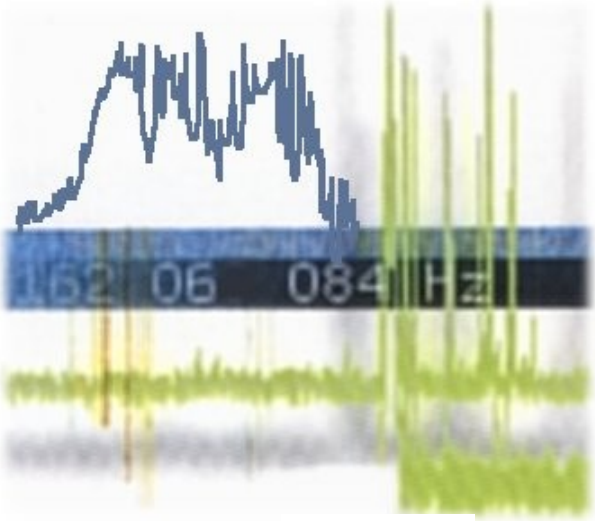
ANALISI DELL'INQUINAMENTO AMBIENTALE DA RADIOFREQUENZA

Vista da

Armido Lazzarotto



C.P.S. Control Engineering

www.cps85.com

C.P.S. Control Engineering Via Leopardi 15/4 - Noventa Padovana 35027 PADOVA – Mod.796612/27155/C

INTRODUZIONE

Al giorno d'oggi l'Azienda, sia di grandi sia di piccole dimensioni, è soggetta a diverse tipologie di minacce, di solito non considerate nell'ambito dell'organizzazione aziendale, ad esempio: personale interno infedele o tentativi esterni atti a carpire informazioni interne riservate. Quindi tutelare tutti i dati, i supporti informatici, i colloqui e gli incontri interpersonali da riprese audio/video o prelevamento dati non autorizzati, è più che mai indispensabile.

Avete notato delle strane coincidenze riguardo a preventivi presentati o a nuovi progetti, con risvolti negativi per la Vostra attività ?
E' tempo di programmare un'analisi dei Vostri Uffici o della Vostra abitazione.

E' necessario sviluppare una sensibilità maggiore a queste tematiche viste anche in un'ottica di concorrenza europea ed internazionale.
Per una sicurezza costante nella tutela della Vostra rete informatica e degli ambienti strategici per la Vostra Azienda, diventa necessaria una programmazione ordinaria di analisi ambientale per neutralizzare alla radice ogni tentativo di intrusione illegale.

Un'Azienda efficiente ed attenta ai propri interessi commerciali deve investire anche nella sicurezza delle proprie informazioni.

PERCHE' BISOGNA PROTEGGERSI

> Non trasformiamo l'acquisto di nuove apparecchiature informatiche, che risolvono problemi contabili ed amministrativi fondamentali per la Nostra Azienda, in un "CAVALLO DI TROIA" che esternamente si presenta "BENE" ma al suo interno può riservare qualche spiacevole sorpresa.

> 45.000 i siti Web per hacker presenti in internet nei quali si possono trovare tools ed applicativi specifici per tentare di introdursi nelle reti aziendali.

> Il 78% di intrusioni nella sicurezza del sistema informatico aziendale proviene dall'interno della rete aziendale.

> Il 56% delle aziende americane dichiara di aver subito attacchi alla propria rete, ma molte altre non lo sanno o lo negano per motivi di immagine.

> La protezione dei propri dati personali è un bene primario che va difeso con tutte le armi disponibili, viste le problematiche a livello sociale e finanziario che ne potrebbero derivare.

CONSIDERAZIONI CHE SI POSSONO TRARRE

> E' necessario intraprendere da parte delle Aziende delle soluzioni ben definite e immediate in tema di sicurezza delle informazioni, per tutelarne l'operato.

> Non si deve accordare fiducia incondizionata a NESSUNO in termini di rete informatica in Azienda.

> Più complessa è la rete LAN o WLAN, maggiore è la necessità di regole ben definite per migliorarne la sicurezza.

> Gli amministratori del sistema informatico all'interno dell'Azienda è preferibile che non decidano in maniera autonoma.

