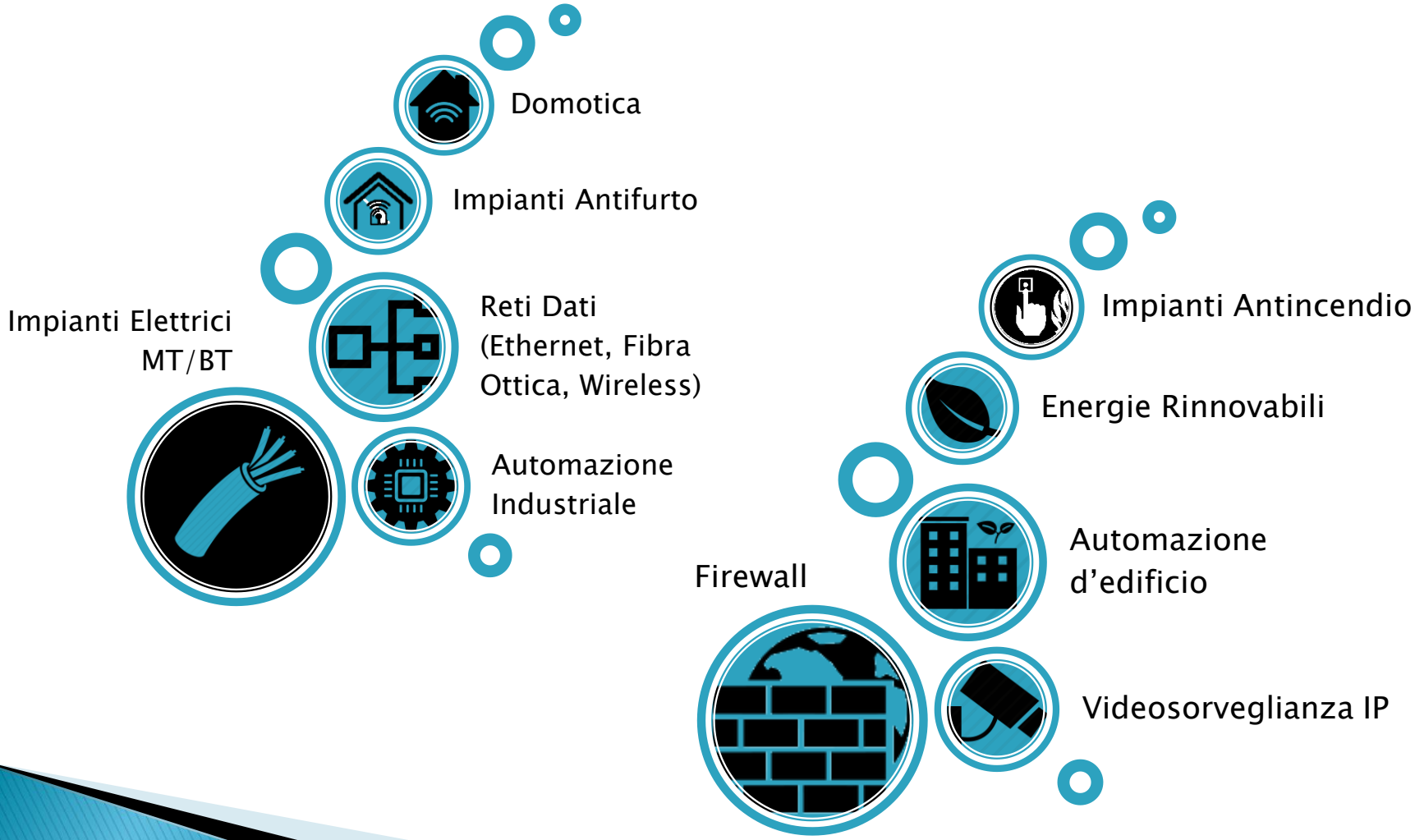
La sicurezza nelle infrastrutture

COMPETENZE


Domotica
Impianti Antifurto
Impianti Elettrici MT/BT
Reti Dati (Ethernet, Fibra Ottica, Wireless)
Automazione Industriale
Impianti Antincendio
Energie Rinnovabili
Automazione d'edificio
Firewall
Videosorveglianza IP

…….. Stiamo vivendo un momento storico di forti cambiamenti….

