Le cyber minacce emergenti e il rischio per i sistemi di Industria 4.0

Nel recente report dell'Enisa, l'agenzia europea che si occupa di sicurezza delle reti e delle informazioni, si parla anche dei trend e delle minacce alla security dei sistemi di automazione, controllo e telecontrollo a presidio di macchinari ed impianti nell'Industria e nelle Utility. Una sintesi e qualche riflessione di Enzo Maria Tieghi, Ceo di ServiTecno e membro del membro del comitato scientifico del Clusit.

A fine gennaio l'Enisa, l'agenzia europea per la Network and Information Security, ha rilasciato il report Enisa Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends.

Si tratta di un documento sullo stato della Cyber Security nell'Unione Europea ed a livello globale, dal punto di vista degli esperti di Enisa, che stilano ogni anno una fotografia con riferimento a minacce più avvertite, crimini cyber ed altri accadimenti avvenuti nell'anno precedente con impatto sui sistemi.

A livello generale il report Enisa evidenzia che:

- I messaggi di posta e di phishing sono diventati il principale vettore di infezione da malware.
- I kit di exploit hanno perso la loro importanza nel panorama del cyberthreat.
- I Cryptominer sono diventati un importante vettore di monetizzazione per i criminali informatici.
- Gli agenti sponsorizzati dallo Stato si rivolgono sempre più alle banche utilizzando i vettori di attacco utilizzati nel crimine informatico.
- Migliorare Skill e Capability sono l'obiettivo principale di chi si deve difendere. Le organizzazioni pubbliche lottano per fidelizzare il personale a causa della forte concorrenza con l'industria nell'attirare i talenti della sicurezza informatica.
- L'orientamento tecnico della maggior parte dell'intelligence rivolta al cyberthreat è considerato un ostacolo alla sensibilizzazione del Management.
- L'intelligence deve rispondere agli attacchi sempre più automatizzati con nuovi approcci e l'utilizzo di strumenti e competenze a loro volta automatizzati.
- L'emergere di ambienti IoT rimane un problema a causa della mancanza di meccanismi di protezione nei dispositivi e nei servizi IoT di fascia bassa. La necessità di architetture e buone pratiche di protezione IoT generiche è ora ancora più pressante.
- L'assenza di soluzioni di intelligence cyberthreat per PMI e utenti finali deve essere affrontata sia dai fornitori che dai governi.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

In un mondo cyberfisico gli obiettivi sono anche fisici

La diffusione dell'IoT, spiega il rapporto Enisa, "rimane un problema a causa della mancanza di meccanismi di protezione nei dispositivi e nei servizi IoT di fascia bassa. La necessità di architetture e buone pratiche di protezione IoT generiche è ora ancora più pressante".

E ancora: "Dall'altra parte, l'aumento del numero di servizi interconnessi a livello globale e la loro dipendenza da IOT per eseguire e facilitare tali servizi, hanno sollevato preoccupazioni per le minacce come gli attacchi DoS che potenzialmente possono causare danni su scala nazionale a Aziende e Infrastrutture Critiche. Un esempio di tali servizi sono gli ospedali collegati ed i servizi connessi. Tuttavia, nonostante le attività di mitigazione e prevenzione in corso in tutto il mondo, le ricerche ci danno un numero di attività DDoS in aumento (del +16%)".

In definitiva "L'incertezza sulla riuscita implementazione della sicurezza informatica e degli standard di qualità continuerà, soprattutto a causa dell'emergere dell'IoT che collega gli spazi cibernetici e fisici. Il panorama delle minacce che emerge dagli attacchi alla supply chain è una delle principali preoccupazioni per la sicurezza informatica, in particolare per i dispositivi a basso costo".

Tre consigli per mitigare le minacce per Industria 4.0 e Utility 4.0

Occupandoci da anni del tema OT/ICS cyber security siamo però andati a vedere che cosa si può trovare nel report Enisa con specifico riferimento a proposito di rischi, minacce ed accadimenti relativi a problemi di security per sistemi e reti di automazione, controllo e telecontrollo a presidio di macchinari ed impianti nell'Industria e nelle Utility. Questi sono tre capisaldi che tutti gli operatori del settore industriale e delle utilities dovrebbero tenere in considerazione.

1 - Preferire la visibilità all'oscurità

Oggi, uno dei motti più azzeccati per meglio proteggere reti e sistemi di fabbrica è sicuramente "Security-by-Visibility", in contrapposizione alla "Security-by-Obscurity" che per lungo tempo è stato uno dei mantra della Cyber Security industriale, ovvero cercare di "nascondere" il sistema da proteggere, rendendolo meno visibile, e coprirne le caratteristiche per renderlo meno attaccabile.

