Erst mit dieser Basis sind eine nachvollziehbare Risikoanalyse und Maßnahmenplanung möglich. Da die Risikoanalysen regelmäßig (jährlich nach Gesetzgebung, praktikabel alle zwei Jahre) wiederholt werden müssen, kommt diesen Grundlagen eine besondere Bedeutung zu. Die Qualität der Definition und der gewählten Dokumentation entscheidet maßgeblich über den Aufwand bei der Wiederholung.
Die rechtzeitige Forderung von IT-Sicherheit für Neuanschaffungen hat den großen Vorteil, dass sich die Anzahl mitigierender Maßnahmen für Bestandstechnik drastisch reduzieren lässt. Zwar erscheinen Ersatzmaßnahmen zunächst günstig, jedoch sind sie häufig in der dauerhaften Aufrechterhaltung ressourcenintensiv.

6 Fazit

Die neuen und überarbeiteten EU-Richtlinien NIS-2 und ihre Begleiter müssen in nationales Recht überführt werden. Nach aktueller Planung wird die nationale Gesetzgebung im Oktober 2024 in Kraft treten und zwei, maximal drei Jahre Umsetzungszeit erlauben. Die Umsetzungsfristen gelten europaweit. Heutige KRITIS-Unternehmen können bereits gut vorbereitet sein oder sind bereits in der Umsetzung der neuen Maßnahmen. Für neue Unternehmen im Geltungsbereich der Gesetzgebung ist der notwendige Hub sehr hoch. Es ist zu empfehlen, die Grundlagen für Risikomanagement frühzeitig zu legen, um die erste Auditierung erfolgreich zu bestehen. Die Qualität der Grundlage entscheidet über den Aufwand und den Erfolg der folgenden Jahre im Management der IT-Sicherheits-Maßnahmen, denn IT-Sicherheit ist ein Prozess, kein Zustand. ■

6 Conclusion

The new and revised EU NIS-2 directives and their companions have to be incorporated into national law. According to current planning, the national legislation will come into force in October 2024 and allow two or a maximum of three years for implementation. The implementation deadlines will apply across Europe. Current CRITIS companies may already be well prepared or already in the process of implementing the new measures. The necessary speed is very high for those companies newly included within the scope of the legislation. It is recommended that the risk management foundations should be laid at an early stage in order to successfully pass the first audit. The quality of these foundations determines the effort and success of the following years in the management of IT security measures, because IT security is a process, not a state. ■

LITERATUR | LITERATURE

[1] ENISA: ENISA Threat Landscape: Transport Sektor, 2023
[2] EU 2022/2555: Richtlinie zu Cybersicherheit von Netz- und Informationssystemen, 2022
[3] EU 2022/2557: Richtlinie zur Stärkung der Resilienz kritischer Einrichtungen, 2022
[4] Bundesministerium des Innern und für Heimat (BMI): Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie; https://ag.kritis.info/wp-content/uploads/2023/07/NIS2UmsuCG-Referentenentwurf-BMI-CI1-Bearbeitungsstand-03072023.pdf, 31.07.2023
[5] BMI: EU-Richtlinien zum Schutz Kritischer Infrastrukturen; https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2023/01/eu-richtlinien-kritis.html, 31.07.2023
[6] BSI: Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf, 31.07.2023
[7] EU 2008/114: Richtlinie zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen, 2008
[8] EU 2022/0272: Cybersicherheitsanforderungen für Produkte mit digitalen Elementen; https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services_en, 31.07.2023
[9] Bundesministerium der Justiz (BMJ): Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV), 2023
[10] BMI: Eckpunkte für das KRITIS-Dachgesetz; https://dserver.bundestag.de/btd/20/054/2005491.pdf, 31.07.2023
[11] BMJ: Eisenbahn-Bau- und Betriebsordnung; https://www.gesetze-im-internet.de/ebo/BJNR215630967.html, 31.07.2023
[12] EU 2003/361/EC; Kleinstunternehmen sowie kleine und mittlere Unternehmen: Definition und Umfang, 2016

AUTOR | AUTHOR

Dr. Ing. Martin Koop
Senior Expert IT-Security
Incyde GmbH
Anschrift / *Address*: Schaumainkai 91, D-60596 Frankfurt a. M.
E-Mail: martin.koop@incyde.com