Herausforderung NIS-2: Wie sollen sich betroffene Unternehmen verhalten?

Mag. (FH) Clemens Malt-Burian, MSc.
HMP Beratungs GmbH

Cyberattacken sind für Unternehmen schon längst kein abstraktes Bedrohungsszenario mehr. Die durch die weltweite Covid-Pandemie beschleunigte Digitalisierung hat zu einer neuen Dynamik der Cyber-Kriminalität geführt. Auch Staaten als Angreifer rücken immer mehr in den Fokus. So kam es in Zusammenhang mit dem russischen Überfall auf die Ukraine zu einer massiven Zunahme von Cyberangriffen auf die zivile europäische Infrastruktur, wie Eisenbahnen, Flughäfen und Stromnetzen (J. Bartz et al., 2023). Gemäß einer aktuellen Studie von KPMG haben sich im Jahr 2023 die Cyberangriffe auf österreichische Unternehmen gegenüber dem Vorjahr verdreifacht.

Dabei sind aber nicht nur die großen Anbieter kritischer Infrastrukturen von Cyberangriffen betroffen. Die KPMG-Studie zeigt, dass auch kleine und mittelständische Unternehmen (KMU) attraktive Ziele für Cyberangriffe sind. Zum einen verfügen diese oft über eine unzureichende IT-Sicherheit, zum anderen stellen diese aufgrund ihres spezifischen Know-hows durchaus lukrative Ziele dar. Hinzu kommt, dass die Transport- und Lieferketten aufgrund der zunehmenden Digitalisierung und der wachsenden Vernetzung verwundbarer und damit für Cyberangriffe besonders interessant geworden sind. Statt einen Anbieter kritischer Infrastruktur direkt anzugreifen, werden bei Supply Chain Angriffen gezielt Schwachstellen auf allen Ebenen einer Lieferkette ausgenutzt. Kriminelle Akteure kompromittieren so beispielsweise ein kleines Unternehmen mit einer unzureichend geschützten IT, und dringen dann in der Lieferkette nach oben vor, wobei sie diese

vertrauenswürdigen Beziehungen ausnutzen, um Zugriff auf die Umgebung vorgelagerter Unternehmen zu erhalten (A-SIT Zentrum für sichere Informationstechnologie – Austria, 2022).

Von NIS zu NIS-2

Die Europäische Union hat auf diese Entwicklungen bereits 2016 reagiert und eine Richtlinie für Netzwerk- und Informationssystemsicherheit (NIS) verabschiedet. Diese NIS-Richtlinie wurde später von den EU-Mitgliedstaaten im Rahmen von nationalen NIS-Gesetzen umgesetzt; in Österreich ist das NIS-Gesetz (NISG) im Dezember 2018 in Kraft getreten. Damit wurde ein erster einheitlicher Rechtsrahmen für eine EU-weite Cybersicherheit geschaffen. Sogenannte Betreiber wesentlicher Dienste und digitale Diensteanbieter werden damit zu angemessenen Sicherheitsmaßnahmen und der Meldung erheblicher Störfälle verpflichtet. Zudem wurde damit die Zusammenarbeit mit den nationalen Behörden sowie die Zusammenarbeit zwischen den Mitgliedsstaaten in strategischer und operativer Hinsicht geregelt und gestärkt (Bundeskanzleramt, 2018).

Die Bedrohungslage hat sich seither jedoch weiter verschärft, und die bestehende NIS-Richtlinie wird der aktuellen Situation nicht mehr länger gerecht. Einerseits sind viele Sektoren von NIS gar nicht betroffen, welche aber sehr wohl als potenzielle Angriffsziele gelten und auch im Hinblick auf ein anzustrebendes hohes gesamteuropäisches Sicherheitsniveau als durchaus kritisch zu betrachten sind. So fallen in Österreich etwa Forschungseinrichtungen im Gesundheitsbereich, Telekommunikationsanbieter, Post- und Kurierdienste, der gesamte Lebensmittelsektor oder das produzierende Gewerbe gar nicht in den Anwendungsbereich des NISG, um nur die wichtigsten Sektoren zu nennen. Zudem wurde die NIS-Richtlinie in den einzelnen Mitgliedsstaaten sehr unterschiedlich umgesetzt, was im Gesamtergebnis zu einem sehr heterogenen Schutzniveau führt. Die Europäische Union sah sich daher veranlasst, eine neue NIS-Richtlinie auf den Weg zu bringen. Diese NIS-2 Richtlinie ist nun seit Jänner 2023 in Kraft und soll noch im Oktober 2024 in nationales Recht umgesetzt werden.

