Jetzt kommt die DSGVO 2.0

Die sogenannte NIS-2-Richtlinie der Europäischen Union sorgt für Unruhe in der deutschen Wirtschaft. Die Anforderungen an die IT-Sicherheit steigen. Viele Unternehmen kämpfen mit der Umsetzung – dabei ist die Bundesregierung selbst spät dran.

Von Corinna Budras, Berlin, und Maximilian Sachse, Frankfurt

Vernetzte Medizin in Frankfurt: *Die IT der Uniklinik lag nach einem Hackerangriff Monate lang lahm.* Foto Lando Hass

An den 8. Oktober 2023 kann Hannah Trenk sich noch gut erinnern. An diesem Tag legten Hacker die Uniklinik Frankfurt lahm. Die Auswirkungen sollten noch über Monate zu spüren sein. Das weiß Trenk damals zwar noch nicht. Aber: „Wir hatten das Gefühl, die Gefahr rückt immer näher an uns heran“, sagt Trenk, die für das Rheumazentrum Mittelhessen das Krankenhausmanagement mitverantwortet. Es ist der letzte Anstoß für die kleine Klinik mit 80 Betten und gut 200 Mitarbeitern, sich eingehender mit der Abwehr vor Hackerangriffen zu beschäftigen – eine Aufgabe, wie Trenk schnell feststellte, zu der die Klinik bald ohnehin von der Europäischen Union verpflichtet sein würde.

Denn mit der neuen Netzwerk- und Informationssicherheitsrichtlinie (NIS-2) weitet die EU die Anforderungen an die IT-Sicherheit deutlich aus. Waren von der vorherigen Regulierung noch weniger als 2000 Unternehmen – vor allem aus der kritischen Infrastruktur – betroffen, dürften es im Falle von NIS-2 Zehntausende Unternehmen mehr sein, schätzt das für die Umsetzung zuständige Bundesinnenministerium. Doch längst nicht alle davon sind so gut vorbereitet wie Hannah Trenk.

Wer mindestens zehn Millionen Euro Jahresumsatz erzielt und 50 Mitarbeiter beschäftigt, fällt unter die neuen Regeln – sofern er in einer als sicherheitsrelevant eingestuften Branche tätig ist. Und diese Sicherheitsrelevanz ist überaus breit gefasst: Neben der Energie- und Wasserwirtschaft geht es um Postdienste, um Banken und Finanzdienstleister, Maschinen- und Fahrzeughersteller, um Teile des Handels. Weil auch digitale Infrastrukturen besser geschützt werden sollen, können selbst Unternehmen aus ganz anderen Branchen durch die Hintertür betroffen sein, etwa weil sie Onlinemarktplätze betreiben oder Cloud-Produkte verkaufen.

Bis zum 17. Oktober muss die Bundesregierung die Richtlinie eigentlich ins deutsche Recht umsetzen, doch diese Frist ist nicht zu halten. Das Bundeskabinett hat das entsprechende Gesetz erst Ende Juli verabschiedet, jetzt muss es erst seine parlamentarischen Runden drehen. Der Bundestag hat sich vergangenen Freitag das erste Mal damit befasst, erst im Frühjahr 2025 ist mit dem Inkrafttreten des Gesetzes zu rechnen. An einigen Stellen fehle es an notwendigen Klarstellungen, moniert etwa der Branchenverband Bitkom. So müsse sichergestellt werden, dass die Hersteller bei der notwendigen Prüfung durch das Bundesamt für Sicherheit in der Informationstechnik keine sensiblen Geschäftsgeheimnisse offenbaren müssen. Auf Kritik stößt in der Digitalbranche außerdem die Ausnahme für die Bundesverwaltung.

„Sehr viele Unternehmen haben vermutlich noch nicht auf dem Schirm, dass sie unter die NIS-2-Richtlinie fallen“, sagt Patrick Grosmann, Rechtsanwalt der Kanzlei FPS in Frankfurt und spezialisiert auf datenschutzrechtliche Anforderungen und das IT-Sicherheitsrecht. Eine Umfrage des IT-Unternehmens Veeam unter europäischen Unternehmen ergab zuletzt, dass bis zu zwei Drittel die Umsetzung der Regeln bis zum 18. Oktober verpassen werden. „Die Unternehmen sind in den Vorbereitungen auf die NIS-2 weit hinterher“, sagt auch Kilian Schmidt, Gründer des Compliance-Start-ups Kertos. Nicht umsonst werde NIS-2 als der „DSGVO-Moment der Informationssicherheit“ bezeichnet. Auch bei der Umsetzung der Datenschutzgrundverordnung hätten Unternehmen zu spät reagiert. Die Umsetzung könne Monate in Anspruch nehmen.

