LA SEGURIDAD NO ES UN JUEGO...¡EL FÚTBOL SI!

Col. Ing. Especialistas – Rosario 2017

Fernando Corvalán / Ing. Fernando Villares

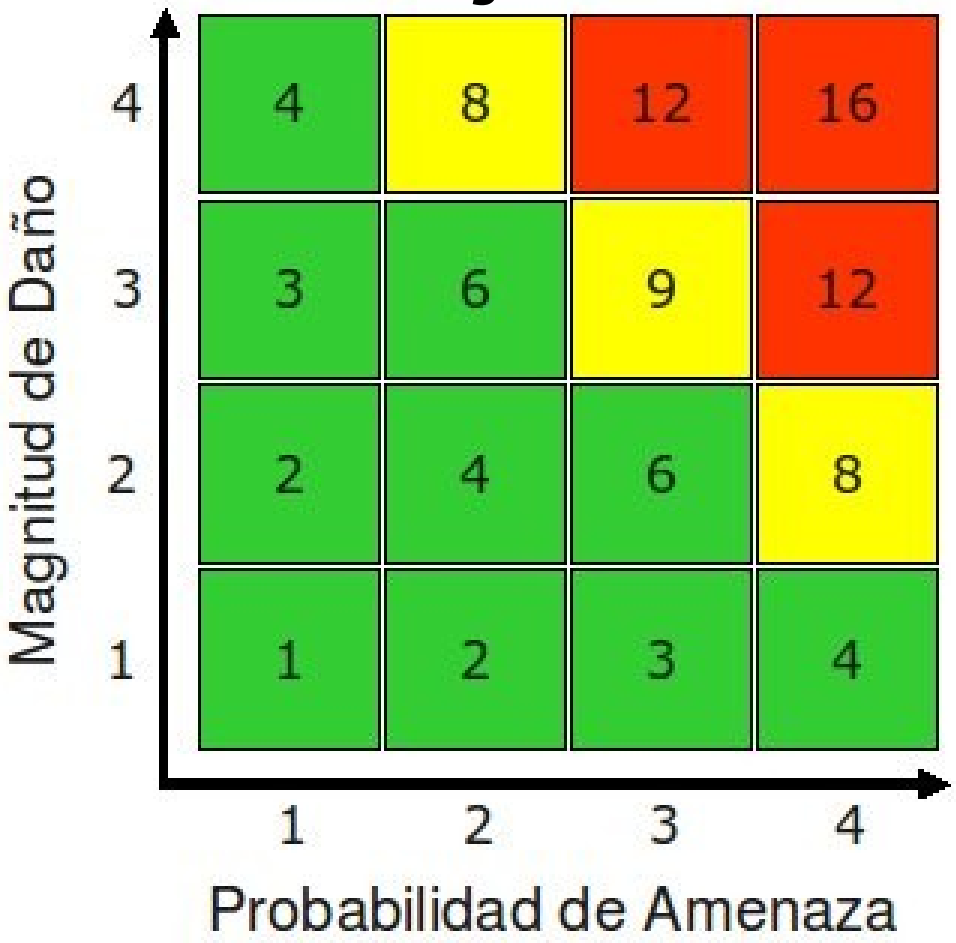
La previa...

- ✔ Bounty de 5 BC en dominio .onion de la deep web.
- ✔ 0 Estrategias de seguridad de los wedding planners.
- ✔ Poco tiempo disponible.
- ✔ Activos informáticos de altísimo valor.
- ✔ Solicitud de absoluto respeto a la privacidad de parte de terceros.
- ✔ Lugar abierto al público y rodeado de redes abiertas.
- ✔ Invitados de muy alta exposición mediática
- ✔ Periodistas inescrupulosos.

El análisis de riesgos

✔ **Riesgo = Probabilidad de Amenaza x Magnitud de Daño. La Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente**

1 = Insignificante (incluido Ninguna)
2 = Baja
3 = Mediana
4 = Alta



Clasificación de Riesgos:

- Alto Riesgo: 12 - 16 (rojo)
- Medio Riesgo: 8 - 9 (amarillo)
- Bajo Riesgo: 1 – 6 (verde)

El análisis de riesgos

- Riesgo alto:

- Equipamiento informático de los organizadores.
- Comunicaciones internas.
- Filtración de imágenes previa y durante evento.
- Ingreso de equipamiento inf. no autorizado.
- Uso de equipamiento no autorizado.
- Filtración de señales radioeléctricas indebidas.
- Fallas colaterales de equipos dedicados al evento (DJ, fotógrafos, cotillón luminoso, micrófonos, enlaces de equipamiento lumínico y de sonido).
- Equipamiento y datos RAW de video y fotografía.
- Datos de los equipos celulares de los invitados.
- Control de infraestructura estática del casino.
-

- Riesgo medio:

- ✔ Uso de drones en las cercanías.
- ✔ Comunicaciones informales entre muchos proveedores poniendo en riesgo detalles.
- ✔ Uso de almacenamiento compartido en la nube.
- ✔ Uso permanente del predio antes del evento.

