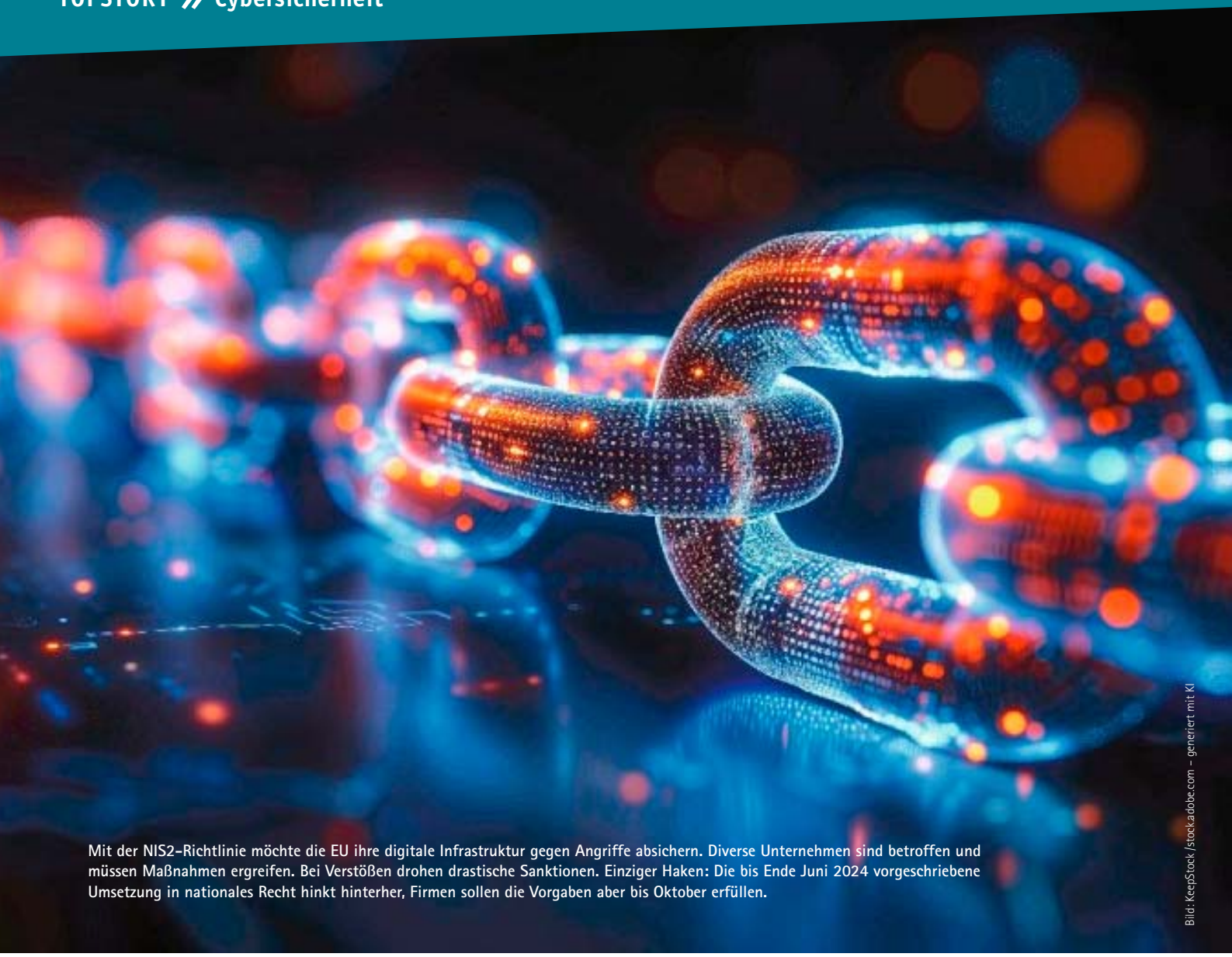

Mit der NIS2-Richtlinie möchte die EU ihre digitale Infrastruktur gegen Angriffe absichern. Diverse Unternehmen sind betroffen und müssen Maßnahmen ergreifen. Bei Verstößen drohen drastische Sanktionen. Einziger Haken: Die bis Ende Juni 2024 vorgeschriebene Umsetzung in nationales Recht hinkt hinterher, Firmen sollen die Vorgaben aber bis Oktober erfüllen.

