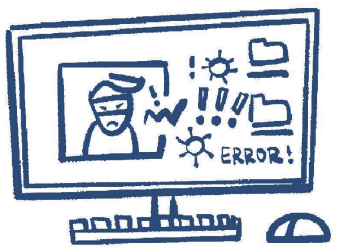
EU will Software und smarte Dinge schützen

Cybersicherheit. Mit dem Cyber Resilience Act reguliert die EU erstmals die Sicherheit von Produkten mit digitalen Elementen, um Attacken aus dem Web vorzubeugen. – Ein Gastbeitrag.



VON LUKAS FEILER
UND SILVIA GROHMANN

Wien. Die Sicherheit von Software ist seit Beginn des Internets eine ungebrochene Herausforderung. Jeden Monat werden zahlreiche neue Sicherheitslücken entdeckt, Unternehmen versuchen, sie durch Sicherheitsupdates möglichst schnell zu schließen. Gelingt dies nicht oder sind noch Updates verfügbar, ist es für Hacker oft ein Leichtes, die betroffenen Systeme zu kompromittieren. Da moderne elektronische Geräte von Spielzeugen über Waschmaschinen bis zu Autos viele Softwareprodukte beinhalten, trifft die Herausforderung unsicherer Software nicht nur die klassische Softwareindustrie, sondern einen Großteil der produzierenden Industrie.

Abhilfe soll hier der neue Cyber Resilience Act schaffen, der vorvergangene Woche im Amtsblatt der EU veröffentlicht wurde. Diese EU-Verordnung gilt für alle Produkte mit digitalen Elementen. Hiermit sind nicht nur klassische Software-Produkte und Computer-Hardware reguliert, sondern auch intelligente Geräte wie vernetzte Waschmaschinen.

Onlineservices miterfasst

Ebenso von der Regulierung umfasst sind Onlinedienste, die mit dem regulierten Produkt verbunden sind und ohne die das Produkt eine seiner Funktionen nicht erfüllen kann. Der Cyber Resilience Act ist damit nicht nur ein Instrument der Produktsicherheitsregulierung, sondern reguliert eine Vielzahl von Onlineservices gleichermaßen. Wird z. B. zusätzlich zu einem Onlinedienst eine App zum Download angeboten, mit welcher der Onlinedienst am Mobiltelefon leichter verwendet werden kann, findet der Cyber Resilience Act wohl auch auf den gesamten Onlinedienst Anwendung.

Hersteller, welche die Entwicklung eines Produkts mit digitalen Elementen ins Auge fassen, müssen zuerst eine Bewertung der mit diesem Produkt einhergehenden Cybersicherheitsrisiken durchführen. Das Ergebnis müssen sie in der weiteren Planung, Konzeption, Entwicklung, Herstellung, Lieferung und Wartung des Produktes beachten. Aufbauend auf dem Ergebnis dieser Risikobewertung, treffen den Hersteller einige Pflichten, um ein angemessenes Cybersicherheitsniveau zu gewährleisten.

Unter anderem ist der Hersteller dazu verpflichtet, Produkte ausschließlich mit sicheren Default-Konfigurationen auf den Markt zu bringen, welche auch jederzeit wieder in ihren ursprünglichen Zustand versetzt werden können. Außerdem darf ein Hersteller keine Produkte mit bekannten Sicherheitslücken in Verkehr bringen.

Der Hersteller ist nicht nur verpflichtet, Sicherheitsupdates unverzüglich und kostenlos bereitzustellen. Er muss auch automatisierte Sicherheitsaktualisierungen in den Standardeinstellungen vorsehen. Der jeweilige Unterstützungszeitraum eines Produkts, also der Zeitraum, in dem die Nutzer die Bereitstellung von Sicherheitsupdates erwarten können, soll nach dem Cyber Resilience Act grundsätzlich an die individuelle Lebensdauer des Produkts angepasst sein. Er wird in vielen Fällen mehrere Jahre betragen. Das Enddatum dieses Unterstützungszeitraumes müssen Hersteller nach dem Cyber Resilience Act auch transparent angeben. Dies soll unter anderem Nutzern dabei helfen, Produkte vergleichen und informierte Kaufentscheidungen treffen zu können.