- Riesgo bajo:

- ✔ Control de los celulares o invitados por protocolo.
- ✔ Control de proveedores que accedían al evento.
- ✔ Medios de prensa en sector apartado relativamente al sector a controlar.

El operativo de seguridad antes del evento

✔ OSINT sobre los invitados, proveedores, etc.

✔ Reconocimiento previo físico del lugar.

✔ Estrategias de segurización de comunicaciones, backups seguros y almacenamiento cifrado de los activos informáticos asociados al evento.

✔ Análisis de los activos informáticos a proteger, riesgos y estrategias de mitigación asociadas.

✔ Relevamiento de señales digitales y análisis de espectro previo al evento para comparación posterior.

✔ Capacitación sobre estrategias de seguridad de la información a empleados clave y con acceso a información sensible.

Las contramedidas ideales:

✔ Uso de BOXCryptor para cifrado de archivos en la nube, acceso solo desde sistemas verificados y con verificación de 2 pasos.

✔ Uso de emails cifrados y firmados digitalmente.

✔ Comunicaciones de voz y texto claves via telegram con autodestrucción de mensajes asi como uso de métodos de divulgación de información parcial y códigos para evitar leaks.

✔ Revisión de seguridad de todos los celulares involucrados y uso de tarjetas SIM y numeracion tuenti para anonimización.

✔ Contratos de confidencialidad.

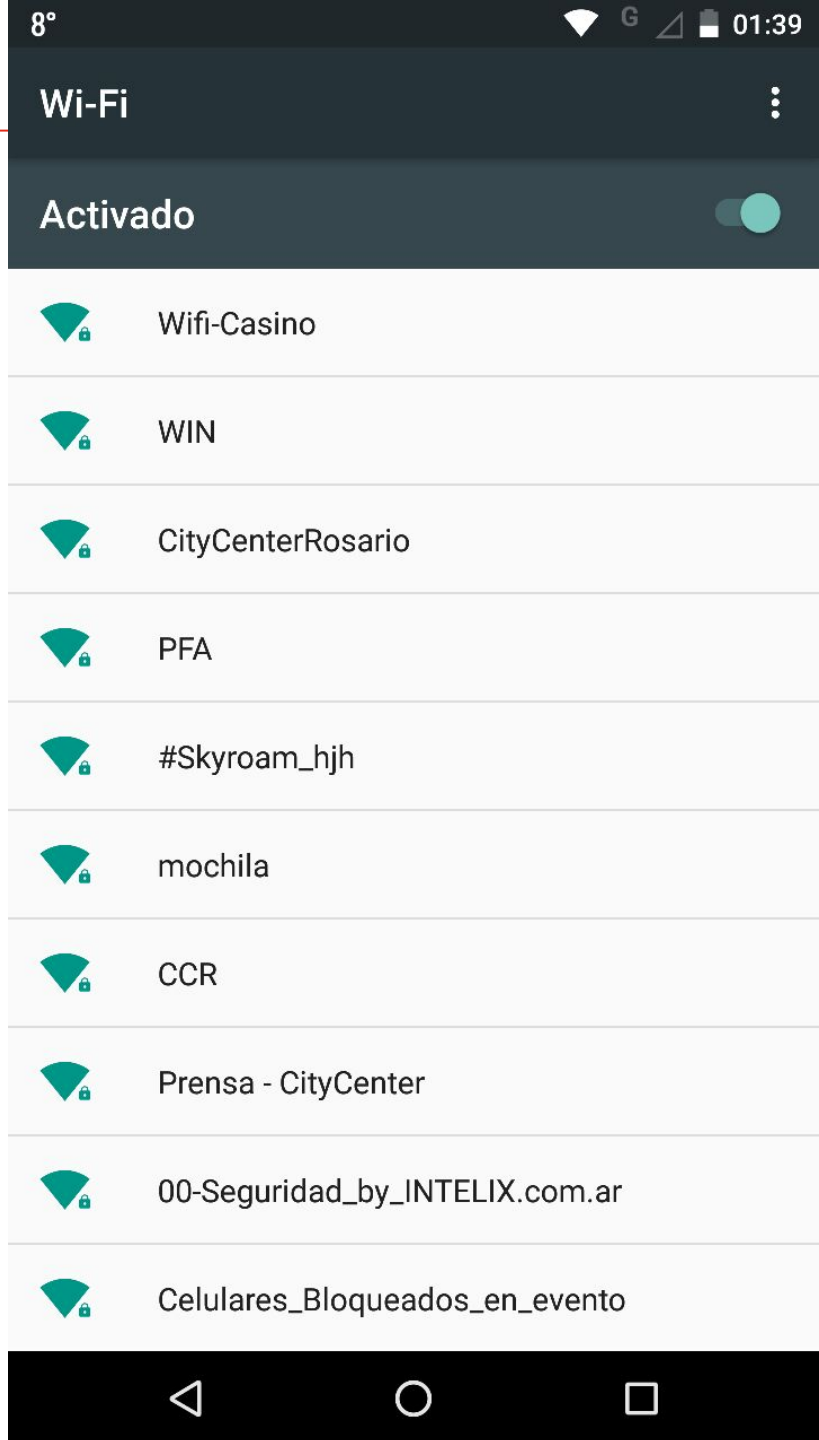
✔ Medidas cautelares, para evitar difusión de imágenes obtenidas ilegalmente, en medios masivos.

