ZfK Zeitung für kommunale Wirtschaft

IT

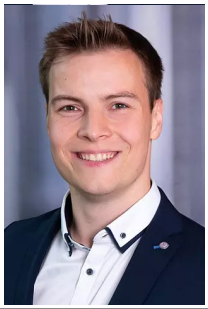
ZfK+ Cybersicherheit: Neue europäische Vorgaben und Hinweise zur Vorbereitung darauf

In Brüssel befindet sich ein neues Gesetz zur Cybersicherheit auf den letzten Metern: Die NIS 2-Richtlinie soll noch dieses Jahr veröffentlicht werden. Ein Gastbeitrag.

13.12.2022

Das geplante europäisches Geset soll das Cybersicherheitsniveau in der EU vereinheitlichen und anheben.

Bild: © Skórzewiak/AdobeStock



Von:
Simon Kessel, Referent Schwerpunktthemen Digitales und Sustainable Finance, Verband kommunaler Unternehmen (VKU) (links)
Heiko Gerstmayr, Ausecus GmbH (rechts)

Die NIS 2-Richtlinie soll die Anforderungen an Betreiber Kritischer Infrastrukturen in allen EU-Mitgliedsstaaten vereinheitlichen. In Deutschland würden dadurch mittelfristig viele kleinere Unternehmen mit Anforderungen für KRITIS-Betreiber konfrontiert.

Neben Hintergründen zur neuen Richtlinie behandelt dieser Artikel allgemeine Hinweise zur Vorbereitung auf die Umsetzung potenzieller neuer Pflichten, welche den Umsetzungsaufwand durch eine frühzeitige und vorausschauende Vorbereitung stark senken können.

Was ist die NIS 2-Richtlinie und wieso ist sie relevant?

Bei der NIS 2-Richtlinie, oder „Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union" wie sie offiziell heißt, handelt es sich um ein europäisches Gesetz, welches das Cybersicherheitsniveau in der EU vereinheitlichen und anheben soll. Sie ist die Nachfolgerichtlinie der NIS aus dem Jahr 2016 und wird sowohl mehr Sektoren als auch mehr Unternehmen Cybersicherheits- und Berichtspflichten unterwerfen.

Unter die Bestimmungen der Richtlinie fallen alle Unternehmen, die in den einschlägigen Sektoren aktiv sind. Kommunalwirtschaftlich relevant sind hierbei insbesondere die Sektoren Energie, Transport, Trinkwasser, Abwasser, digitale Infrastruktur und Abfallwirtschaft.

Ausnahmen

Ausgenommen sind nur Unternehmen, die mit Blick auf ihre Größe als kleines Unternehmen gelten, also weniger als 50 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt. Bei Unternehmenskonzernen oder verbundenen Unternehmen, welche insgesamt die Schwellenwerte überschreiten, fallen auch Tochterunternehmen, welche die Schwellenwerte unterschreiten, unter die Bestimmungen der NIS 2-Richtlinie.

Damit unterscheidet sich die Systematik der NIS 2-Richltinie von der BSI-KRITIS-Verordnung, welche allgemein auf die Anzahl versorgter Personen abstellt. Mit Blick auf diese Schwellenwerte sind Anpassungen am deutschen IT-Sicherheitsrecht zu erwarten. Es ist zudem davon auszugehen, dass weit mehr Unternehmen cybersicherheitspflichtig werden.

21 Monate Zeit zur Umsetzung ab Inkrafttreten

Sobald die NIS 2-Richtlinie in Kraft getreten ist, habe die EU-Mitgliedsstaaten und damit auch Deutschland 21 Monate Zeit ihre Bestimmungen in nationales Recht zu überführen. Deshalb muss man spätestens im 2. Halbjahr 2024 mit den neuen Anforderungen rechnen.

Es ist möglich, dass der Gesetzgeber für die Erfüllung der neuen Pflichten Übergangsfristen einräumt. Dennoch sollte man frühzeitig mit der Vorbereitung beginnen, um nicht von den neuen gesetzlichen Pflichten überfordert zu werden. Zur Orientierung hilft ein Blick auf die aktuell geltenden gesetzlichen Anforderungen.

