Gastbeitrag Cyber Resilience Act

Ein neues Puzzlestück für Europas Cybersicherheit

Der Europäische Rat hat kürzlich den Cyber Resilience Act verabschiedet. Dies wird Europas Cyberlandschaft nachhaltig verändern. Unternehmen müssen Sicherheitsstandards grundlegend neu denken.

Frankfurt, 15. November 2024, 12:24 Uhr — Susanne Werry

Die EU setzt neue Standards für digitale Produkte.
Foto: Picture alliance / CHROMORANGE | Michael Bihlmayer

Am 10. Oktober 2024 hat der Europäische Rat den Cyber Resilience Act (CRA) verabschiedet – ein entscheidender Schritt, der Europas Cyberlandschaft nachhaltig verändern wird. Dieser in drei Jahren Anwendung findende Rechtsakt setzt neue Standards und stärkt die Cyber-Resilienz in einer Zeit, in der Unternehmen und kritische Infrastrukturen zunehmend Ziel von Cyberangriffen werden.

Der CRA ist ein wichtiger Baustein in der umfassenden Cyberstrategie der Europäischen Union, die darauf abzielt, Europas digitale Souveränität zu stärken und ein hohes Maß an Cybersicherheit für alle Bürger und Unternehmen zu gewährleisten. Als Ergänzung zu bestehenden Regelungen wie der NIS2-Richtlinie und dem Digital Operational Resilience Act (DORA) erweitert der CRA den Schutz nun auf alle digitalen Produkte und fordert Unternehmen dazu auf, Sicherheitspraktiken grundlegend neu zu denken. Durch die Einbindung des CRA in die europäische Sicherheitsarchitektur wird ein umfassender Schutzrahmen geschaffen, der ein widerstandsfähiges digitales Umfeld in ganz Europa unterstützt.

Über Lebenszyklus hinweg

Mit dem CRA führt die EU erstmals einen durchgreifenden Sicherheitsstandard für digitale Produkte ein, der von der Produktion über den gesamten Lebenszyklus des Produkts gilt. Der Anwendungsbereich reicht von Smart Home Geräten wie intelligente Waschmaschinen oder Kühlschränke über industrielle Steuerungssysteme zu digitalen Finanzanwendungen - umfasst sind nämlich sowohl Hardware- als auch Softwareprodukte. Der CRA verlangt von Herstellern, digitale Sicherheit als grundlegendes Merkmal zu integrieren – ein Prinzip, das oft als „Security by Design“ bezeichnet wird. Hersteller sind verpflichtet, potenzielle Schwachstellen zu identifizieren, abzusichern und durch regelmäßige Sicherheitsupdates langfristig für eine kontinuierliche Produktpflege zu sorgen. Durch diese Regelungen wird sichergestellt, dass digitale Produkte nicht nur sicher entwickelt, sondern auch während ihrer Nutzung kontinuierlich vor neuen Bedrohungen geschützt werden. Dies macht den CRA zu einem Grundpfeiler in Europas Cybersicherheitsstrategie, der weit über die bisherigen regulatorischen Anforderungen hinausgeht und die Standards für digitale Produkte auf ein neues Niveau hebt.

Erweiterte CE-Kennzeichnung und gestufte Zertifizierungsverfahren

Eine wesentliche Neuerung des Cyber Resilience Act (CRA) ist die Erweiterung der CE-Kennzeichnungspflicht um Cybersicherheitsanforderungen für digitale Produkte. Während die CE-Kennzeichnung bisher hauptsächlich Sicherheitsstandards wie elektrische Sicherheit und Umweltverträglichkeit abdeckte, wird sie durch den CRA um den Aspekt der Cybersicherheit ergänzt. Digitale Produkte dürfen die CE-Kennzeichnung nur tragen, wenn sie nachweislich den Sicherheitsstandards des CRA entsprechen und Maßnahmen zur Schwachstellenbeseitigung und kontinuierlichen Wartung implementiert sind. Je nach Kritikalität des Produkts sieht der CRA zudem gestufte Zertifizierungsverfahren vor: Produkte mit hohem Risiko für

Cybersicherheitsvorfälle, wie solche in kritischen Infrastrukturen, müssen durch eine Drittpartei überprüft und zertifiziert werden, während niedrigere Risikoklassen durch die Hersteller selbst zertifiziert werden können. Für Unternehmen bedeutet dies erhöhte Anforderungen, die auch Auswirkungen auf die Entwicklungszeit neuer Produkte haben wird.

Erhöhte Meldepflichten

Eine weitere Herausforderung sind die neuen Meldepflichten unter dem CRA, der NIS2-Richtlinie und DORA. Diese legen kurze Fristen für die Meldung von Cybervorfällen fest, um Behörden die Möglichkeit zu geben, bei Bedrohungen schnell zu reagieren und die Verbreitung von Schäden einzudämmen. Während die DSGVO für Datenpannen eine Meldung innerhalb von 72 Stunden vorsieht, erfordern die neuen Regelungen für Cybersicherheit noch striktere Fristen: Je nach Gesetz muss die Erstmeldung innerhalb von 4 bis 24 Stunden erfolgen. So müssen Hersteller unter dem CRA, Sicherheitsvorfälle an die Europäische Agentur für Cybersicherheit (ENISA) melden, während Finanzinstitute unter DORA innerhalb von 4 Stunden nach Feststellung eines Vorfalls die zuständigen Behörden informieren müssen.