UNTERNEHMEN & RECHT

diepresse.com/**recht**

Weiters werden Hersteller künftig auch noch einer Reihe an zusätzlichen Informationspflichten unterliegen. Beispielsweise werden Hersteller eine Auflistung von Umständen, die zu erheblichen Cybersicherheitsrisiken führen können, sowie ein Konzept für die koordinierte Offenlegung von Schwachstellen zugänglich machen und eine zentrale Kontaktstelle bekannt geben müssen, bei der in den Produkten entdeckte Schwachstellen gemeldet werden können.

„CE"-Kennung zur Bestätigung

Alle Hersteller müssen ihre Produkte mit digitalen Elementen einem Konformitätsbewertungsverfahren unterziehen und eine Konformitätserklärung ausstellen, welche bestätigt, dass das Produkt den grundlegenden Anforderungen des Cyber Resilience Act entspricht. Diese Konformitätserklärung sowie die technische Dokumentation können von den nationalen Behörden auch zur Einsicht verlangt werden. Der Hersteller bringt eine „CE"-Kennzeichnung an, wodurch er gewährleistet und somit auf eigene Verantwortung erklärt, dass ein Produkt diesen Anforderungen entspricht.

Künftig trifft einen Hersteller auch die Pflicht, Produkte vom Markt zu nehmen oder zurückzurufen, wenn ihm bekannt ist oder er auch nur Grund zur Annahme hat, dass ein reguliertes Produkt den technischen Sicherheitsanforderungen des Cyber Resilience Act nicht entspricht. Im Fall der Nichtkonformität kann die zuständige nationale Marktüberwachungsbehörde einen Rückruf auch anordnen. Liegt ein erhebliches Cybersicherheitsrisiko vor, ist auch die Kommission dazu befugt.

Unter dem Cyber Resilience Act müssen Hersteller künftig jede ihnen bekannt gewordene aktiv ausgenutzte Schwachstelle in ihren Produkten binnen 24 Stunden über eine von der Europäischen Agentur für Cybersicherheit (Enisa) einzurichtende zentrale Plattform melden. Außerdem werden Hersteller nach Bereitstellung entsprechender Sicherheitsupdates auch Informationen über die beseitigte Schwachstelle veröffentlichen müssen. Diese Pflicht umfasst eine Beschreibung der Schwachstelle, anhand derer die Nutzer ihre Auswirkungen und ihren Schweregrad beurteilen können, und Anleitungen, wie die Nutzer die Schwachstelle beheben können.

Neben dem Hersteller nimmt der Cyber Resilience Act auch Importeure und Händler in die Pflicht. Diese müssen sicherstellen, dass sie nur solche Produkte mit digitalen Elementen in den europäischen Markt einführen und dort vertreiben, welche die grundlegenden Anforderungen des Cyber Resilience Act erfüllen und für welche die Hersteller auch die notwendigen Informationen bereitgestellt haben. Dazu zählt auch, dass sie gegenüber der Behörde nachweisen können, dass der Hersteller das Konformitätsverfahren durchgeführt, eine technische Dokumentation erstellt und das Produkt mit einem CE-Kennzeichen versehen hat.

Sollte der Importeur oder Händler Grund zur Annahme haben, dass eines der Produkte, die er einführt bzw. vertreibt, nicht den Cybersicherheitsanforderungen entspricht, muss er die Konformität mittels Korrekturen herstellen oder das Produkt vom Markt nehmen bzw. es zurückrufen. Wenn er Kenntnis von einer Schwachstelle erlangt, muss der Importeur bzw. Händler nicht nur den Hersteller unverzüglich darüber informieren, sondern auch die Marktüberwachungsbehörden der Mitgliedstaaten, in denen er das Produkt bereitgestellt hat.

Geldbußen bis 15 Mio. Euro

Bei Nichteinhaltung der Pflichten des Cyber Resilience Act drohen Herstellern Geldbußen in der Höhe von bis zu 15 Mio. Euro oder 2,5 Prozent des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Sonstigen Akteuren drohen Geldbußen von bis zu fünf Mio. Euro oder ein Prozent des weltweiten Jahresumsatzes.

Da insbesondere Hersteller ihre Entwicklungsprozesse grundlegend überarbeiten werden müssen, tritt der Cyber Resilience Act nicht sofort in Geltung. Die Meldepflicht der Hersteller hinsichtlich Sicherheitslücken gilt ab 11. 9. 2026, die übrigen Verpflichtungen ab 11. 12. 2027.

