CYBER SECURITY UND RISIKOMANAGEMENT

Haben Sie noch den Überblick?
IT-SiG 2.0, KRITIS V, DSGVO und NIS2

ERFAHREN SIE MEHR IM INTERVIEW MIT:

KATHRIN WEBER

Geschäftsführerin
IRM Interim-Risiko-Management GmbH

PATRICK JUNG

Gründer und
IT-Scurity Consultant
ISB PLUS

Vorstellung

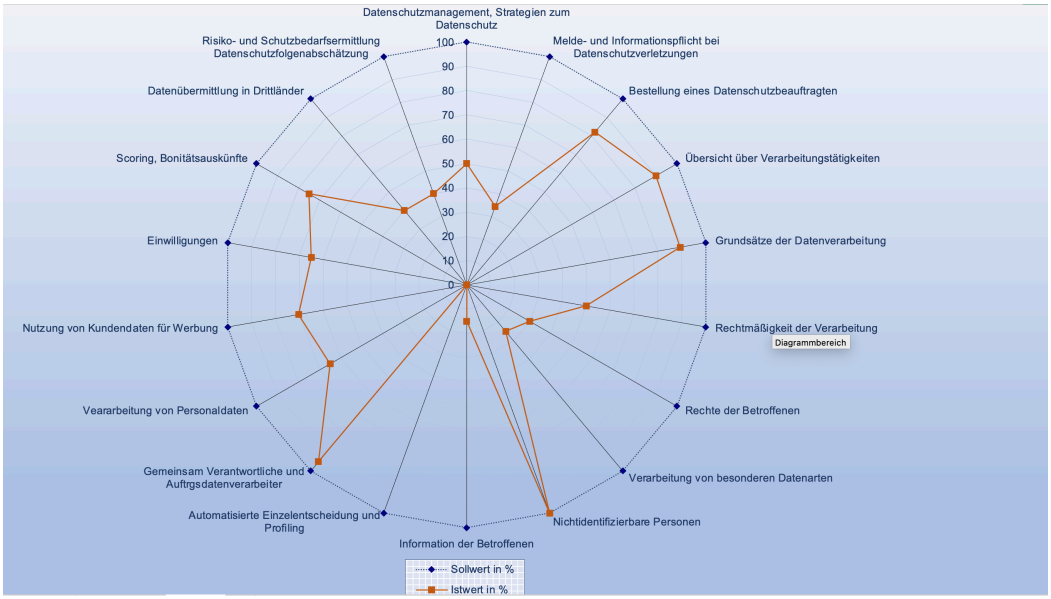
IT-Risiken gehören neben den Personalrisiken zu den größten Risiken für Unternehmen sowie Staat und Verwaltung.
Patrick Jung, IT-Sicherheitsberater und Gründer der Firma ISB-Plus und **Kathrin Weber, Risikomanagerin** und Geschäftsführerin der IRM Interim-Risiko-Management GmbH geben hier einen kleinen Einblick in die gemeinsame Zusammenarbeit zum Thema.

Einleitung

IT-Sicherheitsgesetz und die neue EU NIS 2- Beide Vorgaben zählen zu den wichtigsten Grundlagen in diesem Themenbereich.
Wir haben diese beiden herausgestellt, um einen kleinen Überblick für eine praktische Herangehensweise an die Themen für Unternehmen sowie Staat und Verwaltung zu geben.
Patrick Jung, IT-Sicherheitsberater und Gründer der Firma ISB-Plus und Kathrin Weber, Risikomanagerin und Geschäftsführerin der IRM Interim-Risiko-Management GmbH geben einen kleinen Einblick in die gemeinsame Zusammenarbeit zum Thema und die Frage :

Droht uns nun die Überregulierung der IT-Sicherheit?

Verfolgt man die aktuelle Berichterstattung, fallen zahlreiche (neue) Regulatorien für den IT-Bereich ins Auge und Viele fragen sich, wie diese Fülle der Vorgaben im Unternehmen und/oder in den Behörden umgesetzt werden können.
Schauen wir uns ***zum Vergleich die Einführung der DS-GVO im Jahr 2018*** an, finden wir Ähnlichkeiten. Auch hier befürchteten wir eine Überregulierung, konkret: einen zahnlosen Tiger. Viele Vorschriften, keine durchgreifende Umsetzung.
Das alles ist jedoch nicht eingetreten.
Das Ergebnis vieler implementierten und umgesetzten Datenschutzkonzepte ist vielmehr eine Erhöhung der Qualität und Transparenz der Daten in den einzelnen Einheiten. Damit einhergehend werden auch die Risiken im Datenaustausch sichtbarer und vor allem messbar.



Die Umsetzung der Mindeststandards im Datenschutz und in der IT-Sicherheit trägt damit zum Schutz Ihres Unternehmens bzw. dessen Fortbestand bei.
Die einzelnen Fragen bringen mehr Informationen:

Kathrin: Welche Verordnungen und Gesetze gibt es eigentlich zum Thema IT-Sicherheit und Datenschutz?

