PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5508 di Martedì 21 novembre 2023

Regolamento UE per una maggiore sicurezza dei macchinari interconnessi

In futuro i fabbricanti di prodotti con "elementi digitali" dovranno garantirne la cybersicurezza per tutto il ciclo di vita: la legge sulla ciberresilienza (Cyber Resilience Act).

A fronte del persistere degli attacchi online, p. es. con ransomware, la Commissione UE continua a premere affinché vengano colmate le lacune di sicurezza IT. Dopo leggi come quella sulla cibersicurezza (Cybersecurity Act) del 2019 ? che getta le basi per uno schema di certificazione della sicurezza IT di apparecchi, sistemi e servizi interconnessi valevole in tutta l'UE ? o il recente emendamento della direttiva sulla sicurezza delle reti e delle informazioni (NIS2), a settembre del 2022 ha approvato la bozza di una legge sulla ciberresilienza (Cyber Resilience Act o CRA)1 . Secondo il previsto regolamento sulla ciberresilienza, in futuro i prodotti "con elementi digitali" come hardware e software dovranno essere "immessi sul mercato con un minor numero di vulnerabilità".

L'ambito di validità della bozza è ampio. La Commissione vuole p. es. coprire "qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto", componenti compresi, anche se messi in circolazione separatamente. Particolare attenzione verrà probabilmente rivolta all'Internet delle cose o ai piccoli router ("plaste-router") che, date le loro numerose falle di sicurezza, ad oggi sono spesso vulnerabili. Il regolamento non si applicherà invece a prodotti "sviluppati esclusivamente per scopi di sicurezza nazionale o militari" o specificamente progettati per trattare informazioni classificate. Lo stesso dicasi per settori come quelli dell'aviazione, dei dispositivi medici o delle auto, per i quali già valgono requisiti specifici.

Per quanto riguarda design, sviluppo e processo produttivo, in base alla proposta in futuro prima d'immettere un apparecchio sul mercato i fabbricanti interessati dovranno obbligatoriamente soddisfare dei requisiti essenziali di cibersicurezza. Saranno inoltre tenuti a monitorare eventuali vulnerabilità per tutta la durata del ciclo di vita dell'apparecchio e a porvi rimedio attraverso update automatici e gratuiti. A ciò si aggiungerà l'obbligo di segnalare entro appena 24 ore all' Agenzia dell'Unione europea per la cibersicurezza (ENISA) qualsiasi incidente con ripercussioni sulla sicurezza di hardware o software. In generale dovrà essere introdotta una linea coordinata per la divulgazione delle vulnerabilità.

La CRA prevede che vengano limitate le superfici di attacco degli apparecchi considerati e ridotte al minimo le ripercussioni degli incidenti. I prodotti a cui si applica dovranno garantire la riservatezza dei dati, p. es. mediante crittazione. Dovrà inoltre divenire obbligatorio proteggere l'integrità e l'elaborazione d'informazioni e valori misurati indispensabili ai fini del funzionamento di un articolo.

Al di là di queste disposizioni di base, la Commissione ha individuato una serie di settori critici ad alto rischio. I prodotti del caso sono stati suddivisi in due classi, per ciascuna delle quali è prevista l'introduzione di una specifica procedura di conformità. La categoria I comprende sistemi di gestione dell'identità, browser, sistemi di gestione delle password, programmi antivirus, firewall, reti private virtuali (VPN), sistemi di gestione della rete, sistemi IT di ampia portata, interfacce di rete fisiche, router e chip. A questi si aggiungono sistemi operativi, p. es. per smartphone o desktop, microprocessori e l'Internet of Things (IoT) nelle aziende, che non sono ritenuti particolarmente sensibili.

Nella classe di rischio più alta (classe II) rientrano invece dispositivi desktop e mobili, sistemi operativi virtualizzati e p. es. integrati in macchinari, emittenti di certificati digitali, microprocessori di uso generale, lettori di carte, sensori per robot e

contatori intelligenti. A questi dovranno poi aggiungersi apparecchi IoT, router e firewall per l'industria, che è in generale considerata un "ambiente sensibile". Le falle di sicurezza IT, infatti, si ripercuotono ormai pesantemente anche su macchinari e impianti ? che oggi sono sempre più interconnessi e non più accessibili soltanto a partire dalle superfici aziendali ? e dunque anche sulla prevenzione.