SOMMARIO

PROPRIETA' E DIRITTI ESCLUSIVI DELLA PUBBLICAZIONE

PERCHE' RICHIEDERE UN'ANALISI AMBIENTALE

Tutelare le informazioni, specialmente per chi tratta direttamente o indirettamente dati di carattere riservato, oggi più che mai, è di primaria importanza.

Semplici usi quotidiani come:

- il telefono
- il cellulare
- il telefax
- internet
- Wireless Lan
- PC o desktop o palmare

Elaborazioni come:

- immagini video nel Vostro monitor
- trasferimento dei dati su memorie di massa
- trasferimento dati tramite rete Lan o Access Point

Uso di impianti fissi come:

- telecamere a circuito chiuso o rete Lan
- interfonici interni
- trasferimento dati via radio
- trasferimento immagini via rete Lan o intranet

possono essere veicolo di disseminazione di informazioni riservate, nel caso in cui la "CONCORRENZA" si avvalga di tecnologie atte a trasmettere all'esterno i dati analogico-digitali presenti nei Vostri ambienti sia privati che di lavoro.
Tecnologie ad altissima miniaturizzazione possono essere già presenti nell'ufficio o nell'abitazione che state occupando, oppure possono essere installate con estrema rapidità con coperture molto semplici che si integrano nella Vostra giornata senza destare in Voi alcun sospetto.

COME FUNZIONA UN TRASMETTITORE AMBIENTALE

Di ridotte dimensioni, per la sua costruzione vengono impiegate tecnologie ad alta integrazione ed il montaggio della componentistica interna usa di solito il sistema SMD e per quanto riguarda gli stadi oscillatori sono impiegati quarzi molto precisi, per offrire una stabilità di frequenza in trasmissione impeccabile e quindi più facile da ricevere.

E' provvisto di un microfono ad alta sensibilità in grado di captare anche voci a distanza notevole, e a seconda delle difficoltà di ricezione dei suoni, vengono usati microfoni dedicati con inserimenti nei casi critici (quali rumori di fondo provenienti ad esempio da una musica ad alto volume, traffico, ecc...) di filtri attivi che riescono ad eliminare quasi completamente questo tipo di rumori facendo riaffiorare la voce.

Ha una frequenza di trasmissione molto stabile localizzata di solito nella banda VHF-UHF.
Come antenna può usare un normale cavetto unipolare o può avvalersi, se il caso lo permette, della linea telefonica o del cablaggio inserito nelle canaline interne dell'impianto elettrico.
Per l'alimentazione di questi microtrasmettitori vengono usate tensioni (continue o alternate 50 Hz) comprese in genere dai 3 ai 380 Volts con autonomie, se alimentati a batterie, che vanno da diverse ore a molti mesi. Questi parametri possono essere molto variabili in base al tipo di microtrasmettitore e ai vari sistemi di gestione del consumo di corrente (VOX); in alcuni casi il microtrasmettitore può essere alimentato direttamente dalla linea telefonica con autonomie illimitate nel tempo.

Nel caso di occultamento all'interno di un telefono cellulare l'alimentazione viene fornita dalla batteria che alimenta il telefono stesso.

Può essere in alcuni casi alimentato dalla tensione di rete 220-380 Volts alternati 50-60 Hz con autonomia illimitata.

Oltre a captare la voce può trasmettere immagini video o dati digitali del Vostro PC.
Il segnale a radiofrequenza trasmesso (analogico o digitale) è in genere di debole potenza per evitare eventuali spurie o disturbi indotti in altre frequenze, ma può essere ricevuto a diversi chilometri di distanza da una postazione ricevente, sia mobile che fissa, dotata di solito di registratori digitali (hard disk) in grado di registrare solo quando è necessario sia sorgenti audio che video.

SOLO UN'ACCURATA ANALISI AMBIENTALE PUO' INDIVIDUARE TUTTI I TIPI DI MICROTRASMETTITORI AMBIENTALI ATTIVI O INATTIVI.

C.P.S. Control Engineering Via Leopardi 15/4 - Noventa Padovana 35027 PADOVA – Mod.796612/27155/C

OCCULTAMENTI POSSIBILI DI MICROTRASMETTITORI

- Telefono
- Telefax
- Telefono Cellulare

Vengono installati lungo la Vostra linea Telefonica tradizionale (PSTN) o ISDN o ADSL, anche all'interno delle centraline telefoniche situate nei pressi del Vostro ufficio o abitazione. Non hanno bisogno di alimentazione tramite batterie interne visto che solitamente vengono alimentati dalla linea stessa: in questo modo possono trasmettere 24 ore su 24. Riescono ad inviare varie tipologie di dati e tutte le chiamate in entrata e in uscita anche a diversi chilometri di distanza.