Bild: KeepStock /stock.adobe.com – generiert mit KI

EU-Richtlinie Cybersecurity: 30.000 Firmen müssen handeln – Stichtag ist Oktober 2024

Schutzschild und Damoklesschwert

Cyberangriffe bedrohen die deutsche Wirtschaft und verursachen erhebliche Schäden. 45 % der angegriffenen Unternehmen fürchten anschließend um ihre Existenz. Vor diesem Hintergrund müssen Unternehmen angemessene Maßnahmen ergreifen, um ihre digitale Infrastruktur zu schützen. Doch die dafür verabschiedete EU-Richtlinie „NIS2“ ist nicht ohne und verlangt ihnen einiges ab.

» Hertha Kerz, freie Fachjournalistin in Hamburg

Die erste NIS-Richtlinie stammt aus dem Jahre 2016 und wurde in überarbeiteter Form im Dezember neu veröffentlicht (NIS2). „NIS" steht für „Network and Information Systems". Was diese Vorgabe will, hat sich nicht verändert. Das Bundesamt für Sicherheit in der Informationstechnik (BIS) umschreibt Sinn und Zweck in einer einzigen, wuchtigen Definition: „EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union".

Die NIS musste angepasst werden, weil die Überwachung ihrer Umsetzung nicht lückenlos, das Offenlegen von Sicherheitsvorfällen nicht gewährleistet und manche Regelungen mehrdeutig waren. Das Ziel soll aber maximale Cyberresilienz sein. Alle EU-Mitgliedstaaten sind nun verpflichtet, die NIS2 bis zum 27.7.24 in nationales Recht umzusetzen, damit die Unternehmen sie bis Oktober 2024 implementieren. Es gibt keine Karenzzeiten oder Übergangsfristen.

Flankiert wird die NIS2 von drei weiteren Regelungen, auf die wir der Übersichtlichkeit halber nur online eingehen (mit weiterführenden Hinweisen): dem NIS2UmsuCG, der RCE/CER-Richtlinie und dem Kritis-DachG – Tabelle 1*. Wird von der NIS2 gesprochen, sind also vier Richtlinien und Gesetze gemeint. Sie korrelieren in ihrer Umsetzung mit der Cybersicherheitsagenda der Bundesregierung von 2022 (Tabelle 2*).

Wird der Zeitplan eingehalten?

Viele Gründe stehen jedoch dem Umsetzungstermin entgegen. Denn NIS2 ist (zu) komplex. Die Zusammenarbeit zwischen Regierungen, Unternehmen und Aufsichtsbehörden gestaltet sich zeitraubend, die Realisierung der technischen und organisatorischen Maßnahmen in den Unternehmen ist zeit- und ressourcenintensiv sowie teuer. Und das Dachgesetz für kritische Infrastrukturen (Kritis-DachG) befindet sich erst im Entwurfsstadium. Dazu kann das NIS2UmsuCG mit hoher Wahrscheinlichkeit nicht im Oktober 2024 in Kraft treten, da aktuell erst der zweite Referentenentwurf im Bundestag diskutiert wird. Der Lauf durch die politischen Instanzen bis zur Verabschiedung des Gesetzes im Oktober 2024 ist in Deutschland nicht zu schaffen.

Cybersecurity geht alle an

„Kriegstüchtig" zu werden, ist wieder Thema. Nicht ohne Grund. Auch in der Cyberwelt tobt längst ein Krieg und gefährdet Unternehmen. Die EU geht zurecht dagegen vor mit ihrer NIS2-Richtlinie. Nur scheint die Politik mit dem Umsetzen überfordert – und das droht nun auch der Industrie. Hier hilft nur noch ein Appell: Der Staat muss unter die Arme greifen, sonst geht es schief. Firmen ist zu raten, was die Fachautorin im Resümee schreibt (online: https://hier.pro/ELs85): Zügig informieren, tätig werden, Verbände aktivieren und Anwälte bereit halten.

