Hyperkonnektivität setzt Hyperresilienz voraus – der „Stand der Technik“ ist notwendig, aber nicht hinreichend!

Von Joachim Jakobs

"Die Digitalisierung schafft gewaltige Möglichkeiten für neue Geschäftsmodelle. Damit gehen jedoch auch große Risiken und Rechtsfolgen einher", stellt das Versicherungsjournal im April 2026 fest. Einen Monat später bekräftigt Spiegel Online: „Fehlerhaftes Update hat deutsche Internetdienste lahmgelegt -- Webseiten, Apps, E-Mail: Viele deutsche Internetdienste waren am Dienstagabend nicht erreichbar. Der Grund lag offenbar bei dem Verwalter deutscher Internetdomains.“

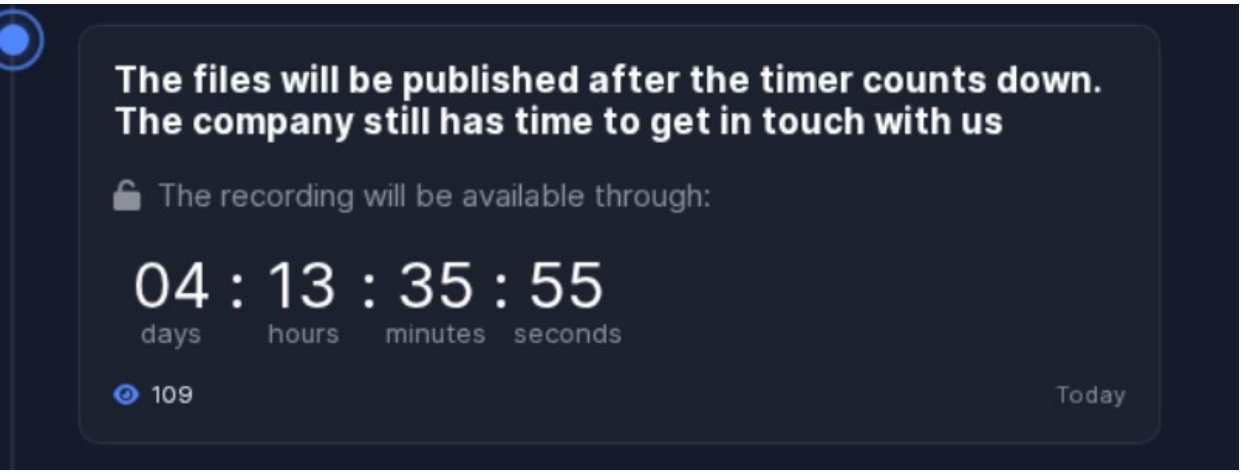
Fehler sind menschlich – Kriminalität auch. Das Wirtschaftsministerium warnt vor Cyberkriminellen, die nicht nur Konzerne, sondern auch „mittelständische Unternehmen“ bedrohten: „Denn sie verfügen häufig über Know-how, das es zu schützen gilt.“

Hinzu kommt für Damian Steffin, Berater für Datenschutz & IT-Compliance bei Ecovis in Rostock, dass die Kleinen „vielfach schlechter geschützt (sind), als sie glauben.“

„Risiko groß, Sorglosigkeit auch“ heißt es beim Bayerischen Rundfunk unter Berufung auf eine Studie des TÜV: „Jedes siebte in einer Erhebung befragte Unternehmen war bereits Opfer eines ernsthaften Cyberangriffs. Gleichzeitig spielt Cybersicherheit für sehr viele der Firmen aber keine große Rolle. Experten sehen eine unterschätzte Bedrohung.“

Warum unterschätzen Mittelständler das Risiko? Gut möglich, dass das mit dem Ratschlag des Bundeskanzlers zusammenhängt, „ein bisschen weniger über Datenschutz und ein bisschen mehr über Datennutzung“ zu reden! Wenn der Regierungschef eines der reichsten Länder der Welt derartige Volksverblödung betreibt, dürften bei Kriminellen Champagner-Korken knallen! Für die Wirtschaftspresse umgekehrt scheint der Spruch Gesetz zu sein: Bei der Recherche zu diesem Text konnte kein Massenmedium gefunden werden, das den Zusammenhang von Digitalisierung, Risiken, Rechtsfolgen und erforderliches Schutzniveau für Geschäftsführer ansprechend erklärt. Kein Wunder: „Die Medien berichten oft nur von einem Waldbrand oder Bränden mit Toten. Über Brandursachen oder wie Brände verhindert werden können, wird eher selten berichtet“, wissen Brandschützer.

