

Esempi di attacchi cyber e guasti accidentali a CPS

Di seguito si descrivono brevemente alcuni tra i più famosi attacchi contro CPS, divenuti noti ai mezzi di informazione.

Si sottolinea che, in generale, i soggetti attaccati preferiscono tacere su quanto subito, salvo che sia impossibile tacere, proprio per evitare di ammettere la propria vulnerabilità e, di conseguenza, perdere la fiducia di clienti e investitori.

1. **Maroochy Shire Sewage Spill.** Nel 2000 un ex dipendente di Maroochy Water Services ha violato 142 stazioni di pompaggio delle acque reflue e ha causato la fuoriuscita di circa un milione di litri di acque reflue nei sistemi idrici locali. L'attacco è stato effettuato solo con un laptop, un PC compatto e un trasmettitore radio. L'ex dipendente vendicativo ha avuto accesso al sistema con le proprie credenziali, colpevolmente non disabilitate dall'azienda dopo il suo allontanamento, e ha agito come un insider, e, muovendosi tra le stazioni di pompaggio dell'infrastruttura ha manipolato le configurazioni di sistema. Questo incidente è un buon esempio per mostrare come l'utilizzo delle credenziali conosciute dagli ex dipendenti possa causare incidenti. Occorre una gestione efficace e puntuale del controllo degli accessi da parte delle organizzazioni, revocando tempestivamente le credenziali a chi smetta di averne necessità o diritto.

2. **Stuxnet.** Nel 2009 l'impianto nucleare dell'Iran è stato preso di mira dall'attacco più complesso conosciuto fino ad oggi. Stuxnet ha infettato più di 100.000 host in 25 Paesi, con il 60% degli host infettati in Iran. Ha preso di mira in modo specifico vulnerabilità esistenti nei sistemi operativi Microsoft e nei PLC Siemens, pur rimanendo nascosto, riuscendo a deteriorare le centrifughe per l'arricchimento dell'uranio,

senza che ai sistemi di monitoraggio arrivassero indicazioni di problemi in corso. Si sostiene che Stuxnet sia stato sviluppato dagli Stati Uniti e da Israele per sabotare il programma iraniano di arricchimento dell'uranio. Tuttavia, non ci sono state conferme ufficiali in tal senso. In particolare, è stato sfruttato il fatto che ai PLC Siemens non fosse stata cambiata la password di default.

3. Saudi Aramco Attack. Nel 2012 il produttore di petrolio e gas Saudi Aramco è stato preso di mira da un malware successivamente denominato Shamoon. Gli aggressori hanno avuto accesso alla rete aziendale e hanno distribuito il malware, che ha eliminato i dati relativi alla produzione. Poiché la distribuzione di quel tipo di malware richiede l'accesso fisico ai computer interni, si ritiene che gli aggressori abbiano avuto anche l'aiuto di un insider. L'attacco, che non è riuscito ad accedere alla componente OT, è stato rivendicato dal gruppo "The Cutting Sword of Justice" per motivi politici.

4. Fukushima Daiichi Nuclear Disaster. Nel 2011 un terremoto ha interrotto l'operatività della centrale nucleare di Fukushima Daiichi danneggiando i sistemi di alimentazione che raffreddano i reattori, provocando contaminazione radioattiva e rendendo necessaria l'evacuazione di circa 100.000 residenti. I disastri naturali sono prevedibili solo in una certa misura; di solito, i rischi che possono verificarsi a causa di questi eventi vengono ignorati durante la progettazione del CPS. L'incidente all'impianto nucleare di Fukushima Daiichi ha portato al riesame delle infrastrutture strutture simili, per verificare quanto siano sicure contro i disastri naturali e i conseguenti guasti provocati da questi ultimi.

5. Tridium Niagara Framework Attack. Nel 2012 gli aggressori si sono infiltrati nel sistema HVAC (Heating, Ventilation and Air Conditioning) di un'azienda con sede negli Stati Uniti. L'azienda utilizzava una versione non aggiornata di Tridium Niagara (software per il monitoraggio e l'individuazione di

anomalie), contenente diverse vulnerabilità che consentono l'accesso backdoor. Queste vulnerabilità erano all'epoca già state rese note e descritte da diverse organizzazioni di sicurezza informatica. Tuttavia, la società vittima non era a conoscenza del problema, né aveva aggiornato i propri sistemi. Il CPS era connesso a Internet con protezione basata su password. Gli aggressori, che hanno ottenuto privilegi di amministrazione senza conoscere la password, sfruttando la vulnerabilità già nota, non hanno comunque avuto accesso ad alcun documento

significativo e la motivazione dietro l'attacco è rimasta sconosciuta.