Patrick: Folgende Gesetze und Verordnungen sind aus meiner Sicht für die meisten Unternehmen relevant:

- IT-Sicherheitsgesetz 2.0, in Kraft seit Mai 2021 https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html
- BSI- Kritisverordnung (BSI-KritisV), in Kraft seit Juni 2017 und seit Januar 2022 in der 2. Änderungsverordnung https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html
- EU NIS2 (Network and Information Security 2) ab Oktober 2024, aktuell noch NIS-Richtlinie (NIS= Netz- und Informationssicherheit), https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-aktuell/KRITIS-Meldungen/221227-veroeffentlichung-nis-2.html https://www.consilium.europa.eu/de/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

- DS-GVO in Kraft seit 2018 https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverordnung.html

Kathrin: Wo liegen die wesentlichen Unterschiede?

Patrick: Das IT-Sicherheitsgesetz 2.0 stärkt die Kompetenzen des BSI als nationale Cybersicherheitsbehörde. Es ist sowohl für Verbraucher und Unternehmen zuständig. Es gibt hier Informationen und Tipps für Verbraucher, um sich vor Angriffen und Betrug zu schützen. Eine wichtige Aufgabe ist die Meldestelle für IT-Sicherheitsvorfälle, hier können Verbraucher, Unternehmen oder Betreiber kritische Infrastruktur Vorfälle melden.
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/it-sicherheitsvorfall_node.html
Das IT-Sicherheitsgesetzt bildet die Basis der Anforderungen an Unternehmen und setzt die Mindeststandards. Zum Beispiel wurden hier Vorgaben für die Detektion und Abwehr von Cyberangriffen erstellt.

Das Ziel ist es, einen einheitlichen Standard im Bereich Cybersicherheit innerhalb der EU festzulegen.

Die KritisV setzt auf dem IT-Sicherheitsgesetz auf und legt fest: Wer zu kritischen Infrastruktur (KRITIS) gehört und welche technischen und organisatorischen Maßnahmen aus dem IT-Sig2 umgesetzt werden müssen.

Die NIS bzw. NIS 2 Richtline ist eine Vorgabe der EU, welche in nationales Recht umgewandelt werden wird. Das Ziel ist es, einen einheitlichen Standard im Bereich Cybersicherheit innerhalb der EU festzulegen. Hiermit soll auch die Zusammenarbeit der nationalen Behörden und Staaten verbessert werden. Damit die Umsetzung auch stattfindet, können Sanktionen verhängt werden.

Kathrin: Wie hängen die einzelnen Vorgaben zusammen?
Patrick: Wie schon beschrieben, setzt die KritisV auf dem IT-Sicherheitsgesetz auf und definiert die Zielgruppen.
Das bedeutet, dass alle mittleren und großen Einrichtungen, die in den von der Richtlinie erfassten Sektoren tätig sind oder unter die Richtlinie fallende Dienste erbringen, in den Anwendungsbereich der Richtlinie fallen. Wer von NIS2 berührt ist, muss ab Herbst 2024 strenge Sicherheitsvorkehrungen treffen. ***Hier werden KMUs ab 50 Mitarbeiter und einem Jahresumsatz ab 10 Mio. € in den Fokus gesetzt.*** Zu den Anforderungen gehören die Erhöhung des Schutzes vor Cyberangriffen, die Einhaltung spezifischer Security-Standards sowie die Gewährleistung, dass Systeme ständig auf dem aktuellen Stand sind. Zudem gelten Meldepflichten, falls es zu Sicherheitsvorfällen kommt.

Wer von NIS2 berührt ist, muss ab Herbst 2024 strenge IT-Sicherheitsvorkehrungen treffen.

Kathrin: Was ist neu?
Patrick: Das BSI ist unsere Cybersicherheitsbehörde und hat folgende **neuen Aufgaben** u.a.:

- Definition von technischen Sicherheitsstandards und Zertifizierungen von Betreibern u.a. Mobilfunk
- Die Vorgabe zur Implementierung einer Angriffserkennung bei Unternehmen

Das BSI übernimmt den digitalen Verbraucherschutz (DVS), hierbei werden unabhängige Beratungen angeboten und ein Warnsystem für Bürger etabliert.
Des Weiteren sollen Sicherheitskennzeichen für Produkte und Dienste eingeführt werden, die bestimmte Sicherheitsstandards erfüllen.

Durch die NIS2 Verordnung werden weitere Unternehmen ähnliche Anforderungen wie bei KRITIS V umsetzen müssen, da Sie entweder direkt unter die Umsatz- bzw. Mitarbeitergrenze fallen oder indirekt als Lieferant eines KRITIS Unternehmens zur Umsetzung verpflichtet sind (Lieferkette).