Nel tempo si è visto che questo tipo di approccio "Security-by-obscurity" non rende il sistema più sicuro.

Quindi ora si preferisce adottare contromisure adeguate alla criticità e importanza del sistema ICS, e al contempo avere la massima visibilità su quanto succede in rete e sul sistema per accorgersi prima possibile di eventuali anomalie di comportamento che possano dare indizi su eventuali compromissioni in atto e incidenti incombenti.

Nel report viene riportato che nel febbraio 2018 è stato segnalato il primo episodio di malware di cryptomining (un server utilizzato per svolgere catene di cryptovalute) trovato nei sistemi SCADA di una utility idrica, collegato a Internet. Si noti, per inciso, che questo incidente non è stato l'unico.

Questo lascia spazio a due considerazioni: in primis, che un sistema collegato a internet, con scarsa protezione perimetrale, è facilmente compromissibile. In secondo luogo, che è indispensabile avere visibilità su quanto avviene nei sistemi ICS per accorgersi all'istante se ci sia incorso qualche attività non prevista e potenzialmente malevola.

2 - Proteggere il perimetro, ma anche segmentare e segregare

Da sempre suggeriamo di segmentare la rete e segregare in modo adeguato i componenti più critici del sistema di controllo.

A questo riguardo lo standard IEC 62443, riprendendo il cosiddetto modello PERA (Purdue Enterprise Reference Architecture), approfondito anche in ISA-95 e ISA99, definisce come la suddivisione in Zone deve essere seguita e come limitare al massimo i Conduit che permettano comunicazioni di informazioni tra una zona e l'altra, che dovranno poi essere presidiati adeguatamente.

Nel report si spiega che "Il 64% dei principali incidenti che riguardavano sistemi o reti di controllo industriale sono stati ransomware" (nel 2018).

Nella stragrande maggioranza di tali incidenti, il ransomware arriva sulla rete del sistema OT/ICS che gestisce l'impianto o la macchina in fabbrica, come "danno collaterale" di un allegato di email o di una navigazione su un sito infetto aperto improvvidamente da un PC negli uffici di sede.

Quasi sempre, una volta arrivato sulla rete di stabilimento il ransomware ha vita facile a propagarsi, infettare altri PC, bloccare il funzionamento criptando i dischi e rendendo inutilizzabile il sistema, e di conseguenza bloccare i sistemi di automazione e controllo, fermando la produzione o l'erogazione del servizio.

Ora, a nostro modo di vedere qui si evidenziano tre ordini di problemi:

- Le policy di awareness/training di security delle Aziende coinvolte non sono così efficaci e qualcuno ancora apre allegati di posta infetti o naviga su siti poco raccomandabili
- Le contromisure tecnologiche di security adottate non sono adeguate a bloccare queste campagne di ransomware
- Il fatto che un ransomware che colpisce la rete di ufficio venga a propagarsi nella rete di fabbrica evidenzia il fatto che non ci sia una protezione perimetrale nè una corretta segmentazione della rete nè una segregazione adeguata dei computer più critici nei reparti di produzione

E molto probabilmente risulta lacunosa anche la pratica di effettuare correttamente i backup di tutti i sistemi utilizzati in fabbrica (PC, PLC, SCADA, ecc.): questo, anche in caso di incidente, potrebbe limitare i danni a poche ore di fermo, con ripartenze veloci, senza causare giorni e giorni di mancata produzione o erogazione del servizio come purtroppo è successo in molte realtà industriali sia nel 2017 che nel 2018 (come ancora riportato in diverse parti del report ETL2018).

3 - Limitare l'accesso da remoto ai sistemi industriali

Nel report ETL2018 di Enisa si evidenzia come la distribuzione indiscriminata di RAT (Remote Access Tool) sui sistemi ICS sia una pratica diffusa e che procura grosse preoccupazioni.

Uno strumento di amministrazione remota (o RAT) è un programma usato da operatori e da altre persone per connettersi ad un computer remoto attraverso Internet o attraverso un network locale, per svolgere poi determinate attività di manutenzione o anche gestione del sistema senza doversi recare di persona sull'impianto per avere fisicamente accesso al sistema stesso: uno strumento per l'amministrazione remota installato sul sistema ICS e che possa replicare video, tastiera e mouse su un altro PC collegato in rete

Il report ETL2018 ci ricorda che "Le reti OT di imprese industriali sono un campo di gloria per gli attori di minacce di spionaggio".

Questi attori utilizzano strumenti di amministrazione remota (RAT) che sono già installati sui sistemi di controllo industriale (ICS). Qui sotto una figura tratta da un recente rapporto che rivela i 20 principali paesi in cui sono stati utilizzati i RAT almeno una volta in incidenti di spionaggio durante il primo semestre del 2018.

