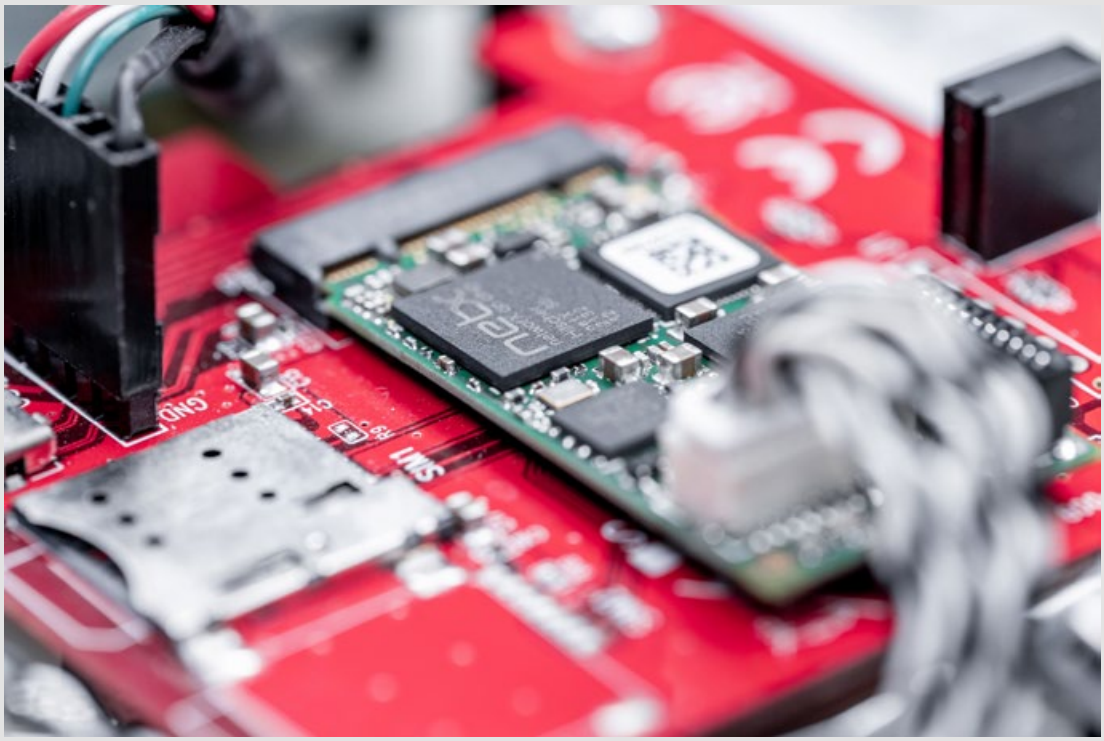
WEGE ZUR CRA-KONFORMITÄT

Cybersecurity, vom regulatorischen Muss zum Wettbewerbsvorteil: Zu den drängendsten regulatorischen Herausforderungen für Produktentwickler und -hersteller gehört der neue Cyber Resilience Act. Bis spätestens 11. Dezember 2027 müssen diese die IT-Sicherheit als fixen Bestandteil in ihre Produkte integrieren. Das reicht von sicheren Standardeinstellungen bis zu kontinuierlichen Updates. Über die Hintergründe dazu und die Möglichkeiten, aus der Notwendigkeit einen Wettbewerbsvorteil zu machen, spricht im Interview Frank Behnke, Head of Cybersecurity bei der Hilscher Gesellschaft für Systemautomation mbH. **Das Gespräch führte Ing. Peter Kemptner, x-technik**

Oft werden Zukunftsthemen schneller als manchen lieb ist zu Gegenwartsmaterien. Das gilt auch für die Bestimmungen des Cyber Resilience Act (CRA, EU 2024/2847). Dieser verpflichtet Hersteller von Produkten mit digitalen Elementen zur Einhaltung grundlegender IT-Sicherheitsanforderungen zum Schutz vor Cyberangriffen über den gesamten Lebenszyklus ihrer Produkte hinweg. Wie kurz diese Frist angesichts der vielfältigen Anforderungen auch auf organisatorischer Seite ist und wie es Geräte-, Maschinen- oder Anlagenherstellern – nicht zuletzt mithilfe von Technologielieferanten wie Hilscher – dennoch gelingen kann, zeigt das folgende Interview.