Der Versicherungsmakler Frank Strötzel berichtet, die Verantwortlichen glaubten, „uns Mittelständlern passiert sowas nicht“. Das könnte auch mit unzulänglicher Kommunikation zusammenhängen.



Kriminelle drohen Daten ihrer Opfer zu veröffentlichen, wenn diese kein Lösegeld zahlen.

Bild: Ransomware.live

Was für ein Irrtum das ist, lässt sich an „Ransomware.live“ erkennen; eine Internetseite, die protokolliert, welche Firmen Erpressungstrojanern zum Opfer gefallen sind; aktuell sind dort 863 Deutsche Opfer gelistet -- sieben davon seit dem 1. Mai 2026. Im Ergebnis werden Deutsche Daten dreimal so häufig unter Kriminellen gehandelt wie die von Frankreich und Italien zusammen.

Damit drohen nicht nur Kosten für die Wiederherstellung von Systemen, Lösegeldforderungen, Gutachten, Anwälten, Gerichten, Geldbußen und Schadenersatzforderungen, sondern der Betrieb steht still, weil Erpressungstrojaner „zunehmend“ Maschinen und Anlagen angreifen und „dabei Schwachstellen in industriellen Steuerungssystemen (ICS)“ ausnutzen.

Und Rechnungen lassen sich nicht mehr bezahlen – die Signal Iduna Gruppe berichtet von einer Hochschule, die nach einem Angriff „monatelang“ keine Rechnungen mehr hätte zahlen können. Davon sei auch ein Gartenbauunternehmen betroffen gewesen, das die Außenanlagen gestaltet habe. So habe die Gartenbauerin kein Geld erhalten und musste „letztlich Insolvenz anmelden“.

Hinzu kommt für den Sicherheitsexperten Matt Hull. dass wegen KI-basierter Angriffswerkzeuge „auch technisch weniger versierte Angreifer [...] nun komplexe Ransomware-Kampagnen in großem Umfang durchführen“ können. So soll es neunjährige Kinder geben, die Internetseiten mit Überlastungsangriffen plattmachen, nur weil sie ihnen „nicht gefallen“.

Die Fähigkeiten der Angreiferinnen nehmen zu – die der Angegriffenen sogar ab: „Laut BSI-Umfrage nimmt das Sicherheitsbewusstsein seit 2023 in Deutschland ab.“ Die Folge: 90 Prozent der Unternehmen in Deutschland sollen der Ansicht sein, sie seien "gut" oder sogar "sehr gut" vor Cyberattacken geschützt. Die Präsidentin des Bundesamts für Sicherheit in der Informationstechnik (BSI) Claudia Plattner hält das für „Wunschdenken“: Die meisten Firmen hätten „noch nicht einmal Seepferdchen, um sicher an den Beckenrand zu kommen“. Wer nicht schwimmen kann, geht unter: Im März 2026 mussten ein Autohaus in Chemnitz und ein Elektronikunternehmen aus Baden Württemberg nach Angriffen Insolvenz anmelden.

Hinter dem Seepferdchen verbirgt sich der „CyberRisikoCheck“, ein – so die Hoffnung – „Wirkungsvoller Schutz für kleine und Kleinstunternehmen“ mit der Behördenbezeichnung „DIN SPEC 27076“. Dadurch sollen Parameter bei „Organisation & Sensibilisierung“, „Identitäts- und Berechtigungsmanagement“, „Datensicherung“, „Patch- und Änderungsmanagement“ sowie „Schutz vor Schadprogrammen sowie IT-Systeme und Netzwerk“ für ein Minimum an Sicherheit sorgen.