Erweiterter Geltungsbereich von NIS-2

Die neue NIS-2 Richtlinie deckt einen wesentlich größeren Anwendungsbereich ab. Das führt nun dazu, dass sehr viele Unternehmen, welche vom bestehenden NISG nicht betroffen sind, von NIS-2 nun betroffen sein werden. Dies trifft auch auf KMU zu. Zwar zieht die NIS-2 Richtlinie eine Grenze – Unternehmen bis 50 Mitarbeiter*innen und 10 Mio. Euro Jahresumsatz sind zunächst einmal nicht betroffen. Gleichzeitig schafft die Richtlinie aber wieder einige Ausnahmen: So sind beispielsweise Vertrauensdiensteanbieter, Anbieter elektronischer Kommunikationsdienste, TLD- und DNS-Diensteanbieter oder generell Anbieter von Services, welche essenziell für die Aufrechterhaltung kritischer gesellschaftlicher Aktivitäten sind, von diesen Schwellwerten ausgenommen. Zudem wird es bei KMU zu einer anteiligen Zurechnung von Partnerunternehmen bzw. zu einer Vollzurechnung von „verbundenen Unternehmen“ (d.h. Konzernunternehmen) kommen. Sind vom aktuellen NISG rund 100 Unternehmen betroffen, gehen Schätzungen bei NIS-2 von 6.000 oder mehr in Österreich betroffenen Unternehmen aus. Darüber hinaus muss damit gerechnet werden, dass Unternehmen unabhängig von ihrer Größe, welche Teil einer Lieferkette von wesentlichen oder wichtigen Einrichtungen sind, von diesen durch vertragliche Vereinbarungen ebenfalls zu umfassenden Cybersecurity-Maßnahmen verpflichtet werden.

Je nach Unternehmensgröße und betroffenem Sektor unterscheidet die NIS-2 Richtlinie zwischen wesentlichen und wichtigen Einrichtungen. Während erstere einer strengeren ex-ante Aufsicht unterliegen und mit einem höheren Strafmaß von bis zu 10 Mio. Euro oder 2 % des weltweiten Umsatzes belangt werden können, unterliegen letztere nur einer ex-post Aufsicht und der

Bußgeldrahmen beträgt auch „nur“ 7 Mio. Euro oder 1,4 % des weltweiten Umsatzes (Bundeskanzleramt, 2024).

Die Vorbereitung auf NIS-2 ist kein IT-Projekt

Im Unterschied zum bestehenden NISG ändert sich bei NIS-2 auch der Fokus: Während sich das aktuelle NISG noch auf primär technische Aspekte konzentriert und meist in der Gesamtverantwortung des CISO angesiedelt ist, macht NIS-2 die oberste Führungsebene eines Unternehmens persönlich für die Umsetzung adäquater Cybersicherheitsmaßnahmen haftbar. Diese müssen stärker als bisher in Sicherheitsprozesse eingebunden sein und geschult werden. Es genügt auch nicht mehr, technische und organisatorische Vorkehrungen nur auf die wesentlichen Dienste eines Unternehmens zu beschränken. Ein betroffenes Unternehmen muss sich mit NIS-2 gesamthaft vor Cyberrisiken schützen und dies auch nachweisen können („*all hazards approach*“). Dies umfasst nicht nur externe Bedrohungen, sondern auch interne Bedrohungen (bspw. durch unachtsame Mitarbeiter*innen) und *force majeure* (z.B. Naturkatastrophen, Pandemien, etc.). Zudem tragen betroffene Unternehmen auch Verantwortung für die Sicherheit der gesamten Lieferkette.