Welche Anforderungen im Bereich Cybersicherheit müssen bereits heute umgesetzt werden?

Die zentralen, kommunalwirtschaftlich relevanten gesetzlichen Anforderungen an die Cybersicherheit werden in Deutschland durch das BSI-Gesetz (BSIG) bzw. spezialgesetzliche Gesetze wie das Energiewirtschaftsgesetz (EnWG) oder das Telekommunikationsgesetz (TKG) geregelt.

Die bestehenden gesetzlichen Anforderungen enthalten primär ein Informationssicherheitsmanagementsystem (ISMS) und Sicherheitsmaßnahmen nach Stand der Technik, die ab dem 01. Mai 2023 den Betrieb eines Systems zur Angriffserkennung einschließen.

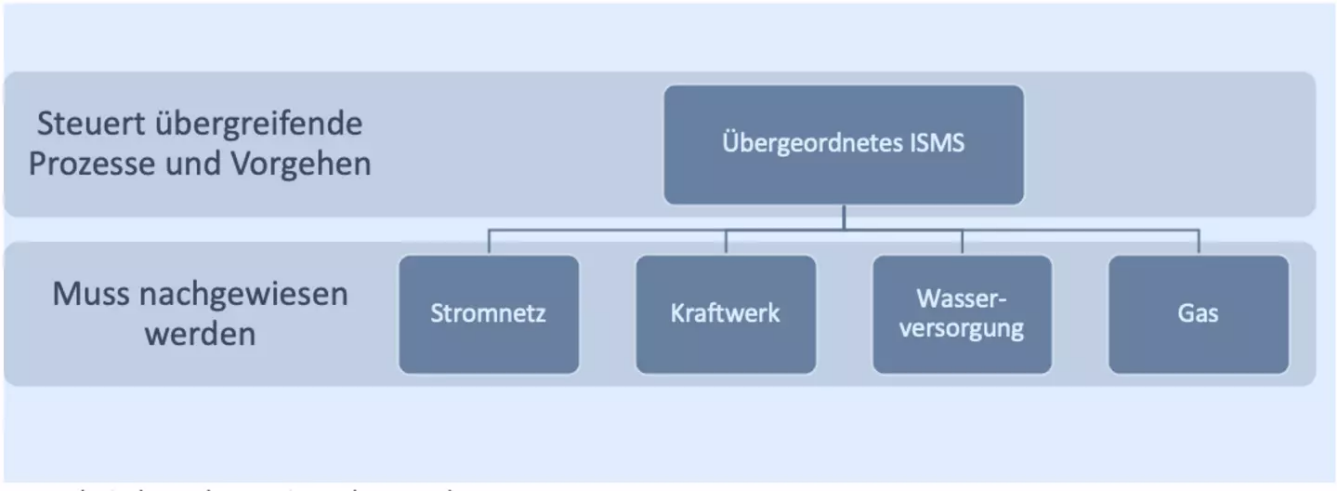
Für Organisationen und Geschäftsbereiche, die jetzt neu mit den Anforderungen konfrontiert werden, bedeutet dies einen erheblichen personellen und finanziellen Aufwand. Insbesondere mit Blick auf das Personal ergibt es Sinn, frühzeitigt mit der Planung zu beginnen und gegebenenfalls entsprechendes Personal aufzubauen.

Ein ISMS verwaltet die Umsetzung von technischen und organisatorischen Maßnahmen, durch die der Ausfall und die Fremdübernahme der Prozesse im Geltungsbereich verhindert werden sollen. Solche Prozesse, wie die die Versorgung mit Strom, Gas und Wasser, werden durch zunehmende Digitalisierung auch aus der Ferne angreifbar.
Systeme zur Angriffserkennung sollen Cyberangriffe erkennen und die Einleitung von sinnvollen Gegenmaßnahmen ermöglichen. Das ist vergleichbar mit einer Brandmeldeanlage, mit der man einen Brand frühzeitig erkennen kann, um die weitere Ausbreitung zu unterbinden.

Hinweise zur Einführung eines skalierbaren ISMS

Wenn man ein ISMS in einem neuen Geschäftsbereich einführen will, kann man meistens große Teile eines bereits bestehenden ISMS verwenden. Oft besteht die einfachste Möglichkeit in einer Erweiterung des bestehenden Geltungsbereichs. Hierbei ist die Schwierigkeit, dass die spezifischen Anforderungen verschiedener Geschäftsbereichs teils sehr unterschiedlich sind.

