

- RELAZIONE TECNICA - BONIFICA AMBIENTALE E TELEFONICA





XX

ATTENZIONE: I CONTENUTI DELLA PRESENTE RELAZIONE TECNICA E TUTTI GLI ALLEGATI EVENTUALMENTE PRODOTTI, RIVESTONO CARATTERE DI ASSOLUTA RISERVATEZZA E NE È FATTO ASSOLUTO DIVIETO DI DIVULGAZIONE PUBBLICA AD OGNI MEZZO.

• PREFAZIONE:

Questa piccola guida tecnica introduce i clienti al mondo delle bonifiche elettroniche. Con questo termine si identifica un'attività tecnica, corredata da strumentazione, che ha lo scopo di trovare in un ambiente delimitato la presenza di microspie o dispositivi elettronici atti a "captare abusivamente" informazioni e dati sensibili.

Si rimane tipicamente interessati a questo tipo di attività quando ci si ritrova in:

- Cause e controversie Civili
- Amministrazione Pubbliche per gare d'appalto
- Si ricoprono funzioni Pubbliche o Istituzionali
- Operatori nel campo della Giustizia, magistrati o giudici
- Riunioni aziendali importanti da parte del management, ricerca e sviluppo ecc...
- Agiate condizioni economiche con tenori di vita elevati
- Furti con o senza scasso in auto, abitazioni o uffici
- Aziende dove i direttori, manager o dipendenti che ricoprono incarichi importanti si licenziano
- Ecc....

In sostanza chi si ritrova in posizioni sociali importanti,di potere, ed economicamente rilevanti sono SEMPRE a rischio INTERCETTAZIONI !!

Affidandosi al nostro Staff riuscirete a eliminare ogni dubbio riguardante la Vostra vita quotidiana.

Inoltre forniamo e istruiamo il personale preposto, per preservare nel miglior modo la propria privacy.

Vi ricordiamo inoltre che il presente documento è strettamente personal

RICORDIAMO INOLTRE CHE I CONTENUTI DELLA PRESENTE RELAZIONE
INFORMATIVA E TUTTI GLI ALLEGATI EVENTUALMENTE PRODOTTI, RIVESTONO
CARATTERE DI ASSOLUTA RISERVATEZZA E NE È FATTO ASSOLUTO DIVIETO DI
DIVULGAZIONE PUBBLICA AD OGNI MEZZO.

Vi ringraziamo per la scelta accordata alla IRX sagl

INDICE:	
• DATI INTERVENTO TECNICO	pag. 4
• TIPOLOGIA DI INTERVENTO RICHIESTO	pag. 4
• LA STRUMENTAZIONE UTILIZZATA	pag. 6
• NOTE TECNICHE SULL'INTERVENTO	pag. 7
• CONCLUSIONI	pag. 8
• CONSIGLI E RIMEDI	pag. 9
• CONSEGNA:	pag.10

DATI INTERVENTO TECNICO:

Esecuzione bonifica elettronica eseguita nelle date e nelle circostanze da Voi indicate:

- 24-05-2016, Lunedì mattina

Abitazione sita in via ______

Ora inizio esecuzione operazioni:

Ora fine esecuzione operazioni:

TIPOLOGIA DI INTERVENTO RICHIESTO

Dopo essere stati contattati, si determinava un tipologia d'intervento urgente richiesta espressamente dal cliente per possibili "attacchi" riconducibili all'ambito famigliare. La tipologia di intervento richiesto e analizzato prevedeva le seguenti voci che andremo a descrivere brevemente:

- Analisi personal computer e reti LAN o WI-FI: richiesta

Non

Verifica hardware e software per l'individuazione di spy-ware,virus, back-door ed ogni altro tipo di possibile attacco informatico effettuabile

- Analisi linee telefoniche analogiche e digitali:

Negativo

Verifica delle linee telefoniche presenti per l'individuazione di possibili micro,traslatori, registratori ed ogni altro tipo di possibile attacco telefonico da poter effettuare.