Strenge Strafen

Die neuen Regelungen unter dem CRA gehen, wie die NIS2-Richtlinie und DORA mit erheblichen Strafandrohungen einher, um sicherzustellen, dass Unternehmen die Cybersicherheitsstandards konsequent umsetzen. Der CRA sieht für Verstöße gegen die grundlegenden Anforderungen an die Cybersicherheit Geldbußen von bis zu 15 Mill. Euro oder 2,5% des weltweiten Jahresumsatzes eines Unternehmens vor, je nachdem, welcher Betrag höher ist. Verstöße gegen weniger schwerwiegende Auflagen können ebenfalls hohe Bußgelder nach sich ziehen, die bis zu 10 Mill. Euro oder 2% des globalen Umsatzes betragen. Auch die NIS2-Richtlinie und DORA enthalten ähnliche, strenge Sanktionsmechanismen: Bei kritischen Infrastrukturen und im Finanzsektor drohen ebenfalls Bußgelder in Millionenhöhe.

Geschäftsführung im Fokus

Die neuen Vorschriften bringen eine klare Erwartungshaltung an die Unternehmensführung mit sich: Cybersicherheit wird nicht mehr nur als technische Notwendigkeit, sondern als strategische Managementverantwortung betrachtet. Führungskräfte stehen persönlich in der Pflicht, die Einhaltung der Sicherheitsstandards zu überwachen und sicherzustellen, dass alle Risiken in der digitalen Infrastruktur adäquat bewertet und gemindert werden.

Bei Verstößen können sie nun direkt haftbar gemacht werden, was den Druck auf das Management erhöht, Cybersicherheitsrisiken aktiv anzugehen. Diese Anforderungen gehen über das bloße Implementieren technischer Maßnahmen hinaus – sie verlangen eine strategische Integration von Cybersicherheit in alle Geschäftsprozesse und Entscheidungsstrukturen.

Unternehmen müssen demnach dokumentieren, dass sie Cybersicherheitsmaßnahmen kontinuierlich evaluieren, aktualisieren und an neue Bedrohungen anpassen. Diese integrierte Sicherheitsstrategie ist nicht nur zur Risikominimierung sinnvoll, sondern wirkt sich auch positiv auf die Wahrnehmung durch Investoren und Kunden aus. Eine starke Cyber-Resilienz wird zunehmend als Qualitätsmerkmal eines Unternehmens angesehen, das Vertrauen aufbaut und Wettbewerbsvorteile schafft. Durch die proaktive Implementierung einer umfassenden Sicherheitsstrategie kann das Unternehmen nicht nur teure Strafen und Reputationsschäden vermeiden, sondern sich auch als verlässlicher Partner positionieren, was langfristig den Unternehmenswert und die Marktposition stärkt.

Cyber-Versicherungen im Wandel

Die gestiegenen rechtlichen Anforderungen haben auch den Markt für Cyber-Versicherungen beeinflusst. Viele Versicherer bieten heute Policen an, die Unternehmen vor den finanziellen Folgen von Cybervorfällen schützen sollen. Der Leistungsumfang dieser Versicherungen ist vielfältig: Einige decken lediglich präventive Maßnahmen und die Kosten für Sicherheitsvorkehrungen ab, während andere sogar Ransomware-Zahlungen einschließen.

Bevor Versicherungen abgeschlossen werden, prüfen die Anbieter jedoch die Cybersicherheitsstandards des Unternehmens. Sie setzen voraus, dass wichtige Schutzmaßnahmen wie Datenverschlüsselung und Zugangskontrollen etabliert sind und regelmäßig überprüft werden.

Es ist wahrscheinlich, dass Versicherer künftig auch die Einhaltung des Cyber Resilience Act und anderer gesetzlicher Anforderungen als Kriterium für Versicherungsverträge heranziehen.

Unternehmen, die sich an die Vorgaben halten, könnten als weniger risikobehaftet gelten und von günstigeren Konditionen profitieren.

Risikoabwägung

Die Anforderungen an Cybersicherheit und -Resilienz haben sich in den letzten Jahren erheblich verschärft. Für Unternehmen ist die Einhaltung der neuen Vorschriften nicht nur eine Frage der Compliance, sondern auch eine Gelegenheit, Vertrauen zu schaffen – sowohl bei Kunden als auch bei Partnern.

Eine starke Cyber-Resilienz-Strategie kann helfen, das finanzielle Risiko zu senken und das Ansehen des Unternehmens zu schützen. Angesichts der drohenden Sanktionen und des erhöhten Haftungsrisikos sollten Unternehmen die neuen rechtlichen Vorgaben zur Cyber-Resilienz ernst nehmen und gezielt Maßnahmen zur Umsetzung einleiten.

Susanne Werry ist Counsel bei Skadden, Arps, Slate, Meagher & Flom.