Il Cyber Resilience Act

di Antonio Tringali

Che lo si voglia o meno ci troviamo in un momento della storia in cui sono rinascenti le minacce della guerra vicina e, visto che i computer sono pervasivi, è logico che la guerra sia ibrida: l'attacco di uno Stato minaccia l'infrastruttura di un altro Stato aggredito. Dalle reti cellulari, a quelle energetiche, alle strutture economiche è tutto controllato da sistemi informatici. La guerra non è cavalleresca; è una rapina a mano armata tra Stati e i computer sono solo altri forzieri da scardinare.

Dall'alba del nuovo millennio è divenuto relativamente semplice per gruppi criminali organizzati attaccare la privacy, le menti e i soldi dei cittadini: riscatti per decriptare le informazioni di un'azienda, furti di denaro in digitale, propaganda per influire sul voto prima delle elezioni. Tutto ciò è cyber-guerra e cyber-criminalità.

Il termine "cyber" deriva da "kubernetes" - navigatore in greco - coniato dal matematico N. Wiener nel 1943 per la scienza della *cibernetica*. Questa si occupa del controllo e della comunicazione nei sistemi biologici, sociali e artificiali. Parte del loro controllo sicuro nella strategia europea è il *Cyber Resilience Act* (CRA), uno dei pilastri del *CyberSecurity Act* del 2019. Il CRA è stato preceduto da altre normative che mirano a preservare la continuità di specifici settori strategici: ad esempio NIS2 per infrastrutture energetiche, trasporti, etc.

Prodotto con elementi digitali

Se un prodotto commercializzato in Unione Europea contiene *elementi digitali* a connessione diretta o indiretta a servizi remoti, il cui impiego possa ledere alla salute, sicurezza o privacy dei consumatori, questo dovrà essere *cybersicuro*. Il prodotto in questione potrebbe essere un computer, uno smartphone, ma anche una TV con accesso a un servizio di streaming, nonché una quantità di sistemi digitali sempre più invisibili che cascano sotto il nome-ombrello di *Internet of Things* (IoT).

È difficile oggi trovare un oggetto con dell'elettronica dentro che non sia connettibile a Internet che, in linea teorica o pratica, non possa essere penetrato da agenti più o meno abili e malintenzionati. Questi attacchi costano una ventina di miliardi di Euro l'anno agli Stati e ai comuni cittadini europei secondo Thierry Breton, Commissario Europeo per il Mercato Interno e i Servizi.

Un altro scopo del CRA è aumentare il livello di fiducia dei consumatori, perché la normativa rovescia la responsabilità di un prodotto dall'utente al produttore per tutta la durata del ciclo

di vita del prodotto stesso. Il software diventa di per sé un prodotto e come tale è da indicare nella documentazione di utilizzo che esso sia coperto dalla marcatura CE.

Durante il ciclo di vita il produttore dovrà garantire informazioni ai suoi clienti relative alle vulnerabilità, nonché aggiornamenti di sicurezza (automatici, ove applicabili). Realizzato l'hardware, ciò che può fare un oggetto fisico è abilitato dal software; su questo ci focalizzeremo, perché può essere cambiato. È previsto che il tempo di supporto sia cinque anni, o un numero di anni inferiore se il prodotto è soggetto a scadenza giustificata.

È interessante notare che se un software è sviluppato o modificato esclusivamente per una pubblica amministrazione, esso risulta esente da queste responsabilità.

Applicabilità

Il CRA si applica a tutti gli *operatori economici* di una catena di fornitura fino al consumatore: sviluppatori software, produttori, distributori, importatori e rivenditori. L'eccezione è per gli sviluppatori open source/free software, a meno che essi non offrano assistenza tecnica a pagamento o usino commercialmente i dati dei propri utenti: in tal caso sono trattati come entità commerciali. C'è esclusione anche per:

1. Le piattaforme *Software as a Service* pure, cioè quelle che offrono software da remoto fruibile tramite ad esempio un browser, a patto che non elaborino i dati degli utenti a scopo commerciale. Ad esempio, GitHub per condividere privatamente o pubblicamente il codice sorgente di progetti software.
2. Tutti i software che siano coperti da altre normative con comparabili livelli di cybersecurity (NIS2, AI Act). Ad esempio, il software di controllo di una centrale nucleare.
3. Dispositivi nei settori elettromedicali, avionici, automotive, della sicurezza nazionale e militari. Questi hanno altre normative a cui adempiere, tipicamente più stringenti.

Proposto nel settembre 2022 a complemento della normativa NIS2, il CRA è stato formalizzato il 19/07/2023 e, dopo una consultazione relativamente breve con le parti in campo, l'accordo politico tra i governi è stato raggiunto il 30/11/2023; è stato definitivamente approvato il 12/03/2024. Di fatto, dalla pubblicazione in Gazzetta Ufficiale Europea ci saranno trentasei mesi per adeguarsi prima che la normativa entri in piena forza attuativa, ma per alcuni dei suoi articoli i tempi saranno di ventuno e diciotto mesi.

