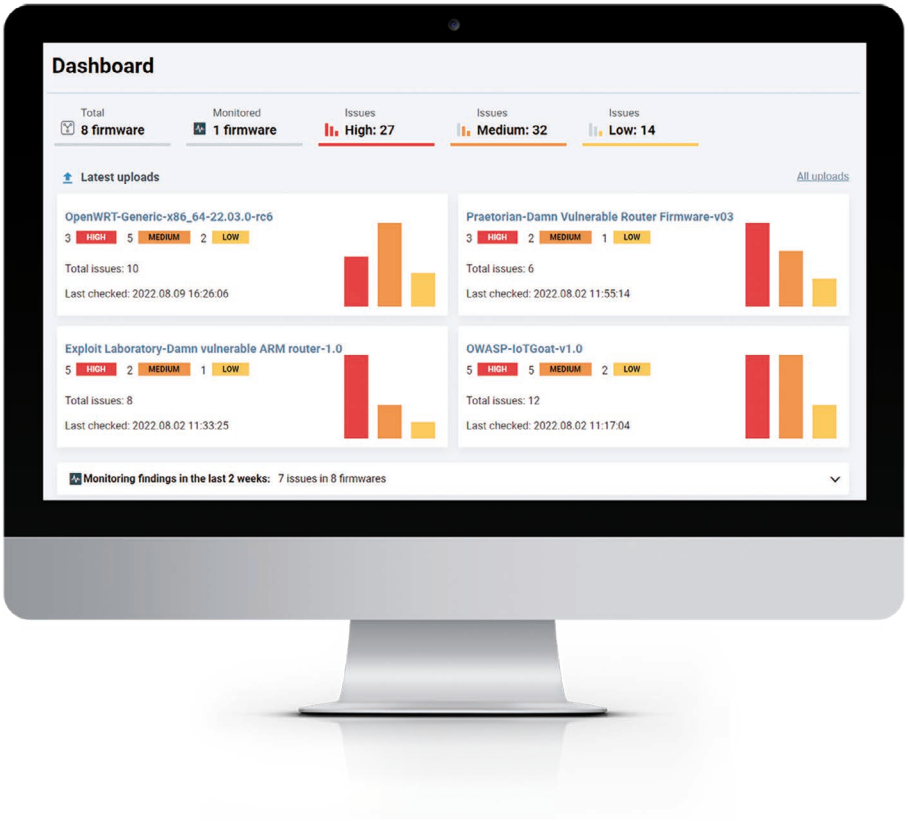
Compliance als Wettbewerbsvorteil sehen

Hersteller kämpfen um Zukunftssicherheit



Die kommenden europäischen Compliance-Richtlinien stellen Hersteller von smarten Produkten und IT-Geräten vor große Herausforderungen. Während dieser Bereich bisher wenig reguliert wurde, werden nun eher überfällige und verbindliche gesetzliche Regeln für die sichere Software- und Produktentwicklung eingeführt. Diese erfassen auch Vorstände und Geschäftsführer durch die erweiterte Haftung, wie sie beispielsweise der EU Cyber Resilience Act vorsieht. Die künftige Compliance-Gesetzgebung wird massive Auswirkungen auf die internen Strukturen in Unternehmen haben – wer frühzeitig in Produkt-Cyber-Resilience investiert, hat einen Wettbewerbsvorteil.

Regelwerke

Übergreifende Regelwerke sind in der Industrie grundsätzlich kein neues Thema: Bereits 1985 verabschiedete der Rat der damaligen Europäischen Gemeinschaft (EG) eine damals nicht unumstrittene Konformitätskennzeichnung für Produkte. Heute gehört das CE-Zeichen zu den etablierten Standards, und die Intention, den Handel durch eindeutige Kennzeichnungen auch über Grenzen hinweg zu erleichtern, hat sich voll erfüllt. Richtlinien, Normen und Gesetze dienen vor allem der Harmonisierung in einer globalisierten Welt. Das bekannte CE-Zeichen gilt in jedem Land der Europäischen Union als „technischer Reisepass“ eines Produktes, den der Hersteller anbringt, wenn die Voraussetzungen dafür erfüllt sind. Werden die Produkte nach den europäischen Richtlinien hergestellt, können die Behörden in jedem Land davon ausgehen, dass die grundlegenden gesetzlichen Anforderungen an Gesundheits-, Umwelt- und Verbraucherschutz sowie an die Sicherheit erfüllt sind. Daher ist es heute selbstverständlich, dass ein Produkt ohne CE-Kennzeichnung nicht in Verkehr gebracht werden darf, und ebenso schnell hat sich im Zuge der Einführung herausgestellt, dass Hersteller mit CE-Kennzeichnung einen Wettbewerbsvorteil haben.