Scenario del cambiamento

- Viviamo l'era dell'informazione dove la tecnologia condiziona le nostre vite e le nostre scelte.
- Le minacce e il contrasto si stanno spostando dalla realtà al virtuale
- La tecnologia offre strumenti per gestire il cambiamento

.....quale e come utilizzarla?

Quale tecnologia utilizzare?

- La tecnologica si sceglie DOPO aver definito :
  - Cosa vogliamo proteggere
  - Da chi ci vogliamo proteggere

  ……. Quale livello di sicurezza ci aspettiamo?
- Perché queste riflessioni?
  - La collaborazione responsabile dell'imprenditore è fondamentale per determinare quali scelte e soluzioni dobbiamo utilizzare

Vediamo degli esempi in merito all'approccio errato al problema…

Falsi allarmi

- Scenario:

  Impianto di allarme in uno stabilimento che genera spesso falsi allarmi

- Evoluzione:

  L'allarme viene inserito solo quando «strettamente» necessario, oppure gli allarmi non vengono più controllati con tempestività.

- Epilogo:

  Impianto inaffidabile è una finta sicurezza

Combinatore GSM

- Scenario:

  Impianto di sicurezza realizzato in maniera corretta, esente da falsi allarmi.

- Evoluzione:

  Al rientro nell'attività trova segni di un'effrazione, ma non ne ha avuto notifiche.

- Causa:

  Scadenza della SIM associata al combinatore GSM dovuta ad una manutenzione incompleta.

Batterie

- Scenario:

  Impianto di sicurezza funzionante ma manutenzione assente

- Evoluzione:

  Furto con black-out , l'impianto non interviene.

- Causa e soluzione:

  Durata media delle batterie è di 4 anni, sostituirle prima della scadenza.

  …..L'utilizzo di gruppi elettrogeni o UPS di supporto non risolve il problema ….

Codici segreti

- Spesso si tende a sottovalutare l'importanza vitale che rivestono i Codici di Sicurezza.
- Utilizzare una combinazione semplice significa rendere inutile un impianto ben realizzato
- Utilizzare codici personali….. Associando un codice a persona si aumenta la responsabilità di gestione
- Tenere sempre in mente …..Chi va a rubare non è uno sprovveduto.

ROUTINE

- Le abitudini possono portarci in errore.
- Definire delle procedure , per quanto ovvie, aiuta a prevenire inconvenienti legati al mancato passaggio di informazioni o a semplici dimenticanze per le operazioni di inserimento o disinserimento dei sistemi di sicurezza.

INIZIATIVE ERRATE

- Un cliente richiede un controllo perché l'impianto di sicurezza aveva un funzionamento anomalo

- Causa…..Sensore tinteggiato dello stesso colore della parete…. Risultato architettonico eccellente, affidabilità del sistema compromessa….

  PRESTARE SEMPRE ATTENZIONE ALLE MANOVRE SULLE APPARECCHIATURE

Dobbiamo allearci con il TEMPO

- Per far fallire il furto , dobbiamo permettere alle forze dell'ordine di intervenire il prima possibile.
- Come allearci con il tempo?
  - Facendo perdere tempo al ladro per raggiungere il suo obbiettivo….. Come?
    - Ostacoli fisici
    - Serrature di sicurezza
    - Generando panico
    - Etc…etc…
  - Spostando i nostri sistemi di rilevazione anche verso l'esterno o sul perimetro dell'infrastruttura

Dove possiamo posizionare la «tecnologia»?