Las contramedidas activas:

- Análisis de espectro desde 500mhz a 5.7ghz en todo el evento y uso de OSINT en real time con BOTS en redes sociales y medios digitales.
- Bloqueo e interferencia activa de frecuencias GSM 2G, UMTS 3G, LTE4G, 2.4ghz y 5,8.
- Escaneo y clonado en alta potencia 2watts con antena OMNI de 15dBi de toda nueva señal de WiFi en 2.4 y 5.8Ghz no interferida.

Herramientas utilizadas.

- ✔InSSIDer
- ✔Kali linux
  - ✔Nmap
  - ✔Kismet
  - ✔Wireshark
  - ✔Metasploit
- ✔LTE discovery (android)
- ✔Wifi Analyzer (android)
- ✔OpenSignal (android)
- ✔Ubiquity AirView
- ✔Inhibidores TAMCE 4G+
- ✔Telegram
- ✔RTL2832u SPEKTRUM



El resultado

telefe noticias
Periodismo

Política Actualidad Internacionales Deportes Tránsito Re

Portada › Actualidad | 04 julio 2017

Celulares bloqueados, conexiones ocultas y famosos indiscretos: así fue el operativo de seguridad "digital" del casamiento de Messi

La difícil misión de evitar filtraciones de la boda del año: antenas para tirar frecuencias de wifi, invitados indiscretos y una recompensa por la lista de asistentes.

[Exclusivo de #IMPULSO] Cómo fue el operativo de seguridad informática del casamiento de Messi

Una empresa de Rosario se ocupó de montar un operativo, único en el país, para evitar que se filtren imágenes y videos durante la ceremonia

15.6°

EN VIVO Radio 2 Seguinos

El bloqueo informático que sorprendió a los famosos en boda de Messi

Una empresa rosarina detectó que había recompensas en la interne profunda para quien lograra filtrar datos o fotos de la boda del año los organizadores y montó un operativo inédito, con bloqueadores un bunker especial. La reacción de los invitados

05 de Julio de 2017

COMENTARIOS

Por: Rosario3

VANITY FAIR

ACTUALIDAD CELEBRITIES MODA REALEZA VANITY FAIR TV REVISTA SU

HOME - CELEBRITIES

Todos los detalles de la boda Messi-Roccuzzo: seguridad israelí, cumbia y sushi

33

Aquí está todo lo que necesita saber sobre el enlace del futbolista Lionel Messi y Antonela Roccuzzo, que tiene lugar este viernes

Por NURIA HERNÁNDEZ | 29 de junio de 2017 / 9:41

El resultado

Conclusiones

- ✔ No hubo ningún tipo de filtración de información previa o posterior al evento por parte de la organización o empleados.
- ✔ Se mantuvo la integridad, confidencialidad y la disponibilidad de la información de la organización.
- ✔ No hubo violaciones a la intimidad e integridad de los anfitriones ni a los invitados.
- ✔ La prensa no lucró ni interfirió con el evento.
- ✔ El operativo de seguridad fue encubierto 100% hasta pasado el evento y ¡SOMOS ROSARINOS NO ISRAELIES!
- ✔ El bloqueo de señales fue efectivo al extremo de lograr que la gente deje sus aparatos y disfrutara la fiesta, vlviéndose un evento cuasi retro.
- ✔ La información de los fotógrafos y camarógrafos estuvo protegida hasta ser entregada en manos del anfitrión.

¡Gracias totales(r)!

@fmvillares / @fercorvalan

www.intelix.com.ar