Position Paper – Cyber Resilience Act

Indice

Sintesi

- DIGITAL SME **accoglie con favore** la proposta di legge di Cyber Resilience Act (CRA) da parte della Commissione Europea, poiché rappresenta un passo necessario per **rafforzare la sicurezza dei dispositivi e dei servizi connessi nel Mercato Unico Europeo**. Tuttavia, sottolinea il problema dei costi aggiuntivi generati dai nuovi requisiti obbligatori per le PMI. Se la possibilità di una certificazione volontaria sulla sicurezza informatica non può essere considerata un'opzione per le PMI, si chiede un certo **grado di proporzionalità e una maggiore guida** per l'attuazione dei nuovi requisiti da parte delle PMI.
- Questo regolamento interagisce con altre importanti normative in materia di sicurezza informatica già in vigore. Copre molti mercati verticali in cui le PMI svolgono un ruolo essenziale. Per questi motivi, DIGITAL SME sottolinea la necessità di **allineamento tra le diverse normative**, al fine di promuovere e agevolare il rispetto delle PMI.
- DIGITAL SME chiede inoltre che siano messe a disposizione delle PMI **adeguate linee guida da parte delle istituzioni dell'UE**, al fine di rimuovere gli ostacoli all'accesso a informazioni chiare sull'interazione tra le diverse normative e su come queste si applicano ai loro prodotti. Occorre fornire ulteriori chiarimenti anche su concetti come "modifica sostanziale" e categorie di prodotti quali "aggiornamenti over-the-air". **DIGITAL SME raccomanda che un supporto pertinente venga offerto alle PMI e armonizzato tra diversi Paesi**. Il supporto adeguato dovrebbe includere finanziamenti, formazione e guide, nonché la raccolta del feedback delle PMI una volta che il CRA sarà in vigore.
- I co-legislatori dovrebbero prendere in considerazione l'istituzione di "sandbox" regolamentari, basati sul modello introdotto nell'Atto sull'Intelligenza Artificiale. **Le PMI possono beneficiare di un ambiente sicuro che consente loro di testare il proprio software e i prodotti di sicurezza informatica prima di entrare sul mercato**. Se attuati, i sandbox regolamentari agevolerebbero il rispetto delle piccole imprese, stimolerebbero l'innovazione e contribuirebbero all'apprendimento regolamentare. Le autorità pubbliche a livello nazionale dovrebbero fornire le condizioni adatte per rendere efficaci i sandbox regolamentari per le PMI. Ciò è necessario poiché le piccole e medie imprese incontrano significativi ostacoli nella creazione di un ambiente di test adeguato e nello sviluppo della capacità di raccolta dati per sfruttare al massimo un sandbox regolamentare.
- DIGITAL SME sostiene l'idea di creare una valutazione standardizzata dei rischi del prodotto. Per semplificare il rispetto delle PMI, **l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) dovrebbe fornire una guida sulla valutazione dei rischi**. Quando si identificano gli standard rilevanti da utilizzare in concomitanza con il Cyber Resilience Act, le PMI dovrebbero essere **attivamente coinvolte come principale parte interessata nel processo decisionale**.
- **Il CRA deve anche tenere conto della sostenibilità**. Dovrebbe essere limitata la capacità dei produttori di apparecchiature originali (OEM) di imporre complessi standard di sicurezza per limitare l'accesso ai loro dispositivi. Questa misura stimolerebbe i mercati post-vendita e garantirebbe il "diritto alla riparazione" per gli utenti. Inoltre, al fine di evitare l'obsolescenza programmata, **si propone che i produttori di prodotti critici forniscano aggiornamenti di sicurezza per l'intero ciclo di vita dei loro prodotti, o per un periodo di cinque anni, a seconda di quale sia più lungo**.

Introduzione

Il 15 settembre 2022, la Commissione europea ha pubblicato la proposta per l'Atto sulla resilienza cibernetica (d'ora in poi CRA), una regolamentazione nell'ambito del quadro normativo europeo sulla sicurezza informatica. Lo scopo del CRA è stabilire i requisiti per la messa in commercio dei prodotti con elementi digitali sul Mercato unico europeo. Inoltre, il regolamento rende i produttori responsabili della sicurezza informatica dei loro prodotti e mira a aumentare la consapevolezza delle problematiche di sicurezza informatica e delle migliori pratiche per gli utenti finali.

La regolamentazione adotta un approccio di sicurezza integrata nel design, in cui i produttori sono obbligati a garantire la sicurezza dei loro prodotti durante l'intero ciclo di vita (dalla pianificazione alla manutenzione), mettendo a disposizione aggiornamenti per almeno cinque anni e segnalando le vulnerabilità sfruttate all'Agenzia dell'Unione europea per la cibersicurezza (ENISA).