Themen des Cyber Risiko Checks nach DIN Spec 27076

Thema	Inhalte
Organisation & Sensibilisierung	Gesamtverantwortung, Zuständigkeit bei IT Notfällen, Definition von Regeln, Kenntnisstand im Umgang mit IT und Netzwerken
Identitäts- und Berechtigungsmanagement	Passwortrichtlinie, Zugriff und Zugang
Datensicherung	Zugriff, Zugang, Ablageort und Häufigkeit von Datensicherung
Patch- und Änderungsmanagement	Häufigkeit und Zeitpunkt von Updates
Schutz vor Schadprogrammen sowie IT-Systeme und Netzwerk	Vertrauenswürdigkeit, Netzwerk Security, Zugriffsberechtigungen, Firewall, VPN, WLAN und Homeoffice Regeln

Tabelle: Wikipedia

Da liegt der Hund begraben – die IT Risk Solutions GmbH präzisiert: „Das Schutzniveau gemäß DIN SPEC 27076 ist selbst bei voller Punktzahl kein sehr gutes Schutzniveau, sondern für ein Klein- oder Kleinstunternehmen das vertretbare absolute Minimum an Informationssicherheit.“

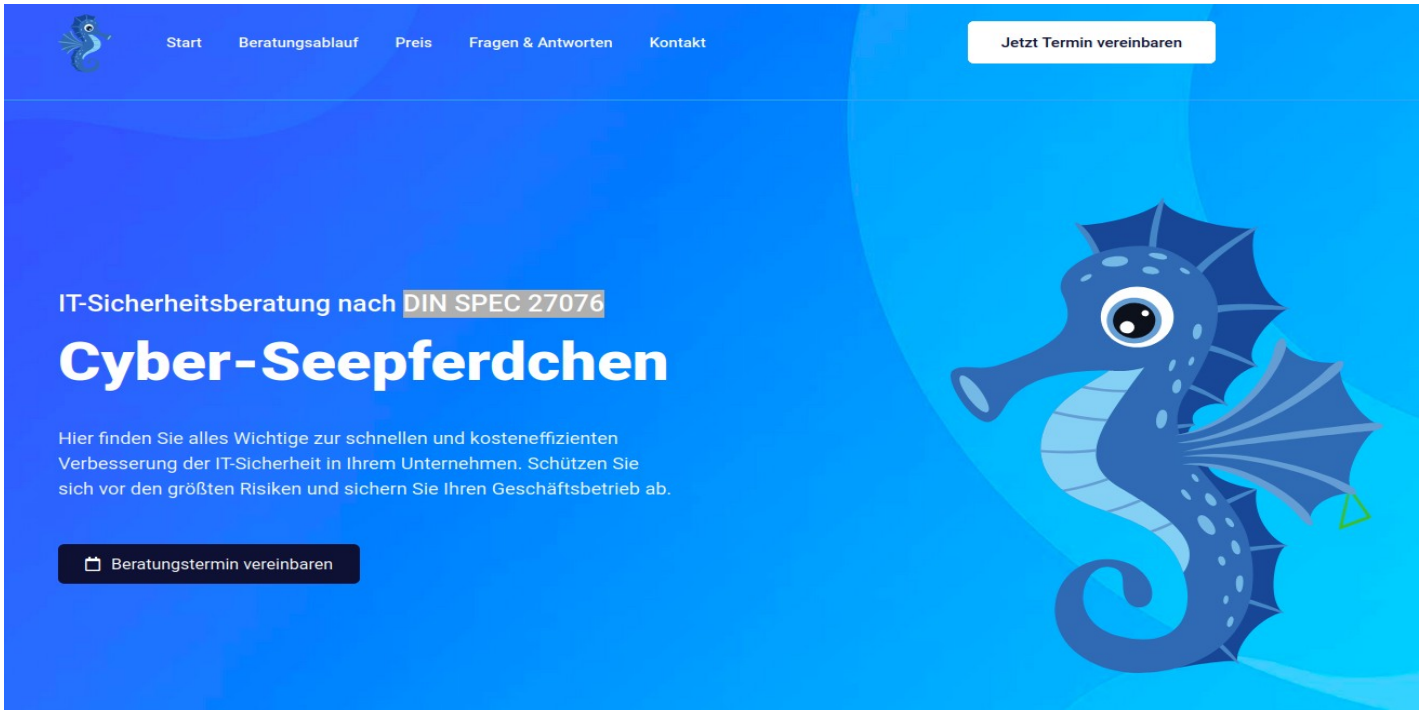


Bild: Lednerb IT-Security GmbH

Das Klassenziel heißt nämlich nicht „Minimum“, sondern gemäß Artikel 32 der Datenschutzgrundverordnung (DSGVO) „Stand der Technik“ (SdT) und diejenige, „die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“, ist „verantwortlich“, dieses Schutzniveau **nachzuweisen**. Dazu verweist das BSI auf das „Handbuch der Rechtsförmlichkeit des Bundesjustizministeriums“ – dort werde der Stand der Technik definiert als: „Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Ziels gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten - wenn dies noch nicht der Fall ist - möglichst in der Praxis mit Erfolg erprobt worden sein."

