TRITON, ovvero quando non ci si può più fidare neanche del sistema di sicurezza dell'impianto critico (centrale elettrica)

Enzo M. Tieghi,
CEO di ServiTecno

di Enzo M. Tieghi

Quando il sistema di allarme/sicurezza non è più affidabile di chi/cosa ci possiamo più fidare?

Gli hacker sono arrivati a compromettere anche i SIS/ESD di impianti critici.

Chi si occupa di controllo di processo in impianti critici e con processi pericolosi li conosce bene. Sono i SIS (Safety Instrumental Systems) a volte anche identificati come sistemi ESD (Emergency Shut-Down Systems).

I sistemi di sicurezza SIS sono i sistemi responsabili della sicurezza operativa e garantiscono l'arresto in emergenza entro i limiti considerati sicuri, ogni volta che un impianto supera tali limiti. L'obiettivo principale è quello di evitare incidenti all'interno e all'esterno dell'impianto (raffineria, impianto chimico o centrale elettrica che sia), come incendi, esplosioni, danni alle attrezzature, protezione della produzione e della proprietà e, soprattutto, evitare danni alla vita o alla salute personale e impatti catastrofici alla comunità. Dovrebbe essere chiaro che nessun sistema è completamente immune ai guasti e, anche in caso di rottura o malfunzionamento l'impianto dovrebbe posizionarsi in una condizione di sicurezza.

A questo servono i SIS o ESD: iniziare procedure di messa in sicurezza, ed anche spegnimento in sicurezza, quando l'impianto può diventare pericoloso per l'incolumità di persone, dell'ambiente e dell'impianto stesso.

Quando l'impianto potrebbe diventare pericoloso?

Quando esce dal controllo degli operatori: se l'impianto è complesso quasi sicuramente gli operatori non lo gestiscono "a mano", ma si fanno aiutare da un sistema di controllo automatizzano, con a bordo logiche gestite da computer, hardware e software.

In pratica e per le norme di sicurezza/safety un impianto complesso, critico e potenzialmente pericoloso (come ad esempio una raffineria o una centrale elettrica a combustibile a ciclo combinato) viene dotato di due sistemi di controllo indipendenti uno dall'altro e di solito ognuno ridondato e fault tolerant.

Perché due sistemi indipendenti?

Perché in caso di problemi sistema di controllo di processo primario, possa subentrare il secondo sistema che mette in sicurezza il processo e l'impianto stesso: il SIS appunto.

Consideriamo quindi i SIS/ESD le “sentinelle” o gli “angeli custodi” pronti ad entrare in azione per salvare vite umane e l’ambiente quando i sistemi di controllo primari non riescono più a fare correttamente il loro lavoro. E questo potrebbe avvenire quando questo sistema di controllo primario ha un problema di funzionamento e/o stia stato compromesso o sabotato.

In una comunicazione del CERT Italiano (ed anche del US ICS-CERT) veniamo a sapere di un incidente accertato in una centrale elettrica:

Ricercatori di sicurezza hanno rivelato l’esistenza di un nuovo esemplare di malware, battezzato TRITON (o Trisis) progettato specificamente per attaccare sistemi di controllo industriali (ICS) in infrastrutture critiche, provocandone il malfunzionamento e l’interruzione dei servizi erogati.

La scoperta è avvenuta a seguito delle indagini su un incidente informatico avvenuto ai danni di una azienda non specificata. Sulla base delle evidenze riscontrate, i ricercatori sospettano che l’operazione sia stata condotta da attori sponsorizzati da uno Stato, anche se non è stata al momento ipotizzata alcuna attribuzione.

Il malware TRITON fornisce un’infrastruttura di attacco costruita per interagire con piattaforme di sicurezza e controllo critico di tipo SIS (Safety Instrumented System) a marchio Triconex (Tricon, Trident, Tri-GP), distribuiti dalla società Schneider Electric.

Un SIS è un sistema autonomo che controlla in modo indipendente lo stato di un processo. Se il processo supera i parametri che definiscono uno stato di pericolo, il SIS tenta di riportare il processo in uno stato sicuro o esegue automaticamente un arresto sicuro del processo (safe shutdown).

Stando a quanto riportato dagli analisti, gli attaccanti sono riusciti ad introdurre il malware TRITON su una workstation industriale SIS con sistema operativo Windows, mascherandolo come un'applicazione legittima Triconex Trilog, un tool impiegato per controllare i log, parte della suite TriStation. Per poter attivare il payload, TRITON richiede che lo switch a chiave sul pannello posteriore del dispositivo Triconex sia in posizione "PROGRAM" (vedi immagine).

In pratica il sistema SIS che dovrebbe "salvare" l'impianto e proteggere l'incolumità di persone e ambiente può essere utilizzato per "spegnere la centrale".

E'come se un sistema antincendio di un edifico fosse manomesso volutamente per far sfollare l'edificio stesso da tutte le persone che vi si trovano dentro (anche questo già visto...).

LINK DI RIFERIMENTO

https://en.wikipedia.org/wiki/Industrial_safety_system#ESD
https://en.wikipedia.org/wiki/Safety_instrumented_system
https://en.wikipedia.org/wiki/Safety_instrumented_system
https://www.certnazionale.it/news/2017/12/15/triton-scoperto-nuovo-malware-progettato-per-danneggiare-sistemi-industriali/
https://ics-cert.us-cert.gov/advisories
https://www.engadget.com/2017/12/17/hackers-shut-down-plant-by-targeting-safety-system/
http://www.bbc.com/news/technology-35746649