# Von der Schwachstelle zur Norm – EU regelt Security neu

**Sicherheitslücken in der Software von Produkten bleiben oft unbemerkt – neue EU-Vorgaben sollen dies ändern. Der Cyber Resilience Act und die Maschinenverordnung setzen klare Anforderungen an den Schutz der Steuerung vor unbeabsichtigter oder vorsätzlicher Korrumpierung. Nun liegt es an der Normung, unter Betrachtung des geplanten Leitfadens zur Maschinenverordnung eine Grundlage für sichere und vertrauenswürdige Technik im europäischen Markt zu schaffen.**

Sicherheitsforscher melden jedes Jahr Tausende von IT-Schwachstellen in Produkten. Diese reichen von Hintertüren in Industriesteuerungen bis zu Funksteuerungen, die jedem Sender blind vertrauen. Viele Anwender sind sich dieser Sicherheitslücken gar nicht bewusst. Und für Hersteller gab es bisher kaum Anreize, mehr Ressourcen in die Behebung der Schwachstellen zu investieren. Nachdem der Markt dieses Problem nicht lösen konnte, reagierte die Europäische Kommission mit einem umfangreichen Gesetzespaket:

Der **Cyber Security Act** legt das Mandat für die Agentur der Europäischen Union für Cybersicherheit (ENISA) fest. Die ENISA soll die Kommunikation über Schwachstellen zwischen den Meldenden, Herstellern, Betreibern und Behörden in Europa verbessern und hat dazu eine europäische Datenbank eingerichtet.

Die **NIS-2-Richtlinie** definiert für wesentliche und wichtige Einrichtungen und Unternehmen Anforderungen an die Absicherung ihrer Netz- und Informationssysteme (NIS) sowie verbindliche Vorgaben für die Meldung von Sicherheitsvorfällen. Viele Mitgliedstaaten sind aktuell mit der nationalen Umsetzung im Verzug.

Der **Cyber Resilience Act** (CRA) regelt die Pflichten der Hersteller zur Vermeidung und im Umgang mit Schwachstellen. So muss eine Erreichbarkeit über einen Notfallkontakt sichergestellt werden. Zur Kommunikation haben sich einige frei verfügbare Spezifikationen etabliert. Diese definieren etwa einheitliche Standards, mit denen beschrieben werden kann, wie kritisch Sicherheitslücken sind (Kritikalität), sowie Datenformate für deren Beschreibung:

Die Spezifikation RFC 9116 der Internet Engineering Task Force (IETF) legt dar, wie Unternehmen in einer einfachen Textdatei weltweit hinterlegen, wer im Notfall über eine Schwachstelle zu informieren ist. Im CRA wird kein konkretes Format für die vom Hersteller anzulegende Liste der im Produkt enthaltenen Software (Softwarestückliste – SBOM) gefordert. Aktuell setzen sich besonders das CycloneDX-Format und der offene Standard ISO/IEC 5692 „System Package Data Exchange“

© Michael Hüter

durch. Durch die SBOM kann automatisiert gemeldet werden, welche Produkte eine Software enthalten, in der eine Sicherheitslücke bekannt ist. Für die im CRA geforderte maschinenlesbare Handlungsempfehlung hat sich das Common Security Advisory Framework (CSAF) ISO/IEC 20153 etabliert. Die Bedeutung des CRA zeigt sich auch in neuen Normungsvorhaben: Allein im Jahr 2025 wird über rund 40 Vorschläge für neue Normen abgestimmt, die unter dem CRA harmonisiert werden sollen.

### EU-Leitfaden konkretisiert Sicherheitsanforderungen der Maschinenverordnung

Die Maschinenverordnung (MVO) richtet sich an die Hersteller und fordert in Anhang III Abschnitt 1.1.9 und 1.2.1, dass bereits bei der Konstruktion ein angemessener Schutz gegen unbeabsichtigte oder vorsätzliche Korrumpierung vorgesehen wird. Darüber hinaus müssen Beweise für ein rechtmäßiges oder unrechtmäßiges Eingreifen erfasst werden.

