bimu
fieramilano
9-13/10/2018

FINE TUNING

Gruppo Par-Tec SpA

IL SOFTWARE PER INDUSTRIA 4.0

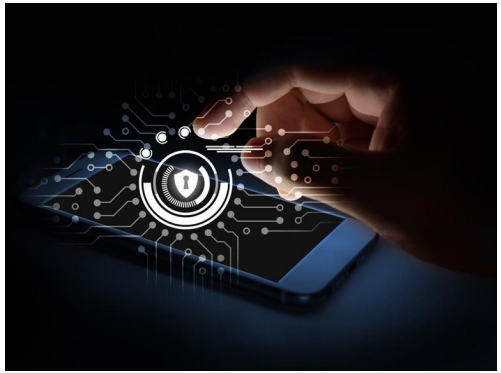
Luca Bonadimani

cecimo · UCIMU-SISTEMI PER PRODURRE · EFIM · ISF 065/2016 · FIERA MILANO

AGENDA

AGENDA

- Cyber Security in ambito iOT
- Industrial Data Intelligence
- Sofware Agent e teleassistenza impianti remoti 24/24 – 7/7



Cyber Security in ambito iOT

- Gli hacker attuali sono ragazzi cresciuti sui devices (cappello bianco o nero);

- Una rapida ricerca su Internet rivela che **la maggior parte dei dispositivi connessi a Internet è facilmente hackerabile** e che proprio **sul web** il potenziale hacker può trovare **tutorial, comandi, script e persino video didattici** in grado di guidarlo verso l'hacking dei dispositivi.

- **hackerare la fotocamera sul vostro computer è molto facile**, basta installare un virus e il modo più semplice per farlo è inviarlo tramite e-mail con un allegato «infetto». Aprendo l'allegato il virus viene avviato e il vostro computer automaticamente connesso a quello dell'hacker.

- Molti programmi consistono in centinaia di migliaia e talvolta milioni di righe di codice ed è quasi garantito che alcune vulnerabilità della sicurezza continueranno ad esserci, ma gli **sviluppatori di software stando diventando sempre più attenti alla sicurezza nella progettazione e nella codifica del codice.**

- Anche i produttori di grandi piattaforme pubbliche di software sono consapevoli che la sicurezza nel loro codice sia fondamentale e per questo incentivano, pagando, tutti coloro che segnalano buchi di sicurezza nel loro software. Facebook in primis.

- In ambito Cyber Security si sta diffondendo il *bug tracking di massa*.

Cyber Security in ambito iOT - Il contesto

- La tecnologia si sta muovendo molto velocemente con molti nuovi dispositivi che si connettono a Internet. Una di queste è la tecnologia dei **robot** in rapido sviluppo.

- I robot avranno milioni di applicazioni tra cui la **sicurezza nelle case e nel mondo degli affari.**

- Anche se questa tecnologia è ancora agli albori, oggi i robot possono già tracciare i suoni, come la voce umana, e tentare di osservare gli occhi di una persona.

I robot intelligenti, pensati per la sicurezza, possono:

- accertare se le persone all'interno di uno spazio sono intrusi indesiderati o autorizzati a trovarsi in quello spazio;

- utilizzare sensori e programmi che riconoscano i modelli vocali, le caratteristiche fisiche, i pattern retina oculare, i badge o possono formulare domande alle persone che incontrano, confrontando le risposte appena apprese con le risposte precedenti;

Col passare del tempo, vedremo probabilmente sempre più robot avanzati fare cose che negli ambienti produttivi sono riservate agli umani.

- 500.000 è il numero previsto di droni che saranno venduti nell'arco del 2018. Un numero da capogiro.

- Alcuni anni fa un drone era un aereo militare che volava in missione in tutto il mondo. Oggi, quando qualcuno menziona il termine drone, si pensa ad un piccolo elicottero, a volte così piccolo da stare nel palmo di una mano, munito di telecamere e altra tecnologia.

- **I droni sono già utilizzati in molte attività umane, in alcuni casi offrendo dei vantaggi enormi rispetto ai limiti fisici del corpo umano.**

- Se vuoi comprare un farmaco di alta qualità a basso costo il posto dove andare è il **mercato anonimo di Darknet**.