Herr Behnke, was ist das Besondere am Cyber Resilience Act?

Der CRA ist eine Verordnung der Europäischen Union, welche die Datenschutz-Grundverordnung und die



Der netX 90 von Hilscher ist der kleinste multiprotokollfähige Kommunikationscontroller auf dem Markt. Er unterstützt **alle gängigen Feldbus- und Industrial-Ethernet-Protokolle** mit hoher Informationssicherheit.

> Bedenkt man, was Unternehmen im Sinne des CRA alles umsetzen müssen, ist die Zeit bis zum Stichtag 11. Dezember 2027 nicht mehr sehr lang. Es hilft, Security nicht als lästige Pflicht, sondern von vornherein als Teil der eigenen Produktqualität zu verstehen.
>
> **Frank Behnke, Head of Cybersecurity, Hilscher Gesellschaft für Systemautomation mbH**

NIS-2-Richtlinie ergänzt. Am 10. Dezember 2024 in Kraft getreten, ist sie ab dem 11. Dezember 2027 bindend. Zu ihren wichtigsten Anforderungen gehören die Durchführung von Risikobewertungen und das Berücksichtigen von Sicherheitsaspekten in allen Phasen der Produktentwicklung, also „Security by Design". Dazu kommt die verpflichtende Einführung eines Verfahrens für den Umgang mit und die Behebung von Sicherheitslücken. Die Pflicht, aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle innerhalb von 24 Stunden zu melden, gilt bereits ab 11. September 2026 (exakt 25 Jahre nach den als 9-11 bekannten Terroranschlägen; Anm. d. Red.).

Warum sollte man den CRA nicht getrennt von anderen Maschinenrichtlinien betrachten?

Bereits am 20. Januar 2027, also in etwas mehr als einem Jahr, wird die neue Maschinenverordnung (EU) 2023/1230 die bisherige Maschinenrichtlinie ersetzen. Sie erweitert den Begriff der Funktionalen Sicherheit unter anderem um den Aspekt des Schutzes vor Korrumpierung. Dafür muss durch konstruktive Maßnahmen verhindert sein, dass durch die Vernetzung von Maschinen gefährliche Situationen entstehen können. Zusätzlich verlangt die Richtlinie einen Schutz der Maschinensoftware vor unbefugter Manipulation. Das spielt natürlich mit den Anforderungen des CRA zusammen. Ähnliches gilt z. B. auch für die erweiterte Funkanlagenrichtlinie und die KI-Verordnung.

Welche Auswirkungen hat dies für die Einhaltung des CRA?