Produkte mit digitalen Elementen, die vor 11. Dezember 2027 in Verkehr gebracht werden und danach keiner wesentlichen Änderung mehr unterliegen, sind von dem Großteil der Verpflichtungen ausgenommen. Dies gilt jedoch nicht für die Meldepflicht der Hersteller hinsichtlich Sicherheitslücken, welche trotzdem Anwendung findet.

Mit dem Cyber Resilience Act wird erstmals EU-weit die Cybersicherheit von Produkten mit digitalen Elementen einschließlich Software und intelligenter Geräte einer harten Regulierung unterworfen. Sowohl auf die Softwareindustrie als auch einen Großteil der produzierenden Industrie kommen damit große Herausforderungen zu. Nur wer zügig die Umsetzung der neuen Anforderungen in Angriff nimmt, wird zu Geltungsbeginn rechtskonforme Produkte auf den Markt bringen können.

Dr. Lukas Feiler, SSCP, CIPP/E ist Rechtsanwalt, Mag. Silvia Grohmann, CIPP/E Associate bei Baker McKenzie.

LEGAL § PEOPLE

Branchen-News aus der Welt des Rechts

Einsteiger der Woche

Mit den Beförderungen von **Rupert Kreuml, Philipp Leitner, Lukas Urban** (Linz), **Jana Seywald** (Wien), **Oskar Takacs** und **Raziye Taskiran** (Wels) sowie **Heidi Lallitsch** und **Raphael Höfer** (Graz) stärkt die Kanzlei Saxinger Rechtsanwalts GmbH ihr Team und baut ihre Kompetenz weiter aus.

Die Kanzlei E+H freut sich, **Karin Köller** als neue Rechtsanwältin und ständige Substitutin im Arbeitsrecht-Team begrüßen zu dürfen. Ihre Schwerpunkte sind Global Mobility, Betriebsübergänge und gesellschaftsrechtliche Fragestellungen.

Events der Woche

Die Herausgeber **Alois Birklbauer** (JKU), **Clemens Oberressl** (Hofrat OGH) und **Bernd Wiesinger** (Haslinger / Nagele) präsentierten ihr Werk „Kommentar zum VbVG" am OGH. Mit Vorträgen von **Georg Kodek, Ingeborg Zerbes** und **Philipp Wolm** bot die Veranstaltung Einblicke in die verschiedenen Facetten des VbVG. Das Werk vereint die Expertise renommierter Juristen aus Justiz, Wissenschaft und Strafverteidigung und ist eine wichtige Referenz im Unternehmensstrafrecht.

Karin Köller, neue Rechtsanwältin bei E+H [beigestellt]

Die Herausgeber von „Kommentar zum VbVG" [beigestellt]

Volker Engelmann und Michael Umfahrer [ÖNK]

Bereits zum 20. Mal veranstaltet Fellner Wratzfeld & Partner mit der Akademie der bildenden Künste Wien das Kunstprojekt „kunstakt" und öffnet seine Räumlichkeiten für vielversprechende Künstler:innen, die ihre Werke unter dem Motto „Echoes of Resilience" ein Jahr lang bei fwp ausstellen. „Der ‚kunstakt' ist ein Projekt, das uns besonders am Herzen liegt. Er bietet einerseits den jungen Künstler:innen eine Bühne, ihre Werke einem großen Publikum zu präsentieren. Andererseits ist es für uns spannend zu sehen, wie sich Kunst mit Recht auf überraschende Weise miteinander verknüpft und sich gegenseitig bereichert", erklärt **Markus Fellner,** Partner bei fwp.

Mit November 2024 hat die Österreichische Notariatskammer bereits zum 14. Mal den Wissenschaftspreis für hervorragende wissenschaftliche Arbeiten verliehen. Ausgezeichnet werden praxisbezogene Arbeiten, die Recht ohne Streit fördern – das Wesensmerkmal notarieller Tätigkeit. Als Preisträger wurde Notariatskandidat **Volker Engelmann** für seine Arbeit „Die Grunderwerb- und Immobilienertragsteuer aus Sicht des Parteienvertreters" prämiert. „Die Arbeit weist eine hohe inhaltliche Qualität auf und ist als umfassendes praxisbezogenes Nachschlagewerk für Notar:innen in Österreich prädestiniert", so **Michael Umfahrer,** Präsident der Österreichischen Notariatskammer.

LEGAL & PEOPLE

ist eine Verlagsserie der „Die Presse" Verlags-Gesellschaft m.b.H. & Co KG
Koordination: René Gruber
E-Mail: rene.gruber@diepresse.com
Tel.: +43/(0)1/514 14 263