De: A. Ripoll & asociados.
Fecha: 30 de Enero de 2.012
Asunto: Informe Técnico

Contenido:

Medios utilizados.
Relación de técnicas empleadas en su realización.
Resultados.
Análisis de las instalaciones.

ANGEL RIPOLL & asociados
DETECTIVE PRIVADO
DIRECTOR DE SEGURIDAD

Licencia D.G.P n. 208
Colegiado n. 2

INFORME TÉCNICO de la inspección realizada el día 27 de Enero de 2.012 , en los locales de la Vicepresidencia de la Generalidad Valenciana.

El material técnico empleado ha sido:

Para el cableado: Wire Finder M508E.

Para el sistema telefónico analógico: Reflectrometro Tektronix 1503 TDR, Analizador de Comparación y Generador de BF MIC03, Insulation Tester PE-453

Para el espectro radioeléctrico: Analizador Datong Ranger 2+, con telemetría y análisis de espectro, Detector de RF CCS, Receptor de análisis Xplorer, de Optoelectronics, Receptor Sun.

Para los sistemas pasivos: Analizador de Banda Ancha Magnético JF02.

Para las cámaras de TV: Detector VCD-43, Detector Rf/Tv y Detector Optico Start S1.

Para las señales de I.R. Receptor fotosensible I.R. CPM.

Para los ordenadores: Programas anti software espia.

Para las redes WiFi: Detector WiFi/Cam Comceptronics y Receptor WLAN Hotspot..

Para los campos magnéticos: Gaussimetro EMF 827

Y además se ha dispuesto de:

Detector de metales, y de señales de AC. Analizador de espectro Standard AX700. Osciloscopio, Analizador y Voltímetro de precisión

TiePie Handyprobe. Cámara fotográfica con objetivo "macro". Sonda de B.F. Lampara de Wood (luz U.V.) y precintos de seguridad (testigos). Generador de ruido rosa REI, ANG2000. Sonda de vibraciones de pared y cristal. Frecuencimetro digital hasta 2.8 Ggh. Scanner AOR. Juego de herramientas profesionales y equipo de iluminación.

El trabajo realizado ha consistido en:

Servicio de análisis telefónico (barrido de tono, detección de RF, análisis ecometrico, consumos de bucle y tensiones de reposo y servicio), servicio de análisis radioeléctrico (detección de emisores, detección de IR), detección de sistemas pasivos, detección de cámaras ocultas (con cables, o via radio), inspección ocular, colocación de testigos, análisis de conductividad sonora de paredes y techos , revisión de los repartidores telefónicos y análisis del sistema informatico.

Después de una visión de conjunto de las instalaciones, se inicia la Inspección, con el siguiente desglose:

Se procede a detectar **cualquier emisión radio eléctrica** generada en los locales donde se sitúa el receptor, bien por captación de sonido ambiente, bien por intervención de las líneas telefónicas. Para ello, se explora el espectro comprendido entre los 200 K/c y los 2,5 Ggh (Con el Datong Ranger). El demodulador discrimina AM, FM, WFM y SC. Estos parámetros representan el 100% de posibilidades de emisión de cualquier dispositivo existente (excepto los GSM). Para excitar aquellos emisores que disponen de VoxControl, se ha activado un generador de sonido . Este equipo, almacena la información radio eléctrica, permitiendo a posteriori su estudio, por volcado en un PC.

Se ha conectado a la **red eléctrica** el receptor, para captar aquellas señales, que utilizan ese cableado para sus emisiones.

Con el Xplorer, y el Rx Sun se han escuchado y analizado las portadores mas fuertes, presentes en cada lugar.

Con el detector CCS, se ha comprobado, que al poner en funcionamiento las terminales telefónicas, no existe ningún GSM asociado a la línea.

Con un **Receptor para IR.** se ha buscado cualquier emisión modulada. La razón de emplear este equipo es que existen emisores que en vez de emitir en radio, lo hacen en señales de IR. (parecidas a las de los telemandos de un televisor).

Con el **Detector de Redes WiFi,** se verifica que no existe ninguna red activa en las proximidades, por el uso de cámaras y micrófonos, por este sistema. Si existe, se comprueba si esta encriptada, y el origen de las señales.

Con todos estos sistemas se detecta cualquier sistema de emisión de audio y vídeo activo, operando desde los locales observados

A continuación se ha explorado el espectro magnético, para detectar **cualquier fuente de alimentación y componentes electrónicos activos** de cualquier tipo . La motivación es la existencia de artificios de escucha accionados por un telemando, y que en caso de estar apagados, no permitirían su detección por señales de R.F. y la detección de sistemas GSM, bien activos o en reposo.