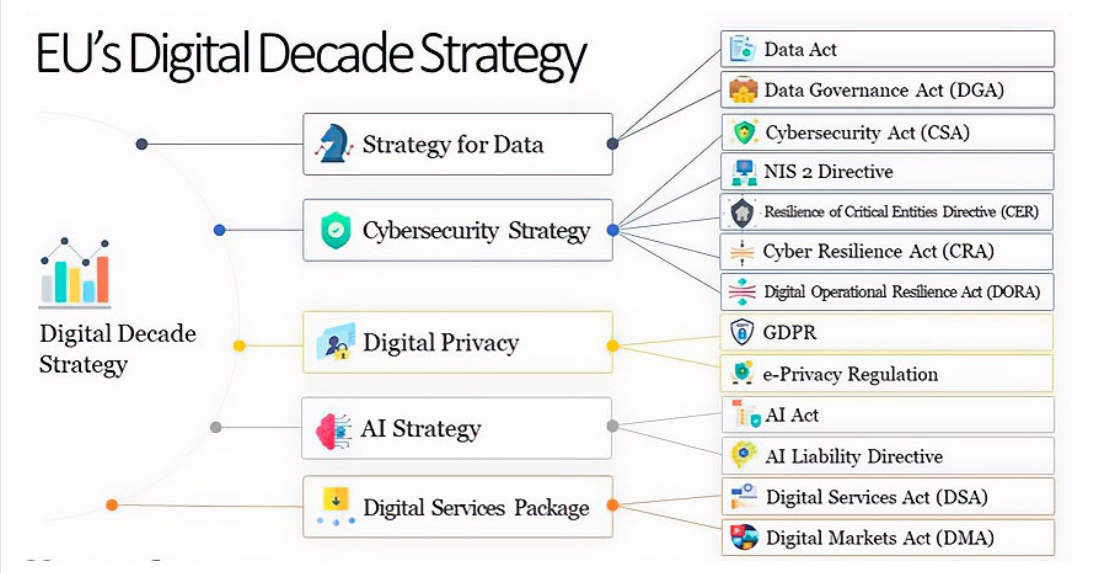
Aufgrund der unterschiedlichen Schutzziele genügt es nicht, die eine oder andere dieser Verordnungen einzuhalten, man sollte beide im Zusammenhang sehen. Hersteller von Geräten, Maschinen und Anlagen müssen nach dem CRA technische Unterlagen, eine Konformitätserklärung und eine CE-Kennzeichnung vorlegen. Diese muss ab Gültigkeit des CRA auch die Softwaresicherheit bei Neuprodukten oder wesentlichen Änderungen an Bestandsprodukten umfassen. Zusätzlich sind die Hersteller verpflichtet, ihre Produkte bis zum Ende seiner Lebensdauer, jedenfalls aber mindestens fünf Jahre lang zu unterstützen, etwa mit Sicherheitsupdates.

Warum halten Sie es für wichtig, die Bestimmungen des CRA bereits heute umzusetzen?

Der CRA gilt nicht nur für Neuprodukte, sondern ausnahmslos für alle Produkte, die ab dem genannten Stichtag in Verkehr gebracht werden. Das schließt auch solche mit ein, die bereits vor diesem Datum entwickelt wurden. Deshalb sollte die laufende Entwicklung eigentlich bereits umgestellt sein, um die zukünftige Marktfähigkeit des Produktes zu gewährleisten. Zudem wird es in vielen Fällen nötig sein, Entwicklungsressourcen zu reservieren, um Bestandsprodukte noch rechtzeitig zu ertüchtigen. Was das angesichts des allgemein beklagten Fachkräftemangels und des verhaltenen Investitionsklimas bedeutet, brauche ich hier wohl nicht extra auszuführen.

Was, wenn ein Hersteller das nicht zeitgerecht schafft?

Kann ein Hersteller diese Anforderungen des CRA nicht erfüllen, verliert er mit der CE-Kennzeichnung für seine Produkte das Recht, diese auf dem europäischen >>



Der Cyber Resilience Act ist Teil der 2021 vorgestellten EU Digital Decade Strategy 2030 mit dem Ziel, **Europa bis 2030 digital souverän, widerstandsfähig und technologisch wettbewerbsfähig** zu machen.

Binnenmarkt in Verkehr zu bringen. Da sich viele andere Märkte auch an diesem orientieren, kann das auch schädliche Auswirkungen auf die Marktfähigkeit der Produkte in anderen Ländern haben. Positiv ist hingegen, dass mit der Erfüllung des CRA automatisch auch z. B. US-amerikanische oder ostasiatische Vorschriften mit erfüllt sind.

Wie sehr lässt sich diese Aufgabe durch Verwendung CRA-konformer Vorprodukte lösen?

Eine wesentliche Neuerung des CRA ist, dass die Verantwortung der Geräte-, Maschinen- oder Anlagenhersteller nicht mehr am eigenen Werkstor endet. Diese müssen auch die Cybersicherheit zugekaufter Komponenten nachweisen und können sich nicht länger darauf zurückziehen, nur die im Haus erbrachten Teile der Gesamtentwicklung zu verantworten. Dennoch ist es gut, auf Vorlieferanten setzen zu können, deren Produkte – und nicht nur die, sondern ihr gesamter Entwicklungsprozess – lückenlos dokumentiert die Vorgaben der CRA erfüllen.

Wie weit ist die Umsetzung der CRA bei Hilscher bereits gediehen?

