Idealtypisches Vorgehen in einem NIS-2 Projekt

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

Im ersten Teil meines Blogbeitrags habe ich mich ausführlich mit der Herausforderung NIS-2 für betroffene Unternehmen auseinandergesetzt. In diesem zweiten Teil möchte ich Ihnen einen Weg aufzeigen, wie ein betroffenes Unternehmen die NIS-2 Anforderungen erreichen kann. Auch wenn die konkrete Ausgestaltung eines solchen Vorhabens sehr individuell ist, lassen sich dennoch bestimmte Phasen identifizieren, welche durchlaufen werden sollten. Ein solches „idealtypisches" Vorgehensmodell stelle ich Ihnen nun vor.

Das Vorgehensmodell orientiert sich am PDCA-Zyklus (Plan-Do-Check-Act), und ist daher nicht als einmaliger Ablauf, sondern als iterativer Prozess zu verstehen. Dies ist auch schon die erste und wichtigste Erkenntnis – NIS-2 Compliance ist nicht durch ein einmaliges Projekt zu erreichen. Vielmehr handelt es sich um eine kontinuierliche Aufgabe, welche in einem entsprechenden Prozess verankert werden muss. Notabene ist es genau das, was die NIS-2 Richtlinie auch fordert. Dennoch kann das von mir vorgestellte Vorgehensmodell auch als Blaupause für ein initiales Projekt herangezogen werden – und in diesem Kontext möchte ich Ihnen das Modell auch vorstellen. Ein solches Projekt verfolgt dabei zwei Ziele: Zum einen soll ein erster, adäquater Security-Reifegrad erreicht werden, welcher die NIS-2 Anforderungen im besten Fall schon erfüllt. Zum anderen geht es aber auch darum, einen Prozess zu entwickeln und zu institutionalisieren, nach dem die Cybersecurity in einem Unternehmen kontinuierlich verbessert und an die fortschreitende Bedrohungslage angepasst werden kann.

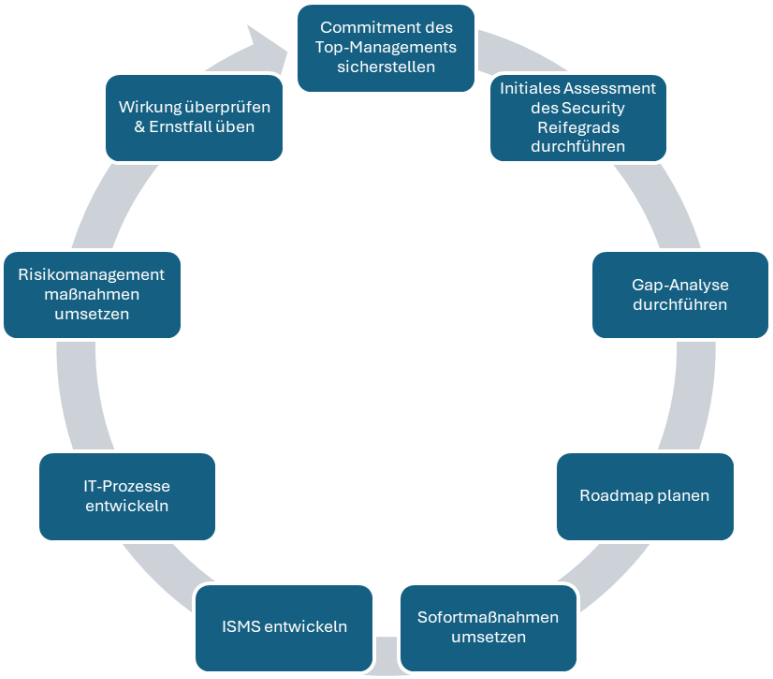

Abbildung 1: Idealtypisches Vorgehensmodell zur Erreichung der NIS-2 Compliance

Zuallererst ist es von entscheidender Bedeutung, das **Commitment des Top-Managements** und die Zustimmung relevanter Stakeholder sicherzustellen. Ein NIS-2-Projekt muss von diesen als strategisches Vorhaben verstanden werden. In der Projektorganisation muss die Verantwortung der oberen Führungsebene klar zum Ausdruck kommen.