Kathrin: Jetzt mal konkret- Zum Thema der Angriffserkennung lässt sich bereits eine Menge sagen. Wie kann eine Früherkennung praktisch umgesetzt werden?
Patrick: Dazu gibt es natürlich unterschiedliche Ansätze wie u.a. die Analyse des Datenverkehrs auf Verbindungen zu Angreifernetzwerken oder die Überwachung von privilegierten Accounts wie Administratoren oder die Nutzung von bestimmten Tools die ein Anwender nicht benötigt wie bspw. powershell, psexec oder mimikatz.
Hierbei gibt es aus meiner Sicht auch keine einfache Antwort, da die Lösungen zum Unternehmen und der IT-Infrastruktur passen müssen. Wichtig ist, dass hier vom Gesetz auch Maßnahmen gefordert sind, wenn ein System etwas meldet. Das bedeutet, Unternehmen benötigen eine klare Strategie, wie sie mit Meldungen umgehen, wie sie die Art des Angriffs verifizieren und wie sie Maßnahmen ergreifen, um diesen einzudämmen.

Kathrin: Gibt es einen zeitlichen Rahmen für die Umsetzung der Angriffserkennung?
Patrick: Die Verpflichtung für die Angriffserkennung besteht seit Mai 2023
Nachzulesen auf
https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-Systeme-Angriffserkennung/faq-systeme-angriffserkennung_node.html

Kathrin: Wie ist Deine Einschätzung? Ist ein System zur Angriffserkennung für die Unternehmen wirklich ein Zuwachs an Sicherheit?

Patrick: Theoretisch sollte es so sein, leider sieht die Praxis anders aus.
In vielen Unternehmen ist die Basis für ein so komplexes System zur Angriffserkennung nicht gegeben.
D.h. es werden z.B. häufig Fehlalarme ausgelöst (False-Positives), was dann wiederum dazu führt, dass entweder die Alarme nicht mehr beachtet oder sehr häufig akzeptiert werden.

Theoretisch sollte es so sein, leider sieht die Praxis anders aus.

Das nächste Problem ist der Umgang mit diesen Alarmen. Viele Unternehmen können die Meldungen und die Kritikalität nicht einschätzen (Bewertung) und haben keine Checkliste mit Maßnahmen zur Eindämmung.

Noch ein weiteres Beispiel sind die administrativen Konten. Viele Unternehmen haben häufig mehr als das Doppelte an administrativen Benutzern in der IT-Abteilung als notwendig wären.
Das macht eine Überwachung sehr schwierig, da sich täglich mehrere administrative Accounts auf unterschiedlichen Systemen anmelden.
Wie soll ein System zur Angriffserkennung da den Missbrauch detektieren?

Kathrin: Was muss ein Unternehmen mit min. 50 Mitarbeiter und einem Jahresumsatz ab 10 Mio. € jetzt tun?

Patrick: Es sind folgende Punkte umzusetzen: z.B….

Es muss als erstes jeweils einen zentralen Ansprechpartner für die Bereiche IT-Sicherheit und Datenschutz geben, der eng mit der Geschäftsführung zusammenarbeitet.
Eine Basisabsicherung sollte mit Bordmitteln erfolgen, das betrifft vor allem folgende Bereiche der IT-Infrastruktur:

- Schutz der digitalen Identitäten
- Netztrennung, Abschottung von sensiblen Bereichen (Server, Backup, Produktion, usw.)
- Sichere Administrationskonzepte
- Schutz des Backups und meiner Daten
- Life-Cycle-Management (Patches und Update)
- Playbook bei Cyberangriffen (Notfallplanung mit Maßnahmen zur Eindämmung)
- Ein funktionierendes Datenschutzkonzept

Ein Meldekonzept für Sicherheitsvorfälle ist umzusetzen.

Kathrin: Wie sieht es dabei zum Thema der Ressourcen aus? Das ist doch sicherlich für die meisten Einheiten ein Thema?

Patrick: Das ist ein absoluter Knackpunkt. Lediglich Unternehmen mit einer klaren Cyberstrategie und ausreichenden eigenen Ressourcen oder Partnerunternehmen mit dem erforderlichen Fachwissen werden in der Lage sein, diese Anforderungen umzusetzen.
Deswegen empfehle ich allen Unternehmern in das Thema Cyber Security frühzeitig zu investieren, denn die Ressourcen an Mitarbeitern und Dienstleistern sind knapp und schnell vergeben.

Wir hoffen, wir konnten Ihnen einen kleinen Einblick in die aktuelle Thematik mit praktischen Ansätzen geben.

Bei Interesse oder Fragen zum Thema wenden Sie sich gern an:

Patrick Jung
ISB-PLUS

Mobil: +49 151 416 550 30
E-Mail: info@isb-plus.de

https://isb-plus.de

Kathrin Weber
IRM Interim-Risiko-Management GmbH

Tel: +49 40 33 313 280
E-Mail: info@interim-risiko-management.de

https://interim-risiko-management.de