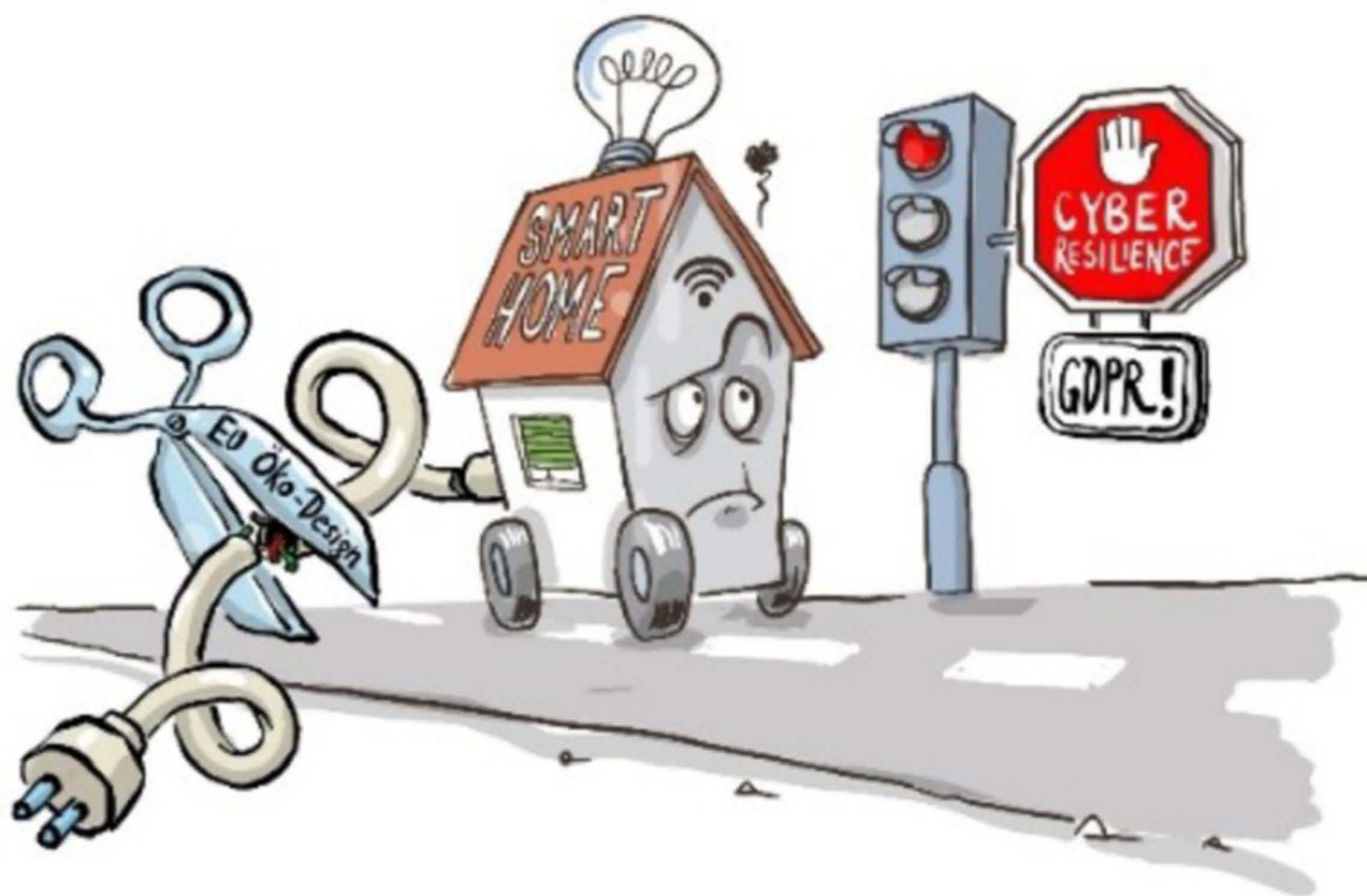




Fotos: Copyright Cordev GmbH

Wird das Smart Home durch neue Verordnungen ausgebremst?

Aktuelle regulatorische Vorgaben der EU stellen hohe Anforderungen beim Datenschutz, der Datensicherheit und jetzt auch beim Stromverbrauch, letzteres allerdings nur für den Standby-Betrieb. Demnächst kommt der Artificial Intelligence Act hinzu, denn künstliche Intelligenz zieht auch vermehrt ins Smart Home ein.