La proposta del CRA, insieme ad altre importanti normative europee sulla sicurezza informatica (come la Direttiva NIS2[1], l'Atto sulla sicurezza informatica[2] e l'Atto sulla resilienza operativa digitale[3]), va nella direzione di creare una sfera digitale più sicura per tutti i prodotti e i servizi nel Mercato unico europeo.

Il regolamento offre una distinzione tra diversi tipi di prodotti, in base al loro profilo di rischio: secondo la Commissione europea, il 90% dei prodotti richiederà una valutazione da parte del produttore stesso. I prodotti critici (come software di gestione delle password, firewall, ecc.) saranno definiti **Classe I** e richiederanno l'applicazione di una **norma armonizzata** o **una valutazione da parte di un terzo**. I prodotti altamente critici (come sistemi operativi e firewall industriali) saranno considerati **Classe II** e dovranno necessariamente passare attraverso **una valutazione da parte di un terzo**.

Contesto

Una relazione dell'ENISA sulla sicurezza informatica per le PMI[4] ha evidenziato che **l'80% delle PMI afferma che un problema di sicurezza informatica avrebbe un grave impatto sul loro business**, mentre il 57% dichiara di rischiare di dover chiudere l'attività. Pertanto, dal punto di vista delle PMI europee, **la sicurezza informatica è considerata una preoccupazione seria da affrontare**.

I costi degli attacchi informatici per le PMI possono essere elevati, spesso al di là delle riserve di liquidità disponibili per le PMI stesse. La resilienza e l'adattabilità sono fondamentali per la sopravvivenza e la crescita di qualsiasi attività, indipendentemente dalle dimensioni. Tuttavia, promuovere la sicurezza delle PMI è essenziale per garantire la sicurezza dell'Europa.

Introdurre requisiti di sicurezza informatica per i prodotti con elementi digitali è fondamentale quando si mira a incrementare il livello di garanzia dei prodotti nel Mercato unico europeo. Una valutazione d'impatto condotta dalla Commissione europea[5] ha rilevato che l'introduzione di requisiti orizzontali

[1] https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

[2] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

[4] ENISA Report (2021), Cyber Security for SMEs – Challenges and Recommendation, https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-forsmes

[5] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

di sicurezza informatica comporterà significativi benefici sia per i consumatori che per le imprese, prevenendo la formulazione di regole di sicurezza divergenti nei diversi paesi.

Inoltre, si stima che il CRA ridurrà i costi sostenuti a seguito di incidenti di sicurezza informatica di una cifra compresa tra 180 e 290 miliardi di euro all'anno. La tutela dei diritti fondamentali dei cittadini dell'UE, come la privacy e la protezione dei dati, sarà ulteriormente rafforzata dall'introduzione di requisiti che migliorano la trasparenza e la sicurezza.[6]

Un altro studio dell'ENISA ha rilevato che, sebbene molti prodotti software delle PMI possano offrire ambienti sicuri e stabili per le imprese private, i rischi per la sicurezza venivano spesso riscontrati nelle grandi aziende tecnologiche. Inoltre, molti degli incidenti di sicurezza informatica che hanno causato danni gravi sono stati causati da errori degli utenti a causa di una scarsa comprensione delle problematiche di sicurezza informatica e di una mancanza di attuazione di misure di cyber-igiene.[7]

Pertanto, l'Alleanza europea delle PMI digitali (DIGITAL SME) riconosce la necessità di aumentare la sicurezza informatica in tutta Europa e accoglie con favore gli sforzi per garantire che i prodotti europei siano introdotti sul mercato con un livello più elevato di sicurezza informatica. Un quadro normativo più solido che consenta un mercato dei prodotti connessi più sicuro e resiliente dal punto di vista della cibersicurezza e che aumenti la consapevolezza degli utenti finali dei prodotti è quindi benvenuto.

Tuttavia, DIGITAL SME invita i decisori politici a tenere presente i costi aggiuntivi generati dai nuovi requisiti orizzontali vincolanti, soprattutto per le PMI. Se non c'è spazio per negoziare un possibile schema di certificazione volontaria per la sicurezza informatica delle PMI, sottolinea la necessità di proporzionalità e di orientamenti sufficienti affinché le PMI possano attuare efficacemente le disposizioni previste dal Cyber Resilience Act.

Principali Osservazioni di DIGITAL SME

Armonizzazione dei requisiti del CRA tra i mercati europei

Sulla base dell'attuale quadro normativo europeo in materia di sicurezza informatica, DIGITAL SME sostiene l'armonizzazione dei requisiti per la sicurezza informatica in diversi settori e accoglie quindi il Cyber Resilience Act.

Tuttavia, come per qualsiasi regolamentazione orizzontale, DIGITAL SME è preoccupata per l'impatto del CRA sui prodotti e sui mercati che sono già soggetti a normative sulla sicurezza informatica. Questi mercati rappresentano una parte significativa del Mercato unico europeo: pertanto, DIGITAL SME raccomanda che siano resi disponibili orientamenti sufficienti alle PMI, in modo che le aziende possano comprendere l'interazione tra le diverse normative europee in materia di sicurezza informatica.