L'ENISA è l'ente europeo preposto alla cybersicurezza delle infrastrutture e delle reti. Il CRA lo rende anche responsabile, insieme all'European Cybersecurity Competence Centre, di addestrare un numero di professionisti per supportare le attività di sorveglianza del mercato e le valutazioni di conformità in collaborazione con il settore privato e gli operatori economici.

Va bene, un mucchio di buoni propositi. Vediamo adesso come si coniughino per chi queste misure le debba applicare, partendo dal basso della catena di fornitura. Anche perché le penali sono ingenti in caso di colpa grave: il CRA fissa multe fino a quindici milioni di Euro o fino al 2,5% del fatturato mondiale per l'anno fiscale precedente dell'operatore economico, secondo quale delle due cifre sia più elevata.

Sviluppatori

Il focus principale è su chi sviluppi commercialmente prodotti di consumo connessi. L'approccio è per una valutazione basata su rischi, utilizzando varie misure di sicurezza e le migliori pratiche di settore già dalla progettazione (*secure by design*).

Il prodotto complessivo deve possedere una configurazione iniziale sicura (*secure by default*), non accessibile da agenti non autorizzati, con la possibilità per i consumatori di ritornare alla configurazione di fabbrica.

In particolare, il prodotto dovrebbe elaborare solo i dati necessari in ossequio al GDPR. Le funzioni essenziali dovrebbero essere sempre disponibili: si pensi alla chiamata di emergenza di un telefono mobile anche in assenza di credito.

Durante tutto il ciclo di vita del prodotto dovrebbero essere forniti aggiornamenti di sicurezza e i propri utenti dovrebbero essere notificati di possibili falle. Ciò implica che il dispositivo su cui è eseguito il software sia sempre aggiornabile, il che potrebbe aumentare i costi di produzione dell'hardware.

Diventa obbligatoria la lista dei componenti su cui si basa il software, in modo simile ai prodotti elettronici, fornendo il *Software Bill of Materials* in uno dei formati standard insieme alla documentazione di prodotto.

Gli sviluppatori dovrebbero redigere una dichiarazione di conformità. Questa dipende dalla *classe* del prodotto:

- Prodotti non critici: ad esempio, linguaggi come Python e framework per lo sviluppo web. Si stima che questi siano circa il 90% dei casi.
- Critici di classe 1: web browser, gestori di password, antivirus, gestori di VPN, ...
- Critici di classe 2: sistemi di virtualizzazione, firewall, CPU *tamper-resistant*.

La normativa suppone che i prodotti critici siano supportati da aziende dalle spalle larghe con valutazione effettuata da un ente di certificazione (ma non è sempre così), per i prodotti non critici basterebbe un'autovalutazione e l'apposizione sulla confezione (se c'è) e nella dichiarazione di conformità della marcatura CE anche per il software. Se il software è scaricato da un sito web, la dichiarazione di conformità deve essere facilmente accessibile ai consumatori.

Qualora lo sviluppatore venga a conoscenza di vulnerabilità deve effettuare entro ventiquattro ore notifica iniziale a un ente nazionale responsabile, seguita dopo settantadue ore da un rapporto più dettagliato. Lo sviluppatore deve pienamente cooperare con le autorità di sorveglianza del mercato e fornire loro il nome e l'indirizzo di ogni operatore economico al quale abbia fornito un prodotto. Tali informazioni devono essere conservate per un periodo di dieci anni.

Produttori

Dopo la progettazione (sicura) i produttori integrano i componenti di terze parti per realizzare un prodotto. Quindi da risorse interne ed esterne raccolgono e indirizzano le vulnerabilità riportate durante il suo ciclo di vita.

I produttori redigono la documentazione tecnica, la manualistica utente, appongono la marcatura CE, compilano la dichiarazione di conformità identificando chiaramente chi sia il produttore e come contattarlo. Nel caso si realizzino aggiornamenti di sicurezza del software, questi devono rimanere disponibili in qualche sito web fino alla fine del ciclo di vita del prodotto o almeno dieci anni, secondo quale sia il periodo più grande.

Soprattutto informano i *Computer Security and Incident Response Team* (CSIRT, vedi dopo) entro ventiquattro ore per una vulnerabilità verificata in un prodotto, fornendo opportuni dettagli e azioni correttive.

Importatori e distributori

La documentazione che manca, in quanto non fornita dal produttore (che potrebbe essere cinese), deve essere fornita dall'importatore, ivi compresa la dichiarazione di conformità. Devono essere fornite informazioni di contatto e istruzioni comprensibili per gli utenti. In assenza di questi requisiti il prodotto non può essere messo in vendita nel mercato europeo.

In caso di vulnerabilità sia il produttore sia la sorveglianza del mercato devono essere informati. Anche importatori e distributori devono conservare la documentazione per dieci anni.