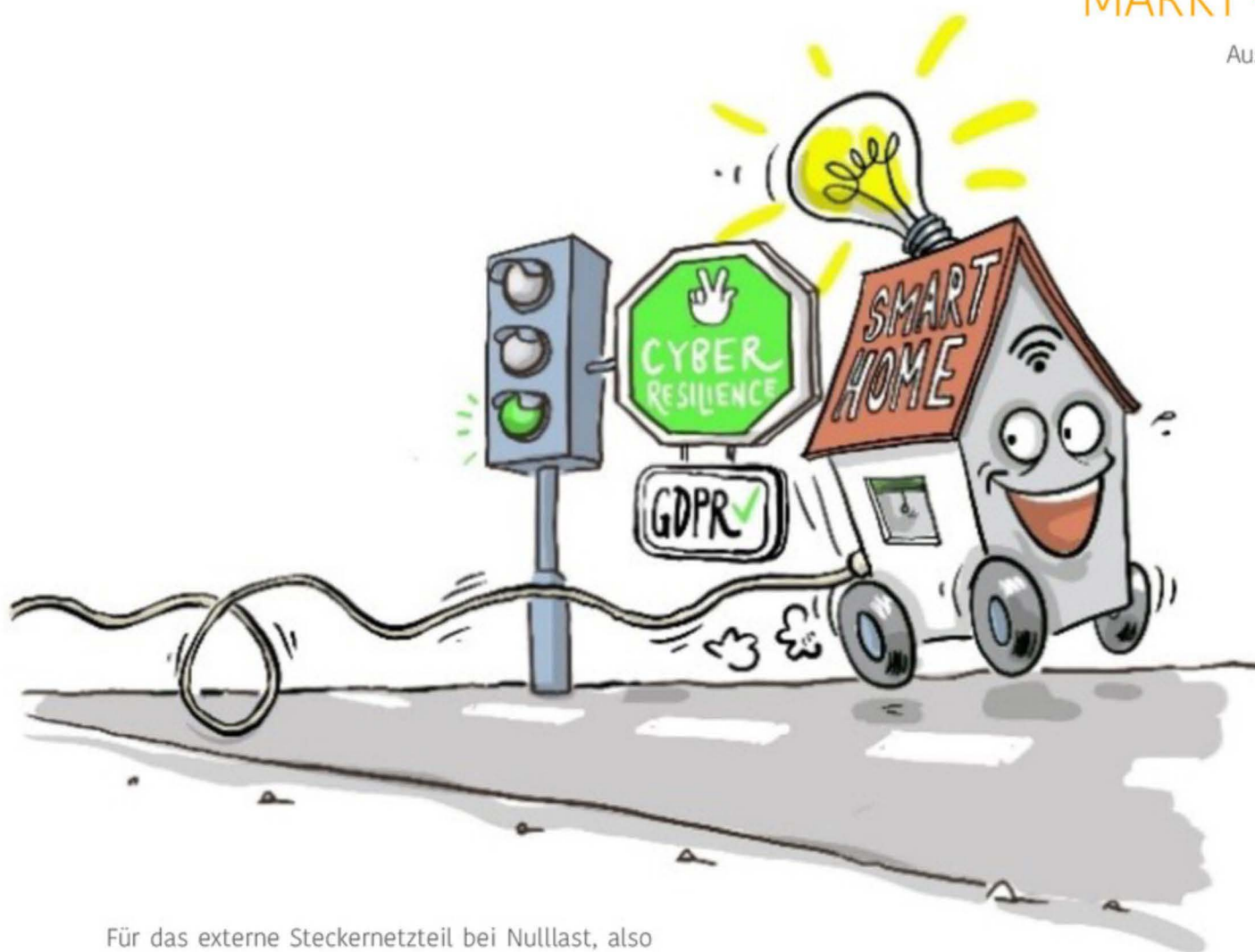
Dieser Beitrag von **Günter Martin** hilft, den Überblick zu behalten und die neuen Anforderungen zu verstehen. Was davon zu halten ist, bewertet das ergänzende Interview. Wenn man es richtig macht, dann wird Smart Home nicht ausgebremst, sondern im Gegenteil - sein Marktwachstum beschleunigt.