Dabei kann das Missachten der neuen Regeln teuer werden: Es drohen Bußgelder von bis zu zehn Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes. Geschäftsführer sind persönlich verpflichtet, die Maßnahmen umzusetzen und zu überwachen – tun sie das nicht, haften sie persönlich. Die konkrete Ausgestaltung der Haftungsregelung werde sich im Laufe des Gesetzgebungsverfahrens herauskristallisieren, sagt Anwalt Grosmann. Sein Arbeitsalltag besteht aktuell vor allem daraus, für Unternehmen zu prüfen, ob sie in den Anwendungsbereich fallen. Manchmal sei das keine so leichte Aufgabe. Länder wie Belgien, Tschechien und Ungarn haben zum Beispiel schon Gesetze verabschiedet – wer dort mit Gesellschaften aktiv ist, muss sich an geltendes Recht halten.

Auch wer die neuen Anforderungen kennt, steht vor einer Herausforderung. „Kleinen Krankenhäusern wie unserem fällt die Umsetzung besonders schwer, denn wir müssen einen unheimlich hohen Aufwand betreiben, um die Einhaltung der Richtlinie bewerkstelligen zu können“, sagt Klinikmanagerin Trenk. Sie ist nicht allein mit dieser Einschätzung, weiß Daniel Graßer, IT-Sicherheitsexperte für den Kölner Cloud-Anbieter Plusserver. „Mit den Anforderungen von NIS-2 tut sich vor allem der kleinere Mittelstand mit 100 bis 500 Mitarbeitern schwer“, sagt er. Oft liege die IT-Sicherheit in den Händen kleiner Teams. „Die sind häufig mit hochkomplexen IT-Sicherheitslösungen aufgrund des Personalmangels überfordert.“

Zumal die Anforderungen im Vagen bleiben. Brüssel verlangt „angemessene Maßnahmen“. Es geht um Mindestanforderungen wie ein Konzept zum Risikomanagement, zum Einsatz von Kryptographie, zur Notfallkommunikation. Ob die Maßnahmen genügen, müssen Unternehmen anhand der eigenen Risikoeinschätzung selbst bewerten. Das macht Aufwand und Kosten vorab schwer einschätzbar.

Das Rheumazentrum Mittelhessen hat keine eigene IT-Abteilung, Trenk wandte sich deshalb an ihren IT-Dienstleister Netgo. Mit diesem organisierte das Klinikum sogenannte Penetrationstests, mit denen professionelle Hacker versuchen, in die Systeme einer Organisation zu gelangen. Danach kann das Unternehmen etwaige Lücken schließen und Sicherheitskonzepte entwickeln. Zudem engagierte das Rheumazentrum einen Drittanbieter, der die IT des Klinikums jede Stunde die Woche überwacht und im Notfall eingreifen kann. Alles in allem sei das eine „Wahnsinnsinvestition“ gewesen, sagt Trenk. Aber sie sei es wert. „Wenn unsere Daten verschlüsselt werden, sind unsere Patienten in Gefahr.“ Gibt es Allergien? Welche Dosierungen eines Medikamentes wurden verabreicht? Das alles sei dann nicht mehr auffindbar.

IT-Sicherheitsanbieter wissen um diese Not vieler Betriebe. IT-Sicherheitsexperte Daniel Graßer spricht von Goldgräberstimmung. Je näher der Implementationstermin rückte, desto stärker haben die Anbieter an der Preisschraube gedreht. Wie jede neue Compliance-Verordnung steigert NIS-2 die Nachfrage nach IT-Unterstützung.

Bleibt die Frage: Was nützt das Ganze? Dass Unternehmen sich besser gegen Hackerangriffe wappnen müssen, steht außer Frage. Spionage, Sabotage und Datendiebstahl haben in der deutschen Wirtschaft zuletzt im Jahr nach Schätzungen des Digitalverbands Bitkom Rekordschäden über 267 Milliarden Euro verursacht, einen großen Teil davon durch Cyberangriffe. Und jahrelang haben deutsche Unternehmen nach Ansicht von Bitkom zu wenig in ihre IT-Sicherheit investiert, auch wenn sich das langsam ändert.

NIS-2 sei eine gute Leitplanke für Unternehmen und verpflichte dazu, sich mit den eigenen Cyberrisiken zu beschäftigen, sagt IT-Sicherheitsexperte Graßer. Nur: Allein die Konzepte in der Schublade zu haben reiche nicht, sagt René Skotnik, der für die Netgo-Gesellschaft Sila Consulting Unternehmen zu Cybersicherheit berät. Es gehe vor allem um die Umsetzung in der Praxis. Auch er fühlt sich an die DSGVO erinnert. „Da hat es auch viele Unternehmen gegeben, die gegen Geld einen externen Datenschutzbeauftragten engagiert haben, der auf dem Papier für den Datenschutz geradesteht.“ Ob die Daten dadurch wirklich besser geschützt seien? Zweifelhaft.

Viele in der Digitalbranche stellen sich zudem die Frage, wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) das alles überprüfen soll. Die Aufgaben des BSI sind in den vergangenen Jahren deutlich angewachsen, jetzt erhält es abermals weitreichendere Befugnisse. In der IT-Branche wird bezweifelt, dass dafür die Ressourcen im BSI ausreichen. Hannah Trenk ist das letzten Endes egal. Sie will einfach, dass ihre Klinik so gut wie möglich vor Hackerangriffen geschützt ist. Einen Fall wie am Uniklinikum in Frankfurt will sie nicht erleben.