Die erforderlichen Governance- und Risikomanagementmaßnahmen sind in der NIS-2 Richtlinie unter Art. 20 und 21 im Detail beschrieben. Neben der oben bereits erwähnten nachweislichen Verankerung einer Top-Management Governance sowie der Gewährleistung der Cybersicherheit entlang der Lieferkette von Lieferanten und Dienstleistern steht ein umfassendes Risikomanagementsystem im Zentrum der Aufmerksamkeit. Die Richtlinie fordert weiters auch konkrete technische Cybersicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IKT-Systemen, Maßnahmen zur Cyberhygiene (u.a. Gerätekonfiguration, Firewalls, systematische Datensicherung, etc.) sowie Maßnahmen zur Verschlüsselung, Zugriffskontrollen und Multifaktor-Authentifizierung. Ein weiterer zentraler Aspekt ist die Erkennung und Bewältigung von Cybersicherheitsvorfällen, und die damit einhergehende fristgerechte Meldung solcher Vorfälle an die zuständigen Behörden. Ein Business Continuity Management mit Backup- und Wiederherstellungsprozessen, einem IT-Notfallplan und einem funktionierenden Krisenmanagement runden das Maßnahmenpaket ab. Entscheidend wird sein, dass diese Maßnahmen nicht am Papier enden. Diese müssen einerseits von umfassenden Schulungsmaßnahmen begleitet sein, und andererseits ist die Wirkung gesetzter Maßnahmen laufend zu überprüfen und der Ernstfall regelmäßig zu üben.

Viele von NIS-2 potenziell betroffene Unternehmen sind nun mit großen Herausforderungen und damit verbundenen Unsicherheiten konfrontiert:

- Anders als beim bestehenden NISG dürfen betroffene Unternehmen nicht darauf hoffen, einen behördlichen Bescheid zu erhalten. Sie sind selbst dafür verantwortlich zu beurteilen, ob sie von NIS-2 betroffen sind.
- Die Auslegung des NIS-2 Gesetzes ist noch offen, gleichzeitig müssen betroffene Unternehmen aber bereits jetzt aktiv werden, um im besten Fall schon bei Einführung des NIS-2 Gesetzes die Anforderungen zu erfüllen.
- Die in der NIS-2 Richtlinie beschriebenen Risikomanagementmaßnahmen sind sehr vage formuliert. Hinzu kommt, dass das nationale Gesetz einzelne Maßnahmen sogar strenger auslegen kann. Was und wieviel muss im Hinblick auf die NIS-2 Compliance also konkret unternommen werden? Eine Konkretisierung notwendiger Risikomanagementmaßnahmen ist frühestens mit der NIS-2 Verordnung zu erwarten, welche voraussichtlich erst im Jahr 2025 folgen wird.

- Die Anforderungen können große Hürden für Unternehmen des Mittelstands darstellen, vor allem, wenn es sich um weniger IT-affine Unternehmen handelt. Neben ohnehin knappen Ressourcen und Budgets verfügen diese oftmals auch nicht über das notwendige Knowhow, um adäquate Maßnahmen umzusetzen.
- NIS-2 sieht zur Herstellung der Compliance keinen allgemeingültigen Standard oder die Möglichkeit einer Zertifizierung vor.

Wie sollen betroffene Unternehmen mit diesen Herausforderungen umgehen?

Eine Orientierungshilfe, ob ein Unternehmen von NIS2 betroffen sein könnte, bietet der Online-Ratgeber der WKÖ. Leider hilft dieser gerade bei unklaren Fällen nicht weiter – im Zweifelsfall kann daher eine professionelle Beratung sinnvoll sein. Ist Ihr Unternehmen von dieser neuen Vorgabe betroffen? Dann betrachten Sie diese zunächst einmal nicht nur als eine weitere notwendige regulatorische Anforderung. Nehmen Sie die NIS-2 Vorgaben vielmehr zum Anlass, sich intensiv mit der Stärkung der Sicherheit und Cyberabwehrfähigkeit Ihres Unternehmens auseinanderzusetzen. Auch wenn es bisher in Ihrem Unternehmen noch keine Cyberangriffe gegeben hat, müssen Sie davon ausgehen, dass es jederzeit zu einem Sicherheitsvorfall mit potenziell verheerenden Folgen für Ihr Unternehmen kommen kann. Vorkehrungen für den Schutz der Netzwerk- und Informationssysteme sind also eine wichtige Investition in die Zukunft. Und auch wenn die Risikomanagementvorgaben noch sehr vage sind – die Richtung ist klar vorgegeben. Nutzen Sie die Zeit bis zum Inkrafttreten des Gesetzes, um ein angemessenes Risikomanagementsystem zu etablieren, sich den größten Cyberrisiken Ihres Unternehmens bewusst zu werden, einen Plan zur Risikominimierung auszuarbeiten und an der Beseitigung der kritischsten Schwachstellen zu arbeiten. Der Gesetzgeber anerkennt dabei die Grenzen des Machbaren und spricht daher auch von einem risikobasierten Ansatz, welcher zur Anwendung kommen soll: Einerseits müssen die gewählten Maßnahmen im Verhältnis zur Risikoexposition des Unternehmens angemessen und verhältnismäßig sein, andererseits setzen die vorhandenen Ressourcen eines Unternehmens in der Erfüllung der Anforderungen gewisse Grenzen.

