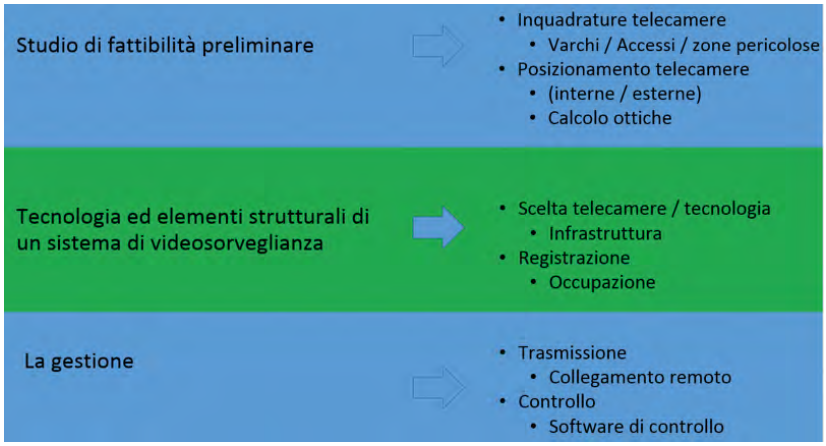
Sei sicuro che l'impianto di videosorveglianza che stai installando sia sicuro?

a colloquio con Luca Girodo, esperto CCTV e sicurezza IT, docente di securindex formazione.
a cura della Redazione

Nell'attuale contesto di allarme generalizzato per le minacce combinate (physical + cyber), quali sono i livelli di rischio dei sistemi di videosorveglianza in rete?
I sistemi di CCTV inseriti in una rete sono, a tutti gli effetti, da considerarsi dei punti di possibile rischio.
Negli ultimi anni abbiamo progressivamente visto crescere il numero di dispositivi esistenti sulla rete. Questo ha portato alla definizione, ormai conosciuta da tutti, di **Internet of Things** o **Internet delle Cose**.
Ogni device che ha a bordo una connessione di rete (cablata o wireless) e un indirizzo IP, può essere raggiunto dall'esterno, se non è protetto in modo adeguato; ovviamente, il nostro impianto CCTV non fa eccezione.
I prodotti dei giorni nostri sono assolutamente **Internet Ready**, cioè tutti hanno protocolli trasmissivi su IP: quindi, sono raggiungibili da un punto qualsiasi della nostra rete interna e, purtroppo, anche dall'esterno. Questo significa che il sistema di sorveglianza può essere intercettato e "visto" anche da persone non presenti nella sala di sorveglianza, o addirittura non presenti in loco.
I malintenzionati odierni sono perfettamente a conoscenza dell'esistenza dei nuovi sistemi e si muovono con lo scopo di eluderli. Sono una vera e propria nuova "specie criminale", con nuove competenze "physical + cyber".
Ciò comporta che gli operatori del settore debbano essere sempre aggiornati sulle tecnologie: gli installatori sulle metodologie di attacco per poter adeguare le contromisure e aumentare i livelli di sicurezza, i produttori sulle specifiche di protezione cyber dei loro apparati. Il tutto avviene ormai con una velocità di adeguamento elevatissima e la tendenza non sembra diminuire.

Gli installatori, inoltre, devono anche svolgere il continuo controllo e manutenzione degli impianti, non solo per un controllo fisico di un device, ma soprattutto per aggiornare i software e i firmware.
Se un sistema TVCC non viene installato e manutenuto correttamente, esso stesso rappresenta una fonte di rischio gravissimo per la nostra rete locale. Per questo, il livello di formazione degli installatori di sistemi di videosorveglianza deve essere adeguato. Un professionista che segue continui percorsi formativi è la sola certezza che il cliente ha per minimizzare questo tipo di rischio.

Qual è il livello di consapevolezza da parte di progettisti, integratori e utilizzatori finali rispetto alle vulnerabilità dei sistemi CCTV?
Durante le sessioni di corso ho avuto modo di confrontarmi con progettisti, installatori ed integratori su questo tema. Dal piccolo installatore al progettista di impianti la sensazione è risultata sempre la stessa: tutti si sono dimostrati preoccupati



per le vulnerabilità dei sistemi CCTV. Sicuramente ha giocato a favore di questo l'evoluzione formativa sull' IoT (Internet delle Cose) che ha portato il settore a domandarsi se gli impianti CCTV potessero essere anch'essi dei punti "sensibili" per la sicurezza delle infrastrutture.