- PC o Notebook

Le informazioni presenti nel Monitor (disegni, tabulati, progetti vari, ecc...) o che vengono elaborate tramite il Vostro PC possono essere facilmente trasmesse all'esterno dei Vostri ambienti da varie tipologie di microtrasmettitori anche di elevata potenza, vista la facilità di avere una alimentazione comoda tramite il PC e di facile occultamento.

- Stampante
- Periferiche

I dati inviati alla Vostra stampante o ad altre periferiche (memorie di massa) possono essere trasmessi in modo tale da avere all'esterno dei Vostri ambienti la copia esatta del documento o dei dati appena spediti alle periferiche.

- Ambienti

Il microtrasmettitore può essere occultato all'interno di oggetti vari o mobili del Vostro ufficio e viste le piccole dimensioni può essere facilmente inserito oltre che nell'arredamento anche in apparecchiature di uso quotidiano tipo la calcolatrice o la macchina del caffè. Il microtrasmettitore può essere munito del dispositivo "VOX" che fa azionare lo stadio di trasmissione solo in presenza di suoni o voci, aumentandone così l'autonomia di trasmissione e rendendolo difficile da localizzare, oppure può essere attivato solo in certi momenti tramite un telecomando ad infrarossi.

C.P.S. Control Engineering Via Leopardi 15/4 - Noventa Padovana 35027 PADOVA – Mod.796612/27155/C

OCCULTAMENTI POSSIBILI DI MICROTRASMETTITORI

- Ambientale Video

Sempre con la stessa tecnica possono essere trasmesse immagini (in analogico o digitale) riprese all'interno dei Vostri uffici o abitazione; se siete già provvisti di un impianto di videosorveglianza il rischio aumenta sensibilmente vista la semplicità di inserimento di un trasmettitore video direttamente all'uscita della telecamera ed autoalimentato dall'impianto stesso.

- Impianto elettrico

Il microtrasmettitore può essere inserito all'interno di qualsiasi presa di corrente o in una scatola di derivazione ed è alimentato direttamente dalla linea elettrica 220-380 Volts e quindi attivo 24 ore su 24, come antenna usa la linea elettrica esistente e quindi riesce a coprire, anche con bassissime potenze, distanze notevoli. L'impianto elettrico può essere veicolo non necessariamente di portanti a radiofrequenza, ma di altri tipi di modulazione chiamate onde convogliate a bassa frequenza che si concatenano con la corrente elettrica presente e riescono a trasferire sia Voce/Video che dati.

- Automobile/Aeromobile/Natante

Al loro interno ci sono moltissime possibilità di occultare un microtrasmettitore senza che il proprietario sospetti qualcosa e anche le situazioni favorevoli all'installazione sono molteplici, quali ad esempio l'ordinaria manutenzione che richiedono. L'alimentazione viene fornita direttamente dall'impianto elettrico a bassa tensione (batterie) e quindi può trasmettere il segnale Audio/Video 24 ore su 24.
Un altro dispositivo installato abusivamente nei mezzi mobili è il localizzatore satellitare per intercettare tutti i Vostri spostamenti, che sfrutta la ricezione di segnali GPS e che tramite la rete Cellulare invia la localizzazione del mezzo compreso Voce e Video direttamente a terzi.
Esiste anche un altro dispositivo più subdolo che rileva solo la posizione del mezzo mobile ma i dati di posizione in questo caso vengono memorizzati all'interno dell'apparecchiatura per circa 10 giorni e poi scaricati tramite segnale Bluetooth™ a favore di terzi: in questo caso l'apparecchiatura che memorizza gli itinerari abusivamente ha una considerevole autonomia, nonostante la piccola batteria interna.

NUOVE TECNOLOGIE CON QUALCHE RISCHIO

- Telefono Cellulare

La Telefonia Cellulare in questi ultimi anni ha avuto una forte evoluzione sia in termini di servizi che numero di apparecchi telefonici portatili. Il rischio nell'uso quotidiano di un Telefono Cellulare è ormai a livelli notevoli, ne elenchiamo alcuni tra i più significativi.