Bild: Tom Oettle

Olaf Stauß,
Redaktion Industrieanzeiger

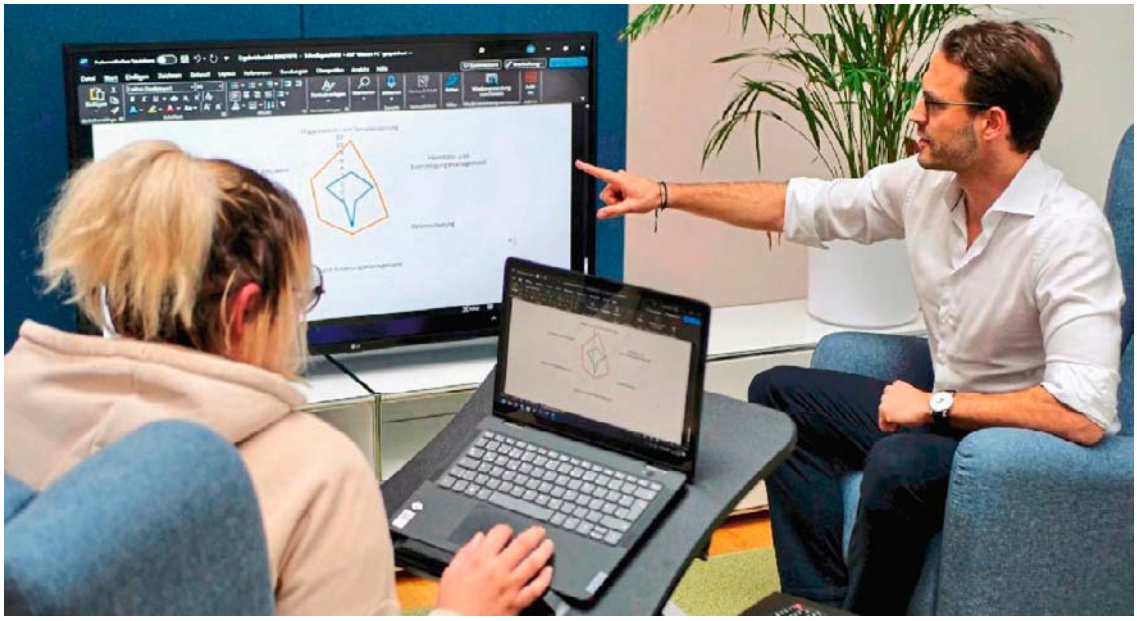

Bild: ItecoConsult

Der Run auf IT-Partner wie ItecoConsult hat begonnen, um die NIS2-Richtlinie erfolgreich umzusetzen. Geschätzt sind 30.000 Unternehmen betroffen, 25.000 auf der Suche nach Unterstützung.

„Unternehmen sollten möglichst früh festlegen, welche Aufgaben sie vergeben", rät Frank Kracht von ItecoConsult. Für KMU empfiehlt er den Cyberresilienzcheck nach DIN SPEC 27076 – einem standardisierten Verfahren.

Bild: Kracht, ItecoConsult

Dazu müssen die Mitgliedsstaaten eine NIS-Behörde und ein „Computer Security Incident Response Team" (CSIRT) einrichten. Das ist eine Gruppe von IT-Fachleuten, die helfen, für Notfälle der Cybersicherheit vorzubeugen oder sie zu bewältigen. Das CSIRT koordiniert die Maßnahmen bei der Reaktion auf Sicherheitsvorfälle. Seine Hauptaufgabe besteht darin, die Kontrolle wiederzuerlangen und Schäden zu minimieren (Tabelle 3*).

Welche Unternehmen betroffen sind

Die Richtlinie betrifft grundsätzlich alle Betreiber kritischer Infrastrukturen (Kritis) und darüber hinaus die Betreiber wichtiger und wesentlicher (digitaler) Dienste. Wer konkret betroffen ist, lässt sich nicht in einem Satz sagen. Bei den „Essential Entities" sind es beispielsweise Unternehmen mit über 250 Mitarbeitern, 50 Mio. Euro Umsatz oder 43 Mio. Euro Bilanzwert. Doch daneben gibt es noch „Important Entities" und mittlere Firmen mit wieder anderen Klassifizierungen. Insgesamt, so wird geschätzt, fallen 30.000 Unternehmen unter die NIS2-Richtlinie. Wer nicht genau weiß, ob seine Firma gefordert ist, sollte dies über einen externen Dienstleister oder das BSI für sich klären.