Creare risorse per le aziende che consentano loro di comprendere tali leggi senza l'aiuto di esperti esterni ridurrà il costo della conformità. Questo è particolarmente vero per le PMI che spesso affidano l'analisi delle normative applicabili a consulenti esterni.

[6] Commission staff working document, Executive summary of the impact assessment report: https://ec.europa.eu/newsroom/dae/redirection/document/89553.

[7] https://www.enisa.europa.eu/news/enisa-news/phishing-most-common-cyber-incidents-faced-by-smes

Sorveglianza del mercato e sanzioni

Il CRA prevede una sorveglianza del mercato da parte di organismi autorizzati per garantire la validità delle dichiarazioni di conformità. DIGITAL SME ritiene che designare **autorità nazionali di certificazione** per svolgere la sorveglianza del mercato semplificherebbe i processi burocratici per le aziende. Dotarle di risorse sufficienti, materiali di orientamento e piani di sensibilizzazione aumenterà la certezza giuridica e diminuirà gli ostacoli alla conformità.

Per quanto riguarda l'applicazione delle sanzioni, quelle previste dall'articolo 53 della proposta e espresse in termini di importi o percentuali sul fatturato mondiale delle imprese sono molto superiori alle risorse disponibili per la maggior parte delle PMI. Se tali sanzioni fossero applicate alle PMI, metterebbero a rischio la loro sostenibilità, pertanto DIGITAL SME suggerisce che la proposta sia adattata in modo che le sanzioni siano commisurate.

Armonizzazione con le normative esistenti

Per ridurre al minimo l'impatto sulle PMI, DIGITAL SME raccomanda di allineare il CRA con la normativa dell'UE esistente, come il Cybersecurity Act, la Direttiva NIS2, RED, DORA, l'AI act, quando possibile, e di fornire linee guida e supporto finanziario per aiutare le PMI a conformarsi meglio al CRA.

Per evitare di sovraccaricare le PMI, i co-legislatori devono assicurarsi che le nuove regole non si sovrappongano a quelle esistenti. Ad esempio, la Direttiva UE 2019/770 garantisce che agli utenti siano forniti gli aggiornamenti di sicurezza per i prodotti digitali, in particolare il software (Articolo 8 - Requisiti obiettivi di conformità). Inoltre, la Direttiva UE 2019/771 stabilisce la stessa obbligazione legale di fornire aggiornamenti di sicurezza per i beni con elementi digitali (Articolo 7 - Requisiti obiettivi di conformità). Per quanto riguarda la protezione dei dati personali, il Regolamento generale sulla protezione dei dati dell'UE (2016/679) richiede che i dati siano trattati in modo sicuro, incluso il proteggerli da trattamenti non autorizzati o illeciti e da perdite, distruzioni o danni accidentali.

L'introduzione dei requisiti di sicurezza informatica per i prodotti con elementi digitali è fondamentale per garantire il livello di sicurezza dei prodotti nel mercato europeo. Sulla base dell'analisi d'impatto condotta dalla Commissione europea, **l'introduzione di requisiti orizzontali di sicurezza informatica avrà significativi benefici**, specialmente per le imprese, **poiché impedirebbe la formulazione di regole di sicurezza divergenti nei diversi paesi.** Un panorama normativo frammentato sarebbe dannoso per le piccole imprese, in quanto aggiungerebbe oneri amministrativi all'incertezza del mercato: tenendo conto di questo contesto, l'armonizzazione dei requisiti è benvenuta.

Identificazione degli standard

Quando si identificano standard o certificazioni adatti, è necessario considerare l'impatto sulle piccole imprese. Gli standard dovrebbero essere raggiungibili per tutte le aziende, in modo che l'impatto sul mercato rimanga minimo. Pertanto, quando si individuano gli standard pertinenti da utilizzare insieme ai requisiti del CRA, le PMI dovrebbero essere considerate come parte interessata chiave e attivamente coinvolte nel processo decisionale, poiché spesso sono i grandi attori a essere in grado di assorbire i costi associati agli standard/certificazioni. L'autovalutazione e la proporzionalità della valutazione di conformità devono essere rese possibili per le PMI mediante lo sviluppo di standard adattati alle PMI.

Nello stato attuale della proposta, i prodotti critici classificati come Classe I dovranno dimostrare la conformità agli standard armonizzati o essere sottoposti a una valutazione da parte di un terzo. DIGITAL SME suggerisce che le certificazioni/gli standard identificati come adatti per i prodotti Classe I dovrebbero essere:

a. proporzionali ai requisiti di gestione della sicurezza e delle vulnerabilità,
b. in linea con le certificazioni/gli standard utilizzati in altre normative sulla sicurezza informatica che richiedono livelli di sicurezza simili,
c. proporzionati al profilo del mercato.

