Deutschland

Genetec Deutschland GmbH
De-Saint-Exupéry-Straße 10
60549 Frankfurt am Main
Deutschland

T +49 695 06028 255

Pressemitteilung

EU Cyber Resilience Act legt die Messlatte für Anbieter von physischen Sicherheitslösungen höher

Fünf Tipps von Genetec, wie Sicherheitsverantwortliche Produktsicherheit, Transparenz und Support während des gesamten Lebenszyklus ihrer Sicherheitstechnologien bewerten können.

FRANKFURT, 10. September 2026 – Am 11. September tritt die Meldepflicht des EU Cyber Resilience Acts (CRA) in Kraft. Vor diesem Hintergrund hat Genetec Inc. („Genetec"), der weltweit führende Anbieter von Software für die physische Sicherheit in Unternehmen, einen Leitfaden für Sicherheitsverantwortliche veröffentlicht. Er soll ihnen dabei helfen zu beurteilen, wie Technologieanbieter vernetzte Produkte entwickeln, warten und unterstützen.

Der CRA legt Cybersicherheitsanforderungen für Produkte mit digitalen Elementen fest, die in der Europäischen Union verkauft werden. Gefordert werden dabei eine sichere Produktentwicklung, Schwachstellenmanagement, Transparenz in der Cybersicherheit und kontinuierlicher Produktsupport über den gesamten Produktlebenszyklus hinweg. Zwar gilt die Gesetzgebung in erster Linie für Hersteller, dennoch wird die Verordnung auch Auswirkungen auf Unternehmen haben, die vernetzte Geräte vertreiben, installieren, beschaffen und betreiben.

„Der Cyber Resilience Act bekräftigt viele Prinzipien des ‚Secure-by-Designs' und des Lebenszyklusmanagements, für die sich Genetec seit Jahren einsetzt", sagt Mathieu Chevalier, Principal Security Architect bei Genetec Inc. „Die CRA-Vorschriften erhöhen die Anforderungen an Produktsicherheit und Transparenz und bieten so Käufern eine klare Grundlage für die Bewertung von Technologieanbietern und optimieren langfristig ihre Cyberresilienz."

Um die neuen Anforderungen an die Cybersicherheit und den Umgang mit Sicherheitslücken gemäß des CRA zu erfüllen, setzen Unternehmen zunehmend auf die Unterstützung von

Technologieanbietern. Um die CRA-Kompetenz potenzieller Technologieanbieter besser beurteilen zu können, empfiehlt Genetec Unternehmen, ihnen fünf zentrale Fragen zu stellen:

Wie lange erhält das Produkt Sicherheitsupdates und Support?

Der CRA unterstreicht die Bedeutung der Produktsicherheit über den gesamten Lebenszyklus hinweg. Sicherheitsverantwortliche sollten deshalb wissen, wie lange der Anbieter Updates bereitstellt, wie er mit Sicherheitslücken umgeht und welchen Support er bietet, wenn Produkte das Ende ihrer Lebensdauer erreichen. Der CRA verpflichtet Hersteller, Sicherheitsupdates während des definierten Supportzeitraums bereitzustellen, der grundsätzlich mindestens fünf Jahre oder die erwartete Nutzungsdauer des Produkts umfasst, sofern diese kürzer ist. Deshalb ist der langfristige Support ein wichtiger Aspekt bei der Bewertung von Produkten.

Wurde Cybersicherheit von Anfang an in das Produkt integriert?

Die Prinzipien „Secured by Design“ und „Secure by Default“ stehen im Mittelpunkt des CRA. Die Sicherheitsverantwortlichen sollen sich deshalb von den Anbietern erläutern lassen, wie Cybersicherheit in das Produktdesign, die Entwicklung, das Testen und den gesamten Lebenszyklus des Produkts integriert ist.

Wie identifiziert, kommuniziert und behebt der Anbieter Sicherheitslücken?

Keine Software ist immun gegen Sicherheitslücken. Die Art und Weise, wie ein Anbieter darauf reagiert, ist ein wichtiger Indikator für sein Engagement im Bereich Cybersicherheit.