- I normali browser Web come Chrome o Firefox non possono accedere a questa rete perché i mercati criminali hanno la capacità di nascondersi dalla normale navigazione web.

- Questa parte di Internet è raggiunta dai servizi T-O-R, dove gli URL sono stringhe senza senso, con dominio .onion.

- Il denaro viene facilmente scambiato usando la criptovaluta Bitcoin, facilmente scambiabile con le valute del mondo reale e in grado di offrire anonimato ai suoi utenti.

Cyber Security in ambito iOT - Le tecniche

La sicurezza informatica consiste nel proteggere l'Internet delle cose (iOT) e i dispositivi connessi che si prevede saranno oltre **50 miliardi entro il 2020**.
La ricerca sulla sicurezza informatica in tutto il mondo e le tecniche di cyber security serviranno a proteggere i dati e i dispositivi connessi a Internet.

Oggi esistono tre principali tecniche per la sicurezza informatica:

- **la crittografia**,
- **l'autenticazione a più fattori**,
- **il rilevamento delle intrusioni**.

LA CRITTOGRAFIA

- La crittografia si basa sull'uso della matematica per prendere i dati e modificarli in modo che siano illeggibili assicurando che i dati, per esempio quelli della carta di credito, trasmessi dal nostro computer a internet, o da altri dispositivi, come il wifi della caffetteria, vengano letti e siano accessibili solo dai destinatari interessati.

- Gli algoritmi di crittografia e decrittografia sono attualmente basati sulla capacità del software di fare *problem solving*. **Scienziati informatici e matematici lavorano costantemente su tecniche sempre più difficili per garantire che i dati siano al sicuro da hacker e ladri.**

L'AUTENTICAZIONE

- L'autenticazione a più fattori utilizza normalmente dispositivi diversi, con inserimento di diverse forme di dati per accedere ad un servizio internet. Facciamo un esempio: per accedere per la prima volta ad un sito social sul proprio smartphone o PC il sito potrebbe generare un codice che ti viene inviato per email o al tuo smartphone, obbligandoti ad inserire anche quel codice.

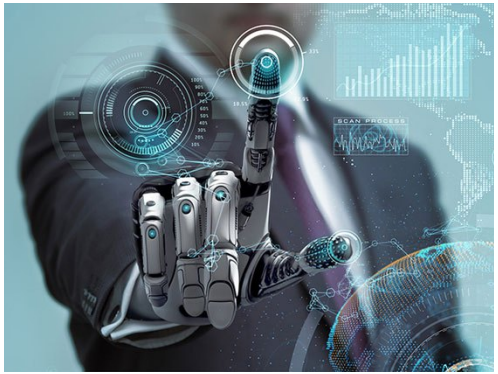
- **Sono già disponibili il riconoscimento vocale e facciale che, presto, diventeranno la normalità.** Dire una password a un sistema di riconoscimento vocale sarà molto più sicuro, poiché è l'unicità della voce che verrà riconosciuta e non la password stessa.

IL RILEVAMENTO DELLE INTRUSIONI

Il rilevamento delle intrusioni si concentra su due **diversi tipi di minacce** di attacco:

- **esterna**, persone o dispositivi che tentano di accedere ai dati interni attraverso codici dannosi, malware, virus o hacker che lavorano per entrare nei tuoi dispositivi;

- **interna,** l'attacco proviene da qualcuno all'interno dell'azienda o da qualcuno che sta tentando di sabotare i dati dell'azienda per la quale lavora.



Industrial Data Intelligence

- L'automazione industriale è l'uso di computer e robot per controllare i processi industriali, come la produzione, senza un intervento umano significativo. Utilizzata correttamente, l'automazione può aumentare la **qualità**, la **sicurezza** e l'**accuratezza** di questi processi.

- È compito delle persone nell'automazione industriale progettare i sistemi, configurare i controller e monitorare i processi.