In questa filiera l'importatore o il distributore che apporti *modifiche significative* a un prodotto o lo piazzi nel mercato con il suo nome è considerato produttore ed è sottoposto ai vincoli di quest'ultimo. Le correzioni di sicurezza che non cambino la funzione intesa per un prodotto non sono considerate modifiche significative.

La cybersicurezza in Italia

Il mitico PNRR prevede 67,5 milioni di Euro per l'intervento "1.8 Cybersecurity", avente come soggetto attuatore l'Agenzia per la Cybersicurezza Nazionale (ACN), con specifica attenzione alla Pubblica Amministrazione. Dei fondi stanziati ventotto milioni sono dedicati alla creazione di CSIRT regionali, in modo che ci sia una risposta pronta ed efficace nel punto più vicino a un problema di cybersicurezza.

Altre entità da creare entro la fine del 2024 sono i Laboratori Accreditati di Prova (LAP). Attualmente ne sono previsti ventinove, in collaborazione con il Centro di Valutazione e Certificazione Nazionale. La dotazione prevista per i LAP è di duecentomila Euro.

I LAP saranno ufficialmente deputati a verificare e certificare software e prodotti connessi secondo i livelli minimi di sicurezza previsti dal CRA. Si presume che i LAP certificheranno secondo lo schema EUCC (in fase di finalizzazione entro il 2024), approccio basato sui rischi per le certificazioni con verifiche proporzionate alla classe del prodotto, possibilmente non facendo costare troppo la procedura alle piccole/medie imprese. EUCC è basato sui *Common Criteria* e soppianterà eventuali altri schemi di certificazione nazionali; una certificazione è valida fino a cinque anni.

Le prospettive

L'Italia ha prevalenza sul territorio di piccole imprese e microimprese. Tradizionalmente la creazione di software prevede soluzioni che magari col tempo evolvono, ma inizialmente sono molto più un coacervo di scarsa progettazione e soluzioni connesse a server non molto ben amministrati.

Rispettare il CRA quanto fa aumentare i costi? Un parallelo possibile può essere fatto con l'industria elettromedicale: ci sono stime che la differenza tra rispettare e non rispettare i criteri di progettazione sicura sia circa il 25%. Quindi è presumibile che i prodotti sviluppati secondo CRA per una parte delle aziende possano condurre a una maggiorazione di costo per i consumatori di grosso modo un quarto in confronto ai prezzi attuali.

Rispetto alle soluzioni fai da te, per esempio utilizzando distribuzioni Linux confezionate in casa, il CRA potrebbe spingere verso distribuzioni certificate da fornitori come Microsoft, i quali agevolano l'appoggio sui loro cloud della parte servizi. Ciò non esime dall'amministrazione dei sistemi, ma vedo sempre più possibile in futuro l'esternalizzazione dei rischi ad aziende specializzate ritornando a basarsi su soluzioni prettamente commerciali.

Non è difficile immaginare una certa quantità di tempo di una o più persone in azienda dedicate a seguire (e fare in modo che siano risolti) i problemi. Il CRA prescrive che i

problemi di cyber-sicurezza siano segnalati presto, però ciò avrebbe senso solo per i problemi più seri e sfruttabili da agenti malevoli, non anche per quelli a basso impatto.

Non si prendano le osservazioni sopra come sterile critica. La cybersicurezza è cosa buona e giusta, ma gli approcci in stile big bang non scalano e tendono ad ammazzare gli operatori economici più deboli, che in Italia si basano ancora su una buona dose di artigianato e con piccoli sviluppatori che supportano imprese più o meno grandi. In questo paese ben difficilmente sarebbe potuto nascere e prosperare Google.

Riferimenti

- https://www.cyberresilienceact.eu/
- https://en.wikipedia.org/wiki/Digital_Single_Market
- https://www.linuxfoundation.org/blog/understanding-the-cyber-resilience-act
- https://www.eunews.it/2023/12/01/nuove-norme-ue-sicurezza-informatica/
- https://single-market-economy.ec.europa.eu/single-market/ce-marking_en#:~:text=The%20letters%20'CE'%20appear%20on,health%2C%20and%20environmental%20protection%20requirements.
- https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework
- https://www.acn.gov.it/
- https://www.csirt.gov.it/
- https://www.cybersecitalia.it/csirt-regionali-pubblicata-la-graduatoria-dei-finanziamenti-da-28-milioni-di-euro-del-pnrr/27862/
- https://www.agendadigitale.eu/sicurezza/cyber-come-funzionano-i-laboratori-accreditati-di-prova-lap/
- https://certification.enisa.europa.eu/

Antonio Tringali

Libero professionista specializzato nello sviluppo di software embedded e non: dalla progettazione all'implementazione di sistemi complessi. Esperto nella risoluzione di problemi tecnici e nella creazione di soluzioni personalizzate per le esigenze dei clienti. Appassionato di tecnologia, costantemente aggiornato sulle ultime novità del settore.

Specializzazioni: System architect, progettazione e sviluppo di applicazioni; debug, configurazione e deployment di sistemi; sicurezza.