Analisi cellulare e spy-phone: richiesta

Non

Verifica hardware e software per l'individuazione di micro o software spy-phone ed ogni altro tipo di possibile attacco su telefonica mobile effettuabile (XX)

- Analisi rilevamento passivo senza emissione di rumori:

Negativo

Verifica eseguita con attrezzature e software per l'individuazione di microtrasmettitori ed ogni altro tipo di possibile attacco ambientale effettuabile in condizione di silenzio

- Analisi rilevamento attivo con iniezione di fonia nell'ambiente: Negativo

Verifica eseguita con attrezzature e software per l'individuazione di microtrasmettitori ed ogni altro tipo di possibile attacco ambientale effettuabile in condizione di rumore generato.

- Ambientali e telefoniche analogiche:

Negativo

Verifica eseguita con attrezzature e software per l'individuazione di microtrasmettitori analogici ed ogni altro tipo di possibile attacco ambientale effettuabile

- Ambientali e telefoniche digitali:

Negativo

Verifica eseguita con attrezzature e software per l'individuazione di microtrasmettitori digitale o spread spectrum ed ogni altro tipo di possibile attacco ambientale effettuabile

- Ambientali GSM, GPRS, UMTS, 3G:

Negativo

Verifica eseguita con attrezzature e software per l'individuazione di microtrasmettitori di tipo GSM che utilizzano ponti ripetitori di telefonica mobile (BTS) ed ogni altro tipo di possibile attacco ambientale effettuabile

- Onde convogliate su rete elettrica:

Negativo

Verifica eseguita con attrezzature e software per l'individuazione di microtrasmettitori digitale che utlizzano la rete elettrica domestica ed ogni altro tipo di possibile attacco ambientale effettuabile

- Microcamere e trasmettitori audio/video:

Negativo

Verifica eseguita con attrezzature e software per l'individuazione di micro-telecamere che utilizzano frequenze tipicamente oltre 1,2 Ghz

- Cablate via filo e registratori a cassette o allo stato solido:

Negativo

Verifica eseguita con attrezzature idonee per l'individuazione di microtrasmettitori/registratori o microfoni cablati che possono essere anche nella condizione di stand-by,spente, antibonifica o semplicemente con batteria esaurita.

Wi-fi e Bluetooth:

Negativo

Verifica eseguita con attrezzature e software per l'individuazione di microtrasmettitori SLAVE di tipo Wi-fi o Bluetooth che utilizzano queste nuove tecnologie per poter colloquiare con altri apparati MASTER posti nelle vicinanze.

- Analisi su autoveicoli:

Negativo

Verifica eseguita con attrezzature specifiche ed ispezione visiva e manuale su zone specifiche del veicolo che meglio si prestano all'installazione di dispositivi di attacco, quali trasmettitori su rete cellulare e localizzatori GPS.

LA STRUMENTAZIONE UTILIZZATA

Il lungo elenco, sopra descritto, di possibili minacce per la propria privacy, necessita di strumentazioni all'avanguardia e di continui e costanti aggiornamenti da parte dei nostri tecnici.

La continua ricerca di nuove tecnologie di attacco ci permette di affinare ed ampliare quotidianamente le nostra conoscenze per l'individuazione di minacce tecnologiche. Le attrezzature professionali impiegate vengono prodotte da professionisti ed utilizzate da oltre un centinaio di Agenzie Governative nel mondo.

Nel dettaglio la strumentazione che andiamo ad utilizzare:

- Rilevatore OSCOR5000E omni-spettrale, per cattura e identificazione frequenze per bonifiche ambientali fino a 3 GHz. La gamma di frequenze coperte permette l'identificazione di "attacchi" audio e video.

Tale strumento permette anche la memorizzazione temporale delle scansioni per eventuale revisione dati post-bonifica o stampa immeditata su carta chimica.

- Rilevatori di radiofrequenze fino a 6 GHz per bonifiche ambientali REI-CPM700 e SWEEPMASTER PLUS con relative sonde per linee telefoniche,onde convogliare,infrarossi e laser.
- Rilevatore di microspie GSM/GPRS e di microspie burst (ad impulsi) da 800 MHz a 2500 MHz
- Rilevatore NEW PRO 7000 Microspie GSM 900-1800, UMTS, 3G e microcamere wireless UMTS
- Rilevatori ST-107 con logger temporale interno e diagnosi real-time per freq. fino 7Ghz.
 - Rilevatore di giunzioni lineari REI-ORION 4000, per poter trovare microfoni cablati, registratori, microcamere occultate o in genere elettronica dietro qualsiasi superficie. Questo apparecchio risulta importante per poter discriminare e ispezionare una superficie sulla quale visivamente non si riscontrano "anomalie".
 - Termo camera FLIR, idonea a riscontrare differenze termiche dovute ad apparecchiature elettroniche in funzione o meno.