Standby-Stromverbrauch begrenzen

Bereits seit vielen Jahren gibt es von der EU ökologische Anforderungen an Produkte. Sie sind unter dem Begriff „Ökodesign“ zusammengefasst. Die neueste Verordnung ist die EU 826/2023 vom 17. April 2023. Damit und mit den Vorgängern sind jetzt praktisch alle am Stromnetz hängenden Geräte erfasst, die man im Haushalt finden kann - von der Kaffeemaschine über Musikinstrumente bis zu motorbetriebenen Gebäudeelementen. Spätestens mit letzteren ist das Smart Home betroffen, gemeint sind z.B. die motorbetriebenen Jalousien, Türen und Tore. Hinzu kommt die Informationstechnik im Wohnbereich und damit auch Router und Smart Home-Steuergeräte.

Sämtliche Geräte müssen mindestens einen Aus-Zustand und/oder einen Bereitschaftszustand haben, soweit dies mit der vorgesehenen Verwendung vereinbar ist. In beiden Zuständen ist die Hauptfunktion des Geräts abgeschaltet. Ergänzend gibt es für einige Geräte den vernetzten Bereitschaftsbetrieb.

> Im **Aus-Zustand** darf noch etwas Strom fließen (siehe Tabelle), wenn dies etwa aus Gründen der elektromagnetischen Verträglichkeit erforderlich ist. Für die permanente Leucht-Anzeige einer Uhr am Backofen reicht das nicht. Das ist kein Aus-Zustand.



Für das externe Steckernetzteil bei Nulllast, also ohne angeschlossenes Gerät, gilt eine frühere Regel (EU 278/2009): es darf maximal 0,3 W verbrauchen. Heutige Netzteile liegen deutlich unter 0,1 W, was sicher damit zusammenhängt, dass dieser Wert der Grenzwert in den USA ist. Für Netzteile über 50 W Volllast-Leistung sind höhere Nulllast-Verbräuche zulässig.

- > Beim **Bereitschaftszustand** gibt es eine Reaktivierungsfunktion, zum Beispiel über eine Fernbedienung, einen internen Sensor oder Timer. Wenn das Gerät seinen Bereitschaftszustand etwa über eine LED anzeigt, darf der Verbrauch etwas höher liegen.

- > Der **vernetzte Bereitschaftsbetrieb** ist für Smart Home-Geräte natürlich fundamental, denn die Vernetzung von Aktoren, Sensoren und Steuereinheit macht das Zuhause ja gerade smart. Oft geht es dann auch noch über einen Router ins Internet. Die Geräte sind ständig im Netz verfügbar und das darf mehr Strom brauchen als der unvernetzte Bereitschaftszustand. Richtig relevant wird das bei HiNA, der hohen Netzwerkverfügbarkeit. Dazu zählen insbesondere Router und Drahtlos-Netzzugangspunkte.

	Zustand	(Heute)	2026	2028
1	Aus-Zustand	0,5 W	0,5 W	0,3 W
2	Bereitschaftszustand mit Reaktivierungsfunktion	0,5 W	0,5 W	0,5 W
	zusätzlich mit Statusanzeige	1,0 W	0,8 W	0,8 W
3	Vernetzter Bereitschaftsbetrieb ohne HiNa	2,0 W	2,0 W	2,0 W
	Vernetzter Bereitschaftsbetrieb mit HiNa	8,0 W	8,0 W	7,0 W

Tabelle: Maximalwerte für den Standby-Verbrauch von Geräten im Haushalt gemäß den EU-Verordnungen 826/2023, 801/2013 und 617/2013, ohne Berücksichtigung von Ausnahmen.

Die neue EU-Verordnung 826/2023 wurde im April 2023 verabschiedet und tritt nach einer Übergangszeit in mehreren Stufen 2026 und 2028 in Kraft. Beim Blick auf Tabelle 1 ändert sich 2026 kaum etwas gegenüber den bisherigen Anforderungen. Der Unterschied liegt im Geltungsbereich. Während bisher Geräte mit externem Netzteil ausgenommen waren, sind sie in der neuen Verordnung aufgenommen. Damit sind jetzt praktisch alle Geräte im Haushalt betroffen, die Strom aus dem öffentlichen Netz ziehen.