Per garantire l'adeguatezza degli standard, DIGITAL SME sostiene l'idea che l'accreditamento degli standard venga considerato una misura responsabile a seguito del completamento di un'esercitazione formale di valutazione del rischio. Infine, **è importante che la Commissione europea adotti misure di salvaguardia che garantiscano la rappresentanza reale ed effettiva delle PMI nei comitati di standardizzazione**. In caso contrario, vi è il rischio che le grandi aziende e le organizzazioni di ricerca stabiliscano standard che non sono adatti alle PMI.

Supporto per gli Standard di Cybersecurity e le Iniziative Open Source

Poiché gli standard di cybersecurity e le iniziative open-source svolgono un ruolo essenziale nella promozione di un ambiente digitale sicuro e trasparente, DIGITAL SME incoraggia la Commissione europea a fornire supporto per lo sviluppo e l'adozione di tali standard e iniziative. Ciò può essere realizzato attraverso finanziamenti, assistenza tecnica e la promozione della collaborazione tra le parti interessate.

Inoltre, DIGITAL SME chiede il riconoscimento e l'inclusione delle soluzioni open-source come un contributo prezioso al panorama europeo della cybersecurity. Ciò comporterebbe garantire che il CRA non penalizzi involontariamente i progetti open-source o imponga loro oneri eccessivi. Sostenendo le iniziative open-source e fornendo un campo di gioco equo per tutti i giocatori del mercato, la Commissione europea può favorire l'innovazione e promuovere un ecosistema della cybersecurity diversificato e vibrante.

Misure a sostegno dell'innovazione delle PMI

DIGITAL SME accoglie con favore gli sforzi della Commissione europea nel coinvolgere le PMI e comprendere l'impatto di questa legislazione su di loro. Tuttavia, data la realtà quotidiana della maggior parte delle PMI, che hanno risorse e capacità limitate per effettuare valutazioni d'impatto, è molto probabile che non saranno in grado di valutare l'impatto fino all'entrata in vigore della legislazione.

Pertanto, DIGITAL SME propone che il CRA includa un **adeguato supporto per le PMI** per soddisfare i requisiti che saranno stabiliti. **Questo supporto dovrebbe essere armonizzato tra gli Stati membri in modo che le differenze geografiche non influiscano sulla competitività**. Dovrebbero essere offerte diverse forme di supporto, tra cui finanziamenti, formazione e guide. Questo supporto è essenziale per rimuovere gli ostacoli che impediscono alle PMI di accedere a informazioni chiare sull'interazione tra tutte le normative che riguardano i prodotti che producono e impiegano. Inoltre, DIGITAL SME suggerisce che vengano fornite **linee guida in merito alla dovuta diligenza che le aziende devono eseguire sui fornitori**. Ciò agevolerebbe un approccio coerente alla dovuta diligenza, evitando

potenziali ostacoli per le PMI in termini di comprensione di come possono dimostrare la conformità, poiché diverse aziende utilizzano test o parametri diversi.

Inoltre, per favorire l'innovazione, **i co-legislatori devono prendere in considerazione l'introduzione di sandbox regolamentari**. Sulla base delle misure introdotte nel Regolamento sull'intelligenza artificiale, **le PMI possono beneficiare di un ambiente sandbox che consente loro di testare il loro software e i prodotti di cybersecurity prima di entrare nel mercato**. Si prevede che le sandbox regolamentari agevolino la conformità, stimolino l'innovazione e contribuiscano all'apprendimento normativo (citazione dell'EC). Ad esempio, le PMI potrebbero utilizzare le sandbox regolamentari per comprendere in quale Classe ricade il loro prodotto e quali requisiti devono soddisfare. A tal riguardo, è anche importante che le sandbox diventino obbligatorie per gli Stati membri al fine di evitare un approccio frammentato nel Mercato Unico.

Le sandbox regolamentari consentono di creare ambienti reali per testare nuove tecnologie, prodotti e servizi o approcci innovativi. Tuttavia, la creazione di tali ambienti di test reali è lasciata alle imprese e, mentre le grandi aziende hanno le risorse finanziarie e la capacità di costruire i propri ambienti di test, le PMI non sempre ne dispongono. Di conseguenza, è fondamentale che le autorità pubbliche a livello nazionale permettano la creazione di ambienti di test per le PMI, al fine di rendere efficaci tali sandbox regolamentari e consentire alle PMI di testare la resilienza cibernetica dei loro prodotti e la conformità ai requisiti del CRA. È attraverso la possibilità per le PMI di testare i loro prodotti con elementi digitali in tali ambienti di test che le autorità pubbliche possono favorire la conformità delle PMI alle regole e, di conseguenza, aumentare il livello di resilienza cibernetica europea.