Wichtig ist Nils Schmidt, Fachanwalt für Arbeitsrecht und Vorstand im DFK – Verband für Fach- und Führungskräfte e.V: "Verantwortlich' zu sein, bedeutet jedoch nicht nur, für eigene Pflichtversäumnisse grade zu stehen, sondern auch für die Versäumnisse derer zu haften, die im Auftrag tätig sind. Das sind Alle, die auf Geheiß der Verantwortlichen an der Planung, Entwicklung, Einrichtung oder Nutzung von Software beteiligt sind, mit deren Hilfe vernetzte Geräte gesteuert oder personenbezogene Daten verarbeitet werden sollen. Innerhalb und außerhalb der eigenen Institution.“

Schwachstellen passen nicht zu diesem Schutzniveau – Fortinet zählt auf: „Schwachstellen bei der Netzwerksicherheit sind eine breite Kategorie von Fehlern, potenziellen Schwachstellen und Schwächen bei Systemhardware, Software, Verwaltung und organisatorischen Richtlinien oder Prozessen.“

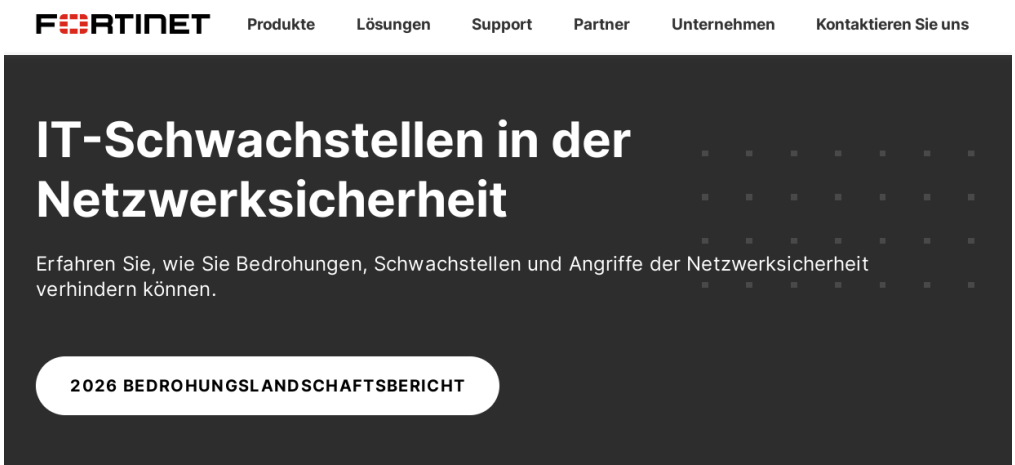


Bild: Fortinet

Das BSI ergänzt: „Auch veraltete Software, die nicht mehr dem Stand der Technik entspricht, ist eine Schwachstelle.“ Bei einer Lünendonk-Umfrage soll jedoch rausgekommen sein, dass 62% der Unternehmen „Teile ihrer geschäftskritischen Anwendungen als veraltet und erneuerungsbedürftig“ ansehen.

