PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5530 di Venerdì 22 dicembre 2023

Conoscenze collaudate nelle nuove specifiche in materia d'industrial security

I componenti di sicurezza funzionale proteggono la vita e la salute delle persone, a tal proposito è importante che la sicurezza non possa essere compromessa nemmeno da manipolazioni dall'esterno.

Pubblichiamo un articolo tratto dalla rivista pubblicata dal KAN (Commissione per la sicurezza sul lavoro e la standardizzazione Tedesco) che evidenzia l'importanza che i componenti di sicurezza funzionale della macchine proteggano la vita e la salute delle persone, per esempio impedendo l'accesso a zone pericolose di macchine e impianti, e sottolinea che occorra che lo stato dell'arte trovi coerente applicazione e che fabbricanti e utilizzatori reagiscano adeguatamente a eventuali falle di sicurezza.

Conoscenze collaudate nelle nuove specifiche in materia d'industrial security

Affinché le funzioni di sicurezza dei sistemi di comando possano intervenire in maniera affidabile occorre che gli stessi sistemi di comando siano sicuri, ossia protetti da avarie e manipolazioni. La crescente frequenza con cui vengono segnalate nuove catastrofi nel settore dell'industrial security fa paura. Ciò non di meno, vi sono motivi di speranza: grazie alle possibilità offerte dallo sviluppo tecnologico, infatti, quasi tutte le falle di sicurezza sono facilmente evitabili ? come dimostra il seguente esempio tipico.

Già nel 1883 Auguste Kerckhoffs aveva enunciato sei presupposti fondamentali di una comunicazione riservata. In base al secondo di questi, il sistema di comunicazione "non deve essere segreto, deve poter cadere nelle mani del nemico senza inconvenienti". Evidentemente Guglielmo Marconi non era al corrente di questo scritto. La telegrafia ? tecnologia da lui ideata per una comunicazione riservata ? presupponeva infatti che nessun altro potesse entrare in possesso di uno degli apparecchi in uso o costruirne uno uguale per poi sintonizzarlo sulla stessa frequenza. Nel 1903 Nevil Maskelyne richiamò l'attenzione su questo problema disturbando una dimostrazione di Marconi con la trasmissione di una serie d'insulti in alfabeto Morse. Oggi Maskelyne è per questo considerato il primo hacker della storia. Benché quella della cifratura sicura con metodi crittografici sia una tecnica nota da molto tempo, oggi lo stesso errore di design si ritrova p. es. nei comandi radio per sistemi di semafori1 e nelle gru industriali.

Mancano definizioni unitarie

Ad oggi il tool per la ricerca di norme relative alla security messo a punto dall'università di Brema ha registrato in una banca dati circa 800 norme e oltre 2000 occorrenze riguardanti disposizioni giuridiche. Il fatto che i documenti facciano uso di termini differenti e, almeno in parte, non definiti in maniera univoca rappresenta però un problema. Mentre in alcuni documenti si parla diffusamente di security o sicurezza delle informazioni, in altri si coniano composti contenenti il termine ciber. Non avendo di per sé un significato univoco, questi neologismi devono essere definiti in maniera esatta all'interno del testo. In alcuni casi per cibersicurezza s'intende un'attività, in altri una misura volta a contrastare attacchi via Internet e in altri ancora uno stato in cui un prodotto risulta protetto dagli attacchi via radio.

Anziché coniare neologismi, sarebbe meglio lavorare con due termini ben definiti come sicurezza delle informazioni o security. Laddove poi, p. es., il significato debba essere limitato agli attacchi via radio, questa limitazione andrebbe indicata con chiarezza. Una soluzione diversa e assai elegante è quella adottata dal regolamento UE in materia di macchine, che al punto 1.1.9 dell'allegato III richiede una "protezione dall'alterazione"risultando così anche più chiaro della direttiva Macchine UE

finora in vigore. Con ciò il documento si concentra sull'obiettivo di protezione consistente nel far sì che, p. es. in caso di accesso remoto, non possano crearsi situazioni pericolose e si astiene dallo specificare da cosa venga esattamente provocata l'alterazione.

