ST white paper

# Anche se isolati, i PLC sono raggiungibili!

*...e si possono sottrarre all'Azienda dati ed informazioni critiche !*

*di Enzo M. Tieghi*

Enzo M. Tieghi,
CEO di ServiTecno

Arriva da CyberX la notizia: ricercatori hanno scoperto un metodo che gli hacker potrebbero usare **per sottrarre furtivamente i dati dalle reti industriali isolate** (non connesse alla rete aziendale e/o ad internet), manipolando il segnale a radiofrequenza (RF) emesso dai **controllori a logica programmabile (PLC)**.

È questo il contenuto di una presentazione fatta nei giorni scorsi, ai primi di Dicembre 2017, al conferenza Black-Hat Europe a Londra (UK).

Il resoconto e le slide della presentazione ci raccontano lo scopo e la metodologia utilizzata per estrarre dati dal PLC.

La tecnica si basa su PLC e segnali RF emessi. I test sono stati condotti utilizzando un normale PLC Siemens S7-1200, ma gli esperti ritengono che l'attacco possa ugualmente funzionare anche su altri PLC, anche di altre marche.

Il metodo di exfiltration scoperto da CyberX non sfrutta vulnerabilità o difetti di progettazione nei PLC. Gli esperti hanno anche notato che non implica alcuna funzionalità RF insita nel dispositivo stesso. Piuttosto, i segnali RF emessi dal dispositivo sono un sottoprodotto di scrittura multipla nella memoria del PLC, in un modo specifico, attraverso un particolare software ladder.

(... e dicono che i dati exfiltrati possono essere catturati utilizzando vari metodi, come un'antenna attaccata a un drone che sorvola il sito, o da un avversario che si camuffa da personale addetto alle pulizie e con un'antenna in tasca...)

Mentre il tasso di esfiltrazione dei dati può sembrare molto lento (un bit al secondo), gli esperti ritengono che il metodo possa essere utile per rubare piccoli pezzi di informazioni tipicamente raccolti in fase di ricognizione prima di un attacco lanciato da un attore sofisticato, compresi topologia, protocolli e dispositivi di rete, proprietà intellettuale memorizzata in HMI e storici, e turni/orari di lavoro, ecc.

**E' vero, si può fare, e lo hanno dimostrato. Ma la domanda è: è uno scenario possibile? La mia risposta: se ci sono di mezzo tanti, tanti, ma tanti soldi, probabilmente si.**

Ma forse non è questo lo scenario tipico di tante aziende di produzione che nell'industria e nelle utility che stanno affinando e mettendo in pratica le strategie per **Industria4.0** e debbono proteggere quotidianamente i propri impianti da **fermate** che, oggi si è scoperto, possono essere causati anche da **virus/malware, sabotaggi** o anche da **accessi non autorizzati o dolosi**.

**In conclusione**: se debbo iniziare a **proteggere dai rischi informatici** la mia rete industriale, i miei **PLC, HMI e SCADA**, anche in ottica **Smart Manufacturing e Industria4.0** inizierei dalla base: una policy per la **OT/ICS Cyber Security**.

In pratica per iniziare:

- progettazione delle applicazioni, della rete e architettura pensata con la sicurezza in mente (security-by-design),
- documentazione e tecniche di programmazione "ordinata",
- criteri di segmentazione della rete e segregazione di dispositivi ed assett critici (come ad esempio descritto da ISA99-IEC62443),
- dispositivi (switch, router, firewall) industriali, con approriate regole e policy definite, documentate e condivise,
- monitoraggio puntuale, manutenzione e gestione della rete e dell'infrastruttura di impianto affidata a tool specifici del mondo industriale e persone competenti,
- eventuali connessioni da remoto monitorate e gestite,
- back-up completo di tutte le applicazioni (PC, PLC, robot, ecc.) e test di restart.

Questi alcuni punti, in ordine sparso, che mi sono venuti in mente e che giudico importanti per verificare livelli minimi, ma adeguati, di protezione dei sistemi in fabbrica.