Nach der neuen Verordnung müssen die Standby-Stromverbräuche in der Dokumentation angegeben werden. Eine Stromsparfunktion muss bei Auslieferung aktiviert sein, zum Beispiel das automatische Aus- oder Standby-Schalten nach einer gewissen Laufzeit. Der Nutzer kann dies deaktivieren, wobei ihm dies so schwer und abschreckend wie möglich zu machen sei. Der Hersteller, Importeur oder Bevollmächtigte darf „keine Geräte in Verkehr bringen, die so gestaltet sind, dass sie einen aktuellen Prüfzyklus erkennen könnten.“

Cyber Angriffe abwehren

Was für die kritische Infrastruktur bereits mit den NIS-Richtlinien der EU geregelt wird, kommt nun für alle Produkte mit digitalen Elementen, die in der Lage sind, mit anderen Produkten zu kommunizieren, sei es Hardware oder Software im Industrie- oder Consumer-Umfeld: Die Widerstandsfähigkeit gegen Cyberangriffe soll gestärkt werden. Der Entwurf des Cyber Resilience Act (CRA) wurde im September 2022 von der EU-Kommission vorgeschlagen und wird, mit noch einigen Änderungen, wahrscheinlich Ende 2024 rechtsverbindlich werden. Dann folgt eine Übergangszeit von 24-36 Monaten.

Auch wenn es noch einige Zeit hin ist und die konkreten technischen Anforderungen noch in (hoffentlich) EU-weit harmonisierten Normen zu definieren sind, macht es Sinn, sich bereits heute damit zu beschäftigen. Der Kernpunkt ist nämlich **Security by Design**: die Cybersicherheit muss einbezogen werden in Planung, Design, Entwicklung, Produktion, Lieferung und Wartung – also schon lange vor dem Beginn der Produktion bis zum Ende des Lebenszyklus. Die Verordnung betrifft Hersteller, Importeure und Händler für Produkte, die im EU-Raum verkauft werden. Ein Produkt ist dabei nach dem oben genannten Geltungsbereich fast schon alles, was einen Chip hat oder nutzt. Im Smart Home dürfte alle Hard- und Software betroffen sein, da hier die Kommunikation miteinander immer dazu gehört. Das gilt auch beim „local Smart Home“, das nur lokal und nicht mit dem Internet verbunden ist.

Natürlich ist das Risiko unterschiedlich. Ein gehacktes IOT-Gerät, das in der Industrie eine große Produktionsmaschine überwacht, ist kritischer als ein Außenthermometer im Smart Home. Allerdings ist auch das nicht vollkommen unkritisch und unterliegt dem Cyber Resilience Act. Ein gehacktes Außenthermometer, das im tiefsten Winter sommerliche Temperaturen meldet und die Heizung abschaltet, ist nur ärgerlich. Werden aber in einer Region alle Geräte gehackt und Tausende müssen frieren, dann werden schon größere Hilfsmaßnahmen nötig. Für einen Hacker ist der Multiplikator-Effekt leicht machbar. Hat er die Schwachstelle eines Geräts gefunden, kann er sie in allen Geräten dieses Typs ausnutzen.

Um sich auf die Anforderungen vorzubereiten, empfiehlt sich ein Blick in die GDPR, der General Data Protection Regulation oder Datenschutzgrundverordnung. In Artikel 32, Sicherheit der Verarbeitung, sind Sicherheitsanforderungen genannt, die in Richtung Cyber Resilience gehen. Diese und einige weitere können und sollten nach ETSI TS 103 645 „Cyber Security for Consumer Internet of Things“ konkret umgesetzt werden. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) bietet dazu ein freiwilliges IT-Sicherheitskennzeichen an. Zusätzlich werden beim Hersteller organisatorische Maßnahmen erforderlich, um das oben erwähnte Security by Design umzusetzen. Hierzu gibt es eine Handreichung von Teletrust mit modellhaften Vorgehensweisen und Handlungsempfehlungen für Entscheider.

Künstliche Intelligenz kontrollieren

Im Juni 2023 hat das Europäische Parlament den Artificial Intelligence Act (AIA) beschlossen. Der Act legt EU-einheitliche Regelung zum Umgang mit Künstlicher Intelligenz fest. Wenn alle Länder zustimmen, könnte AIA 2026 in Kraft treten. Bis dahin wird auf freiwillige Selbstkontrolle gesetzt.

Während die bisher beschriebenen Verordnungen vor allem den Hersteller/Anbieter in die Pflicht nehmen, ist der Geltungsbereich der AIA breiter. Sie umfasst auch den Nutzer von KI-Systemen, sofern sich diese in der EU befinden, konkret auch Behörden und Privatpersonen. Eine Behörde darf zum Beispiel nur mit hohen Auflagen KI einsetzen, um zur Strafverfolgung über Kameras Personen zu identifizieren. Ausnahmeregelungen gelten für die wissenschaftliche Forschung. Hier kann an und mit KI in sogenannten KI-Reallaboren („regulatory sandboxes“) experimentiert und geforscht werden, zeitlich und meist auch räumlich begrenzt. Solche Reallabore gibt es zum Beispiel schon in Baden-Württemberg. Sie beschäftigen sich mit KI in Gesundheit und Pflege oder auch Robotischer Künstlicher Intelligenz.