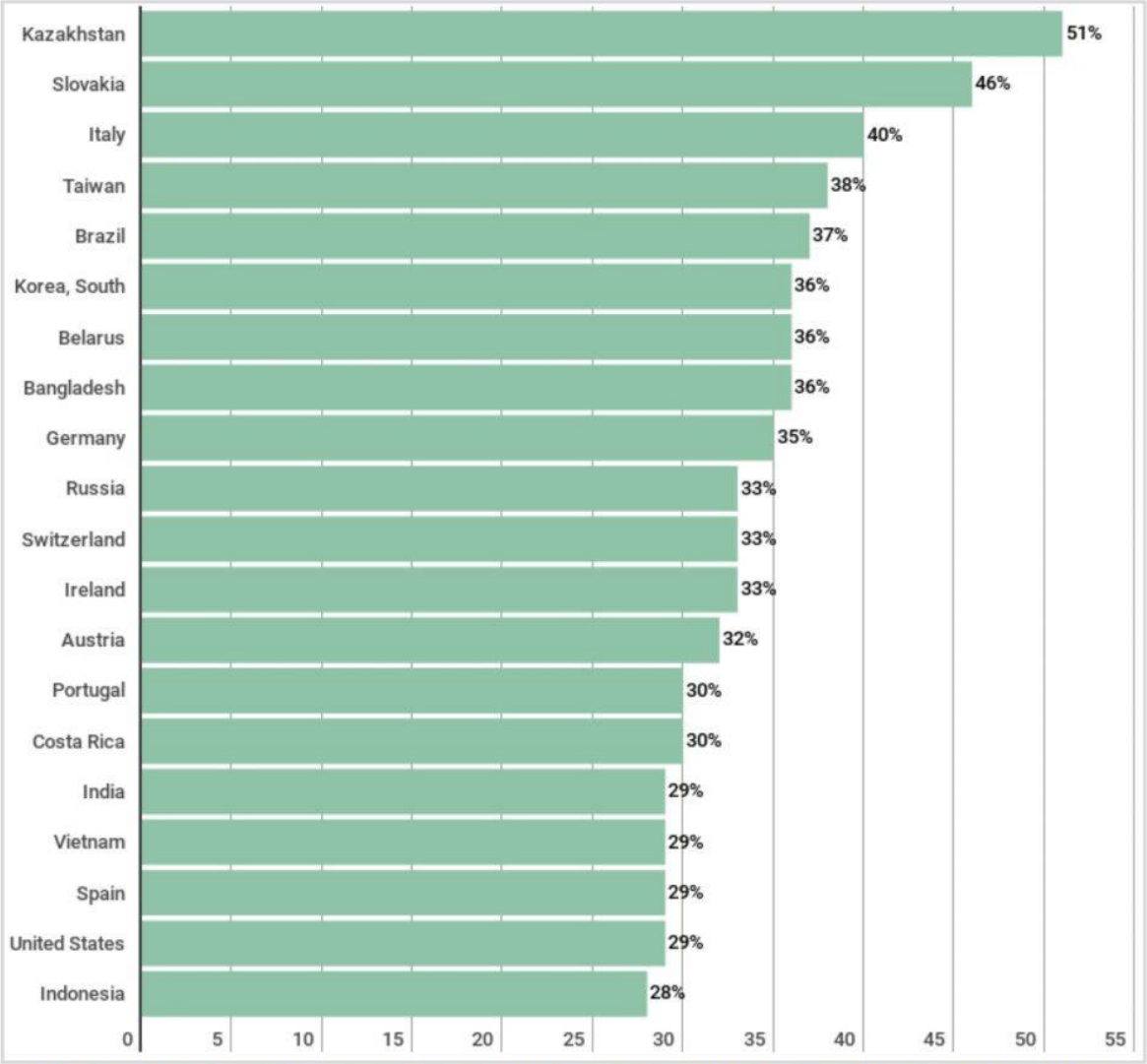

Figure 42: RAT on ICS computers vs. total computers (top 20 countries in H1 2018)[530]

Remote Access Tools (che poi sono RDP, Remote Desktop, VNC, Teamviewer, ecc.) sono installati sul 40% dei computer nei sistemi ICS, e già questo è indicativo e sintomatico dell'usanza di metterlo dappertutto.

Ma se poi scendiamo al dettaglio della ricerca Kaspersky richiamata nel report ETL2018 scopriamo anche che tali tool sono installati legittimamente solo su meno di un terzo dei sistemi ICS: in pratica su quasi il 70% dei sistemi in oggetto tali RAT sono stati installati e sono attivi senza che gli operatori ed i proprietari dei sistemi ne siano a conoscenza!

Emerge quindi nuovamente un problema di scarsa "visibilità" sul sistema ICS.