- Perimetro dell'infrastruttura esterna
  - Recinzione
  - Muro di cinta
  - Varchi
  - Etc…etc..

- Sull'edificio all'esterno
  - Muri perimetrali
  - Varchi

- Sull'edificio all'interno
  - Varchi
  - Soffitti
  - Pareti
  - Finestre

Tecnologie per protezioni perimetrali esterne

- Barriere all'infrarosso
  - PRO:
    - affidabili
    - possono essere montate su terreno/giardino
  - Contro:
    - Necessaria manutenzione …… tagliare l'erba
    - Problemi con nebbia/neve
    - Richiedono allineamento

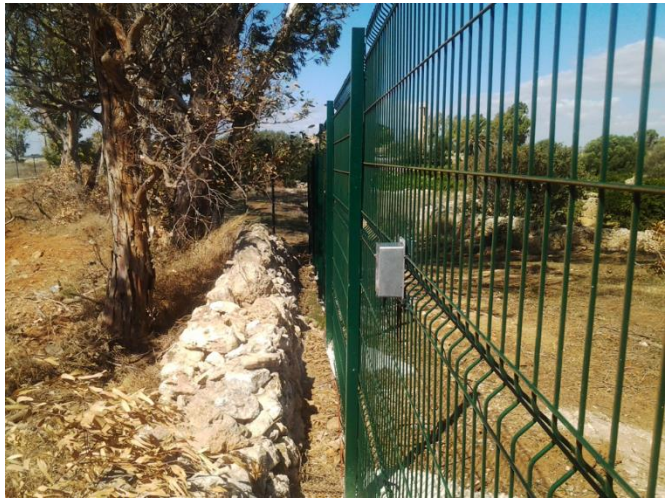
Tecnologie per protezioni perimetrali esterne

- Barriere a microonda:
  - PRO:
    - Affidabilità
    - Funzionamento anche in caso di nebbia

  - Contro
    - Devono essere montate su asfalto, in caso di installazione su terreno generano falsi allarmi
    - Il fascio della microonda è ellittico quindi il montaggio deve tenere conto dei buchi di sistema

Tecnologie per protezioni perimetrali esterne

- Cavi microfonici
  - PRO:
    - Facile installazione
    - Affidabile
    - Scarsa manutenzione



  - CONTRO:
    - Incompatibilità elettromagnetica in zone adiacenti a cabine di trasformazione
    - Incompatibilità elettromagnetica in aree con inverter senza schermatura ma di grande potenza
    - Va progettato , evitando installazioni improvvisate

Tecnologie per protezioni perimetrali esterne

- Cavi tesi in fibra ottica:
  - Affidabilità
  - Immunità ai disturbi
  - Assenza di manutenzione

Questa tecnologia trova impiego nei sistemi antintrusione o antievasione ad alta sicurezza. E' applicabile anche a recinzioni e concertine.

Tecnologie per protezioni perimetrali esterne

- Protezioni interrate
  - PRO:
    - Invisibile
    - Non individuabile
    - Rileva la pressioni sul terreno
  - CONTRO:
    - Installazione invasiva
    - Movimenti del terreno
    - manutenzione

Tecnologie per protezioni sull'esterno dell'edificio

- Sensori di rilevamento da esterno a doppia tecnologia
  - Pro:
    - Affidabili
    - Copertura efficace di varchi e passaggi
    - Si collegano alle centrali convenzionali
    - Previene il contatto con l'infrastruttura
  - Contro
    - L'installazione, la scelta dell'ottica e la modalità di funzionamento necessitano di professionalità
    - In estate sono meno sensibili

Tecnologie per protezioni sull'esterno dell'edificio

- Telecamere TVCC
  - Pro:
    - Visione
    - Registrazione
    - Remotizzazione delle immagini

  - Contro:
    - Manutenzione necessaria (NVR ed HDD hanno vita limitata)
    - Fare molta attenzione alla tecnologia che ci viene proposta

Siamo nel 2015 ancora il mercato propone soluzioni del tardo 900!