Bild: Lünendonk

Mit potentiell tödlichen Konsequenzen: 2021 wurde die Wasserversorgung der Stadt Oldsmar in Florida mit 15.000 Bürgerinnen angegriffen; die Täter hätten versucht, die Konzentration von Natriumhydroxid – besser bekannt als Lauge – um ein Hundertfaches mit Hilfe der virtuellen Gerätesteuerung der Betreiberin aus der Ferne zu erhöhen. Das Einfallstor soll ein Betriebssystem gewesen sein, das seit 2020 nicht mehr von der Entwicklerin unterstützt wird. Die Katastrophe wurde durch einen aufmerksamen Mitarbeiter verhindert, der den Vorgang zufällig am Bildschirm beobachtet und unterbrochen hat.

Hierzulande soll es besser sein: „Die EU stellt sicher, dass Leitungswasser in der gesamten Union bedenkenlos getrunken werden kann“, verspricht der Europäische Rat. Deshalb zählt die „zweite Richtlinie zur Sicherung von Netz- und Informationssystemen“ der EU (NIS-2) die Trinkwasserversorgung zu den „Wesentlichen Einrichtungen“. Und hofft auf „ein hohes gemeinsames Maß an Cybersicherheit“.

Nach Artikel 21 NIS-2 sollen diese Maßnahmen SdT-konform umgesetzt werden:

a)
Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b)
Bewältigung von Sicherheitsvorfällen;

c)
Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d)
Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

e)
Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f)

Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g)
grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h)
Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i)
Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j)
Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

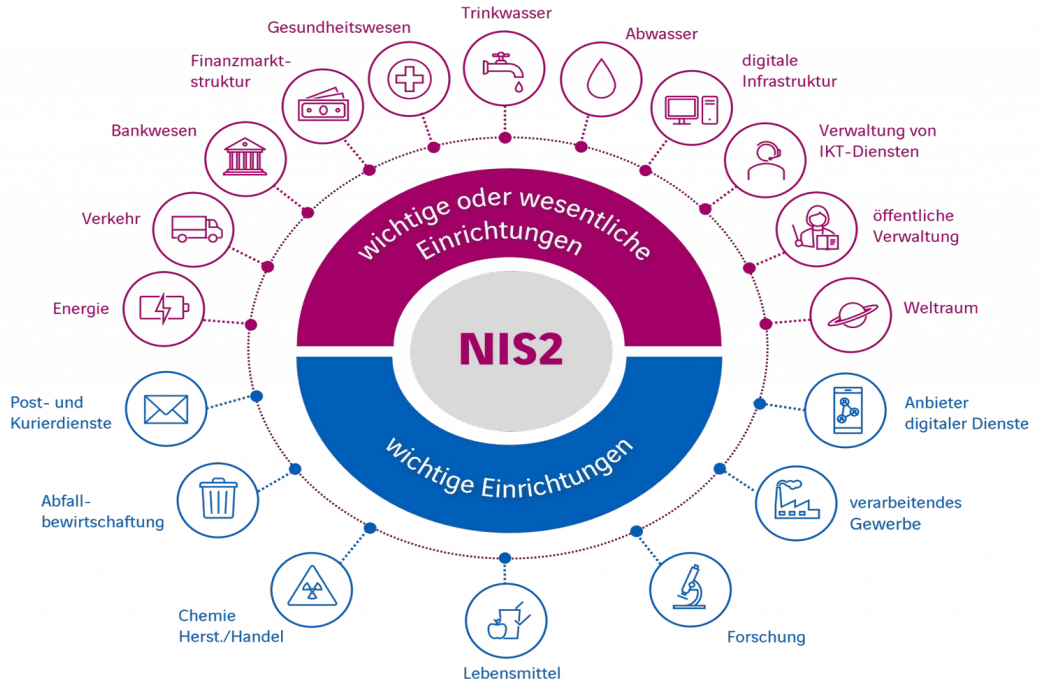
Neben der Trinkwasserversorgung gehören auch Energie, Verkehr, Bankwesen, Gesundheit, Trinkwasser, digitale Infrastruktur, öffentliche Verwaltung und Raumfahrt zu den Wesentlichen Einrichtungen.

Davon sind die Wichtigen Einrichtungen in den Bereichen Post- und Kurierdienste, Abfallwirtschaft, Chemie, Lebensmittel, Maschinenbau und Anbieter digitaler Dienste zu unterscheiden.