6. Target Attack. Nel 2013 le anomalie nel sistema informatico di Target sono state scoperte da un team esterno all'organizzazione, specializzato in analisi per la sicurezza informatica. Gli aggressori avevano avuto accesso alle informazioni personali di oltre 1.000.000 di clienti. L'elenco dei fornitori di terze parti era accessibile nel portale di Target, e gli aggressori hanno scelto Fazio Mechanical (produttore HVAC) e inviato un'e-mail di phishing a uno dei dipendenti, che ha consentito l'installazione del malware e rubato le credenziali di accesso di Fazio Mechanical. Hanno così avuto accesso alla rete aziendale e rubato informazioni personali con la motivazione del guadagno finanziario. Questo incidente è unico per il modo in cui gli aggressori hanno avuto accesso alla rete IT, ovvero compromettendo prima la rete OT.

7. Godzilla Attack! Turn Back!. Nel 2013 i segnali stradali elettronici a San Francisco, (Stati Uniti) sono stati violati e, invece di messaggi su viabilità e traffico, mostravano "Godzilla Attack" e "Turn Back!" I segnali erano controllati da una società esterna che utilizzava ancora le credenziali predefinite per accedere alla rete. L'incidente non ha causato problemi significativi. La società responsabile dei segnali ha affermato che l'attacco è stato compiuto da qualcuno che già

conosceva le credenziali. Si ritiene che la motivazione dietro l'attacco fosse meramente ludica.

8. Brute Force Attacks on Internet-Facing Control Systems. Nel 2013 il proprietario di una stazione di pompaggio del gas negli Stati Uniti ha allertato ICS-CERT in merito a un aumento del numero di tentativi di attacco basati su forza bruta ai propri sistemi, eseguiti da 49 diversi indirizzi IP. Gli attori della minaccia e la motivazione dietro gli attacchi, nessuno dei quali ha avuto successo, sono ancora sconosciuti. Questo caso è un buon esempio per dimostrare come il rilevamento tempestivo dei tentativi di intrusione prevenga ulteriori danni ai sistemi industriali, aumentando la possibilità di una risposta efficace.

9. German Steel Mill Cyberattack. Nel 2014 è stato attaccato l'altoforno di un'acciaieria tedesca. Non essendo stato possibile spegnere la fornace, l'attacco ha provocato ingenti danni fisici. Gli aggressori hanno avuto accesso alla rete aziendale tramite un'e-mail di phishing, quindi si sono trasferiti sulla rete industriale e hanno eseguito il codice dannoso per riprogrammare diversi PLC e compromettere le funzioni della fornace. Hanno sfruttato le vulnerabilità risultanti dalla debole protezione dei confini tra le reti a causa della mancanza di zone demilitarizzate (DMZ) che espongono la rete locale alla rete esterna. L'attacco è stato definito APT (Advanced Persistent Threat) e si ritiene sia stato eseguito da un gruppo con l'obiettivo del furto della proprietà intellettuale.

10. Kemuri Water Company Attack. Nel 2016 Verizon ha pubblicato un rapporto su un attacco a una società di trattamento delle acque. L'azienda aveva memorizzato le credenziali di accesso al sistema OT sul server Web front-end. Gli aggressori, che hanno avuto accesso a tali credenziali tramite SQL injection e phishing, hanno riprogrammato gli attuatori di controllo ma non sono riusciti a causare alcun danno a causa della mancanza di esperienza sui sistemi SCADA.

Tuttavia, si ritiene siano state rubate le informazioni personali di circa 2.500.000 utenti.

11. Ukrainian Power Grid Attack. Nel 2015 la società di distribuzione elettrica ucraina Kyivoblenergo è stata oggetto di un attacco che ha provocato un'interruzione di corrente che ha interessato 225.000 utenti. Gli aggressori hanno avuto accesso alla rete IT tramite e-mail di phishing, quindi hanno acquisito le credenziali per infiltrarsi nella rete OT, ove eseguire il malware, denominato BlackEnergy 3; hanno poi continuato ad attaccare il sistema a intervalli di 30 minuti, per impedire l'attivazione di tecniche di mitigazione.