I trend di vulnerabilità scoperte nei singoli apparati e negli impianti è stato in continua crescita e i corsisti si sono trovati più volte coinvolti in casi del genere.

D'altro canto, ho purtroppo rilevato che le informazioni che si possono facilmente reperire non sono in grado di dissipare i loro dubbi in merito: anzi, in molti casi la sensazione di "insicurezza" è davvero aumentata. Le novità sono in continua evoluzione ma, purtroppo, le fonti di informazione sempre le stesse e, chiaramente, non riescono ad aggiornarsi in tempo utile.

Molto spesso le logiche di un mercato sempre più competitivo portano gli operatori a spostare in secondo piano queste tematiche, dimenticandosi però che un **vero professionista di questo settore deve offrire sicurezza**, che passa anche e soprattutto dai livelli di vulnerabilità degli stessi apparati.

Un professionista deve poi confrontarsi con il cliente finale per capire che cosa intenda con il termine "sicurezza". Il cliente purtroppo approccia solitamente l'argomento solo dal lato economico, sottovalutando l'utilità di una scelta tecnologica.

Non è mia intenzione affermare con questo che il prodotto più costoso sia sempre il migliore, ma che il livello di qualità della componentistica debba avere degli standard minimi per poter garantire l'efficienza dell'impianto stesso. In aula, questa tematica viene sempre affrontata dal punto di vista della professionalità dell'operatore, che deve sempre e comunque essere garantita, anche se questo lo può porre in difficoltà con qualche cliente o addirittura qualche produttore. Il professionista conosce sempre le caratteristiche tecniche di quello che propone, e sarà sempre ben preparato ad affrontare qualsiasi problematica si possa presentare in un progetto.

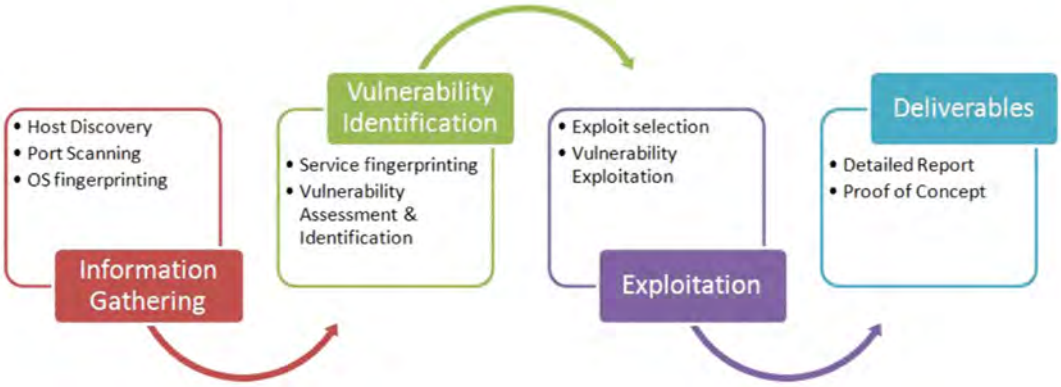
Quali sono gli accorgimenti da adottare e i comportamenti da evitare per assicurare ragionevoli livelli di sicurezza ai sistemi CCTV, sia nella funzione propria di gestione delle immagini che come parti dei sistemi IT delle organizzazioni?

Questa è una tipica domanda che mi viene fatta all'inizio del mio corso. E la mia risposta è sempre la stessa: **l'istallazione a regola d'arte**.

Nella fase di installazione di un sistema CCTV, gli errori più classici e banali sono quelli che compromettono le caratteristiche stesse dell'impianto. Non vorrei sembrare scontato, ma cambiare le password di sistema, disabilitare gli utenti guest, aggiornare sempre i firmware già di per sé aiutano a mantenere un impianto in sicurezza.