Zur „Lieferkette“: Den Mitgliedsstaaten wird geraten, dafür zu sorgen, dass „bestimmte Kleinunternehmen und Kleinstunternehmen“, die eine „Schlüsselrolle für die Gesellschaft, die Wirtschaft oder für bestimmte Sektoren“ einnehmen, „in den Anwendungsbereich dieser Richtlinie fallen“.

Ein Unterschied zwischen beiden Kategorien: Wesentliche Einrichtungen sollten „regelmäßige und gezielte Sicherheitsprüfungen, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden“ erwarten, während die Wichtigen Einrichtungen dem nur ausgesetzt sein sollen, wenn „Nachweise, Hinweise oder Informationen vorgelegt (werden), wonach eine wichtige Einrichtung mutmaßlich dieser Richtlinie […] nicht nachkommt“.

Bild: Axians



Bis 6. März 2026 hätten sich 30.000 Einrichtungen wegen NIS-2 bei einem Portal der Bundesregierung registrieren müssen. Dieser Pflicht sind nach Angaben des Bundesamts für Sicherheit in der Informationstechnik jedoch lediglich 11.500 Einrichtungen nachgekommen.

Das könnte damit zusammenhängen, dass 92 Prozent der Kleinunternehmen nach einer Studie von Schwarz Digits ausschließen, verpflichtet zu sein, „obwohl sie regulierungspflichtig sind“.

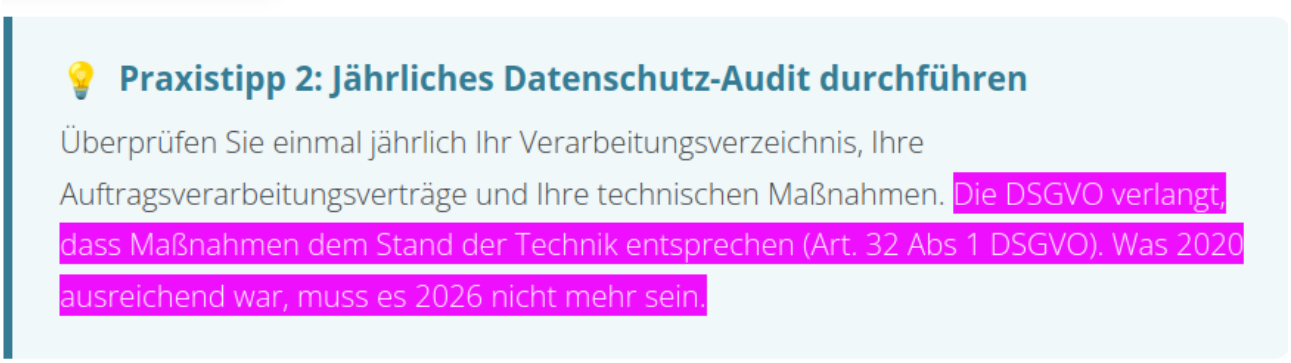
Bereits ein schuldhaftes Versäumen der Registrierungspflicht könnte teuer werden – Anwälte der Kanzlei SKW Schwarz stellen fest: „Formal juristisch gesehen stellt eine verspätete Registrierung bereits den ersten bußgeldbewährten Verstoß dar (bis zu 500.000 €).“ Und darüberhinaus eine Sicherheitsüberprüfung begründen.

Christian Müller, Co-CEO von Schwarz Digits mahnt: „Wer NIS-2 als bürokratische Last missversteht, riskiert nicht nur schmerzhafte Sanktionen, sondern die operative Substanz seines Unternehmens.“

Dieses Risiko wächst – im April wurde bekannt, dass Claude Mythos – eine KI von Anthropic – „tausende’ schwerwiegende Schwachstellen entdeckt“ habe – „darunter in jedem breit genutzten Betriebssystem und Webbrowser.“ Und dass Unbefugte Zugriff auf eben dieses mächtige Werkzeug hatten!

Die technische Leistungsfähigkeit unterstreicht die Beweglichkeit des Ziels „Stand der Technik“ – deshalb rät die BRANDAUER Rechtsanwälte GmbH, ein „jährliches Datenschutz-Audit durchführen“:

„Überprüfen Sie einmal jährlich Ihr Verarbeitungsverzeichnis, Ihre Auftragsverarbeitungsverträge und Ihre technischen Maßnahmen. Die DSGVO verlangt, dass Maßnahmen dem Stand der Technik entsprechen (Art. 32 Abs 1 DSGVO). Was 2020 ausreichend war, muss es 2026 nicht mehr sein.“ Gut möglich, dass die Rechtsanwälte zu den oben genannten „führenden Fachleuten“ gehören.