In einem **initialen Assessment** ist der Security Reifegrad zu ermitteln. Wichtige Anhaltspunkte für ein solches Assessment sind:

- Generelle *Risikoexposition* des Unternehmens
- *Risikokultur und -bewusstsein* in der obersten Führungsebene wie auch bei Mitarbeiter*innen
- *Strategische Bedeutung* von Cybersicherheit im Unternehmen
- Vorhandensein und Reifegrad eines *Governance- und Risikomanagementsystems*
- Ggf. vorliegende *Business Impact Analyse,* um die wechselseitigen Abhängigkeiten sowie die Kritikalität der Geschäftsprozesse und der zugrundeliegenden Ressourcen zu verstehen
- *Schutzniveau wichtiger Vermögenswerte* sowie der *kritischen Infrastruktur* (u.a. Netz- und IT-Infrastruktur)
- *Daten- und Anwendungsarchitektur:* Datenmanagement (u.a. Datenklassifizierung, Verfügbarkeit, Schutz sensibler Daten), Zugriffs- und Verschlüsselungskonzepte, etc.
- *IT-Betrieb*: Systemadministration, Admin-Tools, ITSM-Prozesse
- *Reifegrad der Cybersecurity Prozesse:* u.a. Cyber Risk Management, Cyber Incidents erkennen und bewältigen, Business Continuity Management inkl. Backup- und Wiederherstellungsprozessen, Notfallplänen und dem Krisenmanagement
- *Sicherheitsvorkehrungen in Bezug auf die Supply Chain* (Prüfen von SLAs und vertraglichen Vereinbarungen, Zertifizierungen, Lieferantenaudits und sonstigen Nachweisen zu Risikomanagementmaßnahmen)
- *Technische und organisatorische Cybersicherheitsmaßnahmen*
- Umgang mit *früheren Sicherheitsvorfällen*
- Vorhandene *Zertifizierungen im Security-Bereich*

Eine **Gap-Analyse** dient dazu, die Abweichungen zu den NIS-2 Anforderungen zu ermitteln und die Handlungsfelder zu identifizieren. Dieser Schritt wird anfangs noch mit einiger Unsicherheit behaftet sein, solange das NIS-2 Gesetz noch ausstehend ist. Daher gilt es, sich hierbei zunächst auf die wesentlichen, unumstößlichen Anforderungen zu konzentrieren.

Roadmap Planung: Zu den Handlungsfeldern werden konkrete Maßnahmen definiert und anhand von Dringlichkeit, Wirksamkeit, Aufwand und Ressourceneinsatz bewertet und priorisiert. Entsprechend dieser Priorisierung wird eine Roadmap erstellt und freigegeben, wofür entsprechende Personalressourcen und Budgetmittel bereitzustellen sind.

Sofortmaßnahmen umsetzen: Gegebenenfalls sind besonders dringende Maßnahmen als Sofortmaßnahmen umzusetzen – beispielsweise, wenn im Zuge des Assessments gravierende IT-Sicherheitslücken erkannt wurden. Eine Sofortmaßnahme kann auch sein, das Management und das Personal frühzeitig in Cybersecurity Belangen zu schulen und somit eine wichtige Voraussetzung für den Projekterfolg zu schaffen. Auch die Erstellung eines Cyber Incident Response Plans sollte – sofern nicht vorhanden - möglichst früh in Angriff genommen werden, um auf das Schlimmste vorbereitet zu sein.

Managementsystem für die Informationssicherheit (ISMS) einführen bzw. optimieren: Ein ISMS dient dazu, klare Regeln, Prozesse und die Verantwortung im Bereich der Informationssicherheit innerhalb der Organisation zu verankern. Dazu existieren bereits systematische und bewährte Vorgehensmodelle und Standards. Zu nennen sind v.a. die internationale Norm ISO/IEC 27001 bzw. die darauf aufbauende ISO/IEC 27002, der BSI IT-Grundschutz oder branchenspezifische Normen wie z.B. TISAX für die Automobilindustrie. Der Nachweis am Papier wird aber in jedem Fall nicht ausreichen. Ein ISMS definiert die Governance und schafft die Grundlage, um geeignete Risikomanagementmaßnahmen nach der PDCA-Methodik zu identifizieren, umzusetzen, zu überprüfen und zu erproben, und letztlich das Risikomanagementsystem laufend zu verbessern.

Diese Phase bildet das „Herzstück“ dieses Vorgehensmodells. Damit wird die Grundlage des eingangs erwähnten Ziels geschaffen, einen ganzheitlichen Prozess zur Sicherstellung und kontinuierlichen Verbesserung der Cybersecurity zu schaffen.

