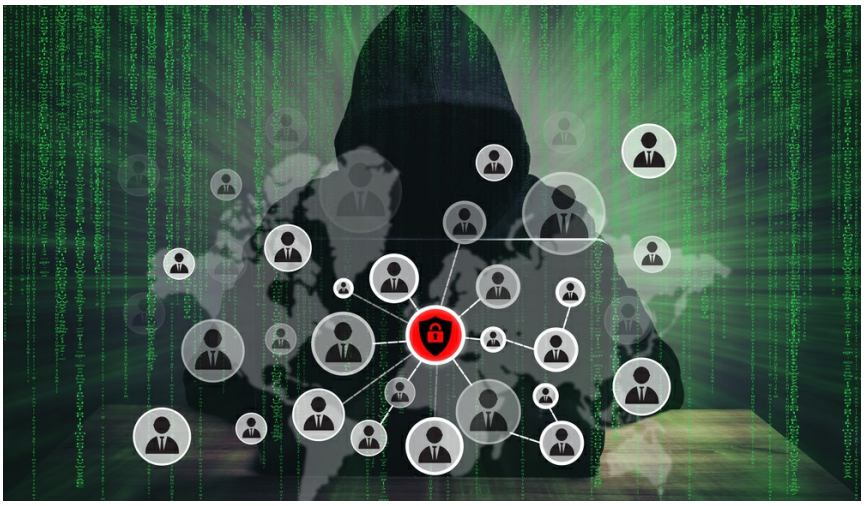
SICUREZZA

Operational Technology e rischio cyber: le minacce ai sistemi produttivi industriali

Un attacco cyber ai sistemi OT (Operational Technology, deputati al monitoraggio e al controllo dei sistemi produttivi, può avere conseguenze disastrose per l'ambiente e le persone. Ma pochi conoscono il tema. Facciamo chiarezza

08 Ago 2018

Roberto Setola
direttore Master Homeland Security, Università CAMPUS Bio-Medico di Roma



Personaggi
R Roberto Setola
Argomenti
A attacchi hacker
Canali
C Cyber Security
F firma digitale
I it
S Setola
P Privacy
S Sicurezza digitale

Articoli correlati

CYBER SECURITY

Cyber attacchi alle infrastrutture critiche, questi i nuovi bersagli degli hacker

18 Apr 2018

di **Corrado Giustozzi**

Gli attacchi mirati alle cosiddette **Operational Technology**, ossia i sistemi deputati al monitoraggio e al controllo dei sistemi produttivi, possono diventare nel prossimo futuro elementi di pressione geopolitica. Il problema della protezione rispetto a questa classe di attacchi non può quindi essere demandata ai soli operatori privati ma è fondamentale una forte sinergia con i soggetti pubblici deputati.

IL QUADRO

Cyber security in Sanità, ecco i principali pericoli e le sfide per l'Italia

22 Mar 2018

di **Luigi Romano**

Condividi

Indice degli argomenti

OT e IT, vantaggi e criticità del connubio

Con la sigla OT (in qualche modo in contrapposizione con la sigla IT) si intendono le **Operational Technology**, ovvero quell'insieme di tecnologie, software e hardware, direttamente connesse con la produzione, trasporto e trasformazione di beni. Cioè con tutto ciò che riguarda i sistemi di monitoraggio e controllo dei sistemi produttivi che vengono anche indicati con altre sigle come **ICS**, **SCADA** o **PLC**.

Negli ultimi anni le OT hanno fatto ricorso in modo sempre più massivo alle tecnologie IT[1] abbandonando progressivamente soluzioni proprietarie a favore di soluzione basate su prodotti off-the-shelf. Questo connubio, **in parallelo agli indubbi benefici** che abbiamo potuto osservare nella nostra vite quotidiana in termini di miglioramento della qualità, dell'efficienza e

dell'economicità delle diverse produzioni, **ha introdotto nel dominio OT le vulnerabilità e le minacce proprie del settore IT**.

