Seguridad en P2P

Qué es y cuáles son las vulnerabilidades de una conexión "peer to peer"

Basado en una experiencia personal durante una auditoria, el autor ofrece aquí detalles acerca de la vulnerabilidad de un sistema conectado P2P describiendo, asimismo, las características de este tipo de enlace. Además, una serie de consejos para evitar el uso malicioso de una red LAN.

Lic. Damián Colaneri
Socio Gerente
T3 Tic Ingeniería SRL
dcolaneri@t3tic.com.ar

En la nota anterior (RNDS Nº 110) vimos la gran cantidad de equipos expuestos en internet a ser invadidos, violando la privacidad de un usuario, lo cual también se convierte en una amenaza para su seguridad en lugar de una herramienta de ayuda. Antes de describir las metodologías para auditar nuestras redes, repasemos un tema que a simple vista parece ideal pero que oculta desventajas si no se procede como corresponde: las conexiones P2P.

¿QUÉ ES "P2P"?

P2P proviene del "peer to peer" o "red de pares", lo cual no es lo mismo que "PtP" o "red punto a punto"; mientras que una red PtP es un enlace directo entre dos dispositivos, un enlace P2P es una conexión entre dos o más pares para conseguir diversos resultados. Es por esto que las redes P2P se clasifican en tres tipos, de los cuales vamos a centrarnos en la conexión P2P de cámaras IP, DVR, NVR, etc., que permiten ver las imágenes desde el exterior de la LAN de forma sencilla. Esto es porque, de forma tradicional y la que se recomienda como buena práctica, al querer conectar un dispositivo a internet y verlo desde fuera era necesario abrir los puertos correspondientes en el router, ya que nos conectaremos desde internet a la LAN de la implementación. Para esto, debemos conocer a la perfección los puertos que utiliza el sistema a instalar y tener acceso de administrador al router, que en muchos casos puede volverse complicado.

Actualmente, los dispositivos vienen provistos de un código QR que al ser leído por un smartphone se conecta automáticamente y muestra el video. Esto es posible porque la conexión P2P del dispositivo genera una conexión saliente desde la LAN a internet. Como vimos en artículos anteriores, los puertos en los router se abren cuando la conexión es de afuera hacia adentro, pero las conexiones de adentro hacia afuera no están limitadas. Esto pasa incluso en firewall económicos o mal implementados. El dispositivo, entonces, trasmite los datos al exterior los cuales, en su mayoría, van hacia a un servidor del mismo fabricante. Luego, nuestro smartphone con el código que leyó se conecta a ese mismo servidor y con ese código da acceso al sistema. Estamos teniendo, entonces, un "gestor" entre nuestro dispositivo y nuestro smartphone que se ocupa de nos enlacemos sin abrir puertos ni saber cuál es nuestra IP pública.

¿QUÉ DICE LA EXPERIENCIA?

Basado en una experiencia personal, durante una auditoria y probando todos los códigos QR de unas DVR, me conecté a una grabadora que se encontraba en otro país, en una fábrica con sus operarios trabajando. ¿Por qué pasó eso? Por un error involuntario del fabricante, se colocaron dos QR idénticos en dos DVR diferentes. El enlace con el servidor lo generó el primer dispositivo que se conectó, que fue la DVR desconocida para mí. Es por esto, y porque tenía usuario y clave por defecto, que termine visualizando algo que no debería.

Si bien esto fue un accidente, ¿cuántas veces podría repetirse? Más allá aún y pensando de forma maliciosa, como solemos hacer para analizar la seguridad: supongamos que vamos de visita a un cliente y podemos estar unos segundos cerca de un dispositivo de seguridad con código QR. Sin que nadie se percate podríamos con nuestro smartphone o mejor aún con un smartwatch, que pasa más desapercibido, leer el código para luego irnos y tener acceso al sistema de cámaras del lugar sin que se percaten. Incluso, con técnicas más avanzadas, podemos usar esta conexión inicial como puerta de entrada a la LAN y luego darle usos diferentes para acceder a servicios corporativos.

Mi recomendación, más allá de jamás dejar usuarios y claves por defecto, es que configuren los accesos a mano y quiten todas las etiquetas de códigos QR de los dispositivos. Si bien muchos pensarán que abrir puertos en los router es peligroso, es un riesgo que podemos auditar y controlar con más precisión.

Como dato de color de distintos usos del P2P, el mensajero WhatsApp funciona de la misma manera: nuestro smartphone se conecta con un server de whatsApp y de ahí se retransmite el mensaje al destinatario y todos los mensajes pasan a través de un servidor de la empresa. Es por esto la importancia de la encriptación extremo a extremo, a diferencia de la encriptación PtP. ■