atacante.

Un ejemplo en el que se puede ver esta situación de un modo más claro es con el tipo de virus conocido como Ransomware. Estos virus encriptan todos los archivos de tu ordenador y piden un pago en bitcoin para que el hacker los desencripte (nunca ocurre, si sufres ese ataque, estás perdido). Si no tienes copias de seguridad recientes o si siempre trabajas con un usuario que tiene permisos de administrador, estás condenado a tener una pérdida importante de todo tu trabajo, que a veces puede ser el trabajo de años, por no hablar de los archivos de valor personal que pueden perderse como fotos o vídeos. Estos virus normalmente aparecen cuando te llega un correo electrónico en el que te envían un archivo adjunto, por ejemplo una factura, al abrir el archivo se desata el caos. Hay que ser lógicos e intentar siempre asegurarte de que conoces al remitente o que sabes bien qué es lo que vas a encontrarte en el archivo que vas a abrir. En estos casos, eres tú quien ha dado acceso al virus a atacar tu sistema y, en la mayor parte de las veces, tu antivirus no podrá detenerlo a tiempo.

Usando la lógica y el sentido común, podemos evitar muchos de los problemas que tenemos a diario con la tecnología.

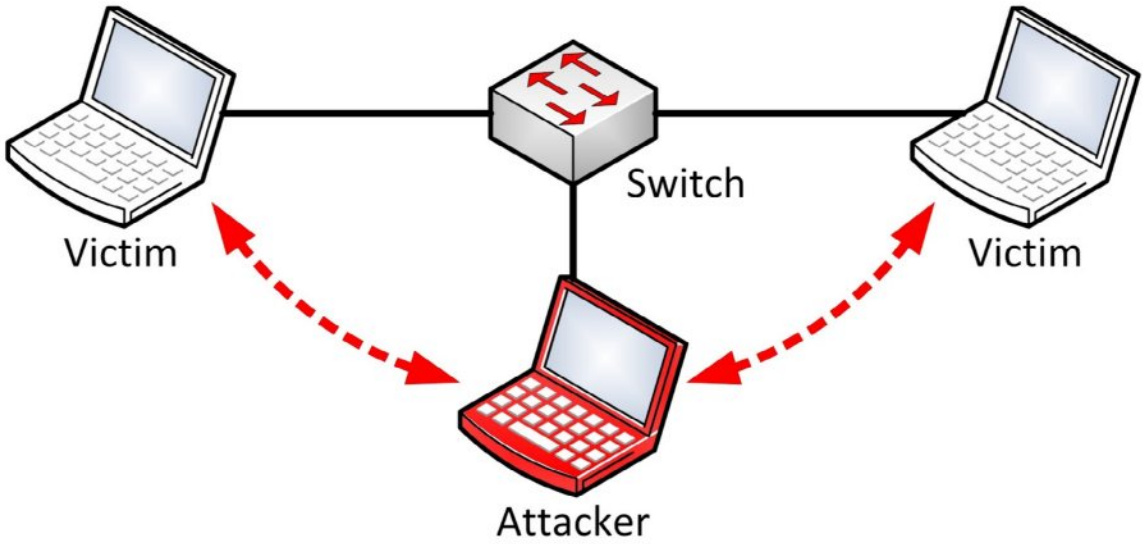


¿Cuáles son las preguntas correctas que hay que hacer a un equipo técnico que comprenda las implicaciones de seguridad?

Preguntas para el lugar donde haremos el evento y, también, para el proveedor que nos proporciona Wifi

Cuando hablamos con los proveedores de Wifi o con los encargados del lugar donde tendrá lugar un evento, tenemos que centrarnos sobre todo en la posibilidad de mitigar ataques MiTM (Man in the middle) ya que son los ataques más comunes y que más pueden afectar al flujo de nuestros eventos.

En este método se introduce un intermediario (el cibercriminal o una herramienta maliciosa) entre la víctima y la fuente, en nuestro caso sería en el router aunque en otros casos podría ser una página de banca online o una cuenta de correo electrónico. Estos ataques son realmente efectivos y, a su vez, muy difíciles de detectar por el usuario, quien no es consciente de los daños que puede llegar a sufrir. Este método sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos a una de ellas. Por ejemplo, en el mundo offline se crearían facturas falsas, enviándolas al correo de la víctima e interceptando los cheques de pago de dichos recibos. En el mundo online, un ataque MiTM es mucho más complejo, pero la idea es la misma. El atacante se sitúa entre el objetivo y la fuente pasando totalmente desapercibido para poder alcanzar con éxito la meta.