Inoltre, con l'obiettivo di **promuovere l'innovazione delle PMI**, poiché il CRA si estende ad altri strumenti legislativi, compresi il CSA e il RED, **deve essere mantenuto il diritto di accesso ai dati da parte di terzi.** In particolare, i requisiti di cybersecurity, sicurezza o privacy non dovrebbero essere utilizzati dai produttori di dispositivi come scusa per limitare l'accesso dei terzi ai dispositivi.

Sostenere le PMI nella conformità e nell'adattamento

Per agevolare l'integrazione dei requisiti del CRA nelle operazioni delle PMI, è importante istituire meccanismi di supporto adattati alle loro specifiche esigenze. DIGITAL SME incoraggia la Commissione europea e gli Stati membri a fornire risorse, come incentivi finanziari, per aiutare le PMI ad adattarsi al nuovo quadro normativo. Questo supporto può essere fornito attraverso hub informativi dedicati, materiali di formazione online e workshop, nonché attraverso la collaborazione con associazioni industriali e camere di commercio.

Inoltre, promuovere una cultura della cybersecurity all'interno delle PMI sarà fondamentale per l'implementazione efficace del CRA. Ciò può essere realizzato enfatizzando l'importanza della cybersecurity nelle strategie aziendali, favorire la collaborazione tra i dipartimenti IT e aziendali e incoraggiare lo sviluppo di competenze interne in materia di cybersecurity. Abilitando le PMI ad adottare un approccio proattivo alla cybersecurity, il CRA contribuirà alla resilienza complessiva del Mercato Unico europeo.

Potenziamento delle capacità e collaborazione

Per implementare efficacemente il CRA e garantirne il successo, è cruciale potenziare le capacità e promuovere la collaborazione tra tutti gli attori interessati. La Commissione europea, in collaborazione

con l'ENISA e altri organismi di cybersecurity, dovrebbe istituire programmi dedicati a supporto delle PMI nell'affrontare i requisiti regolamentari stabiliti dal CRA. Questi programmi potrebbero includere workshop di formazione, assistenza tecnica e sostegno finanziario per gli aggiornamenti di sicurezza, nonché favorire la collaborazione tra le PMI e gli esperti di cybersecurity. Inoltre, le partnership pubblico-private possono svolgere un ruolo fondamentale nella condivisione di conoscenze, migliori pratiche e innovazioni in materia di cybersecurity. Lavorando insieme, le PMI europee possono migliorare collettivamente la loro resilienza alle minacce cibernetiche, contribuendo a un ecosistema digitale più sicuro nel Mercato Unico europeo.

Consultazioni inclusive degli stakeholder

Per garantire che il CRA affronti efficacemente le esigenze e le preoccupazioni delle PMI, è essenziale coinvolgerle in tutte le fasi del processo legislativo, dalla redazione all'attuazione. DIGITAL SME raccomanda l'istituzione di meccanismi strutturati di consultazione che consentano alle PMI di fornire contributi su aspetti chiave del CRA, come l'individuazione di standard adatti, lo sviluppo di linee guida per la conformità e l'allocazione di sostegno finanziario.

Obblighi lungo le catene di fornitura

Mentre il nuovo quadro normativo era inteso a coprire i prodotti fisici, in particolare quelli con tecnologia consolidata, il CRA copre sia i prodotti hardware che software. DIGITAL SME solleva la preoccupazione che l'approccio seguito dal campo di applicazione del CRA debba essere coerente con quello seguito dal Nuovo Quadro Normativo dell'UE in termini di miglioramento del mercato interno dei beni, rafforzamento della sorveglianza del mercato e potenziamento della qualità delle valutazioni di conformità. Pertanto, è necessario modernizzare l'approccio regolamentare e differenziare tra i requisiti per il software e l'hardware.

Inoltre, i regolatori dovrebbero tenere conto del fatto che le PMI spesso non sono in grado di avere una visione d'insieme e una comprensione completa dei diversi componenti di un prodotto con elementi digitali, che vengono fabbricati in diversi punti lungo la catena di fornitura. Ciò potrebbe significare che se gli obblighi non sono chiaramente definiti e non viene fornito un adeguato supporto e orientamento alle PMI, potrebbero involontariamente esporre se stesse a rischi elevati e sopportare un onere legale e finanziario sproporzionato rispetto ai grandi fornitori nella loro catena del valore.