Die Europäische Kommission plant, bis spätestens Januar 2027 einen Leitfaden herauszugeben, in dem die Begriffe praxisnah erläutert und die Pflichten klargestellt werden. Eine von fünf Arbeitsgruppen zum EU-Leitfaden wird sich mit den Abschnitten zum Schutz vor Korrumpierung befassen. Der Leitfaden interpretiert die EU-Verordnung und ist somit eine wichtige Referenz für die Normung.

### Erste Bausteine zum Schutz vor Korrumpierung stehen

Bei CENELEC haben die Normungsarbeiten an prEN 50742 begonnen, in der die Anforderungen der Maschinenverordnung an den Schutz vor Korrumpierung konkretisiert werden sollen. Die Norm soll möglichst mit anderen Security-Standards wie ISO/IEC 15408 (Common Criteria), EN 17640 (Cybersicherheitsevaluationsmethodologie für IKT-Produkte) und IEC 62443 (IT-Sicherheit von industriellen Kommunikationsnetzen) kompatibel sein. Außerdem soll sie auf eine äußerst breite Produktvielfalt anwendbar sein – vom Akkuschrauber über Werkzeugmaschinen und Hebebühnen bis hin zu Sicherheitsbauteilen. Ein Komitee-Entwurf (CD) der prEN 50742 wird im Sommer 2025 erwartet. Im Idealfall würde die Norm so zügig fertiggestellt, dass sie schon vor dem Anwendungsbeginn der MVO am 20. Januar 2027 harmonisiert ist.

Auch in der Überarbeitung der ISO 12100 zur Sicherheit von Maschinen zeigt sich der Trend, neben der funktionalen Sicherheit (Safety) auch Fragen der IT-Sicherheit (Security) zu berücksichtigen. Als zielführender Weg zeichnet sich ab, dass zunächst alle möglichen Gefährdungen in einer klassischen Risikoanalyse erfasst werden. Dabei werden die Gefährdungen der Maschine ohne Schutzmaßnahmen betrachtet. Im nächsten Schritt werden die Maßnahmen umgesetzt. Die Schutzmaßnahmen müssen dann vor Korrumpierung geschützt sein, damit sie ihre Aufgabe zuverlässig erfüllen können. Leitgedanke ist, dass durch die unbeabsichtigte oder vorsätzliche Korrumpierung keine neuen Gefährdungen entstehen können. Dabei muss auch die zuverlässige Auswertung von Signalen wie etwa eine NOT-HALT Anforderung betrachtet werden. Das Institut für Arbeitsschutz der DGUV hat verschiedene Maschinensteuerungen untersucht und festgestellt, dass sich die NOT-HALT-Funktion in vielen Fällen erstaunlich leicht aus der Ferne korrumpieren lässt.

Auch die gleichzeitige Korrumpierung vieler Maschinen muss in der Normung berücksichtigt werden. Falls zum Beispiel ein einzelner Aufzug oder eine Tanksäule ausfällt, ist dies relativ unkritisch. Ein flächendeckender Angriff auf alle Systeme mit identischer Steuerung kann jedoch katastrophale Auswirkungen haben. Während der gleichzeitige Ausfall durch Verschleiß höchst unwahrscheinlich ist, ist die flächendeckende Korrumpierung aller gleichen Systeme ein gravierendes Security-Szenario.

Als ersten Schritt empfiehlt es sich für alle Unternehmen bereits heute, den Notfallkontakt nach RFC 9116 umzusetzen. Auch die wesentlichen Bausteine für die kommenden Normen zur IT-Sicherheit hat die Forschung seit Jahrzehnten dokumentiert. Die gegenwärtige Herausforderung liegt darin, dazu einen Konsens über das gesellschaftlich vertretbare Risiko zu finden und praxisnahe Prüfgrundsätze zu erarbeiten.

*Jonas Stein*
*Institut für Arbeitsschutz der DGUV (IFA)*
*jonas.stein@dguv.de*

*Arne Sonnenburg*
*Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA)*
*sonnenburg.arne@baua.bund.de*