ONEKEY.COM

DEN EU-CYBER RESILIENCE ACT VERSTEHEN

Produkt Cybersicherheit und Compliance erreichen

ONEKEY

WHITEPAPER

ZUSAMMENFASSUNG

Den EU Cyber Resilience Act verstehen und Produktsicherheits-Compliance erreichen

Lesezeit: Ungefähre Lesezeit 15 Minuten.

Dieses Whitepaper richtet sich an Produktverantwortliche, Produkt-Sicherheitsmanager und Compliance-Experten von Herstellern, Händlern und Importeuren vernetzter Geräte, die auf Märkten innerhalb der Europäischen Union tätig sind.

Um die verpflichtenden Anforderungen der Europäischen Union gemäß dem kommenden EU Cyber Resilience Act (CRA) im Bereich Produktsicherheit und Vorfallmeldung zu erfüllen, müssen alle Hersteller sowie deren Importeure und Händler, die ihre Produkte innerhalb der EU vermarkten, die Cyber-Resilienz ihrer Produkte erheblich stärken.

Diese Bemühungen müssen die gesamte Produktlieferkette umfassen, um eine bessere Transparenz der verwendeten Softwarekomponenten sicherzustellen, das Gesamtsicherheitsniveau der Produkte zu erhalten und zu verhindern, dass Produkte mit bekannten Schwachstellen ausgeliefert werden. Zusätzlich sind Hersteller sowie deren Importeure und Händler verpflichtet, die Europäische Agentur für Cybersicherheit (ENISA) innerhalb von 24 Stunden zu informieren, sobald ihnen eine neue Produktschwachstelle bekannt wird.

Als Folge dieser neuen Regulierung und zur Reduzierung des manuellen Aufwands für Hersteller, Importeure und Händler wird die Erstellung von Software-Stücklisten (Software Bill of Materials – SBOMs) sowie die Sicherheitsanalyse der Software-Lieferkette entsprechend den Anforderungen des CRA umfassend automatisiert werden müssen.

Dieses Whitepaper fasst die neuen verpflichtenden Anforderungen des CRA zusammen, beschreibt, wie sich daraus ergebende Risiken reduziert werden können, und erläutert, wie der Produktsicherheitsprozess – vom Design über die Softwareentwicklung bis zum Ende des Produktlebenszyklus – gestaltet sein muss, um diese regulatorischen Anforderungen und entsprechende Sicherheitsmaßnahmen wirksam umzusetzen.

HINTERGRUND

Neuer EU Cyber Resilience Act (CRA) zielt auf mehr Sicherheit und Transparenz ab

Am 15. September 2022 veröffentlichte die Agentur der Europäischen Union für Cybersicherheit (ENISA) den Entwurf des neuen Cyber Resilience Act (CRA), der vom Europäischen Parlament in der gesamten Europäischen Union umgesetzt werden soll. Betroffen sind Hersteller, Importeure und Händler von Produkten mit digitalen Elementen. Der CRA zielt darauf ab, das Sicherheitsniveau aller Produkte mit digitalen Elementen innerhalb der EU zu erhöhen, indem Hersteller verpflichtet werden, einen Rahmen für Cybersicherheit umzusetzen, diesen aktiv zu pflegen und während des gesamten Produktlebenszyklus einzuhalten. Darüber hinaus soll eine erhöhte Transparenz bezüglich der Sicherheitseigenschaften es Verbrauchern und Unternehmen ermöglichen, sicherheitsbewusste Entscheidungen zu treffen.

Begrenzte Handlungszeit für Produkte mit digitalen Elementen

Diese Initiative der ENISA erfolgt angesichts zunehmender Schäden durch Cyberkriminalität, die im Jahr 2021 weltweit Kosten von mehr als 5,5 Billionen Euro verursachten. Viele dieser Cyberangriffe entstehen aufgrund von Schwachstellen in Produkten mit digitalen Elementen und werden durch mangelnde Transparenz seitens der Hersteller bezüglich relevanter Sicherheitseigenschaften verschärft. Obwohl der CRA ein breites Spektrum an „Produkten mit digitalen Elementen“ umfasst – von Betriebssystemen über Desktop- und mobile Anwendungen bis hin zu Hardware-Geräten und Netzwerkausrüstung – konzentriert sich dieses Whitepaper gezielt auf vernetzte Geräte und richtet sich insbesondere an Hersteller, Händler und Importeure solcher Geräte.