Was auf Firmen zukommt

Von diesen Unternehmen fordert das NIS2 umfangreiche technische, operative und organisatorische Maßnahmen, um die Cybersicherheit zu stärken. Dazu gehört ein Risikomanagement für Netzwerke und die Sicherheit in der Lieferkette. Ebenso Pläne, um auf Angriffe schnell reagieren und so die Geschäftskontinuität sicherstellen zu können.

Das Risikomanagement sieht beispielsweise monatliche interne Sicherheitsüberprüfungen vor. Veraltete Software etwa auf Unternehmenscomputern ist ein potenzielles Sicherheitsrisiko, das es zu identifizieren und bewerten gilt. Als Konsequenz muss die Software schnellstmöglich upgedatet oder gar entfernt werden. Diese proaktive Herangehensweise kann potenzielle Risiken frühzeitig erkennen und beheben.

Gleiche Szenarien finden sich für das Lieferkettenmanagement. Hier geht es darum, auch die Zulieferer einzubinden. Das Unternehmen wird zum Beispiel vertraglich festlegen, dass der Zulieferer regelmäßige Sicherheitsüberprüfungen durchführt, Richtlinien einhält und im Falle von Sicherheitsvorfällen angemessen reagiert. Solche Maßnahmen minimieren das Risiko von Cyberangriffen innerhalb der Lieferkette

Der aktuelle Stand

Dieser Artikel bietet einen Überblick über die NIS-2-Richtlinie in ihrer aktuellen Fassung. Die dazugehörigen Gesetze und Vorschriften befinden sich jedoch im Fluss. Es ist zu empfehlen, sich auf dem Laufenden zu halten. Eine zuverlässige Quelle ist beispielsweise die AG Kritis: https://ag.kritis.info/?s=nis2

und stärken die Cybersicherheit des eigenen Unternehmens.

Eine Maßnahme, um die Geschäftskontinuität abzusichern, wäre die Implementierung eines „Business Continuity Management Systems" (BCMS). Mit „Business Impact Analysen" (BIA) prüft das Unternehmen regelmäßig, wie es auf unvorhergesehene Ereignisse wie Cyberangriffe oder Naturkatastrophen reagieren und handlungsfähig bleiben könnte. Basierend auf diesen Analysen zielen Maßnahmen darauf ab, die Geschäftskontinuität zu gewährleisten.

Dies können Backup-Systeme, Notfallpläne, Schulungen für Mitarbeiter sowie regelmäßige Tests und Übungen sein, um die Wirksamkeit der Maßnahmen zu überprüfen. So stellt das Unternehmen sicher, dass es auch in Krisensituationen resilient bleibt und seine Geschäftstätigkeit aufrechterhalten kann (Tabelle 4*).

Hier haben es Unternehmen einfacher, die sich schon mit NIS1 auseinandersetzen mussten. „Aus technischer Sicht gibt es zwischen dem Vorgänger NIS1 und NIS2 nicht besonders große Unterschiede", sagt Frank Kracht, Geschäftsführer der ITecoConsult GmbH & Co. KG, die technische Expertise mit ökonomischem Anspruch vereint. ITecoConsult bietet seit über 20 Jahren IT-Beratung, Systemtechnik und Prozessdesign an. „Ein Cyberangriff ist eine echte Gefahr für den Fortbestand eines Unternehmens und ein Risiko für die Lieferkette. Wer NIS1 erfüllt, wird mit dem Nachfolger wenig Probleme haben", ermutigt Kracht die Firmen, am Ball zu bleiben.