In the most usual MiTM attack , a wi-fi router is used to intercept the communications of the user. En el ataque MiTM más habitual, se utiliza un router WiFi para interceptar las comunicaciones del usuario. Esto se puede realizar configurando el router malicioso para que parezca legítimo o atacando un error del mismo e interceptando la sesión del usuario. En el primero de los casos, el atacante configura su ordenador u otro dispositivo para que actúe como red WiFi, nombrándolo como si fuera una red pública (de un aeropuerto o una cafetería). Después, el usuario se conecta al router y busca páginas de banca o compras online, el criminal captura las credenciales de la víctima para usarlas posteriormente. En el segundo caso, un delincuente encuentra una vulnerabilidad en la configuración del sistema de cifrado de un WiFi legítimo y la utiliza para interceptar las comunicaciones entre el usuario y el router. Éste es el método más complejo de los dos, pero también el más efectivo ya que el atacante tiene acceso continuo al router durante horas o días. Además, puede husmear en las sesiones de forma silenciosa sin que la víctima sea consciente de nada.

Una variante más reciente de este tipo de ataque es el ataque man-in-the-browser. En este contexto, el ciberdelincuente usa una serie de métodos para insertar un código malicioso en el equipo de la víctima que funciona dentro del navegador. Este malware registra, silenciosamente, los datos enviados entre el navegador y las páginas. Estos ataques han ganado en popularidad porque permiten al delincuente atacar a un grupo mayor de víctimas sin la necesidad de estar cerca de éstas.

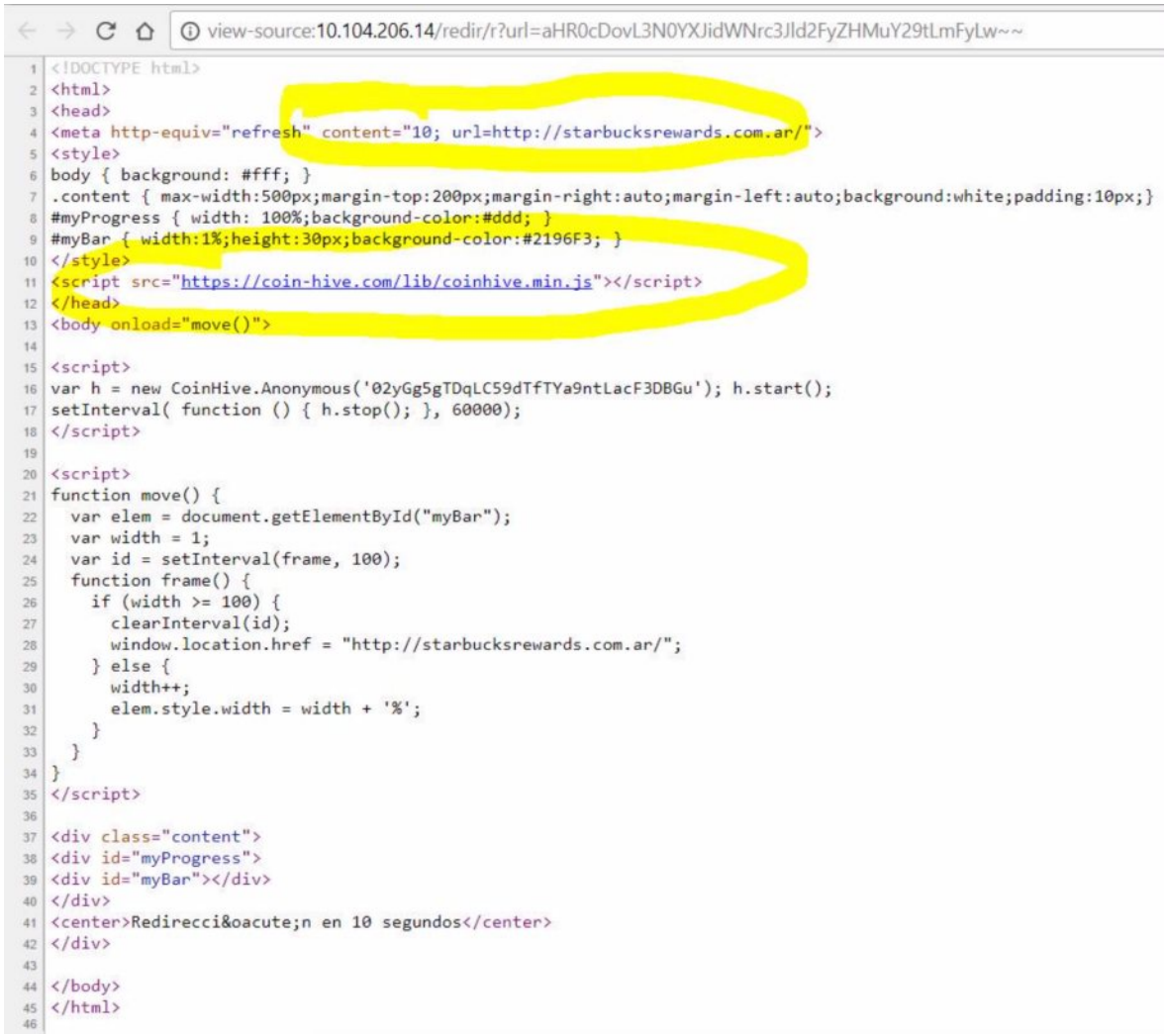
El ataque que es más habitual recibir en eventos es ARPspoof o envenenamiento de las tablas ARP que consiste básicamente en inundar la red con paquetes ARP indicando que la MAC address (identificador único de una tarjeta de red) es la asociada a la IP de la víctima y que la MAC está también asociada a la IP del router (puerta de enlace) de la red. De esta forma, todas las máquinas actualizarán sus tablas con esta nueva información maliciosa. Así, cada vez que alguien quiera enviar un paquete a través del router, ese paquete no será recogido por el router, sino por la máquina atacante, ya que se dirige a su dirección MAC, y cada vez que el router u otro equipo envíen un paquete a la víctima, sucederá lo mismo.