In großen Unternehmen hat sich deshalb die gängige Praxis bewährt, mehrere ISMS einzuführen, welche möglichst viele Aspekte teilen. Ein übergeordnetes ISMS koordiniert das übergreifende Vorgehen, welches durch die Fachbereiche übernommen und konkretisiert werden kann. Dadurch kann man sich Mehraufwand sparen und bleibt gleichzeitig flexibel.



Exemplarisches Schema eines übergeordneten ISMS

Wenn Sie neue Geschäftsbereiche in Ihr ISMS aufnehmen müssen, können Sie diese Tipps befolgen:

- Wählen Sie eine Zertifizierungsgrundlage, die in jedem Geschäftsbereich anwendbar ist. In vielen Fällen empfiehlt sich die universell anwendbare ISO 27001.
- Gestalten Sie die organisatorischen Prozesse Ihres ISMS so allgemein, dass die Prozesse in jedem Unternehmensbereich genutzt werden können.
- Planen Sie Personal vorausschauend. Fachpersonal sollte frühzeitig aufgebaut und eingearbeitet werden. Alternativ können Dienstleister mit branchenübergreifender Erfahrung engagiert werden.

Systeme zur Angriffserkennung

Systeme zur Erkennung von Cyberangriffen sind spezielle IT-Überwachungswerkzeuge, mit denen Cybersicherheitsspezialisten Kommunikationsdaten und Systemstatistiken untersuchen. Auffällige Meldungen werden im Detail analysiert, um einen möglichen Cyberangriff zu qualifizieren. Sobald ein Cyberangriff qualifiziert wurde, müssen geeignete Gegenmaßnahmen eingeleitet werden.

Der Betrieb dieser Werkzeuge und insbesondere die Analyse der Meldungen erfordert umfangreiche Fachkenntnisse über aktuelle Angriffsmethoden und -tools, sowie über die überwachten Systeme und deren Kommunikationsprotokolle.

Der Beruf des Security Analysten ist eine Vollzeitbeschäftigung. Insofern ist für mittelständische Versorgungsunternehmen der Einsatz von spezialisierten Dienstleistern ratsam, auch wenn die Anschaffung von IT-Security Werkzeugen eine spannende Aufgabe ist. Hinweise zur Einführung eines solchen Angriffserkennungssystems liefert die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“.

Fazit

Inwieweit aus der NIS 2-Richtlinie neue Cybersicherheitspflichten erwachsen werden, lässt sich abschließend erst im Rahmen der Umsetzung in den kommenden 21 Monaten sagen. Für Unternehmen, welche aktuell schon Cybersicherheitsmaßnahmen

umsetzen und potenziell weitere Bereiche zertifizieren müssen, lohnt sich die Berücksichtigung der zukünftigen Anforderungen in der heutigen Umsetzung. Dazu gehört insbesondere die Wahl der Zertifizierungsgrundlage für das ISMS und die Auswahl des Angriffserkennungssystems.

Wer erst künftig betroffen sein wird, sollte ein Auge auf die Fristen haben und rechtzeitig mit der Einführung beginnen. Gerade kurz vor Ablauf gesetzlicher Nachweisfristen sind oft wenige Ressourcen auf dem Markt. Dadurch wird die Umsetzung langsamer, kostenintensiver und schwieriger.
Unabhängig von gesetzlichen Pflichten gehen Cybersicherheitsvorfälle häufig mit hohen Kosten und einem Reputationsschaden einher, weshalb wir dieses Thema nur jedem ans Herz legen können.

Mehr zum Thema

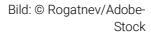


Bild: © Rogatnev/Adobe-Stock

IT

Proaktive Kundenkommunikation ist Trumpf

Bild: © Cortility

IT

"Energieversorger stehen vor zunehmend komplexeren Zusatzaufgaben"

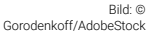


Bild: © Gorodenkoff/AdobeStock

IT

Stadtwerke München installieren neues IT-Monitoring