NOTE TECNICHE SULL'INTERVENTO

L'esecuzione della bonifica, con la presenza di personale da Voi autorizzato, è stata approntata passo-passo andando ad analizzare uno ad uno i locali interessati a tale operazione.

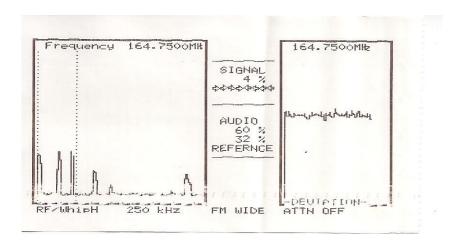
Per questione di riservatezza e privacy non vengono allegate ne foto ne piantine inerenti i locali analizzati

Nell'analisi specifica andiamo ad elencare i singoli locali che sono stati analizzati in ordine cronologico, in presenza di Vs. personale autorizzato a tali operazioni:

- **1°locale analizzato** - Camera da letto matrimoniale – 2° piano - Vengono identificate prese a muro 220Vac principali, con punti luce e prese telefoniche più arredi di vario genere.

Rilevate seguenti frequenze innoque:

164,750 MHz (presenza di ponti trasmissivi uso dati)



- **2º locale analizzato** Bagno adiacente camera da letto matrimoniale 2º piano Vengono identificate prese a muro 220Vac principali, con punti luce e prese telefoniche più arredi di vario genere.
- **3° locale analizzato** Ripostigli adiacenti camera da letto 2° piano Vengono identificate prese a muro 220Vac principali, con punti luce e prese telefoniche più arredi di vario genere.

• **CONCLUSIONI**:

Per ognuno dei sopracitati locali, è stata verificata la **NON PRESENZA** di frequenze "in aria" riconducibili a possibili trasmettitori di qualsiasi natura.

Per ognuno dei sopracitati locali, è stata verificata la <u>NON PRESENZA</u> di possibili apparecchiature elettroniche funzionanti a batteria, di tipo cablato o non funzionanti. In conclusione, l'operazione di bonifica effettuata nei locali da Voi indicati ha dato esito <u>NEGATIVO</u> per quanto riguarda la possibilità di fughe di informazioni sensibili. Vi ricordiamo però che non possiamo certificare il fatto che possibili apparecchiature elettroniche abbiano potuto operare prima del nostro intervento.

Il nostro consiglio è quello di voler provvedere immediatamente, di fronte ai primi dubbi, a richiedere questo tipo di intervento prima che sia troppo tardi!

CONSIGLI E RIMEDI:

Dopo l'operazione di bonifica effettuata Vi sottoponiamo alcuni strumenti che potranno esserVi utili per effettuare o adottare nel tempo efficaci contromisure.

Analisi personal computer e reti LAN o WI-FI:

Analisi periodica dedicata su PC e rete LAN

Eliminazione rete Wi-fi in virtù della facilità di "bucarle" anche su chiavi WEP,WPA2 etc...

Eliminazione uso chiavi USB.

Adozione password alfanumeriche da cambiar periodicamente.

Analisi cellulare GSM, GPRS, UMTS, 3G e spy-phone:

Eventuale utilizzo di disturbatori dedicati in uffici strategici.

Adozione di dispositivi cellulari criptati tra diretti interessati.

Ambientali e telefoniche analogiche e digitali:

Utilizzo di rilevatori palmari professionale tascabili ad es.

ìDET by Raksa dalle ridottissime dimensioni: 77x43x18 mm e dal peso di soli 35 g.



Questo strumento offre un immediato riscontro a possibili dubbi con estrema semplicità.

Tipologia di segnali rilevabili:

ANALOGICI, GSM900 /1800, UMTS (3G), CDMA450, DECT, BLUETOOTH, WI-FI a 2.4 GHz

ALTRI SEGNALI AD IMPULSI.

CONSEGNA	:				
La present in original	e relazione st e al Sig:	ampata su 1	0 fogli total	i, viene rila	sciata
Luogo e data					