> Clonazione da parte di terzi della Sim Card: esistono dei duplicatori in vendita che producono la copia esatta della Vostra Sim Card, con tutti gli effetti collaterali che comporta.

>L'inserimento fraudolento di alcuni File all'interno della Vostra Sim Card tramite una normale telefonata ricevuta (di solito anonima e con caduta della linea repentina). Da quel momento il Vostro Telefonino diventerà una perfetta microspia pilotabile a piacere da parte di terzi e ricevibile in tutto il mondo.

> Il Telefonino lasciato abbandonato per qualche ora può essere un bersaglio da parte di terzi per l'inserimento di un Software specifico che modificherà a Vostro svantaggio le funzioni interne del Telefonino trasformandolo in un perfetto microtrasmettitore.

> Tramite il sistema Bluetooth ™, che ormai equipaggia la dotazione tecnica interna della maggior parte dei Telefoni Cellulari, vengono sottratti senza autorizzazione da parte di terzi i dati interni residenti nel Telefonino come la rubrica, messaggi SMS, chiamate effettuate, ricevute, ecc....

Questi sistemi di intercettazione permettono in qualsiasi momento della giornata a malintenzionati di ascoltare in diretta i Vostri colloqui privati semplicemente componendo il Vostro numero di telefono senza destare sospetti, visto che la gestione del Telefonino è stata modificata escludendo la suoneria, display e illuminazione.

Le nostre Analisi ambientali possono comprendere anche la verifica del Vostro telefono Cellulare compresa la Sim Card.

NUOVE TECNOLOGIE CON QUALCHE RISCHIO

- Reti Informatiche Wireless LAN (via radio)

E' di uso comune ormai sostituire il collegamento via cavo dei PC che compongono la rete LAN di un'azienda con una rete via radio denominata WLAN che collega i PC senza bisogno di cavi e quindi con la massima libertà di movimento. Queste reti per comunicare devono essere collegate ad un Trasmettitore Digitale detto Access Point, che usa la frequenza dai 2,4 ai 5 GHz e tramite dei ponti di trasferimento può raggiungere decine di chilometri. La rete WLAN deve essere protetta tramite delle chiavi di cifratura selezionabili dal Cliente in modo tale da non permettere l'accesso ad estranei alla propria rete interna.
Purtroppo solo una percentuale molto bassa di reti WLAN aziendali è protetta e quindi molte Aziende sono esposte a rischi di prelevamento di dati ed intromissione in rete, con conseguenze che potrete immaginare: sarebbe come abbandonare tutti i dati sensibili dell'Azienda alla merce di tutti i malintenzionati che ne vogliano fare uso.
Le effrazioni che di solito vengono perpetrate a scapito di un'Azienda sono le seguenti:

> formattazione e quindi la perdita di tutti gli archivi aziendali tramite una intromissione in rete (questa situazione può comportare addirittura il fallimento dell'Azienda stessa);

> copia di dati sensibili, ad esempio archivio Clienti o Fatture emesse , usati poi a scapito dell'Azienda.

Le Nostre apparecchiature durante l'Analisi Ambientale riescono in tempo reale ad esaminare eventuali reti WLAN e a testarne la sicurezza tramite dei simulatori specifici; inoltre riescono a captare e a catalogare eventuali Access Point anomali presenti nell'ambiente circostante all'area interessata.

CARATTERISTICHE DELLE NOSTRE ANALISI

Le Nostre Analisi Ambientali vengono eseguite con particolare cura e minuziosità avvalendosi di strumentazioni ad alta tecnologia e Software dedicato, in gran parte prodotto direttamente nei Nostri laboratori e quindi con caratteristiche di assoluta esclusività ed affidabilità nella rilevazione e misurazione dei segnali riscontrati.

In base all'ambiente da analizzare vengono progettate specifiche soluzioni tecniche comprendenti modifiche (Hardware/Software) oltre che sulla Strumentazione di base anche sui dipoli e sonde di rilevamento, in modo da ottenere un'analisi precisa; pensiamo alla diversità ambientale di un'analisi effettuata in un ufficio in pieno centro città vicino a vari trasmettitori di servizi come la telefonia mobile, piuttosto che in un edificio vicino a dei tralicci ad alta tensione.