- A ogni livello di automazione (macchine, controllo, gestione) vi sono componenti hardware, software e di rete, e diversi dispositivi: dai controllori logici programmabili in fabbrica (PLC), al software OPC che fornisce ai tecnici informazioni sulle operazioni.

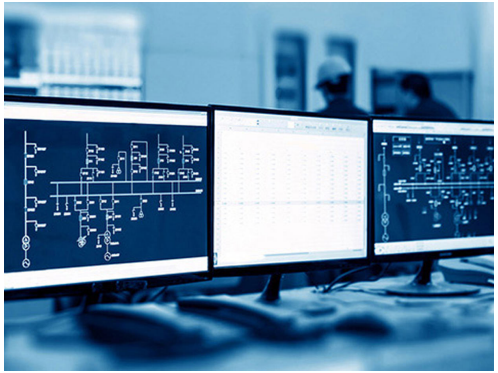
- La principale funzione di SCADA (acronimo per controllo di supervisione e acquisizione dati) è l'acquisizione di dati da dispositivi remoti, come valvole, pompe, trasmettitori e il controllo degli stessi attraverso una piattaforma software.
- Il risultato è il **controllo locale del processo** in modo che questi dispositivi si accendano e si spengano al momento giusto e la **possibilità di acquisire dati** ed eventi per il monitoraggio di questi processi.

- **La massa di dati raccolti per il tracciamento dei lotti di produzione può fornire importanti informazioni e conoscenze se adeguatamente interrogata come fonte di Big Data. Ci si può spingere fino alle analisi di previsione guasti, rotture o difetti, oltre a potenziali interruzioni di servizio.**

- Il layout SCADA di base include l'interfaccia utente, quella per la macchina, un display grafico, allarmi e report, trend, database e **aggiornamenti dei dati in tempo reale**.

- I sistemi SCADA sono utilizzati da organizzazioni industriali e aziende nel settore pubblico e privato per controllare e mantenere l'efficienza, distribuire i dati per decisioni più consapevoli e comunicare problemi di sistema.

- Oggi un sistema SCADA, anche essenziale, richiede che tutte le stazioni di una linea di produzione siano in grado di raccogliere i principali dati riguardanti le condizioni ambientali e tecniche delle lavorazioni. **Tutto questo va a costituire un patrimonio di informazioni che necessita di strumenti di intelligence predittiva per poter esprimere al meglio il potenziale di conoscenza insito nei dati.**



Software Agent
Teleassistenza impianti remoti
24/24 – 7/7

- L'**amministrazione remota** è una scienza simile alla magia per la maggior parte degli utenti di computer. Per fare un esempio, Apple Remote Desktop (ARD) mette a disposizione un modo semplice per gestire tutti i computer Mac in una rete Lan senza mai lasciare la propria scrivania.

- Gli impianti produttivi *ict enabled*, cioè con dispositivi di rilevazione ambientale che operano monitoraggi e raccolgono dati utili all'andamento della produzione, dispongono di interfacce remote di gestione e di visualizzazione. Tale modalità di controllo permette di dislocare **control room** in luoghi e contesti diversi dall'impianto di produzione, così come ricorrere a **servizi in *outsourcing*** in grado di verificare il costante *up and running* degli impianti che lavorano 24/24 e 7/7.

- La **control room** può essere definita come un gruppo funzionale che svolge attività di monitoraggio, registra e risolve incidenti, richieste di servizio e richieste di informazioni.

- L'obiettivo per molte control room è la **gestione dell'incidente fino alla risoluzione e la gestione di richieste fino all'adempimento**. Ciò significa che una struttura di control room, oltre che svolgere una continua attività di monitoraggio, si pone anche come *service desk*, cioè gestisce incidenti e garantisce la continuità operativa di impianti e strutture critiche.

- Ci sono varie strutture e modelli di control room implementati in tutto il mondo. Spesso ci si chiede quale sia il migliore; ciò dipenderà dal tipo, dalla dimensione e dal ruolo della control room all'interno della organizzazione.

FINE TUNING consulenza integrata Srl

ringrazia tutti per l'attenzione

Venite a trovarci

STAND A86 – PAD.13