Es wird erwartet, dass der neue CRA Anfang 2024 durch die Europäische Kommission als Richtlinie verabschiedet wird, ohne dass eine Zustimmung durch das Europäische Parlament erforderlich ist. Selbst unter Berücksichtigung einer Übergangsfrist bleibt nur wenig Zeit, um notwendige Meldepflichten zu etablieren und die übrigen wesentlichen Anforderungen zu erfüllen. Aufgrund der typischerweise mehrjährigen Design- und Entwicklungszyklen ist es notwendig, dass Hersteller bereits jetzt handeln. Lediglich Geräte, die unter die Verordnung (EU) 2018/1139 (Zivilluftfahrt), Verordnung (EU) 2017/745 (Medizinprodukte), Verordnung (EU) 2017/746 (In-vitro-Diagnostika) fallen oder gemäß der Verordnung (EU) 2019/2144 (Typgenehmigung von Kraftfahrzeugen und deren Anhängern sowie Systemen, Komponenten und separaten technischen Einheiten hierfür) zertifiziert sind, sind vom CRA ausgenommen. Angesichts der durchschnittlich mehrjährigen Zeitspanne zwischen Design und Produktion vernetzter Geräte bleibt den Herstellern nur wenig Zeit, um erforderliche Sicherheitsänderungen umzusetzen und die neuen Anforderungen zu erfüllen.

ÜBERBLICK ÜBER DIE CRA ANFORDERUNGEN

Während der CRA erweiterte Verpflichtungen zur Einhaltung der grundlegenden Sicherheitsanforderungen vorsieht – beispielsweise Konformitätsbewertungen durch Dritte für kritische Produkte (sowohl für Klasse I als auch Klasse II) –, bleiben die zugrunde liegenden Anforderungen für alle Produkte gleich. Die neuen Anforderungen des CRA lassen sich grundsätzlich in drei Kategorien einteilen: Governance, Produktentwicklung und Berichtswesen.

Anforderungen an die Produktentwicklung

1. Anforderungen, die das Produkt selbst betreffen, definieren ein Mindestmaß an Sicherheitseigenschaften, um das Produkt vor Cyberangriffen zu schützen und sein Sicherheitsniveau zu erhöhen.

Anforderungen an die Unternehmensführung

2. Anforderungen, die sich auf die Prozesse des Softwareentwicklungszyklus (SDLC) des Herstellers auswirken, wie Konzept und Design, Entwicklung, Produktion und Markteinführung sowie Service und Support, sollen die Sicherheit erhöhen, sichere Produkte zu entwickeln und ihr Sicherheitsniveau auf wiederholbare, transparente und nachhaltige Weise aufrechtzuerhalten, die mit angemessenen Sicherheitskontrollen messbar ist.

Anforderungen an die Berichterstattung

3. Melde- und Informationspflichten gegenüber den Überwachungsbehörden und Nutzern von Produkten über ausgenutzte Sicherheitslücken und Vorfälle, die das Produkt betreffen, stellen sicher, dass Maßnahmen zur Schadensbegrenzung zeitnah umgesetzt werden können. Ziel ist es, den Zeitrahmen, in dem sowohl Endnutzer als auch Anbieter kritischer Infrastrukturen durch kritische Sicherheitslücken Cyberbedrohungen ausgesetzt sind, zu minimieren, um das allgemeine Sicherheitsniveau der europäischen digitalen Infrastruktur zu erhöhen,

indem bereitgestellte Korrekturen oder Zwischenmaßnahmen ergriffen werden, um die Auswirkungen der Sicherheitslücke zu verringern.

