NON C'È DIGITALIZZAZIONE SENZA CYBERSICUREZZA

L'EVOLUZIONE DEL MODUS OPERANDI DEI CYBERCRIMINALI NON HA COMPORTATO UNA VARIAZIONE DEI LORO OBIETTIVI: I SISTEMI DI CONTROLLO DEGLI IMPIANTI DI PRODUZIONE INDUSTRIALE SONO ANCORA UN TARGET PARTICOLARMENTE ATTRAENTE

A cura del WG Software Industriale di ANIE Automazione

Il primo attacco informatico mirato contro i sistemi di controllo dei processi industriali Supervisory Control and Data Acquisition (SCADA), il worm Stuxnet, rilevato per la prima volta su un dispositivo di un dipendente della centrale nucleare di Bushehr in Iran nel giugno 2010, ha dimostrato che le molte ipotesi sull'impatto delle minacce informatiche sugli ambienti OT erano sbagliate, e lo ha fatto utilizzando un malware molto più sofisticato di qualsiasi altro visto in precedenza. L'obiettivo di questo worm era manipolare i PLC industriali al fine di alterare il corretto funzionamento delle centrifughe e fermare così il programma di arricchimento nucleare iraniano in fase di sviluppo. Il worm infettò circa 30.000 risorse informatiche nel Paese per poi estendersi a macchia d'olio a livello globale (oltre 115 i Paesi colpiti, tra cui l'Italia), compromettendo circa 100.000 sistemi.

Il motivo per cui si sono verificati tutti questi attacchi è semplice: di fatto, la superficie di attacco delle organizzazioni industriali sta aumentando. Una tendenza che molti spiegano con la crescente convergenza IT/OT

Tuttavia, per concezione, Stuxnet avrebbe dovuto essere un malware non rilevabile, poiché era in grado di analizzare le comunicazioni inviate ai PLC e di installarsi su un host attraverso un movimento laterale. I cyber-attaccanti hanno analizzato il funzionamento dei protocolli di comunicazione OT rilevando nello specifico carenze in termini di autenticazione e crittografia nel protocollo utilizzato, nonché la mancanza di un controllo anti-replicazione. Una vulnerabilità che ha palesato la necessità di dotare questo protocollo OT di un livello di sicurezza integrato.

Compromettere un sistema di controllo industriale isolato sembrava un compito estremamente complesso e superare questi limiti ha richiesto ingenti investimenti finanziari e in termini di risorse umane, indicando che probabilmente gli aggressori, dotati di una profonda conoscenza degli impianti iraniani, avessero replicato l'infrastruttura in maniera esatta acquisendo attrezzature industriali molto costose.

Stuxnet ha indubbiamente posto le basi per una nuova frontiera della criminalità informatica ai danni degli ambienti industriali.

Un retaggio poliforme

Dodici anni dopo la sua scoperta, la tecnicità e la difficoltà di implementazione di Stuxnet ne fanno ancora un caso da manuale e sicuramente questo worm è stato fonte d'ispirazione per successivi attacchi. Se all'epoca la complessità dell'ambiente industriale e la difficoltà di distribuzione dei malware in ambienti non connessi a Internet suggerivano che attaccare un bersaglio di questo tipo non fosse un investimento interessante, la storia ha raccontato di altri molti attacchi. Nel 2012, ad esempio, Saudi Aramco e RasGas furono vittime di un attacco informatico attribuito allo Stato iraniano. Nel 2013, invece, è stato compromesso il sistema di controllo delle paratie della diga Bowman negli Stati Uniti. Nel 2015, i forni di un'acciaieria in Germania sono stati a loro volta attaccati, con una modalità definita dall'intelligence tedesca "simile a Stuxnet". Allo stesso tempo, anche l'Ucraina è stata colpita da un malware, questa volta mirato agli impianti elettrici del Paese con i malware "Black Energy" e "CrashOverride" nel 2015, e poi "Triton" nel 2017.

Il motivo per cui si sono verificati tutti questi attacchi è semplice: di fatto, la superficie di attacco delle organizzazioni industriali sta aumentando.

Una tendenza che molti spiegano con la crescente convergenza IT/OT. I criminali informatici si procurano accesso agli ambienti IT spesso interconnessi con gli ambienti OT industriali, senza dover effettuare sviluppi specifici o cercare vulnerabilità zero-day in ambito OT: l'accelerazione dovuta alla digitalizzazione crea opportunità non solo per le imprese, ma anche per gli aggressori!

Bisogna esserne consapevoli e tenere in considerazione l'avvertimento di chi opera nell'ambito della security industriale: nessuna digitalizzazione senza cybersicurezza!