Inoltre, DIGITAL SME chiede una chiarificazione su come l'open-source sarà trattato nel CRA al fine di garantire la certezza giuridica e un mercato equo per il software in termini di obblighi e responsabilità. La Commissione europea ha previsto una deroga nel *recital* 10 al fine di evitare che tali disposizioni abbiano accidentalmente un impatto sul software open-source. Tuttavia, la formulazione utilizzata rimane troppo generica, pertanto DIGITAL SME ritiene che il testo del CRA **dovrebbe meglio definire la nozione di "attività commerciale".** Poiché molti prodotti considerati critici (classe I e II) possono avere componenti open-source, la proposta dovrebbe chiarire se la responsabilità e la conformità ai requisiti del CRA spettano allo sviluppatore open-source o al produttore del prodotto. Inoltre, il software fornito da un'azienda di software indipendente dall'azienda di hardware potrebbe fornire software commerciale gratuito o a pagamento, senza che ciò sia necessariamente open-source. In alcuni casi, ciò potrebbe includere anche un componente firmware. In sostanza, dovrebbe essere preso

in considerazione il caso in cui un'azienda di software commerciale fornisce un software che può funzionare con un componente hardware, poiché ciò consentirebbe al mercato orizzontale di prosperare, portando numerosi benefici. Infine, DIGITAL SME raccomanda ulteriori chiarimenti riguardo all'impatto dei requisiti del CRA sui servizi software come servizio (SaaS) e sugli aggiornamenti over-the-air (OTA). SaaS è un modello di licenza che consente di accedere al software senza installarlo su una macchina locale, ma di accedervi online come servizio fornito da una piattaforma. Le applicazioni SaaS non rientrano nel campo di applicazione del CRA, ma questa esclusione è incoerente con il NIS2. Tuttavia, poiché molte catene di fornitura per SaaS si trovano al di fuori dell'Europa, la Commissione europea potrebbe considerare l'inclusione di SaaS nel campo di applicazione della legislazione. È necessaria una precisazione sul fatto che l'aggiornamento OTA, ovvero la distribuzione wireless di aggiornamenti di nuovi software, firmware o altri dati ai dispositivi mobili, rientri o meno nel campo di applicazione del regolamento, il che dovrebbe essere chiarito.

Adattarsi alle esigenze specifiche dell'industria

Per affrontare meglio le sfide uniche affrontate dai diversi settori, DIGITAL SME raccomanda che il CRA tenga in considerazione le specifiche caratteristiche di ciascun settore, come il ritmo dello sviluppo tecnologico e il tipo di rischi coinvolti. Questo approccio personalizzato contribuirebbe a garantire che i requisiti stabiliti nel CRA siano pertinenti e proporzionati per le PMI che operano in settori diversi.
A tal fine, la Commissione europea dovrebbe lavorare a stretto contatto con associazioni di settore e gruppi di esperti per acquisire una comprensione completa delle esigenze e delle preoccupazioni specifiche di ciascun settore. Tali consultazioni non solo fornirebbero preziose informazioni, ma favorirebbero anche la cooperazione tra settore pubblico e settore privato nella ricerca di un ecosistema digitale più sicuro e resiliente.

Definizione del ciclo di vita e sostenibilità

Le imprese di tutte le dimensioni dovrebbero integrare considerazioni di sostenibilità nelle proprie operazioni e produrre prodotti digitali che durino più a lungo. Le associazioni dei consumatori denunciano da decenni che i fornitori di sistemi operativi o hardware essenziali spesso rifiutano di fornire gli aggiornamenti necessari, rendendo i dispositivi elettronici non più sicuri o addirittura obsoleti (fonte originale nel Regno Unito menzionata qui). Qui entra in gioco il diritto alla riparazione e il diritto all'aggiornamento nel contesto del CRA, poiché garantire gli standard più elevati di sicurezza informatica richiede di consentire ai fornitori di assistenza e manutenzione post-vendita l'accesso in modalità "scrittura" ai dati e al dispositivo.

Pertanto, è di primaria importanza limitare la capacità dei produttori di apparecchiature originali (OEM) di imporre complessi standard di sicurezza per limitare l'accesso ai loro dispositivi. Solo così il mercato dell'assistenza post-vendita rimarrà competitivo e aperto alla maggior parte delle aziende europee ICT, ovvero le PMI. Pertanto, per evitare l'obsolescenza programmata e garantire il "diritto alla riparazione" per gli utenti, si propone che i produttori di prodotti critici forniscono aggiornamenti di sicurezza per l'intero ciclo di vita dei loro prodotti, o per un periodo di cinque anni, a seconda di quale sia più lungo.

Inoltre, è necessaria una chiara definizione del requisito di fornire supporto per il ciclo di vita dei prodotti. Se un'azienda interrompe un prodotto, non è chiaro se sia ancora tenuta a fornire supporto e aggiornamenti di sicurezza se il prodotto è ancora in uso o accessibile. Ad esempio, non è ancora completamente chiaro se l'azienda dovrebbe fornire patch di sicurezza se un'applicazione è stata dismessa o sostituita da una versione più recente. Allo stesso modo, è necessario chiarire le aspettative delle aziende che dichiarano fallimento e i loro obblighi di assistenza.