CRA-Anforderungen decken Sicherheitslücken in der Lieferkette ab

Die folgende Abbildung gibt einen Überblick über die wesentlichen Anforderungen und deren Bezug zu den jeweiligen Phasen im Lebenszyklus der Produktsicherheit. Ihr Ziel ist es, die Ansätze „Defense-in-Depth“ und „Secure-by-Design“ zu unterstützen und sicherzustellen, dass Produkte den erhöhten Sicherheitsanforderungen des europäischen Marktes gerecht werden. Ein zentrales Erfordernis des CRA ist dabei das Management von Risiken in der Lieferkette.

RISIKEN IN DER LIEFERKETTE

In modernen Anwendungen bestehen 80–90 % der Codebasis aus Software-Komponenten von Drittanbietern – sowohl Open Source als auch proprietär. Dazu gehören beispielsweise Krypto-Bibliotheken zur Sicherung sensibler Informationen während der Übertragung oder Closed-Source-SDKs zur Steuerung von Hardware-Modulen externer Anbieter, die in vernetzten Geräten integriert sind. Da ein Großteil des Codes nicht direkt vom Hersteller kontrolliert wird, stammt ein erheblicher Anteil des Risikos und der Angriffsfläche vernetzter Geräte von diesen Drittanbieter-Softwarekomponenten. Zu diesen Risiken gehören unter anderem:

Risiken durch Drittanbieter bleiben oft unerkannt

Mangelnde Transparenz: Direkte Abhängigkeiten und die Einbindung von Drittanbieter-Komponenten sind zwar oft bekannt, doch endet die Lieferkette nur selten an dieser Stelle. Drittanbieter-Komponenten basieren häufig auf weiteren Abhängigkeiten, die wiederum selbst Abhängigkeiten besitzen. Eine vollständige Transparenz der gesamten Lieferkette wird zusätzlich erschwert, wenn der Quellcode der betroffenen Komponenten nicht verfügbar ist – ein häufiger Umstand für Importeure oder Händler vernetzter Geräte.

Software von Drittanbietern kann das allgemeine Sicherheitsniveau senken

Niedrigere Sicherheitsstandards: Die Entwicklungspraktiken sowie das Sicherheitsniveau von Anbietern von Open-Source-Komponenten und kommerziellen Standard-Softwarekomponenten (COTS) von Drittanbietern werden selten überprüft. Dies

führt zu Szenarien, in denen ein erheblicher Teil des Endprodukts möglicherweise nicht den Sicherheitsanforderungen des Herstellers entspricht, was den Sicherheitsstandard des gesamten Produkts senkt.

Software von Drittanbietern kann ebenfalls anfällig sein

Anfällige Komponenten: Jeder Dritthersteller arbeitet in unterschiedlichen Intervallen daran, neue Versionen für seine Softwarekomponenten bereitzustellen. Darüber hinaus würde die Aktualisierung einer solchen Abhängigkeit in einem angeschlossenen Gerät strenge Tests erfordern, um unbeabsichtigte Nebenwirkungen und die Beeinträchtigung vorhandener Funktionen zu vermeiden — insbesondere, wenn das Gerät Sicherheitsanforderungen erfüllt. Das hat zur Folge, dass Softwarekomponenten von Drittanbietern, die einmal im Lieferumfang enthalten waren, selten aktualisiert werden, selbst wenn neuere Versionen Sicherheitsupdates enthielten.