Der AIA ordnet KI-Anwendungen in drei Risikogruppen:

1. **Inakzeptables Risiko:** Erheblicher Schaden für die Gesundheit, Sicherheit, Grundrechte oder die Umwelt der Menschen. Verboten.
2. **Hohes Risiko:** Einsatz bei kritischer Infrastruktur, der Strafverfolgung oder in der Bildung. Mit hohen Auflagen erlaubt.
3. **Begrenztes Risiko:** Spamfilter, Videospiele, Suchalgorithmen, Deep Fakes oder Chatbots.

Der AIA betrifft auch das Smart Home. Dort ist bereits heute KI im Einsatz, etwa bei der Spracherkennung zur Steuerung von Smart Home-Komponenten oder der Routenplanung von Saugrobotern. Auch bei Mährobotern hält KI langsam Einzug, sie kommen dann ohne Begrenzungsdraht aus. KI-basierte AAL-Systeme können erkennen, dass ein Notfall vorliegt und ein Bewohner Hilfe braucht. Zur frühzeitigen Erkennung eines Lecks in der Wasserleitung lernt KI die Verbrauchskurve und erkennt kritische Abweichungen. Dank KI-basierter Bilderkennung öffnet sich die Haustür, wenn ein Bewohner davorsteht. Alle diese Beispiele liegen im Bereich des begrenzten Risikos, soweit die KI zum Beispiel nicht in die Grundrechte der Bewohner oder anderer Menschen eingreift. Technisch wäre das möglich, aber klar verboten.

Die EU-Vorgaben im Überblick

EU ÖkoDesign (Standby-Stromverbrauch)

- EU 826/2023 vom 17. April 2023: Standby-Verbrauch Haushalt
- EU 801/2013 vom 22. August 2013: Standby-Verbrauch TV, Haushalt
- EU 617/2013 vom 26. Juni 2013: Standby-Verbrauch PCs, Notebooks

EU Cyber Resilience Act (CRA)

- EU Cybersecurity: Übersicht mit Links u.a. zu CRA, NIS2, DORA, Chips Act
- EU Cyber Resilience Act vom 15.9.2022 ohne Anlagen
- EU Cyber Resilience Act vom 15.9.2022 Anlagen 1-4
- Teletrust-Handreichung 2023: „Security by Design“
- ETSI TS 103 645 V2.1.2 vom Juni 2022: IOT-Datensicherheit nach DSGVO
- BSI IT-Sicherheitskennzeichen nach ETSI TS 103 645

EU Artificial Intelligence Act (AIA)

- EU Proposal vom 21. Juni 2021

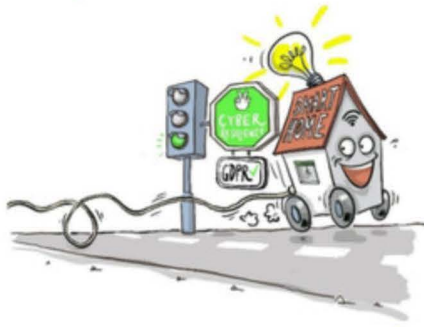
Foto: Günter Martin, Cordev GmbH



Autor

Günter Martin ist Diplom-Informatiker und Geschäftsführer der Cordev GmbH. Das Unternehmen berät Anbieter von IoT-Geräten, zum Beispiel auch Smarter Haushaltsgeräte, bei der Entwicklung und Vermarktung.

Daneben ist er Beirat für Cybersecurity bei der Smart Home Initiative Deutschland.



Nachgefragt!

BusSysteme >> Herr Martin, was halten Sie von den neuen Verordnungen?

Günter Martin >> Auf der einen Seite reden wir vom Bürokratie-Abbau. Auf der anderen Seite entstehen neue regulatorische Vorgaben, die wieder mehr Bürokratie bedeuten. Es muss ja wieder mehr gemeldet, geprüft, genehmigt, dokumentiert und umgesetzt werden. Wenn es neue Regeln gibt, dann muss auch das Verhältnis von Aufwand und Nutzen stimmen. Das ist beim Thema Cyber-Security und der künstlichen Intelligenz der Fall.

BusSysteme >> Den Standby-Stromverbrauch haben Sie nicht erwähnt. Seine Begrenzung halten Sie also für falsch?