IT-Prozesse entwickeln bzw. optimieren: Konkrete Maßnahmen zur Sicherstellung der Cybersicherheit erfordern zwingend IT-Prozesse, welche bereits einen angemessenen Reifegrad haben und die Geschäftsprozesse eines Unternehmens bestmöglich unterstützen. Um ein Beispiel zu nennen: Um Cybersicherheitsvorfälle zu erkennen und zu bewältigen, muss die IT-Infrastruktur eines Unternehmens zunächst ausreichend überwacht werden. Dann müssen geeignete Prozesse implementiert sein, damit Störungen als solche überhaupt erkannt und den Verantwortungsträgern zugewiesen werden, und schließlich muss eine Störung mit den Auswirkungen auf Ebene des Geschäftsprozesses oder des Kundenservices korreliert werden können, um deren Tragweite zu verstehen. Dies schafft die Grundlage, um den Incident richtig zu kategorisieren und angemessene Schritte einzuleiten: Was ist zu tun, um die Störung schnellstmöglich zu beheben? Wer muss sich darum kümmern? Welche Sofortmaßnahmen zur Schadensminimierung sind zu treffen? Wer ist über den Vorfall zu informieren? Diese Fragen sollten nicht erst im Ernstfall gestellt werden. Je besser mögliche Störungen und deren Schritte zur Bewältigung bereits im Vorfeld definiert, geschult und geübt wurden, umso schneller und zielgerichteter kann mit Störungen umgegangen werden, und bewahrt ein Unternehmen im besten Fall vor ernsthaften Schäden. Die Ausrichtung der IT-Prozesse sollte sich stets an den Maßnahmen, Prinzipien und Methoden des IT-Service-Managements (ITSM) orientieren. Dadurch wird eine optimale Unterstützung der Geschäftsprozesse durch die IT-Organisation erreicht. Denn adäquate IT-Prozesse dienen nicht nur

der Cybersicherheit, sondern tragen auch insgesamt dazu bei, dass eine Organisation ihre Geschäftsziele erreichen kann.

Risikomanagementmaßnahmen umsetzen: Sind die IT-Prozesse so weit vorbereitet, können die Cybersecurity-Maßnahmen in Angriff genommen werden. De facto erfolgt dieser Schritt aber meist Hand-in-Hand mit der Ausrichtung der IT-Prozesse.

Wie in nachfolgender Abbildung nochmals zusammenfassend dargestellt, muss für eine nachhaltige Sicherheitsarchitektur an drei Ebenen angesetzt werden: zuoberst braucht es ein ISMS, welches die Security Governance regelt, und zuunterst müssen angemessene IT-Prozesse geschaffen werden. Dies sind die Voraussetzungen, um die richtigen Cyber Security Maßnahmen nach den Vorgaben der Governance auf einer soliden Basis von IT-Prozessen umsetzen zu können.