Chiarire le aspettative per le imprese cessate e fallite

Per garantire la certezza del diritto e stabilire aspettative chiare per le aziende che rischiano la cessazione dell'attività o il fallimento, DIGITAL SME raccomanda che il CRA includa disposizioni specifiche sugli obblighi di tali aziende. Ciò potrebbe comportare la definizione dell'entità della loro responsabilità in termini di fornitura di supporto e aggiornamenti di sicurezza per i prodotti dismessi, nonché delle conseguenze della mancata conformità.

Chiarendo le aspettative delle aziende in queste situazioni, il CRA può garantire che gli utenti finali continuino a ricevere il supporto e gli aggiornamenti di sicurezza necessari, fornendo al contempo la certezza del diritto alle aziende che si trovano ad affrontare circostanze difficili.

Approccio basato sul rischio

DIGITAL SME crede fermamente che l'approccio basato sul rischio adottato nella proposta CRA sia quello giusto per identificare quali prodotti e software richiedano una maggiore sicurezza. Attualmente, la normativa impone a ogni produttore di implementare misure di sicurezza specifiche nel proprio software, senza considerare la necessità per il prodotto specifico e il caso d'uso.

DIGITAL SME sostiene un approccio in cui gli operatori che identificano una vulnerabilità nelle loro valutazioni del rischio adottino misure per mitigare i rischi per gli utenti finali. L'autovalutazione e la proporzionalità delle procedure di valutazione della conformità dovrebbero essere facilitate per le PMI attraverso lo sviluppo di standard adattati alle loro esigenze.

Per supportare le PMI nella conduzione delle valutazioni del rischio, DIGITAL SME suggerisce che la Commissione europea e l'ENISA collaborino per sviluppare linee guida, risorse e migliori pratiche semplificate in linea con i requisiti del CRA. Queste risorse dovrebbero essere facilmente accessibili e specificamente progettate per le PMI, fornendo istruzioni chiare e concise senza richiedere competenze esterne. Ciò aiuterebbe a ridurre l'onere sulle PMI e garantirebbe un approccio coerente alle valutazioni del rischio nell'intero mercato unico europeo.

Inoltre, DIGITAL SME chiede maggiore chiarezza sui requisiti di valutazione del rischio nella proposta. Il CRA impone ai produttori di valutare i rischi per la cibersicurezza associati ai prodotti con elementi digitali prima di metterli sul mercato (Art. 10, 2). Tuttavia, la proposta manca di definizioni chiare dei metodi di valutazione del rischio da utilizzare o se saranno considerati equivalenti quelli comuni (ISO, NIST, OCTAVE, COSO, AS/NZS, ecc.). DIGITAL SME raccomanda che la Commissione europea e l'ENISA forniscono un elenco di metodologie e quadri riconosciuti per la valutazione del rischio da utilizzare come riferimento per le PMI.

DIGITAL SME sostiene anche la necessità di fornire passaggi più chiari alle PMI da seguire durante la conduzione delle valutazioni del rischio, che potrebbero essere affrontati attraverso una guida alla valutazione del rischio dell'ENISA. Un'area che dovrebbe essere considerata nella valutazione del

rischio è il mercato dei servizi post-vendita e di manutenzione. In molti settori, questo rappresenta una parte significativa del mercato e coinvolge una grande proporzione di PMI.

DIGITAL SME ritiene che le categorie di fornitori di servizi post-vendita e contratti di manutenzione per i prodotti debbano essere ulteriormente chiarite all'interno del CRA. Dovrebbero essere inclusi criteri chiari per determinare la categoria di rischio di questi fornitori di servizi al fine di garantire che siano soggetti a adeguate norme e requisiti di sicurezza informatica in base alle loro attività e rischi specifici. Inoltre, il CRA dovrebbe fornire linee guida sul processo di due diligence per questi fornitori di servizi al fine di garantire un approccio coerente sul mercato.

La frequenza delle valutazioni del rischio dovrebbe essere anche chiarita nel CRA, insieme a informazioni esplicite sulla portata, tempistica e trigger per la riesame. Ciò contribuirebbe a ridurre le discrepanze tra gli oneri imposti ai produttori da diversi Stati membri e prevenire eventuali svantaggi competitivi derivanti da requisiti divergenti. I processi per valutare i rischi per la cibersicurezza associati ai prodotti con elementi digitali sono dettagliati nell'Articolo 10 e richiedono chiarimenti riguardo alla loro frequenza. Stabilire tempistica e metodi per tutte le aziende per effettuare valutazione del rischio ridurrà il rischio di discrepanze tra gli oneri imposti ai produttori da diversi Stati membri, mettendo di conseguenza le aziende soggette a impegni più elevati in una posizione di svantaggio competitivo e commerciale. Le stesse considerazioni si applicano agli articoli 41, 42, 43 e 44 del regolamento, che manca di un sistema centralizzato che stabilisca metodi e tempistiche armonizzati.