Während die Verpflichteten mit ihren Pflichten hadern, dreht sich die Welt unaufhörlich weiter – Marktforscher jubelten im April 2026 über die „nächste Welle hypervernetzter Innovationen“ die uns mit der neuen Mobilfunkgeneration 5G ins Haus stehen soll: Eine Million Geräte pro Quadratkilometer sollen künftig per Funk vernetzt und die Kommunikation zwischendrin mit Hilfe der Quanten-KI-Cloud ausgewertet werden: „Dies umfasst eine breite Palette von Komponenten wie NFC-Tags, Sensoren, Mikrocomputer, tragbare Geräte, Industrieroboter, Hausautomationsgeräte und Fahrzeuge. Außerdem sind vielfältige Akteure des IoT beteiligt, darunter Privatpersonen, Unternehmen und öffentliche Verwaltungen.“

Pessimisten befürchten jedoch, dass sich so ein schlaues Auto Schadsoftware an einer schlauen Verkehrsampel einfangen und mit dieser anschließend weitere Fahrzeuge infizieren könnte.

Im Gesundheitswesen ist das ähnlich: Diabetiker benötigen ihr Insulin zum exakten Zeitpunkt und in genauer Dosierung. Medizinische Implantate könnten den Patientinnen das Leben erleichtern. Vorausgesetzt, dass niemand einen Cyberangriff auf das Implantat unternimmt.

Wenn Pizzabuden ihre Ware mit Hilfe von Robotern ausliefern, ist es wichtig, dass sich der Automat an Verkehrsregeln hält – und nicht bösartig von Dritten plötzlich auf die Hauptstraße gelenkt werden kann.

Bild: Coco Robotics

UNO-Generalsekretär António Guterres befürchtet den böswilligen Einsatz von KI-Systemen „zu terroristischen, kriminellen oder staatlichen Zwecken“ was „ein schreckliches Ausmaß an Tod und Zerstörung, ein weit verbreitetes Trauma und tiefe psychologische Schäden in unvorstellbarem Ausmaß verursachen“ könnte.

Gerald Spindler, Professor für Telekommunikationsrecht der Universität Göttingen bewertet IT-Sicherheitslücken von „Hardwareprodukten“ deshalb als „Konstruktionsfehler", „wenn bei der Inverkehrgabe des Produktes nicht der Stand von Wissenschaft und Technik berücksichtigt wurde“. Solche Konstruktionsfehler können Schadenersatzklagen begründen – auch gegen die Verantwortliche persönlich.

Daher sollten diese die Definition des Justizministeriums zum „**Stand von Wissenschaft und Technik“** zur Kenntnis nehmen; das ist demnach der „Entwicklungsstand fortschrittlichster Verfahren, Einrichtungen und Betriebsweisen, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlich vertretbarer Erkenntnisse im Hinblick auf das

gesetzlich vorgegebene Ziel für erforderlich gehalten werden und das Erreichen dieses Ziels gesichert erscheinen lassen. Dabei können im Bereich der Gefahrenabwehr wirtschaftliche Gesichtspunkte – als Teil der Verhältnismäßigkeitserwägungen – keine Rolle spielen. Im Bereich der Vorsorge hat diese Vorrang vor wirtschaftlichen Gesichtspunkten."

Wer hypervernetzte Dinge verkauft/betreibt, muss für Sicherheit sorgen. In Echtzeit. Über die gesamte Lieferkette. Wirtschaftliche Gesichtspunkte können da keine Rolle spielen. Das sollten wir nicht nur den heute Verantwortlichen sagen, sondern auch den Erstsemestern der Natur- und Geistswissenschaften, die in fünf Jahren – etwa als Jungunternehmerin! – Verantwortung übernehmen wollen. Denn sonst erhalten sie kein (Wachstums-)Kapital und riskieren den Schutz der Cyberversicherung.

Bild: **DALL-E**