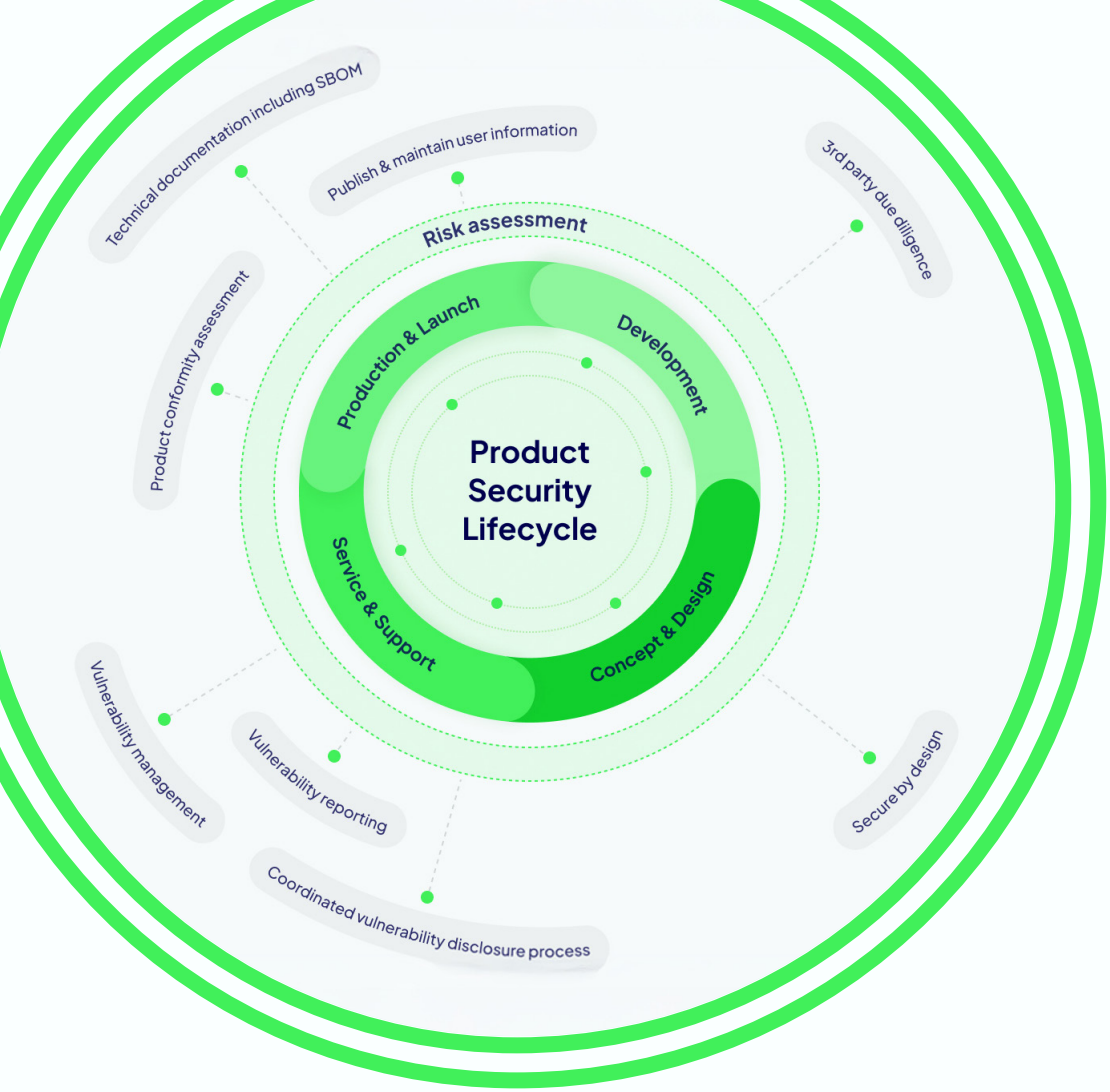
Angreifer konzentrieren sich zunehmend auf die Lieferkette

Angriffe auf die Lieferkette: Lieferketten sind in den Fokus von Cyberkriminellen gerückt, da sie als lukrativer Einstiegspunkt in die Infrastruktur ihrer Ziele gelten. Bedrohungsakteure haben begonnen, aktiv Hintertüren in Open-Source-Komponenten einzubauen und Malware über Open-Source-Repositorys zu verbreiten.