Con este sistema se detecta cualquier equipo electrónico situado en los locales. (independientemente de su peligrosidad**)**

Con los detectores de cámaras de TV, se procede a verificar que no exista ninguna emplazada en el local, aunque funcione con cables directamente. Así mismo se explora con un detector especifico para cámaras vía radio, o WiFi.

En los casos en que es recomendable se han seguido los pasos siguientes:

Se han observado los terminales telefónicos, y en general cualquier aparato susceptible de ocultar elementos de grabación o escucha (enchufes múltiples de AC y TF etc.), procediendo a una inspección ocular minuciosa para detectar cualquier manipulación

extraña, y se ha procedido a sellar con laca de U.V., para poder detectar en futuras Inspecciones, si ha sido alterado.

Se ha medido la **conductividad sonora** de paredes y mamparas, para evaluar la posibilidad de que desde un local contiguo se pueda escuchar con una Sonda (en el caso de locales situados en edificios compartidos).

En los **techos practicables,** se ha realizado una inspección ocular, desmontando algunos tramos, para ver el estado físico del cableado, y apreciar la existencia de dispositivos extraños a la instalación normal, o cableado parásito.

Respecto a las **líneas telefónicas** y una vez descartada la presencia de emisores en el cableado o en las terminales, se ha inspeccionado el Repartidor, y se han analizado los pares dubitados (en las líneas analógicas), comparándolos con otros, para observar cualquier anomalía en los parámetros físicos de los mismos.

Para señalar los pares se ha inyectado una portadora modulada de HF, desde el terminal, hasta el Repartidor, que permite seguir todo su recorrido, y detectar cualquier derivación a otro par.

Se ha procedido al seguimiento físico y electrónico de toda la línea, desde el repartidor hasta las terminales.

Finalmente, con laca fluorescente al U.V. se han marcado los bornes, para posteriormente, advertir cualquier manipulación.

Con relación al **sistema informatico**, se ha verificado su vulnerabilidad, respecto a manipulaciones maliciosas. En caso de ser procedente, se han instalado y ejecutado programas capaces de detectar la presencia de programas espía (troyanos, key logers, etc.)

Respecto a las condiciones generales de Seguridad de la empresa, se evalúan: control de accesos, seguridad física, detección de incendios y lucha contra el fuego, salidas de emergencia, alarmas y cerraduras, almacenamiento de mercancías peligrosas y destrucción de documentos.

Los locales estudiados han sido: 9 salas, y 10 terminales telefónicas.

El resultado final de todo ello ha sido, según mi leal saber y entender, que: **NO SE HA DETECTADO LA PRESENCIA DE NINGÚN DISPOSITIVO DE ESCUCHA.**

Ahora bien, respecto a las condiciones de Seguridad de los locales observados debo señalar lo siguiente:

En la mayoría de los despachos, la impresora, esta conectada a la red (1). Así mismo, se carece de destructores de papeles.

En el despacho del Vicepresidente, existe una puerta que da a la escalera, desde cuyo rellano, se escucha perfectamente lo que se habla en el interior. Convendría verificar la ausencia de objetos extraños (grabadora, etc), en dicho punto.

En el despacho del Portavoz, existen unas rejillas, que comunican físicamente con el antedespacho, que además, es el puesto de trabajo de un ordenanza, y dispone de sillones, para visitas. A causa de estas rejillas, lo que se habla en el despacho, se escucha fuera. Convendría cerrarlas, con lamina de contrachapado y burlete de silicona.

En la Sala de Juntas grande, hay instalado un sistema de megafonía inalámbrica Bosch. Este equipo, por sus características de emisores, puede ser captado desde el exterior, con un equipo adecuado, como por ejemplo, un receptor de la misma marca y modelo (2). Debiera ser sustituido, por un equipo convencional, cableado, por la más elemental norma de seguridad.

Este informe se acompaña por un manual sobre Protección de la Información, para el exclusivo uso del cliente, ya que cuenta con Derechos de Autor.

1) Al imprimir por red, todo el documento viaja por la red. Es impreso por una sola impresora, pero, la

información, ha llegado a toda la Red. Si en alguno de los PC conectados, existe un programa tipo "snifer", puede ser recibido. Indudablemente, esto se evita, simplemente conectando el PC a la impresora con un cable de USB.

2) Todo lo que va por radio, por radio se puede oír, con un receptor adecuado. En este caso, estas emisiones, de poca potencia, pueden ser copiadas, desde cierta distancia, con un equipo semejante, al instalado en la sala, y una antena adecuada, para permitirle mayor distancia.

Angel Ripoll