Un pericolo ancora in circolazione?

La domanda è pertinente e la risposta inequivocabile. Uno scenario simile a Stuxnet è ancora possibile nel 2022, perché il principio rimane lo stesso: ci sono sempre state, ci sono e ci saranno sempre vulnerabilità zero-day che assicurano ai criminali informatici un vantaggio offensivo.

La più grande differenza rispetto al passato, nel caso dovesse succedere nuovamente un attacco agli impianti industriali, è che non avremmo più un alibi.

Difendere la fabbrica digitale contro le minacce informatiche è, infatti, un prerequisito fondamentale per la trasformazione digitale divenuto assodato, e da anni sono stati sviluppati e divulgati diversi standard per la protezione da attacchi. Inizialmente si è introdotta la serie di standard ISO/IEC 27000, anche in ambito produttivo, ma successivamente è stato consolidato lo standard IEC 62443 che è il riferimento per la cy-

Uno scenario simile a Stuxnet è ancora possibile nel 2022, perché il principio rimane lo stesso: ci sono sempre state, ci sono e ci saranno sempre vulnerabilità zero-day che assicurano ai criminali informatici un vantaggio offensivo

bersecurity della fabbrica digitale. Questo standard è stato realizzato perché si rivolge direttamente alle esigenze di protezione degli ambienti industriali e ha l'obiettivo di garantire la confidenzialità, l'integrità e la disponibilità delle informazioni in ambito Operational Technology, ma anche nell'integrazione con l'Information Technology della fabbrica stessa verso i sistemi superiori.

Più che affidarsi a una singola misura, lo standard IEC 62443 prevede di adottare, contemporaneamente, diverse contromisure complementari, ognuna delle quali fornendo uno strato di difesa.

Se un attaccante fosse in grado di superare il primo livello, dovrebbe poi conquistare il secondo, e poi il livello successivo, e così via prima di poter raggiungere l'obiettivo finale.

Per ogni strato, l'attaccante deve necessariamente cambiare metodologia d'attacco, obbligandolo così a dover studiare e affrontare ogni volta diversi tipi di attacco. Questa strategia è comunemente chiamata "difesa in profondità".

Genericamente si può pensare di suddividere la protezione in tre livelli: soluzioni per la sicurezza di impianto, come la gestione degli accessi e delle procedure; soluzioni per gestione delle reti di comunicazioni, come l'utilizzo di firewall e concetti di protezione di cella; "integrità di sistema" - il livello più interno - dove sono definite tutte le misure per rendere più robusti i PLC e gli altri componenti di automazione. Prerogativa fondamentale dello strato "integrità di sistema" è quello di definire e aiutare tutti i ruoli per una corretta gestione degli aggiornamenti software e rilevamento di malware.

Lo standard introduce anche il concetto di protection level con il quale si combinano, a valle di una fase di identificazione di vulnerabilità rispetto alle tre dimensioni, due misure estremamente differenti tra di loro: le misure legate agli aspetti tecnologici e quelle procedurali. Inoltre, IEC si rivolge, dando delle definizioni e misure dedicate, agli operatori degli impianti produttivi, ai system integrator e ai produttori di componenti coprendo tutti gli aspetti della sicurezza informatica.