12. TRITON. Nel 2017 il Safety Instrumented System (SIS) di una società di servizi petroliferi e gas del Medio Oriente è stato spento a causa dell'esecuzione riuscita di un malware denominato TRITON. Un controller SIS, realizzato da Schneider Electric e connesso a un PC Windows, è stato disattivato lasciando l'intera utility vulnerabile agli incidenti OT. Gli aggressori si sono prima infiltrati nella rete IT, quindi sono passati all'OT sfruttando la debole protezione del confine tra queste reti.

13. Cryptocurrency Malware Attack on SCADA. Nel 2018 è stato scoperto un malware sul sistema OT di un'azienda europea di servizi idrici. Il malware, progettato per estrarre la criptovaluta Monero utilizzando i server HMI e SCADA della vittima, era in grado di funzionare in modalità invisibile, ma l'IDS ha rilevato un aumento dell'utilizzo della CPU e della larghezza di banda. L'aggiornamento dei sistemi OT richiede pianificazioni a lungo termine e quindi la maggior parte dei sistemi non può ricevere tempestivamente gli aggiornamenti più recenti. In questo caso, le applicazioni HMI non aggiornate, collegate a Internet per consentire la gestione remota, sono state violate dagli aggressori per accedere al sistema.

14. Norsk Hydro Ransomware Attack. Nel 2019 la società produttrice di alluminio Norsk Hydro ha subito un attacco

ransomware successivamente denominato LockerGoga. Gli aggressori hanno effettuato l'accesso e crittografato i dati critici, provocando l'arresto della rete aziendale e l'interruzione di molte operazioni, inclusa l'elaborazione degli ordini. Poiché gli avversari, dopo aver ottenuto l'accesso al sistema, hanno scelto di eseguire un ransomware precedentemente noto, si stima che l'attacco mirasse a interrompere la produzione per colpire la reputazione dell'azienda piuttosto che a un guadagno finanziario.

15. Riviera Beach Ransomware Attack. Nel 2019, i servizi idrici di Riviera Beach (una piccola città situata in Florida, USA) sono stati oggetto di un attacco ransomware. Gli aggressori hanno inviato un'e-mail di phishing e il destinatario ha consentito all'attacco di raggiungere tutte le reti cittadine, compresi i sistemi di utenza idrica, a causa dell'interconnessione alla rete informatica senza alcun meccanismo di protezione specifico. Il consiglio comunale ha accettato di pagare il riscatto di 65 Bitcoin (circa \$ 600.000 entro quella data); tuttavia, gli aggressori non hanno inviato la chiave di decrittazione. Quindi il consiglio comunale ha deciso di rinnovare i sistemi oggetto dell'attacco.

16. Florida Water Treatment Poisoning Attack. L'8 febbraio 2021 un attaccante ha tentato di avvelenare Oldsmar, una città della Florida negli Stati Uniti. L'attaccante ha avuto accesso al computer che ospita il software di controllo del trattamento dell'acqua tramite un programma di accesso remoto (TeamViewer), quindi ha aumentato la quantità di idrossido di sodio al di sopra del livello normale. Il cambiamento di concentrazione dell'acqua è stato rilevato da un operatore e immediatamente annullato e l'accesso remoto è stato disabilitato. L'avversario non ha infatti falsificato le letture del sensore per ingannare l'operatore, contrariamente a quanto avvenuto per Stuxnet, quindi il cambiamento inaspettato è stato rilevato tempestivamente. Il modo in cui sono state acquisite le credenziali del computer è ancora

sconosciuto. In questo incidente, avere personale IT operativo 24 ore su 24, 7 giorni su 7 (che non è il caso della maggior parte dei sistemi industriali) per supervisionare il sistema ha impedito che si verificasse un disastro dalle gravi conseguenze.