GEGENMASSNAHMEN GEGEN LIEFERKETTENRISIKEN

Anforderungen der Lieferkette an die Produktsicherheit

Schwachstellen in der Lieferkette spielen eine zentrale Rolle im CRA. Aufgrund der Schwere solcher Risiken sind umfassende Gegenmaßnahmen gerechtfertigt. Der CRA erkennt diese Herausforderungen ausdrücklich an und adressiert Lieferkettenrisiken aus verschiedenen Perspektiven.



PRODUKTSICHERHEIT

Aus Sicht der Produktsicherheit ist der CRA ziemlich direkt, wenn es um Abschnitt 1 der grundlegenden Sicherheitsanforderungen geht, die Risiken in der Lieferkette betreffen: Sie verlangt vom Hersteller, sicherzustellen, dass das Produkt zum Zeitpunkt der Veröffentlichung frei von bekannten ausnutzbaren Sicherheitslücken ist und dass dieses Sicherheitsniveau während des gesamten Produktlebenszyklus aufrechterhalten wird. Die naheliegende Strategie zur Erfüllung dieser Anforderung besteht darin, sich ausschließlich auf die neuesten Versionen von Drittanbieter-Abhängigkeiten zu verlassen, die frei von bekannten Sicherheitslücken sind (Common Vulnerabilities and Exposures/CVE4).

Um zu vermeiden, von bekannten Sicherheitslücken betroffen zu werden, bei denen es nicht möglich ist, einfach die neueste Softwareversion zu verwenden, müssen die Auswirkungen bekannter Sicherheitslücken bewertet und entweder als gemindert oder nicht zutreffend eingestuft werden, oder — falls sie tatsächlich ausnutzbar sind — auf individueller Ebene gemindert werden, z. B. durch Rückportierung von Sicherheitspatches. In der Regel ist die Folgenabschätzung, um festzustellen, ob bekannte Sicherheitslücken behoben werden müssen, ein manueller Prozess, bei dem die CVE, die zugehörigen Patches und die Ressourcen in

Kombination mit der Zielumgebung oder dem Quellcode analysiert werden.

Um den Aufwand manueller Folgenabschätzungen für jede bekannte Sicherheitslücke zu reduzieren, kann eine binäre Software-Kompositionsanalyse (SCA), die in den Kontext der Konfiguration und Einrichtung des Zielprodukts gestellt wird, diesen Prozess enorm unterstützen, da bekannte Sicherheitslücken mit geringer Wahrscheinlichkeit, dass sie die Konfiguration des Zielprodukts beeinträchtigen, automatisch ermittelt und verworfen werden. Auf diese Weise kann der Schwerpunkt auf die Behebung der verbleibenden bekannten ausnutzbaren Sicherheitslücken gelegt werden. Binary SCA optimiert manuelle Folgenabschätzungen, indem Schwachstellen mit geringem Risiko automatisch ignoriert werden und der Schwerpunkt im Verhältnis zum Design des Zielprodukts auf ausnutzbare Schwachstellen gelegt wird.

GOVERNANCE

Der CRA definiert zahlreiche Anforderungen, die auch Fragen im Zusammenhang mit der Lieferkette abdecken:

- Softwarekomponenten müssen identifiziert und eine Softwareliste (SBOM) muss verwaltet werden.
- Sicherheitslücken müssen unverzüglich behoben werden und Sicherheitsupdates müssen an die betroffenen Benutzer verteilt werden.
- Produkte müssen regelmäßig getestet und auf ihr Sicherheitsniveau überprüft werden.
- Für alle Komponenten von Drittanbietern ist die gebotene Sorgfalt erforderlich. Es muss sichergestellt werden, dass solche Komponenten das allgemeine Sicherheitsniveau des Produkts nicht gefährden.

Wie kann die Lieferketten-Steuerung eingehalten werden?