Voraussetzung ist ein etabliertes Schwachstellenmanagement. Dazu gehören regelmäßige Sicherheitstests, ein koordiniertes Verfahren zur Offenlegung von Sicherheitslücken, deren zügige und risikobasierte Behebung, die sichere Bereitstellung von Updates und klare Informationen zu behobenen Schwachstellen.

Ist der Anbieter transparent in Bezug auf seine eigenen Cybersicherheitspraktiken?

Cybersicherheit ist eine gemeinsame Verantwortung. Verantwortungsbewusste Anbieter erläutern, wie sie ihre Produkte entwickeln, testen und warten, und geben Kunden und Systemintegratoren klare Leitlinien für eine sichere Bereitstellung. Es ist deshalb wichtig zu hinterfragen, ob der Anbieter die Produktsicherheit regelmäßig

überprüft, Schwachstellen und Sicherheitsupdates kommuniziert und Anleitungen zur Systemhärtung bereitstellt.

Wie unterstützt der Anbieter die langfristige Cyberresilienz?
Die Cybersicherheit eines Produkts endet nicht mit der Installation. Deshalb ist es entscheidend, mit vertrauenswürdigen Technologiepartnern zusammenzuarbeiten. Unternehmen sollten prüfen, wie der Anbieter den Supportzeitraum des Produkts festlegt und kommuniziert, mit Sicherheitslücken umgeht, Sicherheitsupdates bereitstellt, den sicheren Betrieb unterstützt und das Ende der Lebensdauer des Produkts organisiert. Und: mit welchen Nachweisen belegt der Anbieter, dass das Produkt während seines gesamten Lebenszyklus die geltenden Cybersicherheitsanforderungen erfüllt?

„Unternehmen, die am besten für den Umgang mit zukünftigen Cyberbedrohungen gerüstet sind, betrachten Cybersicherheit als eine kontinuierliche Partnerschaft und nicht als eine einmalige Beschaffungsentscheidung“, ordnet Chevalier ein. „Der CRA trägt dazu bei, diesen Ansatz zu stärken, indem er Anforderungen hinsichtlich Transparenz, diszipliniertem Schwachstellenmanagement und langfristigem Produktsupport festlegt – davon profitieren Hersteller, Systemintegratoren und Unternehmen, die auf vernetzte physische Sicherheitslösungen angewiesen sind.“

Seit mehr als 25 Jahren setzt Genetec auf Maßnahmen zur cybersicheren Entwicklung seiner physischen Sicherheitstechnologien. Das Unternehmen entwickelt Lösungen auf Basis einer offenen Architektur und stellt die Cybersicherheit dabei in den Mittelpunkt. Dazu gehören Verschlüsselung, Identitäts- und Zutrittsmanagement, kontinuierliche Überwachung, Schwachstellenmanagement sowie Leitlinien, die Kunden dabei helfen, ihre Systeme langfristig widerstandsfähig zu halten.

Weitere Informationen zu Best Practices im Bereich Cybersicherheit für physische Sicherheitssysteme finden Sie unter https://www.genetec.com/trust-cybersecurity.

Über Genetec

Genetec ist ein global agierendes Technologieunternehmen, das seit über 25 Jahren die physische Sicherheitsbranche entscheidend prägt. Mit dem Lösungsportfolio von Genetec können Unternehmen, Behörden und Kommunen weltweit Menschen und Betriebsanlagen sichern und gleichzeitig die Privatsphäre des Einzelnen schützen sowie betriebliche Effizienz realisieren.

Genetec bietet die weltweit führenden Produkte für Videomanagement, Zutrittskontrolle und ALPR, die alle auf einer offenen Architektur aufbauen und deren Kernstück Cybersicherheit ist. Das Portfolio des Unternehmens umfasst zudem Lösungen für die Einbruchserkennung, Sprechanlagen und das digitale Beweismanagement.

Genetec hat seinen Hauptsitz in Montreal, Kanada, und betreut seine mehr als 42.500 Kunden über ein umfangreiches Netzwerk von akkreditierten Vertriebspartnern und Beratern in über 159 Ländern.

Weitere Informationen über Genetec gibt es unter www.genetec.de.

Pressekontakt:

Patrick Rothwell
Miriam Seyd
Fink & Fuchs AG
Tel.: +49 611 74131-0
E-Mail: genetec@finkfuchs.de