Doch können Unternehmen, die sich nie mit diesem Themenkomplex auseinandersetzen mussten, die Richtlinie überhaupt umsetzen? „Grundsätzlich sind die genannten Themen der EU-Richtlinie für Experten greifbar, also auch umsetzbar", meint Benjamin Richter, Geschäftsführer der Cyber Complete GmbH. Cyber Complete ist auf Projekte im Bereich Informationssicherheit spezialisiert und Teil der ComSec-Gruppe. Die Security-Experten verfolgen einen ganzheitlichen Ansatz zur Informationssicherheit und bieten Dienstleistungen zu Themen wie ISO 27001, NIS2, TISAX und Datenschutz an. Sie führen auch Fortbildungen und Trainings im Bereich Informationstechnologie und Datenschutz durch.

Die Umsetzung der Richtlinie im Unternehmen erfordert die Zusammenarbeit verschiedener Abteilungen und Verantwortlicher unter der Geschäftsleitung (GL). Die GL ist für die Einführung der Richtlinie und die Bereitstellung benötigter Ressourcen verantwortlich. Und: „NIS2 erwartet von der Geschäftsführung, dass sie sich in der Cybersecurity weiterbildet, um Gefahren und Risiken zu bewerten", erklärt Kracht. Ein Geschäftsführer wird dadurch aber nicht schon zum IT-Spezialisten – und das könnte ihm die qualitative Bewertung von Gefahren und Risiken faktisch unmöglich machen. „Viele IT-Abteilungen arbeiten aufgrund des Fachkräftemangels am Limit, so dass eine NIS2-Implementierung ohne externe Hilfe schwer umzusetzen ist", konstatiert Kracht.

Nicht ohne externe Dienstleister

Nicht wenige suchen deshalb Unterstützung bei externen Dienstleistern. Aber das Feld der Anbieter ist groß. So sind in Deutschland rund 25.000 Unternehmen auf der Suche nach einem IT-Partner. Denn das Umsetzen der Richtlinie steht und fällt mit der eigenen IT-Abteilung (die aber häufig nicht genau weiß, was im Einzelnen getan werden muss) beziehungsweise der kompetenten Unterstützung durch einen externen IT-Dienstleister. Die weitere Geschäftstätigkeit hängt davon ab, ob die Vorgaben der Richtlinie implementiert werden.

Bild: Richter, Cyber Complete

„Grundsätzlich sind die Maßnahmen der EU-Richtlinie für Experten greifbar und also auch umsetzbar", meint Benjamin Richter, Geschäftsführer von Cyber Complete.

Bild: Schäfers

Tim Philipp Schäfers, renommierter White-Hat-Hacker, erklärt seinen Job: „Unternehmen zahlen Geld für valide gemeldete kritische Schwachstellen – eine Art Finderlohn."

Bild: Dr. Daily

Dr. Christoph Dally, Fachanwalt für IT-Recht: „Das Thema NIS2 ist als geschäftskritisch zu behandeln."

Die Auswahl sollte aber nicht überstürzt stattfinden. „Der Dienstleister sollte bereits einiges an Erfahrung mitbringen und nicht triviale Projekte erfolgreich durchgeführt haben", sagt Richter. „Bei sogenannten ‚One-Man-Shows' wäre ich vorsichtig. Nicht wegen fehlendem Know-how sondern im Blick auf mögliche Vertretungen oder potenziell längerfristige Arbeitsausfälle."

Bei der Auswahl eines externen IT-Dienstleisters empfiehlt es sich, bestimmte Kriterien zu berücksichtigen, um den Anforderungen der NIS-2-Richtlinie gerecht zu werden. Dazu zählen Erfahrung und Expertise des Dienstleisters in der Cybersicherheit, seine Zuverlässigkeit und Reputation sowie das Einhalten von Compliance-Standards und relevante Zertifizierungen. Weitere Aspekte sind ein effektiver Kundensupport mit angemessener Reaktionszeit, Anpassungsfähigkeit an individuelle Anforderungen sowie eine transparente Kommunikation und klare Berichterstattung über Sicherheitsmaßnahmen. Dann ist der Grund gelegt für eine erfolgreiche Partnerschaft mit dem IT-Dienstleister.

„In den meisten Fällen findet ein Auftakt-Workshop vor Ort statt, um den Kunden kennenzulernen und schnellstmöglich den Status Quo zu ermitteln", erklärt Richter. „Danach entwickeln wir gemeinsam einen realistischen Projektplan. Hierfür haben wir Checklisten entwickelt."