Jetzt ist die Einführung von Tools zur Analyse der Softwarekomposition von entscheidender Bedeutung. Die Analyse der Softwarezusammensetzung (SCA) beschreibt den automatisierten Prozess zur Bestimmung der Softwarekomponenten (Open Source und COTS), die in einem Endprodukt enthalten sind. Das Ergebnis einer SCA ist eine SBOM, die entweder aus Quellcode, Metadaten wie Paketmanagerinformationen oder aus einer Binärdarstellung abgeleitet wird. Da in der Regel nicht garantiert werden kann, dass Quellcode für alle Softwarekomponenten verfügbar ist, die von Drittanbietern entlang der Lieferkette bereitgestellt werden, kann SCA sich oft nur auf kompilierte binäre Repräsentationen einer Softwarekomponente verlassen.

Durch die Einbeziehung binärer SCA in den Prozess zur Identifizierung und Verwaltung von Sicherheitsrisiken im Zusammenhang mit Komponenten von Drittanbietern, die im Produkt verwendet werden, kann die Generierung des Inventars von Softwarekomponenten von Drittanbietern automatisiert werden. Dies wird erreicht, indem der binäre Firmware-Build dekonstruiert wird, um sicherzustellen, dass alle Softwarekomponenten, die letztendlich den Benutzern der Produkte zur Verfügung gestellt werden, untersucht werden können.

Die SBOM umfasst identifizierte Softwarekomponenten, zugehörige Versionen sowie das enthaltene Patch-Level. Dieselbe Folgenabschätzung bekannter Sicherheitslücken, die für die erste Version des Produkts durchgeführt wurde, muss für jede neu veröffentlichte Sicherheitslücke, die einen Teil des Produkts betrifft, wiederholt werden. Basierend auf der SBOM können bekannte Sicherheitslücken identifiziert werden, die jeden Teil des Produkts betreffen. Dieser Vorgang muss regelmäßig wiederholt werden, um einen aktuellen Überblick über die Sicherheitslücken zu erhalten, die das Produkt betreffen.

SBOMs müssen den Binärcode aus der Lieferkette enthalten

Ein automatisiertes „Security-Quality-Gate“ mit binärer Software Composition Analysis (SCA) als Teil des Build-Prozesses unterstützt dabei sicherzustellen, dass ein Produkt oder Produkt-Update erst freigegeben wird, wenn alle sicherheitsrelevanten Probleme behoben wurden. Durch das automatische Anhalten von Release-Pipelines, falls ausnutzbare Schwachstellen identifiziert werden, lässt sich gewährleisten, dass Sicherheitsprobleme aus Drittanbieter-Software möglichst frühzeitig erkannt und adressiert werden.

Die ONEKEY Product Cybersecurity & Compliance Plattform (OCP) ermöglicht es Herstellern (Händlern / Importeuren), die Produktsicherheit automatisiert und in mehreren Schritten über den gesamten Produktlebenszyklus hinweg sicherzustellen:

Die einzigartige und proprietäre Binary-Extraction-Technologie von ONEKEY ermöglicht eine tiefere und präzisere Analyse binärer Firmware-Images, ohne dass der Quellcode erforderlich ist. ONEKEY erstellt automatisiert eine detaillierte SBOM, inklusive aller Software-Abhängigkeiten auf sämtlichen Ebenen der Firmware.

Im nächsten Schritt verwendet ONEKEY, basierend auf künstlicher Intelligenz und maschinellem Lernen, Natural Language Processing (NLP), um öffentlich bekannte Schwachstellen zu identifizieren, die diese Software-Version betreffen.

Darüber hinaus analysiert der KI/ML-basierte Ansatz von ONEKEY automatisch die Voraussetzungen für die Ausnutzbarkeit dieser Schwachstellen.

Mittels einer integrierten und automatisierten Risikoanalyse prüft ONEKEY, ob die Voraussetzungen für eine Ausnutzung der Schwachstellen beim Zielgerät erfüllt sind, und filtert somit nicht relevante Sicherheitslücken aus. Diese einzigartige Methode verkürzt Reaktionszeiten erheblich, reduziert den manuellen Aufwand bei der Bewertung von Risiken und ermöglicht es Entwicklungs- und Product Security Incident Response Teams (PSIRT), effizienter und schneller zu handeln.