Ahora que entendemos el tipo de ataques que podemos recibir, surgen una serie de preguntas necesarias que hay que hacer a nuestro proveedor de Wifi para cerciorarnos de que podemos estar seguros de estos ataques.

¿Hay posibilidad de que unos usuarios no se vean con otros dentro de la misma wifi?
Cuando los usuarios de una red wifi pueden verse entre ellos (puedes hacer un ping o simplemente ver los archivos que tiene compartidos con la red), se puede realizar el ataque MiTM.

¿El router es capaz de detectar/detener ataques de ARP Spoofing?
Hay routers que son capaces de detectar estos ataques o simplemente vienen preconfigurados para que estos ataque sean inmediatamente mitigados. Es importante conocer si nuestro router tiene alguna de estas opciones.

Este tipo de ataque fue el que se llevó a cabo en el caso de Starbucks donde un atacante editó los paquetes que pasaban por el puerto 80 (el de internet) y modificó las cabeceras de las páginas que visitaban los usuarios de la red añadiendo un código en estas para minar criptomonedas.



¿Los dispositivos que se utilicen en el evento van a estar en una red separada de la red de los asistentes/invitados?

Si tenemos los dispositivos que vamos a utilizar en el evento en la misma red a la que acceden los asistentes, corremos el riesgo de que alguien realice un ataque MiTM y consiga el control de nuestros dispositivos. No queremos, por ejemplo, ver a un atacante poniendo contenido adulto en los monitores.

¿Los datos de acceso que vienen por defecto para la configuración del router van a cambiarse?

Uno de los errores más comunes es dejar los datos de acceso del router por defecto (que no la contraseña del wifi). Un atacante lo primero que va a hacer es entrar a http://192.168.1.1/ o http://192.168.0.1/ y probar si funciona el usuario admin y contraseña admin o 1234. Podemos evitar muchísimos problemas solo cambiando estos datos preconfigurados.

¿Se pueden tener logs de las conexiones al router y de los sitios a los que conectan cada una de las ip?

La mejor forma de saber si sufrimos un ataque es tener el tráfico de nuestra red controlado. Si tenemos logs de las conexiones de cada uno de los usuarios de nuestra red, podremos conocer si alguien está accediendo a un sitio malicioso.

¿Se puede mitigar un ataque de denegación de servicio/de autenticación dentro de la red?
Este ataque es menos común en redes wifi, pero si alguien quiere arruinar tu evento, será uno de los más efectivos. Consiste en congestionar la red de forma que cada usuario que se conecta a la red se desconecta al momento, denegando así el servicio y haciendo que ningún usuario pueda conectarse a internet.