Comunicazione rapida come fattore decisivo

Una comunicazione rapida ed efficace è la chiave di un'adeguata reazione a falle di sicurezza. Eppure la situazione sul fronte comunicazione non è affatto buona, come dimostra la falla di sicurezza della libreria software Log4J che ha fatto notizia nel dicembre del 2021. Questa libreria software è parte integrante non solo di molti servizi server, ma anche di numerosi componenti industriali. Mentre all'epoca qualcuno puntava il dito contro un uso errato della libreria facendo presente che i problemi di sicurezza avrebbero potuto essere evitati se solo si fosse letta la documentazione, molti produttori si chiedevano se fossero interessati da falle di sicurezza. E in non pochi casi hanno dovuto attendere parecchi mesi per riuscire a sapere se questo problema riguardasse i loro prodotti.

In sintesi, mancavano
? un contatto di emergenza per la security all'interno dell'azienda,
? un formato unitario per raccomandazioni operative e
? uno standard secondo il quale i fabbricanti potessero segnalare anche che un determinato prodotto non era interessato da una lacuna di sicurezza.

Alla mancanza d'informazioni e interfacce unitarie viene posto rimedio con una serie di specifiche aperte che sono state messe a punto da varie associazioni d'imprese, autorità e organizzazioni e possono essere immediatamente attuate da ciascuna azienda (vedi tabella). Un contatto d'emergenza come da specifica IETF RFC 9116 viene archiviato in un semplice file security.txt all'interno del sito web 4 . Qui un fabbricante può anche rimandare alla sua lista di raccomandazioni operative (CSAF). A ciascun prodotto hardware o software viene assegnato un identificatore univoco a livello mondiale (CPE), in modo che gli avvisi internazionali (CVE) possano essere associati automaticamente ai prodotti giusti e alle relative versioni. La criticità della lacuna di sicurezza viene classificata il meglio possibile attraverso un indice univoco a livello mondiale (CVSS). Sulla base della specifica aperta SPDX per ogni progetto è possibile documentare in formato leggibile a macchina quali librerie sono state utilizzate. Attraverso un apposito programma, per ciascun prodotto gli utilizzatori hanno la possibilità di verificare regolarmente se vi sono avvisi di sicurezza e di visualizzare le raccomandazioni operative del caso.

Alcune grandi imprese puntano già adesso su queste specifiche. È ora fondamentale che a breve il loro esempio venga seguito da tutte le altre aziende, in modo che le informazioni su problemi di sicurezza vengano diramate rapidamente e con risparmio sui costi.

Per cominciare, le aziende dovrebbero ora almeno garantire la reperibilità in caso d'incidenti di sicurezza e rendere noto un contatto di emergenza. Con le istruzioni riportate su https://cert.dguv.de ciò è fattibile in una manciata di minuti.

Specifiche aperte sulla sicurezza delle informazioni

Informazione in entrata	A cura di	Specifica
Contatto di emergenza proprio	Produttore, utilizzatore	“security.txt” RFC 9116
Identificatore del prodotto / ID (nome produttore, nome prodotto, versione, lingua...)	Produttore	CPE
Distinta base del software (Software Bill of Materials - SBOM)	Produttore	SPDX
Avviso di lacuna di sicurezza	Autorità di numerazione CVE	CVE
Security Advisory (raccomandazione operativa sulle CVE)	Produttore	CSAF
Caratteristiche per la valutazione della criticità	Produttore	CVSS

Serie delle specifiche aperte che, insieme, contribuiranno in modo decisivo all’industrial security. Nei prossimi anni produrranno quell’accelerazione della comunicazione in caso di falle di sicurezza della quale allo stato attuale vi è urgente bisogno.

Jonas Stein

Fonte: KanBrief 3/23

www.puntosicuro.it