Die ONEKEY Product Cybersecurity & Compliance Plattform (OCP) bietet automatisierte Sicherheitsprozesse und Kontrollmaßnahmen, die gemäß dem EU Cyber Resilience Act erforderlich sind:

ONEKEY kann eine Software Bill of Materials (SBOM) direkt aus einem binären Firmware-Image generieren. Die erstellte SBOM kann sowohl in maschinenlesbaren (z. B. CycloneDX, SPDX) als auch in menschenlesbaren Formaten (CSV, EXCEL) exportiert werden, um sie anderen Systemen, Endanwendern und Regulierungsbehörden zur Verfügung zu stellen.

Das Firmware-Monitoring von ONEKEY überprüft das Zielprodukt täglich auf neue Zero-Day-Schwachstellen sowie bekannte Sicherheitslücken und führt automatische, auf KI/ML basierende Risikoanalysen für alle identifizierten Schwachstellen durch. Dies ermöglicht Herstellern, auf neu auftretende Schwachstellen schnellstmöglich zu reagieren und Sicherheits-Patches bereitzustellen und zu verteilen.

Analyse und Monitoring für eine automatisierte Sicherheitsprüfung von Drittanbieter-Komponenten – integrieren Sie ONEKEY einfach als automatisiertes Quality-Gate für beliebige Drittanbieter-Komponenten oder Produkte.

CRA MELDEPFLICHTEN

Anforderungen an das Berichtswesen innerhalb der Lieferkette

Ein zentrales Ziel des CRA besteht darin, den Austausch und die Zusammenarbeit zwischen unterschiedlichen Akteuren in digitalen Ökosystemen zu fördern. Daher müssen sowohl Nutzer als auch Marktüberwachungsbehörden mit relevanten sicherheitsbezogenen Informationen zu Produkten versorgt und CRA-spezifische Dokumentationen bereitgestellt werden.

- Hersteller sind verpflichtet, während der gesamten Lebensdauer eines Produkts Informationen über ausgenutzte Schwachstellen mit den Marktüberwachungsbehörden und der ENISA zu teilen. Dies schließt auch Schwachstellen ein, die Drittanbieter-Komponenten betreffen, die im Produkt enthalten sind.
- Nutzer und Behörden müssen über mögliche Gegenmaßnahmen sowie über die Verfügbarkeit von Sicherheitspatches informiert werden.
- Darüber hinaus müssen Hersteller von Drittanbieter-Komponenten und Maintainer von Open-Source-Software benachrichtigt werden, wenn eine Schwachstelle Anwendungen betrifft, die unter ihrer Verantwortung stehen.

Auswirkungen auf Händler und Importeure

Diese Anforderungen unterstreichen, dass Sicherheit nicht nur eine einmalige Anstrengung ist. Es ist ein Prozess und erfordert eine kontinuierliche Wartung. Regelmäßige Überprüfung der SBOM einer Firmware auf neu veröffentlichte Sicherheitslücken. Gehen Sie proaktiv auf diese Anforderung ein und unterstützen Sie die Überprüfung und Bewertung sicherheitsrelevanter Probleme, indem die Anwendbarkeit validiert und die Auswirkungen auf das Produkt bestimmt werden.

Händlern und Importeuren fehlen häufig die technischen Fähigkeiten und die notwendigen Einblicke in die betroffenen Produkte, um die Einhaltung des CRA zuverlässig feststellen zu können. Um sich nicht ausschließlich auf die Selbsteinschätzung des Herstellers zu verlassen, können Händler und Importeure dieselben Techniken anwenden, um die SBOM aus der Binärdatei zu generieren Firmware und um alle bekannten ausnutzbaren Sicherheitslücken aufzudecken.

Unterstützung für CRA Einhaltung?