Il futuro per la cybersecurity

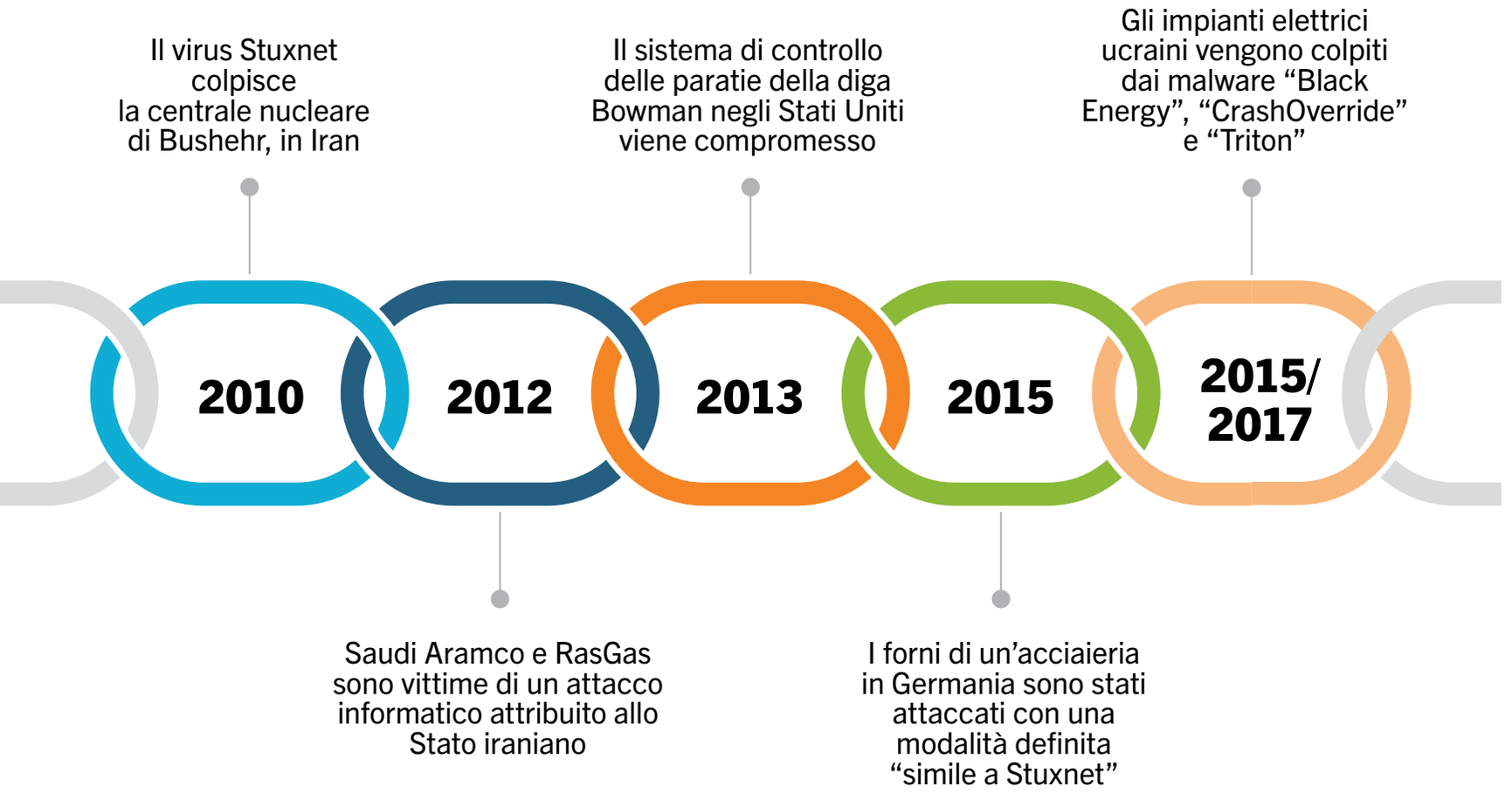
Per evitare un altro attacco come Stuxnet è davvero importante attuare tutte le contromisure necessarie e lo standard IEC 62443 ci può dare un aiuto importante che parte con la definizione dell'analisi dei rischi fino all'implementazione delle misure tramite il concetto di protezione in profondità.

In merito alle normative ci sono degli sviluppi ulteriori in quanto la storia degli attacchi informatici ci ha insegnato che anche la sicurezza funzionale delle macchine e degli impianti può essere compromessa.

La buona notizia è che ci sarà a breve l'aggiornamento ufficiale della nuova direttiva macchine (nuovo regolamento macchine) che presenterà aggiornamenti anche per la cybersecurity.

Sarà inserito un nuovo paragrafo "protection against

UNA CATENA DI ATTACCHI INFORMATICI



corruption" che indica che le macchine dovranno essere progettate e realizzate al fine di evitare situazioni di pericolo.
Non solo in termini di hardware, ma esplicitamente anche i software dovranno essere progettati e configurati per garantire una protezione adeguata contro attacchi accidentali o intenzionali (quindi possibili attacchi cyber fisici).
Il paragrafo, sempre riferito alla cybersecurity, prevederà inoltre che la macchina sarà tenuta a collezionare le evidenze di un intervento legittimo o illegittimo nelle modifiche del software installato sulla macchina.
Sempre in ottica di convergenza tra safety e security, nella stessa normativa sarà previsto anche un aggiornamento in merito alla safety e affidabilità dei sistemi di controllo.
Gli stessi dovranno essere progettati e realizzati al fine di prevenire situazioni potenzialmente pericolose. Inconsapevolmente, gli autori di Stuxnet hanno influenzato e impresso una forte accelerazione agli attacchi informatici in ambienti OT.
Sarà interessante osservare come i responsabili OT si adatteranno nei prossimi anni per far coesistere l'uso di nuove tecnologie e la cybersecurity.
Una bella sfida, ma rispetto al 2010 ora siamo a conoscenza dell'utilità imprescindibile di un approccio completo di cybersecurity di tipo "difesa in profondità" e abbiamo gli strumenti per difenderci. ■