Tecnologie per protezioni INTERNE dell'edificio

- Barriere all'infrarosso sui varchi
  - Pro
    - Affidabili
    - Basso impatto architettonico
    - Manutenzione Bassa
    - Rilevano l'attraversamento del varco
    - Valida soluzione per antiaggressione notturna
  - Contro
    - Necessaria predisposizione sull'infrastruttura

In ambito aziendale/industriale ottima soluzione per la protezione di serrande o varchi di magazzini.

Tecnologie per protezioni interne dell'edificio

- Contatti magnetici finestre
  - Pro
    - Basso impatto architettonico
    - Affidabili
    - Rilevano l'apertura dell'infisso
  - Contro
    - Non efficenti come antiaggressione
    - Non rilevano la rottura del vetro
    - Assicurarsi che la tecnologia proposta non sia eludibile ….. Con una calamita si possono manomettere!

Tecnologie per protezioni INTERNE dell'edificio

- Sensori rottura/rilevamento urti vetro
  - Pro
    - Basso impatto architettonico
    - Fissati sul vetro per rilevare gli urti
    - Fissato 3 – 4 metri per la rottura
  - Contro
    - La rottura vetro «lavora» sugli ultrasuoni, problemi in caso di vibrazioni
    - Costi elevati se si hanno molti superfici vetrate, necessario un sensore che rileva gli urti per ogni superficie vetrata
    - Possibilità di falsi allarmi

Sensori controllo rottura di vetro Sensori a rottura vetro

Tecnologie per protezioni interne dell'edificio

- Sensori di rilevamento
  - Infrarossi passivi
    - rilevano temperatura emessa dal corpo umano

Sensori ad infrarosso

  - Doppia tecnologia
    - Ultrasuoni / infrarossi
    - Microonde/infrarossi (i più utilizzati)
    - Acustici/infrarossi
    - Vibrazioni/infrarossi

Sensori a doppia tecnologia

La scelta va fatta definendo il tipo di infrastruttura da proteggere…..

Sistemi di inserimento/disinserimento

- Tastiere alfanumeriche da interno/esterno
- Chiavi elettroniche di prossimità interno/esterno
- Telecomando
- Inserimento automatico da centrale di allarme
- Da remoto tramite istituto di vigilanza
- Sistemi biometrici integrati con l'automazione di edificio:
  - Impronte digitali
  - Lettura del flusso sanguigno
  - Lettura dell'iride

Biometria

- Lettura delle impronti digitali, già disponibili sul mercato ed integrabili con i sistemi di automazione
  - % di errore 1 su 10.000

Biometria

- Lettura flusso venoso palmo della mano
  - Pro
    - % di errore 0
    - Pratico per l'utilizzatore
    - Utilizzabile in soluzioni custom
    - Può sostituire il badge

  - Contro
    - L'implementazione necessita sempre di un integratore di sistemi

Biometria

- Lettura dell'Iride
  - PRO
    - % di errore 1 su 1.500.000
  - CONTRO
    - L'implementazione necessita sempre un integratore di sistemi

Come far comunicare il sistema all'esterno

- Sistemi tradizionali
  - Combinatori telefonici per linea fissa
    - PRO:
      - Affidabilità garantita dal gestore
    - CONTRO
      - Inutilizzabile in caso di taglio del cavi
  - Combinatori telefonici per linea mobile per SMS o messaggi vocali
    - PRO
      - Affidabilità garantita dal gestore
    - CONTRO
      - Inutilizzabile in caso di «jamming»

Come far comunicare il sistema all'esterno

- Sistemi evoluti o integrati con building/home automation tramite:
  - Invio di email informative su rete
  - Invio di push notification su smartphone o tablet
  - Invio di screenshot telecamere
  - Invio di messaggi video/audio «live» del sistema di TVCC