Günter Martin >> Nein, aber für unnötig komplex. Die EU sagt, die Bevölkerung in Europa spart damit 530 Millionen Euro pro Jahr ab 2030 bei der Stromrechnung. Jeder Europäer spart also 1,18 € pro Jahr. Es wird auch Kohlendioxid eingespart, nämlich 1,36 Millionen Tonnen pro Jahr. Das ist schon eine eindrucksvolle Zahl, es sind allerdings nur 3 kg pro Einwohner. Ein Deutscher hat im Schnitt einen jährlichen CO₂-Ausstoß von 8,1 Tonnen, der sich um 3 kg oder weniger als 0,4 Promille verringert. Natürlich begrüße ich jede Einsparung und es ist richtig, die Entwickler in Richtung Strom-Einsparung zu lenken. Diese Richtung wird aber zurecht und mit einigen Erfolg schon lange verfolgt und die letzten Bruchteile an Einsparung müssen nicht mit solch komplexen regulatorischen Vorgaben herausgepresst werden. Die Industrie schafft das mit der technischen Weiterentwicklung auch ohne den damit verbundenen Bürokratie-Aufwand.

BusSysteme >> Sind Sie bei der Cyber Security, also dem Cyber Resilience Act (CRA), auch so kritisch?

Günter Martin >> Ganz im Gegenteil. Ich bin froh, dass es Systemanforderungen geben wird, die Widerstandsfähigkeit von Systemen gegen Cyberangriffe zu stärken. Und noch ein Stück mehr froh bin ich, dass dies EU-weit einheitlich erfolgt. Wir brauchen keine Cybersecurity „Made in Germany“ oder „Made in France“ und weitere 25, sondern einheitliche Standards.

Der CRA enthält noch keine konkreten technischen Cybersecurity-Anforderungen. Ich hoffe sehr, dass diese für die jeweiligen Produkte in EU-weit harmonisierten Normen definiert werden, danach sieht es derzeit auch aus. Die Anforderungen werden allerdings die Anbieter vor einige Herausforderungen stellen. Security by Design und ein professionelles Vulnerability Management erfordern nicht nur technische, sondern vor allem organisatorische Maßnahmen. Hier muss auch das Top Management aktiv mitwirken.

BusSysteme >> Wird künstliche Intelligenz richtig kontrolliert?

Günter Martin >> Es wird kontrolliert, wofür KI angewendet wird, und das ist aus meiner Sicht genau der richtige Weg. Mit dem Artificial Intelligence Act (AIA) werden bestimmte Einsatzfelder verboten, andere stark oder nur geringfügig eingeschränkt. Ich sehe in der Künstlichen Intelligenz ungeheures Potenzial für eine bessere Welt, das wir nicht tot regulieren dürfen. Daher freue ich mich, dass die Forschung und Entwicklung im AIA mit einem vernünftigen Sandbox-Ansatz Freiheiten auch in Europa behält. Der Spott „Die USA erfinden, die EU reguliert“ muss nicht schon wieder drohen.

Um KI zu kontrollieren, reichen Gesetze und Verordnungen allein allerdings nicht aus. Missbrauch kann damit natürlich nicht sicher verhindert werden und Unverständnis darüber, was KI ist und kann, führt zu verzerrten gesellschaftlichen Diskussionen. Notwendig ist eine breite Aufklärung über Chancen und Risiken mit dem Ziel: Verstehe und kontrolliere KI und lass dich nicht von ihr kontrollieren. Fachmedien, wie zum Beispiel die BUS/SYSTEME, können dazu einen wichtigen Beitrag leisten.

BusSysteme >> Bremsen die neuen Verordnungen Smart Home aus?

Günter Martin >> Nein, aber sie geben eine Richtung vor. Smart Home macht eine leichte Kurve. Dann geht es mit Vollgas weiter, weil die neue Richtung genau das ist, was Verbraucher zurecht wollen: Sicherheit vor Cyber-Angriffen, intelligente Systeme, die beherrschbar sind, und weniger Energieverbrauch. Letzteres wird zwar längst zum Beispiel durch smarte Heizungssteuerung viel umfassender erreicht als die geringen Einsparungen beim Standby. Aber es bleibt zumindest das Marketing-Argument, auch dort Strom zu sparen. Wenn die anderen beiden Punkte, Sicherheit und Intelligenz, auch noch gut umgesetzt und vermarktet werden, dann wird Smart Home nicht ausgebremst, sondern im Gegenteil - sein Marktwachstum kräftig beschleunigt.



Günter Martin, Cordev GmbH

Günter Martin, Geschäftsführer der Cordev GmbH