I fabbricanti sono chiamati a valutare la conformità dei loro prodotti mediante un'apposita procedura interna o tramite un esame da parte di enti riconosciuti. Laddove un produttore punti sulle norme armonizzate o abbia già ottenuto un certificato nel quadro di un sistema europeo di certificazione della cibersicurezza, si potrà dare per scontato che il suo hardware o software sia conforme al regolamento. Importatori e distributori saranno tenuti a verificare l'osservanza delle previste procedure da parte del produttore nonché la marcatura CE dell'apparecchio. Per i prodotti di scarsa criticità i fabbricanti saranno autorizzati a compilare da sé una dichiarazione di conformità. Per quanto riguarda la classe di rischio II, sarà invece necessaria una valutazione da parte di terzi.

La Commissione ritiene necessario intervenire, visto che fino al 2021 i crescenti episodi di cibercriminalità hanno causato costi il cui volume è stimato a 5500 miliardi di euro l'anno. In un ambiente interconnesso un incidente di cibersicurezza ai danni di un prodotto potrebbe avere ripercussioni negative su un'intera impresa o catena di fornitura e in molti casi ? p. es. in quello del malware WannaCry ? le conseguenze potrebbero farsi sentire nell'arco di pochi minuti anche al di là dei confini del mercato interno. Ciò comporterebbe un blocco delle attività economiche e sociali e potrebbe addirittura rappresentare un rischio per la vita.

Critiche alla bozza del regolamento

In un suo commento l'ente tedesco di assicurazione obbligatoria contro gli infortuni (DGUV) ha criticato il fatto che già il concetto chiave di cibersicurezza non sia definito in modo chiaro e ha fatto notare come, a seconda delle norme o dei regolamenti considerati, questo termine stia di volta in volta a indicare uno stato, un'attività o un prodotto. Più in generale, risulterebbero problematici i termini dal significato non chiaramente definito contenenti il prefisso "ciber". A seconda delle fonti considerate, p. es., il concetto di cibersicurezza non abbraccerebbe gli attacchi via radio o tramite interfacce USB.

La DGUV vede in modo critico anche l'obbligo dei fabbricanti di segnalare entro 24 ore grandi quantità di dettagli circa una falla di sicurezza. In molti casi, infatti, effettuare degli accertamenti in tempi così brevi non sarebbe realistico. Nello stesso tempo ? così la DGUV ? non sarebbe propriamente necessario divulgare dettagli utilizzabili ai fini di un attacco. Nel suo commento la DGUV sostiene l'importanza di trasmettere soltanto quei dati di cui le autorità hanno davvero bisogno, p. es. per diramare un avvertimento circa un prodotto o stimare gli effetti di una vulnerabilità. Secondo l'ente tedesco di assicurazione obbligatoria contro gli infortuni, anche i due anni concessi per adeguarsi ai nuovi requisiti sarebbero troppo pochi per quei fabbricanti che dipendono da altri prodotti e devono p. es. attendere una valutazione della conformità.

Jonas Stein, responsabile del gruppo di lavoro "Security" della DGUV, fa anche notare che non è possibile svolgere adeguati accertamenti sui sistemi operativi, visto che si evolvono di continuo, e ricorda che in molti casi ? basti ricordare Linux ? sono di tipo open source. Nel caso dei software liberi, tuttavia, non vi sarebbe un unico produttore responsabile della procedura di conformità. Lo stesso settore open source, così Stein, teme di cadere nella trappola della responsabilità: i software liberi sono infatti opera di tanti singoli sviluppatori, i quali potrebbero essere chiamati a rispondere di potenziali falle. "Data la carenza dei mezzi finanziari e delle risorse che servono per svolgere le procedure proposte in merito alla conformità CE, alcuni progetti potrebbero dover essere completamente sospesi", lamenta la Free Software Foundation Europe (FSFE).

A metà luglio il Consiglio dei ministri UE e la commissione competente per l'industria del Parlamento UE hanno preso posizione rispetto alla proposta della Commissione, cosicché a breve potranno prendere il via i negoziati circa un compromesso finale. Gli Stati membri sostengono l'importanza p. es. di una dichiarazione di conformità semplificata, di un maggiore sostegno per le piccole imprese e di un chiarimento della durata di vita dei prodotti attesa dai fabbricanti. Fanno inoltre notare che dovrebbe essere previsto l'obbligo di segnalare le vulnerabilità sfruttate e gli incidenti di sicurezza alle autorità nazionali competenti, e non all'ENISA. I deputati rivendicano a loro volta definizioni più circostanziate, tabelle di marcia osservabili e una più equa ripartizione delle responsabilità e premono nello stesso tempo affinché anche dispositivi per case intelligenti, smart watch e telecamere di sicurezza private trovino posto nella categoria ad alto rischio.

Dr. Stefan Krempl

Fonte: KanBrief 3/23

www.puntosicuro.it