Strenge Sicherheits- und Berichtspraktiken, wie sie von dem CRA gefordert werden, erhöhen den Aufwand für die bestehenden Produktentwicklungszyklen. Dennoch sind sie eine Notwendigkeit, um den heutigen erhöhten Sicherheitsanforderungen und der ständig wachsenden Bedrohungslandschaft gerecht zu werden. Und natürlich, um die regulatorischen Anforderungen der ENISA zu erfüllen und Strafen von bis zu 15 Millionen Euro oder 2,5% des weltweiten Jahresumsatzes zu vermeiden.

Es stehen in der ONEKEY Plattform verschiedene Tools zur Verfügung, um die Dokumentation, Prozesse und die Automatisierung der Cybersicherheit zu verbessern. Um die Einführung des CRA zu erleichtern, steht innerhalb der Produktsicherheitsplattform von ONEKEY ein automatisierter Support zur Verfügung, der das Schwachstellenmanagement oder die Bewertung der Lieferkette unterstützt und bei der Erfüllung der Berichts- und Dokumentationsanforderungen hilft. Darüber hinaus bietet ONEKEY fachkundige Beratung und Beratungsressourcen, um Hersteller, Importeure und Händler bei der Einhaltung der CRA zu unterstützen

AUTOMATISIERUNG UND UNTERSTÜTZUNG BEI DER ERFÜLLUNG UND EINHALTUNG DER CRA SICHERHEITS-ANFORDERUNGEN

Beratung und Automatisierung durch die Sicherheitsexperten von ONEKEY

ONEKEY reduziert nicht nur den manuellen Aufwand, indem die von der Ratingagentur geforderten Prozesse um automatische Kontrollen erweitert werden, sondern unterstützt auch Hersteller, Importeure und Händler von Produkten mit digitalen Elementen bei der Einführung der von der Ratingagentur geforderten Prozesse mit Lückenanalysen und Implementierungsunterstützung.

Die automatisierte Firmware-Sicherheitsanalyseplattform von ONEKEY kann Verstöße gegen grundlegende Cybersicherheitsanforderungen, wie sie in Anhang I, Abschnitt 1 der CRA definiert sind, automatisch erkennen und melden. Die technischen Experten und Sicherheitsforscher von ONEKEY erweitern die automatisierten Funktionen von ONEKEY und stehen auch zur Verfügung, um Lücken bei der Einhaltung der CRA durch ein Produkt zu identifizieren und Penetrationstests und Schwachstellenanalysen an betroffenen angeschlossenen Geräten durchzuführen.

SCHLÜSSELERKENNTIS

Hersteller müssen jetzt handeln, um die Produktkonformität sicherzustellen:

Angesichts der zunehmenden Angriffe auf vernetzte Geräte hat die EU grundlegende Anforderungen zur Erhöhung des Sicherheitsniveaus verbundener Geräte definiert und einen Rahmen geschaffen, um die Zusammenarbeit und den Informationsaustausch über neue Sicherheitslücken und neu auftretende Bedrohungen zu fördern.

- Der CRA umfasst die regulatorischen Anforderungen zur Herstellung solcher cyberresistenter vernetzter Geräte, insbesondere aus Sicht des Supply-Chain-Risikos.
- Um die erhöhten Sicherheits- und Compliance-Anforderungen zu erfüllen und Lieferkettenrisiken zu begegnen, ist die Implementierung automatisierter Sicherheits- und Compliance-Kontrollen, d. h. eine ganzheitliche binäre Softwareanalyse, erforderlich. Die automatische anfängliche Softwareanalyse und die kontinuierliche Überwachung werden den Aufwand für die Implementierung und Aufrechterhaltung der CRA-Compliance erheblich reduzieren.

Interessieren Sie sich für weitere Diskussionen mit unseren Sicherheitsexperten darüber, wie Sie die Einhaltung der Sicherheitsvorschriften für Ihre CRA-Produkte erreichen und aufrechterhalten können? Bitte kontaktieren Sie unsere Sicherheitsexperten unter: experts@onekey.com

ONEKEY
onekey.com
+49 211 1587 41 04
info@onekey.com

SecurITy made in Germany

V20240900IDE