Esiste poi la necessità di effettuare la valutazione dei rischi ai quali il nostro sistema può essere esposto. Parliamo della fase di progettazione: se un impianto CCTV si collega ad una rete aziendale, è obbligatorio fare uno studio preliminare ed un controllo successivo all'installazione per verificare se i nostri apparati hanno creato dei punti di vulnerabilità all'interno dell'infrastruttura (ad esempio, porte di comunicazione rimaste inutilmente aperte verso l'esterno).

Successivamente, questa infrastruttura deve essere sottoposta alle stesse policy di sicurezza di tutte le apparecchiature che si trovano in rete, il che significa:



- aggiornare i software ed i firmware;
- verificare se l'infrastruttura sia protetta da firewall all'interno dell'azienda, verificando che sul firewall ci siano le configurazioni corrette;
- confermare se la videosorveglianza debba essere vista da remoto;
- controllare dove vengono registrate le immagini (ora dati) e se le registrazioni sono esse stesse protette come tutti i dati aziendali. A tal proposito vorrei ricordare che tali registrazioni hanno una validità massima di 48 ore e durante questo periodo non possono andare perse o distrutte.

Un valido sistema per testare la conformità alle politiche di sicurezza è quella di eseguire un **Penetration Test** sulla infrastruttura, cosa che permette di confermare o meno le vulnerabilità nascoste e la conformità all'analisi del rischio svolta precedentemente durante lan fase di progettazione dell'impianto. Anche per i sistemi di videosorveglianza non interconnessi con una rete si devono adoperare le stesse cautele. Il concetto deve essere focalizzato sul fatto che le immagini sono dei dati e quindi come tali devono essere trattati.

Quali sono i contenuti formativi delle sue lezioni su Videosorveglianza e Sicurezza dei dati all'interno del corso di securindex propedeutico alla certificazione IMQ AIR?

Il mio training per la certificazione IMQ AIR è strutturato in sessioni composte da diversi passaggi formativi. Dapprima si introducono i concetti di Safety e Security, per affrontare poi la fase di progettazione di un impianto di videosorveglianza, sia esso analogico o over IP. Vengono successivamente analizzate tutte le componenti di un sistema, mettendo in rilievo le "features" necessarie (ad esempio, se si tratta di un apparato da interno o esterno, individuare il fattore di forma), poter identificare il prodotto più adatto alla realtà del cliente e definire come inserirlo nel progetto globale.

Il termine **progetto** è uno dei focus del corso, è il tema principale di tutto il modulo formativo, in quanto solo una adeguata fase di progettazione permetterà poi ai professionisti di offrire al cliente finale il prodotto finito adatto alle sue esigenze, realizzando così quello che il concetto di "Sicurezza" racchiude.

Oltre alla parte dedicata specificatamente al calcolo degli obiettivi, delle focali, ai corretti dimensionamenti degli apparati di registrazione, a come e dove posizionare le telecamere, nel corso si affrontano le nozioni di collegamento degli apparati in rete, sia locale che geografica.