17. Colonial Pipeline Ransomware Attack. Il 7 maggio 2021 Colonial Pipeline, una compagnia con sede a Houston (Texas) che trasporta benzina e carburante per aerei mediante un sistema di oleodotti, principalmente negli Stati Uniti sudorientali, ha subito un attacco informatico ransomware che ha avuto un impatto sulle apparecchiature computerizzate che gestiscono l'oleodotto. La Colonial Pipeline Company ha interrotto tutte le attività dell'oleodotto per contenere l'attacco. Sotto la supervisione dell'FBI, la società ha pagato l'importo richiesto dal gruppo DarkSide (75 bitcoin o \$ 4,4 milioni di dollari.) Al ricevimento del riscatto gli attaccanti hanno fornito alla compagnia uno strumento informatico per ripristinare il sistema, che tuttavia ha richiesto un tempo di esecuzione assai lungo per giungere al completo ripristino. La Federal Motor Carrier Safety Administration ha emesso una dichiarazione di emergenza regionale per 17 Stati e Washington DC per mantenere aperte le linee di rifornimento di carburante nei giorni successivi all'attacco. È stato il più grande attacco informatico su un obiettivo di infrastrutture petrolifere nella storia degli Stati Uniti. L'FBI e varie fonti dei media hanno identificato il gruppo criminale DarkSide come parte responsabile, ritenendo che lo stesso gruppo avesse rubato 100 gigabyte di dati dai server aziendali nei giorni precedenti. Il 7 giugno, il Dipartimento di Giustizia ha annunciato di aver recuperato 63,7 bitcoin (circa 2,3 milioni di dollari) del pagamento del riscatto. Questo è stato uno dei primi attacchi informatici aziendali di alto profilo che ha avuto inizio da una password personale di un dipendente violata, e probabilmente trovata nel dark web, piuttosto che da un attacco diretto ai sistemi dell'azienda.

Gli attacchi contro i CPS si articolano generalmente in più fasi, e quelli avanzati possono eseguire l'intera Cyber Kill Chain (CKC). L'integrazione di reti IT e OT senza che ci sia una protezione dei confini solida e sicura è l'elemento che si riscontra sia usato più frequentemente negli attacchi.



Le 10 vulnerabilità più sfruttate nei CPS

Gli aggressori prendono di mira principalmente le aziende prive di personale di sicurezza con esperienza nella sicurezza industriale tramite e-mail di phishing; altre (con) cause negli esempi analizzati sono sempre legate al fattore umano, ad esempio il mancato aggiornamento di sistemi e applicativi software o una gestione carente delle credenziali, dal non modificare le password di fabbrica dei dispositivi a non disabilitare tempestivamente le credenziali di chi non ne abbia più diritto o necessità. Anche carenze progettuali e/o implementative, talvolta volute per comodità di accesso remoto semplificato, che rendono debole o inesistente la separazione tra le parti IT e OT di un sistema – eventualmente in concomitanza con le “disattenzioni” di cui sopra – possono consentire a un attaccante di accedere facilmente alla parte OT, ove poter causare ingenti danni.

Quando gli effetti degli attacchi si manifestano a livello OT, a causa degli eventuali danni inferti a cose e/o persone, per l'azienda vittima può essere più difficile occultare l'evento. D'altro canto, la maggior parte delle aziende soggette a violazione dei dati rifiuta di pubblicare un rapporto pubblico sugli incidenti per non intaccare la propria reputazione. Le informazioni sugli incidenti sono per lo più disponibili tramite agenzie di stampa o blogger di sicurezza informatica che affermano di ottenere informazioni tramite informatori (ad esempio, ex o attuali dipendenti sotto pseudonimo), rendendo più difficili ulteriori esami.



Questo articolo è stato estratto dal white paper “Industrial Cybersecurity” disponibile in maniera gratuita al seguente link:

<https://www.ictsecuritymagazine.com/pubblicazioni/industrial-cybersecurity/>

Articolo a cura di **Luca Durante**

Profilo Autore



Luca Durante è Primo Ricercatore presso l'Istituto di Elettronica e Ingegneria dell'Informazione e delle Telecomunicazioni del Consiglio Nazionale delle Ricerche (CNR-IEIIT) di Torino.

Nel 1996 ha conseguito il Dottorato di Ricerca in Ingegneria Informatica presso il Politecnico di Torino, è autore di oltre 70 articoli per riviste e conferenze internazionali, ed è stato ed è tuttora Responsabile Scientifico per il CNR in Progetti Europei e in contratti di ricerca con aziende.

È stato inoltre general co-chair, program co-chair e membro del comitato di

programma di conferenze internazionali, associate editor di IEEE Transactions on Industrial Informatics e revisore per riviste internazionali.

Gli interessi di ricerca vertono principalmente sulle tematiche di sicurezza

informatica, attualmente declinati sulle policy di sicurezza per il controllo di accessi e la sicurezza dei sistemi cyber-fisici.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/esempi-di-attacchi-cyber-e-guasti-accidentali-a-cps/>