Hilscher hat in der Produktentwicklung bereits vor rund drei Jahren begonnen, die sogenannten Security Development Lifecycle Processes nach IEC 62443-4-1

Rittal – Das System.

Schneller – besser – überall.

Prozesssichere Bearbeitung mit intuitiver Bedienung – schon bei kleineren Kupfermengen lohnend!

Mehr Infos für Sie:
www.rittal.at/pts4

SCHALTSCHRÄNKE STROMVERTEILUNG KLIMATISIERUNG

FRIEDHELM LOH GROUP

Der CRA zielt auf den Schutz von Daten, Systemintegrität und kritischen Funktionen vor Cyberbedrohungen ab und **macht Cybersecurity zu einem Kriterium für die CE-Kennzeichnung**.

einzuführen. Der Audit-Termin beim TÜV als benannte Zertifizierungsstelle ist beantragt, er sollte demnächst stattfinden. Die Zertifizierung der IT-Security nach IEC 27001 erwarten wir in etwa zur selben Zeit. Das halte ich auch für sehr wichtig, denn es braucht ein sicheres Umfeld, um ein über seinen gesamten Lebenszyklus sicheres Produkt ohne Komplikationen entstehen zu lassen.

Wie sollten Unternehmen vorgehen, um diesen Status zu erreichen?

Zunächst muss klar erkannt werden, dass die Anforderungen des CRA nicht nur das Produkt selbst, sondern die gesamte Organisation des Herstellers betreffen. Eine detaillierte Ist-Analyse bestehender Produkte und der Entwicklungs-, Produktions- und Supportprozesse hilft, den genauen Handlungsbedarf zu identifizieren. Dazu gehört aus meiner Sicht eine Risikobewertung. Diese muss heute ganz selbstverständlich die Security mitberücksichtigen. Dabei müssen auch Schnittstellen einbezogen werden, die bislang als unkritisch galten, etwa serielle Anschlüsse.

Welche Tools können Unternehmen bei dieser Umstellung unterstützen?

Produkte und deren Entstehungsprozesse zu definieren, gehört klassisch zu den Aufgaben von Produktlebenszyklusmanagement (PLM) oder Applikationslebenszyklusmanagement (ALM). Wer diese Methoden und >>

Jetzt auch für kleinere Fertigungen
Automatisierte Stromschienenbearbeitung

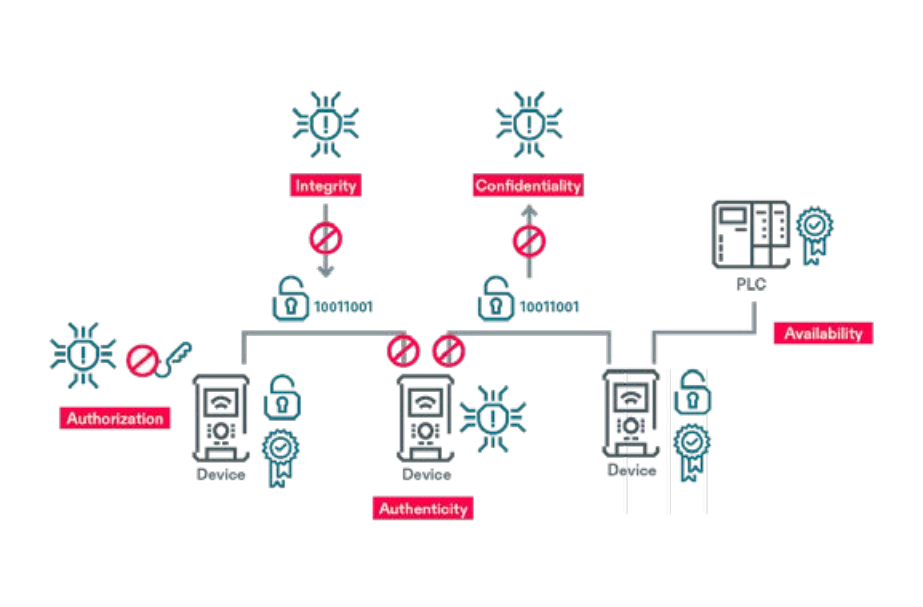
Das neue Punching Terminal PT S4 ermöglicht ein schnelles, präzises und flexibles Stanzen und Ablängen von Flachkupferschienen.