Infine, il CRA dovrebbe chiarire se le valutazioni del rischio dovrebbero concentrarsi sull'applicazione o sull'implementazione di un prodotto, nonché su eventuali modifiche alla categoria di rischio del prodotto in base alla sua distribuzione e uso. L'ambiente in cui viene distribuito un prodotto e il suo successivo utilizzo possono spostare un prodotto da una categoria all'altra, e il livello di conformità pertinente dovrebbe essere chiarito. Per affrontare eventuali discrepanze negli obblighi tra gli Stati membri, DIGITAL SME propone un sistema centralizzato per metodi e tempistiche armonizzati per le valutazioni del rischio e processi correlati, gestito dalla Commissione europea o dall'ENISA con il contributo degli attori del settore.

Concluding Remarks

In conclusione, DIGITAL SME accoglie con favore il duplice obiettivo della CRA: da un lato, aumentare il livello di sicurezza informatica dei prodotti connessi e gli obblighi dei produttori; dall'altro, sensibilizzare sulle migliori pratiche e incoraggiare gli utenti a segnalare eventuali minacce di sicurezza informatica sui loro prodotti. Ciò comporta il coinvolgimento delle PMI, degli attori del settore e delle autorità regolatorie durante l'intero processo, al fine di garantire che la regolamentazione rimanga efficace, pertinente e adattabile al panorama della sicurezza informatica in continua evoluzione.

DIGITAL SME apprezza l'ambito orizzontale dei requisiti, elemento chiave per potenziare la sicurezza informatica lungo tutta la catena di fornitura dei prodotti con elementi digitali. Tuttavia, la regolamentazione non fornisce un sufficiente supporto alle PMI per valutare l'interazione tra le diverse normative in materia di sicurezza informatica, né per navigare tra le incongruenze che probabilmente si verificheranno tra gli Stati membri. Pertanto, le istituzioni europee dovrebbero fornire finanziamenti adeguati, formazione e guide, nonché raccogliere regolarmente i feedback delle PMI una volta che la

CRA sarà applicata. Il punto di partenza potrebbe essere una guida alla valutazione del rischio redatta da ENISA per agevolare la conformità delle PMI.

Inoltre, DIGITAL SME incoraggia le istituzioni europee a considerare lo sviluppo di un solido quadro di certificazione in materia di sicurezza informatica, in collaborazione con gli attori del settore e gli esperti di sicurezza informatica, al fine di garantire che le PMI possano dimostrare la loro conformità alla CRA in modo standardizzato e riconoscibile. Ciò non solo rafforzerebbe la posizione complessiva della sicurezza informatica del Mercato Unico Europeo, ma aumenterebbe anche la fiducia tra le imprese e i consumatori.

Un'altra azione che potrebbe favorire la conformità e stimolare l'innovazione, soprattutto dal punto di vista delle PMI, sarebbe l'introduzione di aree di sperimentazione regolamentare, in cui le aziende possono testare il proprio software e i prodotti di sicurezza informatica prima di entrare sul mercato e comprendere a quale classe appartiene il loro prodotto.

DIGITAL SME raccomanda inoltre l'istituzione di un meccanismo di feedback continuo per le PMI, al fine di condividere le loro esperienze, sfide e suggerimenti in merito alla conformità alla CRA. Questo ciclo di feedback consentirebbe alla Commissione europea e ad altre autorità competenti di individuare aree di miglioramento e aggiornare le linee guida, il supporto e i requisiti normativi, se necessario.

Infine, al fine di mantenere gli standard più elevati di sicurezza informatica e stimolare i mercati di manutenzione e post-vendita (in cui le PMI sono molto presenti), dovrebbe essere presa in considerazione un'azione coordinata per evitare l'obsolescenza programmata e garantire il "diritto alla riparazione" per gli utenti nella regolamentazione. Pertanto, i produttori di prodotti critici dovrebbero fornire aggiornamenti di sicurezza per l'intero ciclo di vita dei loro prodotti, o per un periodo di cinque anni, a seconda di quale sia più lungo.

In generale, è di cruciale importanza che le PMI siano coinvolte in tutte le fasi di sviluppo e attuazione della CRA, per assicurarsi che le esigenze della maggioranza delle aziende europee del settore delle tecnologie dell'informazione e delle comunicazioni siano considerate in tutti i requisiti. DIGITAL SME ritiene che il successo della CRA nel raggiungere i suoi obiettivi dipenda largamente dal coinvolgimento attivo e dal supporto delle PMI in tutte le fasi del suo sviluppo e attuazione. Lavorando insieme, le PMI, gli attori del settore e le autorità regolatorie possono costruire un ecosistema digitale più resiliente, sicuro e innovativo che beneficia tutte le parti coinvolte.

Per ulteriori informazioni su questo documento di posizione, si prega di contattare:
contact.italy@digitalsme.eu.