Tutti i dati rilevati, compresi i grafici delle misurazioni effettuate e la relativa consulenza tecnica che riporterà le situazioni a rischio individuate con le opportune soluzioni, saranno raccolte in un unico supporto CD-ROM che verrà rilasciato al Cliente.

Inoltre su eventuale richiesta potrà essere fornita un'apparecchiatura elettronica di facile utilizzo che permetterà al Cliente di monitorare i propri ambienti mantenendo una soglia minima ma costante di sicurezza anche subito dopo il Nostro intervento.

C.P.S. Control Engineering Via Leopardi 15/4 - Noventa Padovana 35027 PADOVA – Mod.796612/27155/C

DETTAGLI TECNICI SULLO SVOLGIMENTO DELL'ANALISI

Analisi Impianto Elettrico: verifica caratteristiche sinusoide + armoniche e rilevamento portanti spurie (inquinamento da campi elettromagnetici: convogliate FM, protocolli Analogico/Digitali e varie), iniezione segnali campione in linea con verifica ricezione armoniche, rilevamento carichi induttivi e capacitivi anomali configurati nella linea elettrica da analizzare, campionamenti Tensione Frequenza (To Drift). Misurazione di tracce di inquinamento da radiofrequenza con analisi specifica in tutte le derivazioni dell'impianto elettrico compresa la massa a terra, con verifica dispersione di dati convogliati in linea tramite la presa di terra.

Analisi Impianto Telefonico: ISDN, LAN, PSTN, verifica di inquinamento da campi a radiofrequenza ed elettromagnetici, inserzioni ON LINE con lettura dati di ritorno, simulazione centrale telefonica, misurazione con sistema GAUSS® dei segnali magnetici Centralino, linea, derivazioni, apparecchi telefonici + Fax, misure isolamento capacitivo differenziato conduttori in linea. Rilevazioni di segnali concatenati anomali con induttori specifici. Analisi conduttori con rilevazione tracce a radiofrequenza tramite cavità.

Analisi Ambientale: rilevamenti di inquinamento da campi a radiofrequenza da 10 Hz a 15GHz, LF/MF/HF/VHF/UHF/SHF, analisi portanti anche QPSK Audio/Video, analisi terminali Wireless (11Mbps, 22Mbps, 54Mbps) LAN/VoIP, Hubs, Switches, Router, Firewall, NAS/Server, Printserver, irraggiamento ambientale con frequenze campione, utilizzo di cavità specifiche HI/FREQ, ausilio di Magnetometro ad ampio spettro. Analisi di spettro specifico su Wireless LAN 2,4 GHz, 5GHz. Analisi di spettro su Banda **Wi-Fi® Frequency > A>G** per individuazione di eventuali Access Point, AP repeater, Bridge, Bridge multipunto con documentazione pacchetti dati e localizzazione GPS del dispositivo. Analisi completa Banda **Bluetooth™ ISM** con individuazione di eventuali Link, Bridge installati.Analisi Modulazioni tipo OFDM, FM Hopping, CCK, OFDM + BPSK. Analisi Protocolli tipo TCP/IP, UDP, ARP, FTP, TFTP, http, DHCP, SMTP, SNTP, SMNP.

Rilevazione Infrarosso: ricezione ed analisi sorgente con spettro da 350nm a 800nm con inserzione filtri ottici per l'accuratezza del rilevamento di modulazioni audio sia analogiche che digitali. Individuazione anche di spurie ottiche residue con pesatura segnale ed eventuale decodifica.

Emissione Report Finale : con relazione Tecnica e dati relativi alle misurazioni su supporto **CD-ROM o DVD.**

* Le Procedure, le Tecniche, la Strumentazione, le Antenne impiegate per i rilevamenti potranno subire variazioni in base all'ambiente , all'orografia del terreno, all'intensità dei disturbi interni ed esterni.