- Werkzeuge mit Schnellwechselfunktion für individuelle Anpassung und minimale Rüstzeiten
- Einfache Programmierung, flexible und benutzerfreundliche Bedienung
- Hohe Präzision ohne Nacharbeit – auch bei dicken Materialien
- Konstante und präzise Qualität durch drei CNC-gesteuerte Achsen
- Einfache Datenintegration durch Software PowerCut, ansteuerbar über Eplan Software

IT-INFRASTRUKTUR SOFTWARE & SERVICE

RITTAL

www.rittal.at/ras



Die Anforderungen der Maschinenverordnung und des Cyber Resilience Act werden den Produktwicklungsprozess maßgeblich verändern.

die dazu dienenden Softwaretools bereits anwendet, wird es leichter finden, diese Aufgabe zu lösen. Wer nicht, sollte vielleicht die Gelegenheit nutzen, diese in seinem Unternehmen einzuführen.

Damit allein wird es aber noch nicht getan sein, oder?

Natürlich nicht. Für viele Unternehmen ist die Herstellung der CRA-Konformität ein größerer und nicht trivialer, abteilungsübergreifender Vorgang. Die gute Nachricht ist, dass Hilscher seine Hausaufgaben gemacht hat. Unsere Kunden brauchen zumindest in Bezug auf die Eigenschaften der Chips und Module für die industrielle Kommunikation viele Dinge nicht selbst zu erledigen. Sie können auf vollständig dokumentierte, den Anforderungen des CRA entsprechende, Eigenschaften zurückgreifen.

Welche CRA-konforme Eigenschaften unterstützen Hilscher-Produkte konkret?

Unsere Produkte unterstützen das Secure Boot, das einen Gerätehochlauf mit manipulierter Software verhindert, und signierte Firmware-Updates. Sie bieten die für die interne und externe Verschlüsselung der übertragenen Daten erforderliche Hardwarebeschleunigung. Das ist bei stärkeren Mikroprozessoren kein Thema, in der Preisklasse, in der unsere Chips angesiedelt sind, war das nicht ganz so einfach umzusetzen. Das dritte Kriterium des CRA, das unsere Hardware erfüllt, ist die Möglichkeit, nicht verwendete Ein- und Ausgänge sicher zu deaktivieren, sodass diese als mögliche Angriffskanäle wegfallen.

Welche Hilscher-Produkte erfüllen diese Kriterien?

Unser Hauptprodukt, der netX 90, ist ebenso CRA-ready wie der erst heuer vorgestellte netX 9xx. Da der europäische Gesetzgeber beispielsweise die Verschlüsselung auf dem Stand der Technik verlangt, werden wir die Konformität dieser sehr langlebigen Produkte wohl über Patches über sehr lange Zeiträume hinweg sicherstellen. Das dient natürlich auch dem Schutz von Bestandskunden. Diese finden es damit leichter, die Security über die gesamte Lieferkette zu gewährleisten. Dazu werden sie ab etwa Mitte 2026 Zertifikate nutzen können.

Wie können Ihre Kunden von der CRA-Konformität Ihrer und damit ihrer eigenen Produkte profitieren?

Da ist rasch beantwortet: Wer die CRA-Konformität nicht gewährleisten kann, kann die CE-Kennzeichnung nicht erlangen und wird vor hohen Hürden bei der Vermarktung seiner Produkte stehen. Es ist also ein Muss. Die Erkenntnis, dass Security nicht nachträglich dazugebastelt werden kann, ist aber auch eine Chance: Analog zum seit Jahrzehnten etablierten „Quality by Design“ wird „Security by Design“ das Erreichen eines hohen Maßes an Datensicherheit mit voller Transparenz erleichtern. So kann aus der regulatorischen Notwendigkeit auch ein Vorteil im globalen Wettbewerb werden.

Vielen Dank für das Gespräch.

www.hilscher.com