OT, il problema della sicurezza dei processi

Il problema è che le OT hanno una serie di peculiarità che rendono di converso di non semplice trasposizione le misure di protezione che usualmente vengono adottate per i sistemi IT. Infatti, **gli OT si caratterizzano in primo luogo per il tipo di informazioni scambiate sulla rete**: quantità estremamente elevata di pacchetti di informazioni dalle dimensioni molto contenute (dell'ordine di qualche byte) provenienti da una grande pluralità di sorgenti. Questo implica che meccanismi come la **cifratura** (usualmente impiegata per evitare la disclosure delle informazioni) o la **firma digitale** (che si utilizza per evitare la alterazione dei dati) risultano di difficile adozione in quando introdurrebbero un elevato overhead e un non accettabile ritardo nella elaborazione del dato. Questo perché l'altro aspetto da considerare è il vincolo dell'hard **real-time**, ovvero della necessità di garantire un tempo massimo di esecuzione per ciascun task. Questo vincolo, che è fondamentale per il controllo di molti processi industriali onde evitare che lo stesso possa porsi in situazioni critiche e/o pericolose, unitamente al fatto che **questi processi operano a ciclo continuo 24×365 rende nei fatti difficile sia l'utilizzo di sistemi di anti virus che le attività di patching**. Il tutto reso più complesso dal fatto che questi sistemi hanno un istallato estremamente ampio ed un tempo di vita dell'ordine di oltre dieci anni.

Le conseguenze di un cyber attacco ai sistemi OT

L'aspetto di maggiore criticità legata alla cyber security dei sistemi OT è stato evidenziato anche nella relazione dei

Servizi di Intelligence al Parlamento del 2016 in quanto un attacco cyber verso questi sistemi può creare potenziali impatti non solo di ordine economico, ma anche **cinetico,** ovvero la possibilità di **danneggiare oggetti fisici**. In altri termini mediante un attacco cyber è possibile alterare opportunamente il funzionamento di un processo al punto di portarlo ad un punto di rottura meccanico.

Il progetto Aurora

Questo era, per altro, l'obiettivo del progetto Aurora condotto dal Idhao National Lab (USA): usare **un attacco cyber per distruggere un gruppo elettrogeno da 27 tonnellate**. Ovvero la dimostrazione che un attacco immateriale, una sequenza di zeri ed uno, è in grado di fare un danno meccanico paragonabile a quello ottenibile una carica esplosiva, con il vantaggio che **l'azione può essere sferrata da migliaia di chilometri di distanza e che le possibilità di risalire all'autore sono estremamente ridotte**. Questo comporta che un attacco cyber contro questi sistemi, oltre ad al danno economico per mancato funzionamento e danno di immagine (come per un normale attacco cyber ad un sistema IT) è in grado di creare **problemi all'ambiente ed alla salute delle persone**.

Un altro aspetto da non trascurare sono i tempi di ripristino. Infatti, mentre la sostituzione di un componente di un sistema informatico è una operazione che può avvenire in un arco di tempo stimabile nelle ore o al massimo nei giorni. **La riparazione di un componente meccanico (come il gruppo elettrogeno distrutto durante l'esperimento Aurora) può richiedere tempi dell'ordine dei mesi se non addirittura degli anni**.

Occorre dire, però, che fino al 2010 pochissimi ritenevano possibile attuare sul campo un'azione come quella del progetto Aurora.

Condizioni per il successo di un

attacco a sistema OT

Questo perché affinché l'azione sia veramente dannosa contro un sistema OT non deve limitarsi semplicemente paralizzare/bloccare il sistema (cosa che può essere fatto in principio anche con un **semplice attacco DoS**), ma deve essere in grado di "condurre" il processo fisico in uno stato critico. Per fare questo occorre, oltre alle opportune conoscenze informatiche (sia quelle proprie della componente IT che con riferimento alle peculiarità dei sistemi ICS in termini di protocolli, linguaggi e sistemi) ma anche **una specifica conoscenza del processo fisico sotteso e, non ultimo, una dettagliata comprensione della semantica delle diverse variabili**. Infatti, non solo l'attacco cyber deve essere in grado di inviare comandi legittimi (sintatticamente corretti), ma deve essere anche in grado di sapere **quali comandi inviare e a quali oggetti** (correttezza semantica).

Security by obscurity

Per lungo tempo si è ritenuto che la complessità dei sistemi OT rappresentasse una adeguata barriera: una security by obscurity rafforzata dalle peculiarità di questi sistemi. Infatti l'unico episodio di cui si ha notizia riguarda un attacco portato a termine contro i sistemi di gestione delle acque nella cittadina di Maroochy Shire (Australia), ma in questo caso l'autore dell'attacco era uno degli sviluppatori del sistema che aveva poi cercato di mettere in piedi una estorsione.