Und Frank Kracht ergänzt: „Unternehmen sollten möglichst früh festlegen, welche Aufgaben sie nach außen vergeben." Für KMU empfiehlt er den Cyberresilienzcheck nach DIN SPEC 27076. „Er analysiert die Cyberresilienz nach einem standardisierten Verfahren. Der Abschlussbericht beinhaltet eine Punkteauswertung und visualisiert die aktuellen Cyberrisiken. Er listet die notwendigen Maßnahmen nach ihrer Priorität auf und benennt mögliche Fördermittel."

Unternehmen können den Cyberrisiko-Check auch vom BSI durchführen lassen. Die Behörde bietet auch entsprechende Weiterbildungen an. Eigenständig durchführen lässt sich der Check aber nur, wenn das IT-Personal das dafür nötige Wissen hat.

Hohe Kosten für Unternehmen

Mit dem Umsetzen der Richtlinie sind Kosten und oft umfangreiche strukturelle Anpassungen verbunden – Tabelle 5*. Wichtig ist, wie flexibel sich angebotene Lösungen an die spezifischen Anforderungen anpassen und wie gut integrieren lassen. „Da wir uns immer in bestehenden IT-Umgebungen befinden, versuchen wir so minimalinvasiv wie möglich zu arbeiten", versichert Kracht. „Wir arbeiten möglichst 'agent less' und setzen auf Schnittstellen wie WMI, SNMP und APIs bestehender Systeme." Und Benjamin Richter von Cyber Complete ergänzt: „Im Gegensatz zu großen Systemhäusern stellen wir uns komplett auf den Kunden ein und versuchen ihm nicht unsere Standard-Software aufzuzwängen. Als ein agiles Team können wir uns auch mit Kundensoftware beschäftigen, die kein Standard ist."

Das hört sich alles sehr teuer an – und es ist teuer, bestätigt Richter. „Auch bei kleinen Unternehmen liegen die Kosten im fünfstelligen Bereich, sollte dort noch keine Basis für Informationssicherheit vorhanden sein. Bei größeren Unternehmen können sehr schnell sechsstellige Summen zusammenkommen."

NIS2 – Bürde und Chance

Die anfallenden Kosten lassen sich nicht generell beziffern. Die NIS2 betrifft weit über 30.000 Unternehmen in Deutschland, der Zeitaufwand für ihre Implementierung variiert je nach Sektor, Branche, IT-Infrastruktur, Neustrukturierung der Unternehmensprozesse, Unternehmensgröße und spezifischen Anforderungen zwischen drei Monaten und zwei

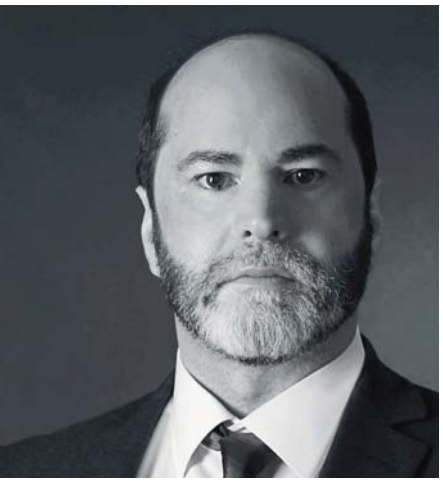

Bild: Ferner

„IT-Sicherheit wird zu einer haftungsträchtigen Aufgabe der Geschäftsleitung", sensibilisiert Jens Ferner, Fachanwalt für IT-Recht.

Jahren. Und der Kunde muss häufig auch nach dem IT-Infrastruktur-Upgrade betreut werden.

So bleiben Dienstleister lange involviert. „Während der Projektphase ist mindestens ein Mitarbeiter fester Ansprechpartner beim Kunden", verspricht Richter. „Nach dem Projekt kommt es auf den Service an, den er benötigt. Das ist je nach Branche und Größe unterschiedlich." Doch auch dabei bleibt es nicht. Die Mitarbeiter müssen mit den neuen IT-Gegebenheiten vertraut gemacht werden. „Wir bieten eine Vielzahl an persönlichen, aber auch an Remote-Schulungen an", sagt Richter.

