„Augen zu gilt nicht mehr”

Codewerk · 21. Juli 2023

Der Cyber Resilience Act der EU: Neues Bürokratiemonster – oder überfällige Sicherheit?

Interview mit Timon Eßlinger, Codewerk GmbH

Es sind beeindruckende Zahlen, die der Dragos Year-in-Review Report 2022 für die Industrie aufführt: Im Vergleich zum Vorjahr haben Ransomware-Attacken auf Industrie- und Infrastrukturunternehmen um satte 87% zugenommen. Fast jeder zehnte Angriff zielte auf die Nahrungsmittelindustrie, jeder zwanzigste auf den Energiesektor. Entsprechend hoch ist der Handlungsdruck. Der neue Cyber Resilience Act (CRA) setzt innerhalb der EU gemeinsame Security-Standards für alle digitalen Produkte, die miteinander oder mit dem Internet verbunden werden können. Was bedeutet das für die Industrie, und wie können Lieferanten von Schlüsselkomponenten wie Software dabei helfen? Wir sprachen mit Timon Eßlinger, bei der Codewerk GmbH Experte für Cyber Security.

87% mehr registrierte Angriffe auf Industrie und Infrastruktur – heißt das, dass tatsächlich die Bedrohung gestiegen ist oder vor allem das Bewusstsein dafür?

Timon: Beides sind zwei Seiten einer Medaille: Zum einen nehmen die Angriffe faktisch zu. Zum anderen bekommt das Thema deshalb auch endlich die notwendige Aufmerksamkeit. Früher hat man Cyber Security gern mal wegen der Kosten ausgeblendet. Aber Augen zu

gilt nicht mehr. Heute investieren Unternehmen und Institutionen in Sensibilisierung und physischen Schutz – aber auch in resiliente Hardware, Software und Applikationen. Das ist, wenn man so will, der positive Effekt der Bedrohung.

Der Cyber Resilience Act der EU soll ja dazu beitragen, die IT- und Datensicherheit weiter zu stärken. Wer ist davon betroffen?

Alle Unternehmen, die Produkte mit digitalen Elementen herstellen. Darüber hinaus gibt es Verpflichtungen für Händler und Importeure. In unserem Kundenkreis ist das Bewusstsein, dass sie handeln müssen, sehr ausgeprägt – da geht es ja um sensible Industrieanlagen, viele davon in der Prozessindustrie, und um Schienenverkehr. Von beiden Bereichen hängen Millionen Menschen, Arbeitsplätze, unsere Güterversorgung ab. Entsprechend wichtig ist die Resilienz gegen Angriffe, Missbrauch oder sogar simple „Schusseligkeit“.

Und was können eure Kunden nun tun?

Sie müssen sogar etwas tun. Denn natürlich ist ihnen bewusst, dass sie ihre Anlagen und Infrastrukturen absichern müssen. Das Problem ist, dass sie mit der Hard- und Software für deren Betrieb ein Fremdprodukt einkaufen. Und ausgerechnet dieses Fremdprodukt kommt an einer ganz verwundbaren Stelle zum Einsatz. Der Cyber Resilience Act nimmt deshalb nicht nur die Betreiber in die Pflicht, sondern auch die Hersteller. Das Ziel ist es, über die gesamte Wertschöpfungskette Cyber-Security-Maßnahmen zu etablieren – also in Design, Entwicklung, Produktion, Inbetriebnahmen und nicht zuletzt während des Betriebs.

Was meinst du: Verändert sich damit etwas Entscheidendes?

Ja, auf jeden Fall. Denn der CRA verpflichtet die Hersteller und ihre Lieferanten, Security als Produktbestandteil zu verstehen. Es nicht am Ende noch draufzupacken, wenn die Entwicklung abgeschlossen ist – sondern „Security by Design“ zu gewährleisten. Also Sicherheit, die von Anfang an in der kompletten Wertschöpfungskette des Produktes und in allen Prozessen enthalten ist.

Wie könnt ihr als Codewerker euren Kunden helfen? Seid ihr selbst Cyber Security ready?

Nicht nur das – wir wollen hier führend sein! Aufbauend auf der Tatsache, dass wir seit jeher Software für kritische Industrien und Infrastrukturen entwickeln. Nehmen wir ein Zugsteuerungssystem. Wir prüfen heute schon, wie sicher unsere Software darin ist. Ein Beispiel ist Fuzzing, wo wir zufällig Inputdaten generieren und damit versuchen, das System zum Absturz zu bringen. Das tun wir schon in einer sehr frühen Phase, in der wir den Source Code noch gut und mit überschaubarem Aufwand beeinflussen können. So kommt man selbstverständlich in eine Sicherheitsroutine rein, die mit allen anderen Funktionstests mitläuft. Ein anderes Beispiel: Penetration Testing. Wir suchen gezielt Sicherheitslücken in bestimmten Protokoll-Implementierungen und finden dann ganz sicher auch welche.

Das beruhigt mich jetzt als Bahnfahrer nicht unbedingt …

Klar. Aber wir in der Softwareentwicklung denken etwas anders. Für uns ist die Frage entscheidend, ob solche Lücken in normalen Betriebsabläufen überhaupt ausgenutzt werden können – beziehungsweise wie man genau das verhindert. Man muss Bedingungen in die Software schreiben, die ausschließen, dass jemand einen potenziellen Fehler als Schwachstelle nutzen kann. Wir kapseln den Fehler sozusagen ein und helfen so, schädliche Auswirkungen zu verhindern. Wenn etwa aufgrund einer Sicherheitslücke unauthentifizierte Schreibanfragen möglich sind, müssen wir beispielsweise ausschließen, dass dann ein Passwort einfach mit beliebigen Werten überschrieben werden kann. Die Verantwortung für die Sicherheit liegt aber letztlich immer beim Hersteller.

Aber sollte der Cyber Resilience Act nicht gerade alle Wertschöpfungsbeteiligten mehr in die Pflicht nehmen?

Das tut er auch. Wir werden sehr schnell erleben, dass wir als Entwickler erweiterte Verantwortung wahrnehmen müssen: Ob bei der Dokumentation, wo wir bestätigen, dass Security schon in den Architekturen berücksichtigt ist; oder beim Testing – ist die Software so gehärtet geschrieben, dass sie bei unerwarteten Eingaben nicht abstürzt oder schadhafter Code ausgeführt werden kann? Und wir müssen im Detail dokumentieren, aus welchen Komponenten die Software geschrieben wurde, damit man bei Incidents gezielter nachbessern kann – das ist die sogenannte Software Bill of Materials oder SBOM.

Da kommt ja einiges auf euch zu.

Aber wir wissen, was Sache ist, und haben die entsprechenden Kompetenzen. Ganz abgesehen davon, dass Security für uns schon immer Herzenssache war. Schon unseren Kunden und deren Kunden zuliebe. Timon Eßlinger arbeitet seit 2020 bei der Codewerk GmbH. Die ersten Berührungspunkte mit dem Softwareunternehmen hatte er schon während seines Studiums und seiner Masterarbeit. Bei Codewerk ist er an der Entwicklung von Kommunikations-Gateways für Bahnsysteme beteiligt – ein Thema, bei dem auch seine persönliche Expertise in Cyber Security gefragt ist.