Auch Software benötigt zukünftig eine Kennzeichnung

Anfang des Jahres 2024 wird eine dem CE-Kennzeichen vergleichbare Regulierung in Kraft treten – mit einem wesentlichen Unterschied. Neben der Hardware wird dann auch der unsichtbare Teil aller netzwerkfähigen Geräte und Anlagen zentraler Bestandteil der Zertifizierung. Die einzelnen Komponenten eines jeden Gerätes mit eingebautem Mikrochip – Router, Drucker, industrielle Steuerungen – enthalten Komponenten unterschiedlichster Hersteller. Nahezu jeder dieser Bausteine bringt seine eigene Software mit. Nur selten ist der Hersteller eines Gerätes auch der Entwickler aller enthaltenen Komponenten und der für den Betrieb des Gerätes notwendigen Software. Oftmals besteht die Software – bei interner, von außen nicht sichtbarer Software auch Firmware genannt – aus Open-Source-Komponenten. Solche Softwareprodukte sind in der Regel lizenzfrei und sogar im Quellcode verfügbar. Damit geht ein immenses Risiko einher, denn jede Software kann eigene und häufig unerkannte Cyber-Schwachstellen enthalten. Der EU Cyber Resilience Act wird dies in Zukunft ändern. Hersteller müssen künftig vollständig offenlegen, welche Komponenten verbaut sind und welche Soft- und Firmware mitgeliefert wird. Das neue Gesetz geht sogar noch einen Schritt weiter und fordert eine Analyse der verbauten Komponenten auf Schwachstellen, die von Hackern ausgenutzt werden können oder generell als Risiko für das Gerät gelten. Denn auch bei Geräten mit Netzwerkfähigkeit, die seit Jahren oder Jahrzehnten gebaut oder im Einsatz sind, werden immer wieder gravierende Sicherheitslücken bis hin zu kritischen Zero-Day-Schwachstellen entdeckt.

Autor:
Jan Wendenburg
CEO
ONEKEY
https://onekey.com/

Kritische Produkte

Besonders kritisch: Anlagen, die in der Produktion eingesetzt werden, oder smarte Devices und Netzwerkinfrastruktur, die in der Wirtschaft, Industrie oder Gesundheitswesen und Verwaltung genutzt werden – vielfach auch in kritischen Infrastrukturen. Für Hacker sind versteckte digitale Schwachstellen tief in der Firmware verborgen ein beliebtes Einfallstor in die IT- und Produktionsinfrastruktur. Jedes Gerät in einem Netzwerk ist eine potenzielle Schwachstelle, über die auch ein krimineller Vollzugriff auf Server, Daten, Anlagen und Produktion erfolgen kann.

Software Bill of Materials ermöglicht mehr Transparenz

Hersteller müssen künftig angeben, welche Softwarekomponenten in ihren Geräten und Anlagen verbaut sind. Das Stichwort heißt Product Cybersecurity Compliance, eine Software Bill of Materials (SBOM) ist der elementare Baustein, um den Produkten mit digitalen Elementen eine Identität zu geben. Mit Hilfe einer Firmware-Analyseplattform kann beispielsweise bis ins Detail entschlüsselt werden, welche Soft- und Firmware-Komponenten in einem Gerät verbaut sind und welches Gefährdungspotenzial davon ausgehen kann. Eine SBOM kann vollautomatisch als „Software-Stückliste“ für alle enthaltenen Softwarekomponenten erstellt werden. Dabei wird sowohl eigene Software als auch Software von Drittanbietern identifiziert, die bisher ungeprüft in einem Endprodukt eingesetzt werden konnte. Die Sicherheitsprüfung sowie eine SBOM werden in wenigen Monaten zur Pflicht - und Hersteller und Inverkehrbringer haften künftig auch für zugekaufte und integrierte Komponenten Dritter – auch für Software aus Open Source-Quellen.