Letztendlich geht es also darum, die identifizierten Cyberrisiken nicht nur nach Schadensausmaß und Eintrittswahrscheinlichkeit zu bewerten, sondern auch die möglichen Maßnahmen zur Risikominimierung im Hinblick auf den Aufwand und die Machbarkeit sowie die zu erwartende Wirkung zu beurteilen und zu priorisieren. Bei einer behördlichen Überprüfung ist es im Zweifelsfall entscheidend, glaubwürdig und nachvollziehbar darzulegen, dass man sich ernsthaft mit den Cyberrisiken auseinandergesetzt hat. Außerdem sollte ein nachvollziehbarer Plan vorgelegt werden können, der aufzeigt, warum bestimmte Maßnahmen bereits umgesetzt wurden, während andere noch ausstehen. Auch wenn die angedrohten Strafen abschreckend wirken – aus Erfahrung mit dem bestehenden NISG sprechen die Behörden zunächst meist erst Empfehlungen zur Verbesserung des Schutzniveaus aus, bevor es tatsächlich zu Sanktionen kommt.

Trotz der fehlenden Zertifizierungsmöglichkeit wird eine Orientierung an der aktuellen ISO/IEC 27001 und im Speziellen der erläuternden ISO/IEC 27002 in jedem Fall einen sehr guten Abdeckungsgrad gewährleisten. Gleichzeitig stärkt das auch das Vertrauen von Kunden, Partnern und Behörden in die Cybersicherheitsmaßnahmen des Unternehmens. Zudem sieht das EU-Cybersicherheitsgesetz die Einführung eines einheitlichen europäischen Zertifizierungsrahmens für IKT-Produkte, -Dienstleistungen und -Prozesse vor. Ob und inwieweit damit auch ein Nachweis der NIS-2 Compliance erbracht werden kann bleibt abzuwarten.

Ein letzter Tipp: Betrachten Sie ein NIS-2 Projekt zur Erreichung der NIS-2 Compliance nicht lediglich als ein rein technisches Vorhaben! Denn bei korrekter Umsetzung haben die ergriffenen

Maßnahmen weitreichende Auswirkungen auf Geschäftsprozesse, das Management und das Personal, und sogar auf die Unternehmenskultur. Warum ist das so?

Ein Unternehmen muss einerseits seine Schwachstellen kennen und andererseits die Auswirkungen verstehen, die ein potenzieller Cyberangriff auf die Vermögenswerte (Assets) und das Business haben kann. Die Schwachstellen sind zwar häufig in einer nicht ausreichend geschützten IT zu finden. Gemäß der eingangs erwähnten KPMG-Studie zur Cybersecurity in Österreich 2023 wird aber immer öfter der Mensch als die größte Schwachstelle eines Unternehmens angegriffen. Social Engineering ist zwar kein neues Thema mehr, jedoch werden die Angriffsmuster mit dem zunehmenden Einsatz von künstlicher Intelligenz immer perfider: So sind Cyberangriffe etwa durch Deep-Fake oder Voice Cloning kaum noch als solche erkennbar. Eine Organisation muss daher als Ganzes mehr sensibilisiert werden, und der angemessene Umgang mit Cyberbedrohungen muss zu einem Teil der DNA eines Unternehmens werden.

Das Wichtigste in Kürze

Die NIS-2 Richtlinie und ihre Auswirkungen auf Unternehmen: Die NIS-2 Richtlinie lässt eine signifikante Veränderung in der Herangehensweise der EU an die Cybersicherheit erkennen. So sind wesentlich mehr Unternehmen als im bisherigen NISG von der Regelung betroffen. Neu trifft es auch viele KMU, die wesentliche oder wichtige Dienste in verschiedenen Sektoren anbieten oder Teil einer Lieferkette sind.

NIS-2 als umfassendes Regelwerk: NIS-2 macht die oberste Führungsebene eines Unternehmens für die Cybersicherheit verantwortlich. Es gilt ein „all hazards approach“: Die Maßnahmen müssen sich auf das gesamte Unternehmen beziehen, nicht nur auf die wesentlichen Dienste.