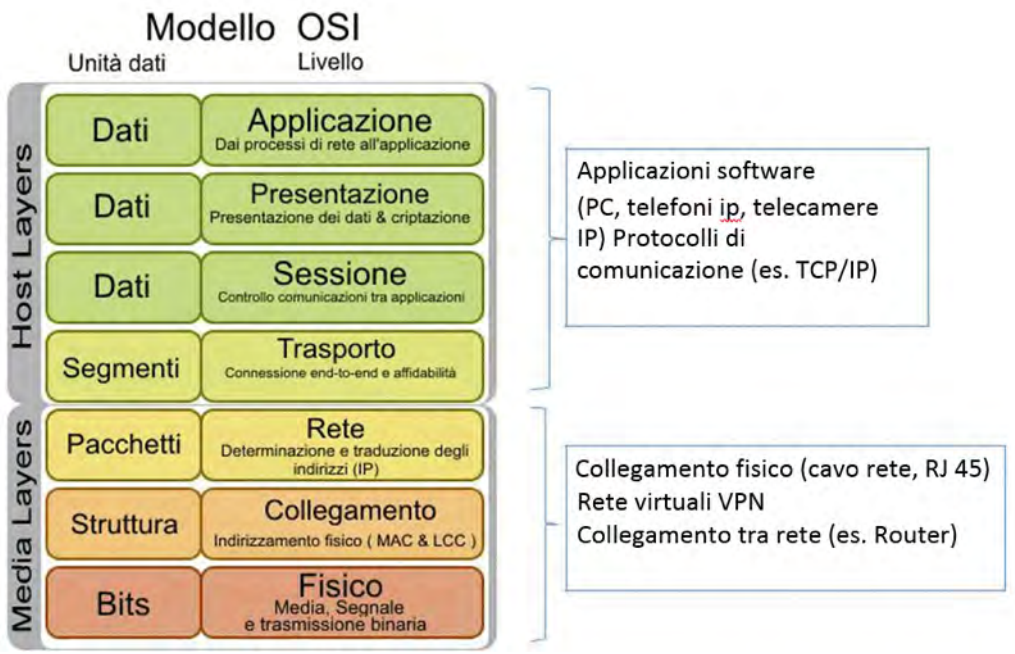
Questa sessione di networking parte dal modello ISO/OSI sul trasporto dei dati fino ad affrontare le tematiche del trasporto dei dati, soffermandosi su tutte le principali metodologie di connessione e di infrastruttura.

Tutta la parte di networking permetterà al corsista di concepire il sistema di videosorveglianza come parte di un sistema network più evoluto e complesso che gli permetterà di inserirlo correttamente anche in infrastrutture già esistenti, o di realizzarne di nuove.

Si procede poi alla parte tecnica, con l'analisi di progetti reali, in modo che i partecipanti possano interagire e mettere in pratica tutto ciò che hanno appreso fino a quel momento.

La sessione in cui collettivamente i corsisti sono invitati ad esprimersi è, col tempo, diventata un appuntamento irrinunciabile delle lezioni poichè condividere i progetti reali porta ad un costruttivo confronto per tutta la classe.

Il training ritorna poi in forma prettamente accademica e



si procede analizzando come l'eseguire un Pen-Test sia un efficace strumento di misura per la realizzazione di ogni progetto. In questa fase possiamo riassumere tutte le best-practice che avremo messo in campo durante la progettazione e studieremo come validare tutte le varie parti del sistema che completa l'intero progetto.

L'argomento sicurezza dei dati viene dettagliato con la spiegazione delle moderne tecnologie e con l'interazione delle stesse con le vigenti norme di legge, al fine di poter fornire al partecipante una completa formazione professionale che potrà a sua volta offrire come servizio professionale ai propri clienti.

Il modulo si conclude con ancora esempi di applicazione di tutti gli strumenti di analisi video avanzati e la loro capacità di generare nuove opportunità per gli installatori. Casi pratici e casi di insuccesso motivano un secondo di momento di confronto tra i corsisti.

Quali saranno gli sviluppi della proposta formativa di securindex per questa area?

Tutti i corsi securindex sono strutturati in moduli di quattro ore dedicate a specifiche aree tematiche.

Questo permette a noi docenti di poter strutturare i corsi utilizzando le aree di maggiore interesse per le classi che veniamo a formare.

Nel Q4 del 2017 prenderanno il via nuove aree di approfondimento sulle reti locali LAN, sulle reti geografiche WAN ed un corso specifico sulle applicazioni di analisi video complesse.

Per le loro caratteristiche, questi corsi sono definiti di livello avanzato e il requisito minimo per la partecipazione sarà il superamento dell'esame IMQ-AIR.

Inoltre, siamo già pronti ad erogare corsi sulla sicurezza delle reti e degli apparati CCTV sia a livello di Assessment che a livello di Penetration Test. I corsi avanzati saranno strutturati con un modulo di training teorico ed un blocco di esercitazione per ogni area tematica.

Altri moduli sono in fase di realizzazione e di fine tuning, al fine di proseguire il mio personale impegno ad offrire un portafoglio sempre più ampio di moduli di corso per continuare a rispondere alle crescenti e sempre più precise richieste dei partecipanti ai corsi di mia competenza.

CONTATTI - LUCA GIRODO
www.linkedin.com/in/luca-girodo-8b046a16