¿Qué debemos preguntar al proveedor de servicios o plataformas (sitio web, registro en línea, aplicación de registro en el sitio, aplicación móvil, 1-2-1?
Muchas veces vemos en los medios cómo muchas plataformas y empresas han sido atacadas por hackers perdiendo así datos y dinero. Aunque nunca estamos seguros al 100%, debemos interesarnos en que los servicios y plataformas que contratamos estén al día con la seguridad y que trabajen activamente en la resolución de errores para evitar, en la medida de lo posible, que sufran uno de estos ataques que puedan afectarnos directamente.
Para estar al corriente de la seguridad de una plataforma, deberíamos conocer los siguientes siguientes datos:

- *¿Se pueden contratar test de seguridad perimetrales y de penetración (pentesting) externos para comprobar la seguridad de la plataforma?*
  Muchas veces la mejor manera de comprobar la seguridad de una plataforma o de un servicio es contratando tú mismo a otra empresa que realice tests de seguridad (aprobados previamente por la plataforma a testear). De esta forma te aseguras tener un informe fiable de las posibles fallas de seguridad que puedan tener, y en el caso de que las tuviesen puedes hablar con el equipo técnico que lleva los servicios para preparar un plan de resolución de estos.

- *¿Las API son públicas o privadas?*
  La mayoría de plataformas y servicios tienen una API pública o privada, es importante saber si el servicio que vas a contratar dispone de una y, sobre todo, como se solicita el acceso a esta.

- *¿Qué información se puede obtener mediante las API? ¿Toda o parte de la información que se provee es sensible?*
  Una vez sabemos que la empresa dispone de una API, tenemos que saber a qué tipo de información se puede acceder a través de esta y, sobre todo, ver si provee información sensible que pueda verse sin los permisos necesarios. Por ejemplo, que un usuario sin autenticar, o con un rol sin los suficientes permisos (un asistente por ejemplo) pueda ver datos privados de otros eventos a los que no tiene acceso.

- *¿El proveedor se ha sometido a algún test de seguridad en el último año?*
  Independientemente de que el proveedor te deje realizar tus propios tests de seguridad, es importante saber si ellos realizan tests regularmente (lo normal es que se los haga una empresa externa para corroborar la fiabilidad de los resultados) y, sobre todo, si se han sometido a algún test de penetración en el último año.
  Empresas como Tesla o Google pagan a los hackers que consiguen penetrar en sus servicios. Siempre tienen plataformas de test que son réplicas de las originales para que no afecten a los datos reales.

- *¿Se trabaja activamente en la resolución de problemas de seguridad conocidos como, por ejemplo, los que se pueden encontrar en el Open Web Application Security Proyect (OWASP)?*
  https://www.owasp.org/index.php/Main_Page
  Los errores de seguridad aparecen cada día y los hackers pelean por encontrar cualquier hueco por el que colarse donde no pueden. Hay bases de datos abiertas que contienen la mayoría de los agujeros que se van encontrando como el caso de OWASP. Es importante que el equipo técnico de tu proveedor esté al tanto de los errores que puedan afectarles y trabajen continuamente en la resolución de estos.

- *¿Tienen contratado algún tipo de firewall (como el WAF de Amazon o Cloudflare) para protegerse de ataques de denegación de servicio?*
  Aside from the provider allowing you to make your own security tests, it's important to Es importante que la plataforma o servicio de tu proveedor esté enmascarada con un firewall o balanceador de por medio como son el WAF de Amazon o Cloudflare ya que evitan que se conozca la IP directa del servidor. Además, estos firewall tienen reglas que permiten detectar y, en muchos casos, mitigar ataques de denegación de servicio o incluso algunos que afectan a la misma plataforma como XSS o SQL Injection.

- *¿Tienen contratado algún monitor de rendimiento?*
  ¿Qué ocurre si estás en mitad de tu evento y se cae el servidor de tu proveedor dejándote sin servicio? Muchos proveedores tienen contratados servicios como Pingdom (https://www.pingdom.com/), que se encargan de monitorear continuamente que un servicio esté activo. En el caso de una caída avisa inmediatamente al equipo técnico que puede encargarse de ver cuál es el problema y ofrecer una rápida respuesta evitando tiempos de demora.

Conclusiones finales

La seguridad es una gran desconocida para muchos pero con un poco de información básica podemos asegurarnos de que los servicios que utilizamos cumplan unos mínimos de seguridad necesarios para evitar la mayor parte de los errores.

Debemos ser conscientes una vez más de que el primer paso en la seguridad de nuestros sistemas somos nosotros mismos, debemos aplicar la lógica y el sentido común ya que desde el nacimiento de internet y con el avance de la tecnología y los smartphones estamos expuestos cada minuto.

Nunca estaremos protegidos al 100% pero podemos disminuir en un gran porcentaje las posibilidades de que nos ocurra algo que no deseamos.