Geänderte Haftung

Die Haftung kann zukünftig nicht mehr auf den Drittanbieter abgewälzt werden, der Hersteller des Endgerätes trägt die volle Verantwortung für die damit verbundenen Risiken und Sicherheitslücken. Daher ist bei der Verwendung von Softwarekomponenten aus dem Open-Source-Bereich besonders darauf zu achten, dass sich im OSS-Repository leicht Schadcode verstecken kann oder eine Komponente mit eigener Firmware eigene Malware, Bugs oder andere Schwachstellen enthält, die dem Entwickler des Endproduktes nicht bekannt sind.

SBOM ist hilfreich

Die Software Bill of Materials ist daher für Hersteller und Betreiber von smarten Produkten äußerst hilfreich: Für den Hersteller ist diese Stückliste ein wichtiger Baustein zur Selbstkontrolle und als Nachweis gegenüber Dritten. Dazu zählen auch die Käufer der Produkte, die ebenfalls eine Cybersecurity-Compliance einhalten müssen. Für den Betreiber einer Infrastruktur

© AdobeStock/Maksim Kabakou

ist eine SBOM eine wichtige Grundlage für die Überprüfung der Cybersecurity und Compliance von zugekauften Geräten. Durch standardisierte, maschinenlesbare SBOM-Austauschformate wie CycloneDX, SPDX und andere können alle wesentlichen Softwarekomponenten in Produkten, Systemen und ganzen Anlagen schnell inventarisiert werden. Dies ermöglicht automatisierte ganzheitliche Compliance-Bewertungen und unterstützt externe Audits.

Product Cybersecurity für mehr Technical Compliance

Mehr denn je zuvor wird zudem die Verantwortung auch in die Hände von Geschäftsführungen, Vorständen und Aufsichtsräten gelegt. Bei Verletzungen, die Auswirkungen auf die IT-Sicherheit und Integrität eines Unternehmens haben, drohen den Unternehmen, aber auch den Führungskräften empfindliche Geldbußen. Die persönliche Haftung von Entscheidungsträgern und Verantwortlichen nimmt durch die neue Gesetzgebung deutlich zu. Product Cybersecurity und die dadurch erzielbare Technical Compliance betreffen durch die neuen Regulierungen also unmittelbar die Chefetage. Rechtzeitige Vorkehrungen verschaffen Unternehmen und den Entscheidern daher mehr Sicherheit vor Cyberangriffen, aber auch vor möglichen Forderungen aufgrund von gesetzlichen Haftungsvorgaben. In der Regel wird die hauseigene Entwicklungsabteilung mit dieser Herausforderung kaum fertig – Unternehmen müssen heute zusätzlich auf neue, automatisierte Technologien und externe Experten setzen, um das Risiko von Sicherheitslücken in den eigenen Produkten zu senken und damit den Markt vor Cyberattacken zu schützen.

Effektiver Schutz

Eine effektive Absicherung und ein modernes Schutzkonzept beginnen mit der Analyse des Bestandes, und der Kenntnis darüber, welche Risiken bereits vorhanden sind. So lässt sich das Bedrohungspotenzial überblicken, und der unternehmenseigenen Entwicklung sowie dem Produkt-Cybersecurity-Incident-Response-Team (PSIRT) wird wirksame Unterstützung zuteil. Dies ist die Grundlage für ein nachhaltiges Technical Compliance Management. Die CE-Kennzeichnung hat bereits vor vielen Jahren die Sicherheit für physische Produkte als Selbstverständlichkeit etabliert, der EU Cyber Resilience Act denkt das CE-Siegel weiter und überträgt es auf die unsichtbaren digitalen Inhalte. Digitale Produkte mit eigenen Chipsätzen und Zugriff auf Netzwerke werden so zukünftig geschützt und ebenso nach einem einheitlichen Standard zertifiziert. Die Regulierung mag zunächst unbequem erscheinen, erhöht in einer zunehmend digitalisierten und vernetzten Welt jedoch die Betriebssicherheit und lässt eine gesamte Branche entlang der Wertschöpfungskette profitieren – und bringt die gesamte europäische Cyber Resilience auf ein neues Niveau, das mehr Zukunftssicherheit verspricht. ◄