Il worm Stuxnet

Nel 2010 lo scenario è però cambiato radicalmente grazie, o meglio a causa, del worm Stuxnet. Questo worm che ancora oggi è considerato come uno dei programmi software più complessi mai realizzati ed il cui costo di sviluppo è stimato in oltre 20 milioni di dollari è il primo

specificatamente progettato per attaccare i PLC della **Siemens** e nello specifico per **alterare la velocità di rotazione di alcuni motori** qualora specifiche condizioni fossero verificate (in estrema sintesi il worm verificava se il computer è connesso con un PLC e gli invia una "sfida" e qualora il messaggio di risposta è coretto, provvedeva ad aggiornare il valore della variabile dove è memorizzata la velocità di rotazione). **Nessuno ha certezza su chi fossero gli autori di questo worm**, ne quali i reali obiettivi. Molti rumors indicano che l'obiettivo primario di Stuxnet era il **sito atomico di Natan** (Iran) e nello specifico la distruzione delle centrifughe per l'arricchimento dell'uranio; suggerendo che dietro l'ideazione del worm possano esserci **nazioni storicamente contrarie al programma atomico iraniano**. A prescindere dagli autori e dagli obiettivi, una cosa è evidente: **Stuxnet è stata la prima vera cyber-weapon realizzata in grado cioè di creare danni "mirati" a strutture meccaniche sfruttando le vulnerabilità cyber dei sistemi OT**.

I black-out elettrici in Ucraina

Dopo Stuxnet altri malware specificatamente progettati per attaccare un OT sono stati scoperti: Irongate (2014), **Dragonfly** (2016) questi malware avevano il compito di "analizzare" il processo controllato dallo specifico PLC/SCADA (nello specifico l'analisi del protocollo OPC per creare una mappa dei dispositivi esistenti nella rete OT). **Il malware Blackenergy 3 è ritenuto la causa del black-out elettrico occorso in Ucraina nel dicembre del 2015**. Il malware, dopo aver appreso il corretto funzionamento del sistema, è stato in grado di inviare comandi "leciti" con l'obiettivo di disconnettere alcune sottostazione dalla rete elettrica (e successivamente rendere non operativo il sistema di telecontrollo cancellando alcuni file di sistema). Interessate notare come il CERT USA ha evidenziato che

questo malware è stato rinvenuto in diversi sistemi di controllo di utility americane e che lo stesso era residente su questi sistemi da diverso tempo, in alcuni casi anche da più di 5 anni.

A distanza di un anno, nel dicembre 2016, un secondo balck-out ha colpito l'Ucraina e questa volta il gestore elettrico Ukrenergo ha esplicitamente affermato che la causa è da ricercare in "*external interference from the computer network",* **ovvero in un attacco cyber condotto tramite il malware CrashOverride.** Questo malware, in maniera similare a Blackenergy 2, è in grado di introdurre comandi "leciti" riuscendo a manipolare il comportamento della rete elettrica al fine di creare un black-out.

I pericoli della manipolazione di un sistema SIS

L'ultimo attacco in ordine temporale è quello scoperto nel dicembre del 2017 con il nome di Triton. La particolarità di questo malware è che il suo target sono i sistemi SIS (Safety Instrumental System) ovvero quella porzione dei sistemi ICS, generalmente separata dai normali sistemi di gestione di processo, che sono utilizzati per prevenire eventi catastrofici. È evidente che una **manipolazione di un sistema SIS,** in concomitanza con un evento di altra natura, può creare una situazione estremante pericolosa.

La cosa più interessante è che per la quasi totalità degli osservatori ritiene che tutti questi malware (escluso Stuxnet) sono delle proof-of-concept, ovvero come dei test per verifica le reali potenzialità e capacità di queste cyber-weapon.

Non esistono dati certi su chi vi sia dietro questi test, mentre è evidente, come sottolineato anche dall'ultimo Global Risk Report che *"le cyber capacità di attacco si stanno sviluppando più rapidamente che la abilità di gestire eventi ostili"* evidenziando come vi sia una

potenziale escalation legata a state-on-state cyber attack.

Attacchi ai sistemi OT e geopolitica

L'impressione è che queste azioni possano diventare nel prossimo futuro elementi di pressione geopolitica, cosa per altro riconosciuta anche dalla NATO che ha indicato il cyberspace come un ulteriore Dominio delle operazioni.

In questo scenario è evidente che la protezione rispetto a questa classe di attacchi non può essere demandata ai soli operatori privati ma è fondamentale una forte sinergia con i soggetti pubblici deputati.