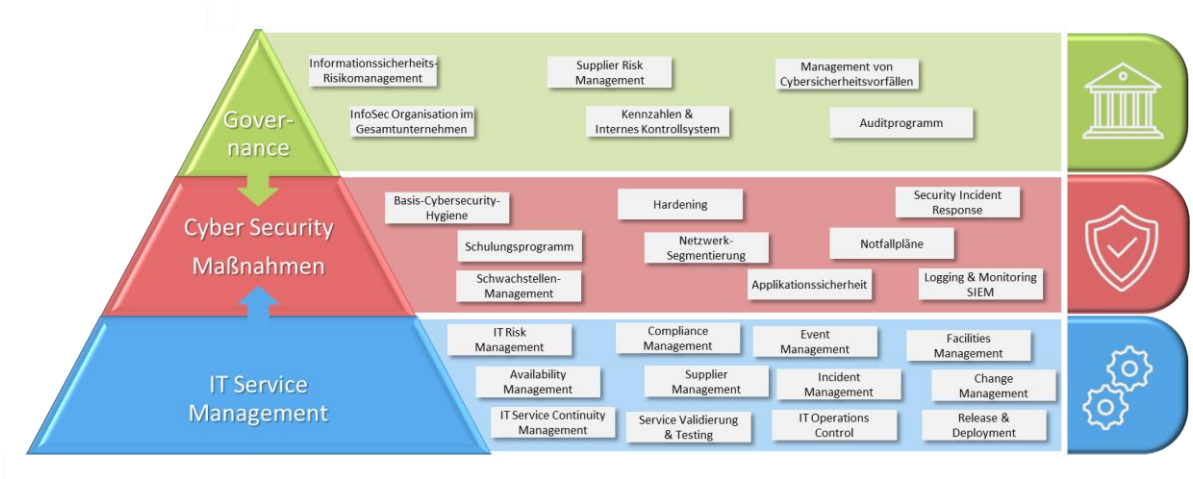

Abbildung 2: Modell für eine nachhaltige Sicherheitsarchitektur

Wirkung überprüfen und Ernstfall üben: Erst dieser letzte wichtige Schritt macht den PDCA-Zyklus vollständig und darf auf keinen Fall unterlassen werden. Gängige Methoden sind z.B. Penetrationtests, der Einsatz von Red-Teams oder Cybersicherheitsübungen. Legen Sie sich konkrete, realitätsnahe Krisenszenarien zurecht, spielen Sie sie durch und üben Sie die Notfallprozesse regelmäßig, um im Anlassfall auch in einer Stresssituation richtig reagieren zu können. Dies hilft auch, eine mögliche Krisensituation bzw. deren Bewältigung end-to-end besser zu verstehen. Viele einzelne Elemente auf technischer, prozessualer und organisatorischer Ebene müssen optimal ineinandergreifen, um ein zufriedenstellendes Ergebnis zu erzielen. Daraus resultieren wieder wichtige Erkenntnisse, um das Cyber Security Regelwerk im Unternehmen kontinuierlich weiterzuentwickeln.

Gerne begleiten wir Sie auf Ihrem Weg zur NIS-2 Compliance.

Wir von HMP bieten Ihnen ein professionelles Projektmanagement für Ihr Cybersicherheitsvorhaben. Dabei entwickeln wir einen nach Ihren Bedürfnissen zugeschnittenen Umsetzungsplan. Change-Management ist ein erfolgskritischer Faktor in einem NIS-2 Projekt. Je nachdem, wie stark das Thema Cybersecurity in Ihrem Unternehmen schon präsent ist, können umfangreiche Maßnahmen notwendig sein, um Mitarbeiter*innen auf das Thema Cybersecurity zu sensibilisieren und das Management von der Notwendigkeit des Projekts zu überzeugen. Wir sind erfahren darin, sie während eines solchen Veränderungsprozesses anzuleiten. Gemeinsam mit Ihren Fachexpert*innen führen wir ein initiales Assessment des derzeitigen Compliance-Levels durch, identifizieren Abweichungen zu den NIS-2 Anforderungen und ermitteln den konkreten Handlungsbedarf. Wir priorisieren diesen entsprechend Ihren vorhandenen Ressourcen und legen

gemeinsam die Roadmap fest. Darüber hinaus unterstützen wir Sie gerne in der Entwicklung und Optimierung Ihrer IT-Service Management Prozesse, um eine solide Basis für die Umsetzung der Cybersicherheitsmaßnahmen zu schaffen.

Im Bereich der Überprüfung der Cyber-Resilienz, dem Aufbau eines ISMS und der Umsetzung von konkreten Cybersicherheitsmaßnahmen arbeiten wir mit SBA Research zusammen. Durch ihre Forschungsaktivitäten auf dem Gebiet der Informationssicherheit entwickelt diese Einrichtung praktische und anwendbare Lösungen, welche die aktuellen Herausforderungen in der Cybersicherheit adressieren. SBA betreibt selbst ein ISMS gemäß ISO 27001 und ist eine „Qualifizierte Stelle“ (QuaSte) gemäß NIS-Gesetz – und somit legitimiert, die Sicherheitsvorkehrungen bei Betreibern wesentlicher Dienste zu überprüfen.

Sie befinden sich bereits auf dem Weg zur NIS-2 Compliance und suchen nur gezielte Unterstützung zu spezifischen Themenfelder? Auch dann helfen wir Ihnen gerne weiter. Sei es, wenn es um die Entwicklung einer Cybersecurity-Strategie geht, um die Ausarbeitung eines Desaster Recovery Plans, oder um ein Konzept zur Überwachung der IT-Infrastruktur – unser Ziel ist es, Ihnen eine umfassende und maßgeschneiderte Lösung für Ihre Cybersicherheitsbedürfnisse zu bieten.

Ihr persönlicher Ansprechpartner bei HMP:

Mag. (FH) Clemens Malt, MSc.

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

HMP BERATUNGSGMBH