Como realizar un testing básico

Protección para sistemas electrónicos

La vulnerabilidad de los elementos que componen un sistema de seguridad electrónica está latente. Y a mayor número de sistemas instalados, más probabilidades de que se transformen en blancos de ataque. Aquí, una manera sencilla de detectar esos factores de vulnerabilidad.

Lic. Damián Colaneri
Socio Gerente
T3 Tic Ingeniería SRL

Retomamos la línea de la primera nota -RNDS Nro 108- sobre vulnerabilidades en los sistemas de seguridad electrónica, ya sea por falla del fabricante o por mala implementación del instalador y en esta ocasión explicaremos algunas técnicas básicas mediantes con las cuales se pueda armar un pequeño check-list, a realizar al terminar una implementación, la cual iremos desarrollando en esta y en próximas notas. Estas técnicas no requieren de una software especializado ni se necesitan conocimientos de seguridad de la información: es netamente una guía sencilla para adoptar como buena práctica y dar un mejor servicio a los clientes.

Más allá de lo expresado anteriormente, mi recomendación profesional es que se trabaje a modo de anticipación. Con esto quiero decir que debemos prepararnos hoy para los problemas de mañana. Por ejemplo, según estudios realizados en los últimos meses, se estima que durante 2018 se duplicarán la cantidad de dispositivos IdC, lo cual podría implicar que tengamos el doble de cámaras, DVR, NVR y alarmas instaladas, que podrían transformarse en el principal objetivo de vector de ataque.

Por eso las empresas deben capacitar a su personal en seguridad de la información. Este capital humano que sumarán será altamente rentable en el corto y mediano plazo, cuando seguramente un cambio en las normas de implementación solicitará que las mismas sean analizadas por personal calificado en dicha área. Las empresas más pequeñas podrían contratar el servicio con una consultora cuando sea necesario.

SISTEMAS SEGUROS

Muchos podrían pensar la vulnerabilidad de un sistema solo es importante si la implementación está conectada a una red WAN, como Internet, y que si ésta implementación es en un banco que cuenta con área de seguridad informática, por ejemplo, no tendrán problemas. Esto es erróneo: siempre debe aplicarse seguridad, que llamaremos de aquí en adelante "hardening", no importa donde se implemente. En el caso de grandes empresas, Gobierno o bancos es donde más atención debemos prestar a la seguridad de nuestra implementación.

Comenzaremos por la seguridad en implementaciones más chicas para luego crecer hasta las corporativas.

Usaremos Google como herramienta para encontrar fallos de implementaciones caseras, simple y efectivo. El browser, mas allá de realizar búsquedas estándares, tiene herramientas para realizar búsquedas más precisas, entre ellas "inurl".

Este parámetro sirve para que Google nos muestre todas las páginas que en su dirección (url) incluyan alguna palabra que nos interese, en lugar de buscar las palabras en el contenido de la página. Ahora, como bien sabemos, cada marca dispone de un acceso web para visualizar, o configurar y cada una de ellas tiene su factor de composición de url. Esto lo sabemos simplemente con descargar el manual del dispositivo que nos interese, el cual también nos informará el usuario y clave por defecto.

Como ejemplo práctico (sirve para todas las marcas de dispositivos solo cambiando el factor de composición de url): tipeando en Google "inurl:/view.shtml" sin las comillas, accederemos a varias cámaras o DVR que no tienen ningún tipo de autenticación o la tienen por defecto. Así podemos probar con la marca que queramos.

También tenemos otro comodín, "intitle", el cual busca en el título de la web y no en la url. Conociendo los títulos que cada marca usa podemos buscar, de la misma manera, cámaras libres. Ejemplo intitle: "Live View", que nos permite ver varias cámaras, pero me voy a detener en algo particular: si luego de realizar la búsqueda anterior vemos alguna que el link termina en "/anonymous" significa que la DVR/NVR está protegida con contraseña pero permite el ingreso anónimo. Resumiendo: aunque tiene usuario y clave, con solo tildar "anonymous" accederemos al sistema.

Para ejemplificar lo expuesto que están los sistemas mal implementados, dejo una web que recopila y hace estadísticas de sistemas abiertos o con claves irrisorias como 123456. Si ingresan a http://www.insecam.org/en/, verán que hay más de cien mil dispositivos indexados y permite filtrar por país. También cada marca tiene la posibilidad de sumar la suya. ■