APPARECCHIATURE ELETTRONICHE USATE PER L'ANALISI

Strumentazione per l'analisi della Linea Elettrica e cablaggi vari

Oscilloscopio a doppia traccia con interfaccia ingresso dati a bassa frequenza
Filtro discriminatore di segnali modulati in frequenza fino a 400Hz
Analizzatore di rete con simulazione Test di segnali modulati

Strumentazione per l'analisi e test della Linea Telefonica Analogico/Digitale

Analizzatore digitale di segnali in linea telefonica
Stazione di misura Tensione/Corrente con riferimenti di simulazione
Interfaccia seriale per segnali in linea
Interfaccia parallela per segnali linea
Analizzatore segnali e portanti a bassa frequenza in linea telefonica
Simulatore completo di centrale telefonica Telecom Italia

Strumentazione per l'analisi di inquinamento da Radiofrequenza Ambientale

Analizzatore di spettro 2,4 GHz a scansione continua per analisi Access Point Wireless Wi-Fi®™ e localizzazione GPS degli Access Point anomali
Analizzatore di spettro 5 GHz a scansione continua per analisi Access Point Wireless Wi-Fi®™ e localizzazione GPS degli Access Point anomali
Analizzatore di spettro 2,4 GHz a scansione continua per analisi protocolli GFSK (Gussian Frequency Shift Keying) Bluetooth ™
Software dedicato per la gestione e la rilevazione automatica di Access Point Wireless Wi-Fi®™
Power Meter Hewlett - Packard 431/C con interfaccia analogica segnali a Radiofrequenza
Analizzatore di Spettro con filtri digitali da 1 Hz a 1,299 GHz
Analizzatore di Spettro dedicato da 2,399 GHz a 2,500 GHz
Analizzatore di Spettro dedicato da 900 MHz a 2,170 GHz
Analizzatore di Spettro dedicato 2 GHz a 10 GHz
Analizzatore di Spettro dedicato da 10 GHz a 13,550 GHz
Rivelatore di Segnale a sintonia continua da 20 Hz a 1,500 GHz
Rivelatore di Segnale a sintonia continua da 1 GHz a 5 GHz
Rivelatore di Segnale a banda stretta da 1 MHz a 400 MHz
Unità di memorizzazione ed elaborazione portanti a Radiofrequenza con analisi di segnali criptati
Simulatore Tests di portanti a radiofrequenza
Frequenzimetro da 1 Hz a 1,3 GHz con filtri digitali selezionabili
Rivelatore caricato per la direzionalità del segnale ricevuto
Sonda con diodo a Tunnel per tracce segnali radio
Sonda di carico per gamma GSM/DCS/PCS
Software per la gestione dell'analisi in Frequenza
Software per la rivelazione di Armoniche ad ampio spettro
Software per la gestione dell'analisi di Spettro

C.P.S. Control Engineering Via Leopardi 15/4 - Noventa Padovana 35027 PADOVA – Mod.796612/27155/C

APPARECCHIATURE ELETTRONICHE USATE PER L' ANALISI

Strumentazione per il rilevamento Laser Infrarosso

Sensore per gamma infrarosso per segnali da 1 mm a 800 nm
Sensore per gamma laser per segnali da 400 nm a 800 nm
Amplificatore di precisione per l'elaborazione dei segnali sonde
Analizzatore digitale di spettro IR

Antenne e sensori RF

Le Antenne e adattatori di impedenza per la rilevazione di portanti a Radiofrequenza, vengono selezionate ed eventualmente costruite nei Nostri Laboratori in base alle caratteristiche degli ambienti da analizzare e dell'orografia del terreno circostante all'edificio.

Rilevamento di Campo Elettromagnetico a Bassa Frequenza

Analizzatore di segnali elettromagnetici a bassa frequenza con ponte di trasferimento dei segnali misurati a Raggi Infrarossi per non alterare la misura
Sensore di Campo Elettromagnetico a banda stretta
Sensore di Campo Elettromagnetico a banda larga
Sonde di rilevazione campo magnetico a basso segnale

IL NOSTRO PARCO APPARECCHIATURE E' COSTANTEMENTE AGGIORNATO E MODIFICATO, DI CONSEGUENZA QUESTA LISTA STRUMENTAZIONE E' PURAMENTE INDICATIVA.

C.P.S. Control Engineering Via Leopardi 15/4 - Noventa Padovana 35027 PADOVA – Mod.796612/27155/C

C.P.S. Control Engineering Via Leopardi 15/4 - Noventa Padovana 35027 PADOVA – Mod.796612/27155/C