Die NIS-Richtlinie macht Sinn. Cybersecurity hat schon lange hohen Stellenwert in der Wirtschaft, auch ohne NIS. „In meiner Tätigkeit als BCM-Consultant stelle ich vermehrt fest, dass Cybersicherheit und Datenschutz von Kunden aktiv eingefordert wird", berichtet Frank Kracht. „NIS2 definiert letztlich Mindeststandards an die Cybersicherheit für den Umgang mit Risiken und wird sich zum Wettbewerbsvorteil entwickeln." Und Richter appelliert: „Auch nicht betroffene Unternehmen können sich an dieser Art Framework sehr gut orientieren und danach ihre Informationssicherheit aufbauen."

Cybersecurity will geprüft sein

Viele Unternehmen wollen mehr als ein Upgrade der IT-Infrastruktur. Sie suchen nach Spezialisten, die ihre Systeme auf die Probe stellen – also professionelle Hacker. Leider ist diese Anforderung nicht in der NIS2-Richtlinie verankert. Es ist jedoch entscheidend, nicht nur Upgrades zu installieren, sondern auch ihre Widerstandsfähigkeit zu prüfen. Das tun die IT-Dienstleister intensiv, haben aber meist keine ausgeprägten Hackerfähigkeiten. Und so hat sich der White-Hat-Hacker geradezu als Beruf etabliert.

„In den letzten Jahren erfreuen sich sogenannte Bug Bounty Programme immer größerer Beliebtheit", erklärt Tim Philipp Schäfers, White-Hat-Hacker und IT-Sicherheitsberater. „Dabei zahlen Unternehmen Geld oder vergeben kostenfrei Produkte für valide gemeldete kritische Schwachstellen in ihren IT-Systemen. Also eine Art Finderlohn." Schäfers hat sich hier einen Namen gemacht.

NIS2 schreibt einen Mindeststandard an Informationssicherheit vor. Das schließt auch ein professionelles Patch- und Incidentmanagement ein. Patches und Releases werden von den Softwareherstellern bereitgestellt – vergleichbar mit denen von Microsoft. Allerdings gibt es auch IT-Abteilungen, die unternehmenseigene Software programmieren und damit Patches und Releases selbst entwickeln müssen. „Bei schwerwiegenden Incidents sind Meldepflichten an Aufsichtsbehörden vorgesehen", weiß Schäfers – bei signifikanten Bedrohungen innerhalb von 24 h zur Frühwarnung und innerhalb von 72 h als offizielle Meldung.

Zum Best Practise gehört es, dass Firmen konkrete Ansprechpartner beispielsweise im Bereich Datenschutz benennen. „Bei der Meldung von Schwachstellen stand ich bei größeren Unternehmen häufig vor dem Problem, überhaupt korrekte Ansprechpartner zu finden", beklagt Schäfers.

Cybersicherheit behinhaltet auch, Informationen zu klassifizieren – wie wichtig und wie vertraulich sie sind, und wer welche Berechtigungen hat. „Es geht also nicht nur um den Schutz vor Angriffen von außen, sondern auch von innen", betont Schäfers. „Aber die Mehrzahl der Schäden wird von außen verursacht."

Rechtliche Aspekte und Fallstricke

Von hoher Relevanz sind die rechtlichen Aspekte und Konsequenzen: Überwacht wird das Einhalten der NIS2-Richtlinie vom BSI, dem CSIRT und der Bundesnetzagentur. Diese Institutionen arbeiten eng mit dem BMI zusammen (Tabelle 6*). „Bei Nichteinhaltung sieht der Sanktionskatalog unter anderem Bußgelder von zehn Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes vor", warnt Dr. Christoph Dally, Fachanwalt für IT-Recht. Zudem haften Geschäftsführer auch persönlich.

*Lesen Sie **online** weiter, um mehr über die rechtliche Seite der NIS2 zu erfahren: hier.pro/ELs85. Hier finden Sie auch die **Tabellen mit Hinweisen** und erfahren Resümee und Tipps unserer Fachautorin.