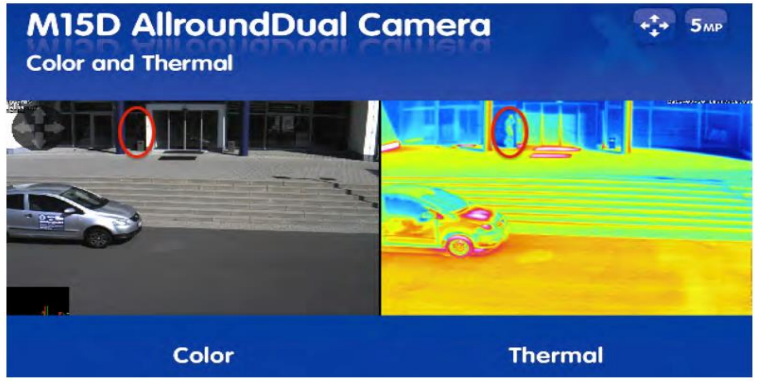
  Pro
  - Comunicazione biunivoca con il sistema di sicurezza
  - Integrazione con tutti gli impianti

  Contro
  - Richieste misure di prevenzione contro «il jamming»
  - Richieste misure di IP Security «serie»

……per concludere!

- Difendersi dal « jammer »

- Utilizzare la TVCC e la termografia per difendersi



JAMMER

- I jammer sono disturbatori di frequenze che vanno a saturare una o più specifiche bande, impedendo di fatto le comunicazioni finché è in azione in un raggio variabile.
- Tutte le trasmissioni di tipo wireless sono soggette a questo rischio, cancelli automatizzati, cellulari di nuova e vecchia generazione , reti WiFi
- **Utilizzando il JAMMER vengono oscurate tutte le telecomunicazioni**

Come difendersi dal JAMMER

- Scansionare la rete WiFi aziendale, se i canali si saturano inviare le e.mail di notifica
- Crearsi un canale di trasmissione con una sede secondaria ed automatizzare il controllo con cadenze di pochi minuti o secondi
- Se si hanno più sedi far comunicare le centrali tra di loro.

Se una centrale non mi risponde devo riceve notifiche dal supervisore esterno

Come difendersi dal JAMMER

- Apparati utilizzabili:
  - **Firewall UTM con sistema di notifica**
  - **Controllori programmabili**
  - **Home Building Automation**
  - **Centrali di allarme evolute**

TELECAMERE

- I marchi sul mercato si riuniscono in 3 grandi gruppi:
  - Aziende specializzate nelle telecamere analogiche
  - Aziende nate analogiche e convertite in digitale
  - Aziende native digitali

TELECAMERE

- Le telecamere analogiche consentono di avere una visione estremamente definita mantenendo dei costi contenuti.

  Ma è davvero questo che ci interessa ?

- L'innovazione è rappresentata dall'Analisi Video, resa possibile grazie alle telecamere IP.

ANALISI VIDEO

- Nei sistemi analogici l'analisi è affidata alla sorveglianza, il limite è l'attenzione umana.

- Telecamere digitali professionali: analisi video nel dispositivo. Il software elabora il video e avvisa l'utente quando rileva qualcosa di insolito.

ANALISI VIDEO

- Che cosa è possibile fare ?
  - Lettura delle targhe
  - Analisi dei movimenti nell'inquadratura, con possibilità di discriminare:
    - area di rilevazione
    - direzione
    - intensità dei movimenti stessi.
  - Rilevazione dei volti
  - Rilevazione dell'audio
  - Interfacciamento con molti altri sensori
  - Conteggio degli accessi
  - Analisi termografica

LE POTENZIALITA’

- Una telecamera IP è una fonte di informazioni in grado di comunicare con altri apparati.
- Può notificare eventi rilevati all’operatore tramite software ed applicativi, richiamandone l’attenzione solo su eventi e permettendo una supervisione più completa e mirata.
- Totale integrazione con i sistemi di automazioni con forti potenzialità

Grazie per l'attenzione