Erforderliche Risikomanagementmaßnahmen: NIS-2 fordert unter anderem ein umfassendes Risikomanagementsystem, die Gewährleistung der Sicherheit entlang der Lieferkette, umfassende technische und organisatorische Cybersicherheitsmaßnahmen, Prozesse zur Erkennung und Meldung von Cybersicherheitsvorfällen und ein Business Continuity Management.

Überprüfung und Schulung der Maßnahmen: NIS-2 verlangt, dass die Unternehmen die Wirkung ihrer Maßnahmen laufend überprüfen und den Ernstfall regelmäßig üben. Außerdem müssen sie umfassende Schulungsmaßnahmen durchführen, um das Bewusstsein für Cybersicherheit zu erhöhen.

Die Herausforderungen und Chancen von NIS-2: Unternehmen müssen selbst beurteilen, ob sie von NIS-2 betroffen sind, und angemessene Sicherheitsmaßnahmen und Meldepflichten erfüllen. Viele Fragen zu den konkreten Anforderungen sind noch offen, dennoch muss bereits jetzt gehandelt werden. Dies kann eine große Herausforderung sein, vor allem für KMU, die oft über weniger Ressourcen und Know-how verfügen. Die NIS-2 Richtlinie sollte jedoch zum Anlass genommen werden, die eigene Cyberabwehrfähigkeit zu stärken und in die Zukunft zu investieren. Es sollte ein risikobasierter Ansatz verfolgt werden, welcher die vorhandenen Ressourcen auf die Behebung der kritischsten Schwachstellen fokussiert. Wichtig ist auch, dass ein NIS-2 Projekt nicht als rein technisches Vorhaben verstanden wird – es betrifft die Organisation als Ganzes.

Möchten Sie jetzt mit den Vorbereitungen für die Cybersicherheits-Richtlinie starten? Dann lesen Sie auch den zweiten Teil meines Blogbeitrags zu NIS-2, welcher ab Mitte April auf der HMP Webseite verfügbar sein wird. Ich stelle Ihnen dort ein idealtypisches Vorgehensmodell zur Erreichung der NIS-2 Compliance vor. Erfahren Sie dabei auch, wie HMP Sie in einem NIS-2 Projekt unterstützen kann.

Ihr persönlicher Ansprechpartner bei HMP:

Mag. (FH) Clemens Malt, MSc.

+43 (0)676 4060412
clemens.malt-burian@hmp.co.at

HMP BERATUNGSGMBH

Referenzen

A-SIT Zentrum für sichere Informationstechnologie – Austria, i. Z. (2022). *Supply Chain Security.* Von https://www.onlinesicherheit.gv.at/Themen/Experteninformation/Supply-Chain-Security.html abgerufen

Bundeskanzleramt. (2018). *Erläuterungen des NIS Gesetzes.* Von https://www.bundeskanzleramt.gv.at/dam/jcr:24b93885-8b30-4770-8782-c20453591f7d/Erlaueterungen-NISG.pdf abgerufen

Bundeskanzleramt. (2024). *Die neue NIS-2-Richtlinie*. Von https://www.nis.gv.at/nis-2-richtlinie.html abgerufen

Europäische Union. (2022). *NIS-2 Richtlinie der Europäischen Union*. Von https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&qid=1674579731975&from=EN#d1e3310-80-1 abgerufen

Europäische Union. (2023). *Das EU-Cybersicherheitsgesetz*. Von https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-act abgerufen

J. Bartz et al. (2023). *"Vulkan Files": Russland plant den Cyberkrieg*. Von https://www.zdf.de/nachrichten/politik/ausland/vulkan-files-cyberangriff-hacker-ukraine-krieg-russland-100.html abgerufen

KPMG. (2023). *KPMG Studie: Anzahl der Cyberattacken innerhalb eines Jahres verdreifacht*. Von https://kpmg.com/at/de/home/media/press-releases/2023/05/kpmg-studie-anzahl-der-cyberattacken-innerhalb-eines-jahres-verdreifacht.html abgerufen

Wirtschaftskammer Österreich (WKÖ). (2023). *Cybersicherheitsrichtlinie - NIS2*. Von https://ratgeber.wko.at/NIS2/ abgerufen

Wirtschaftskammer Österreich (WKÖ). (2024). *Cybersicherheits-Richtlinie NIS 2*. Von https://www.wko.at/it-sicherheit/nis2-uebersicht abgerufen