ERGEBNISBERICHT

NIS2 STATUS CHECK

banet_ot

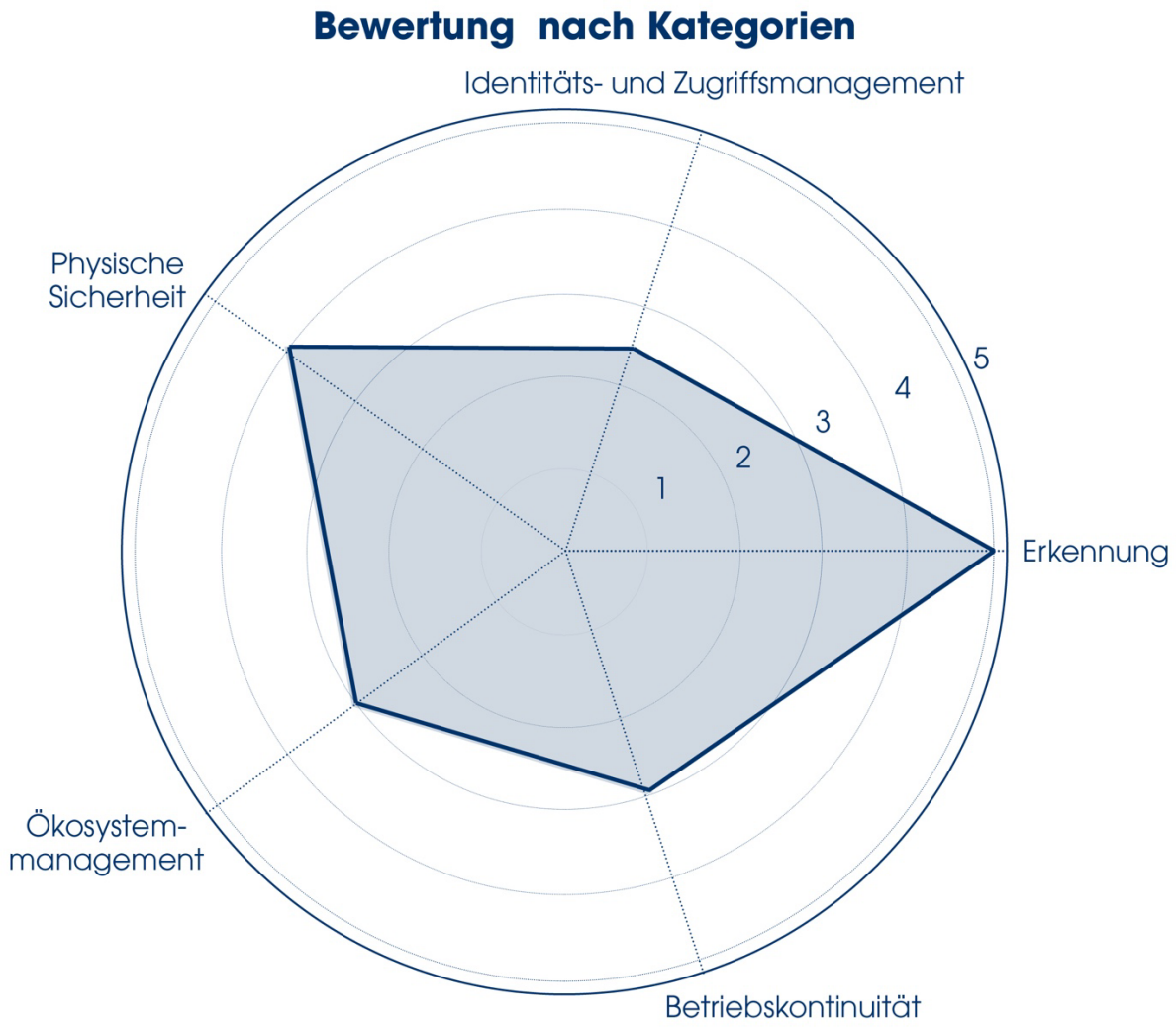
ENTSORGUNGSBETRIEB MÜLLER GMBH

(Abfallentsorgung)

INHALTSVERZEICHNIS

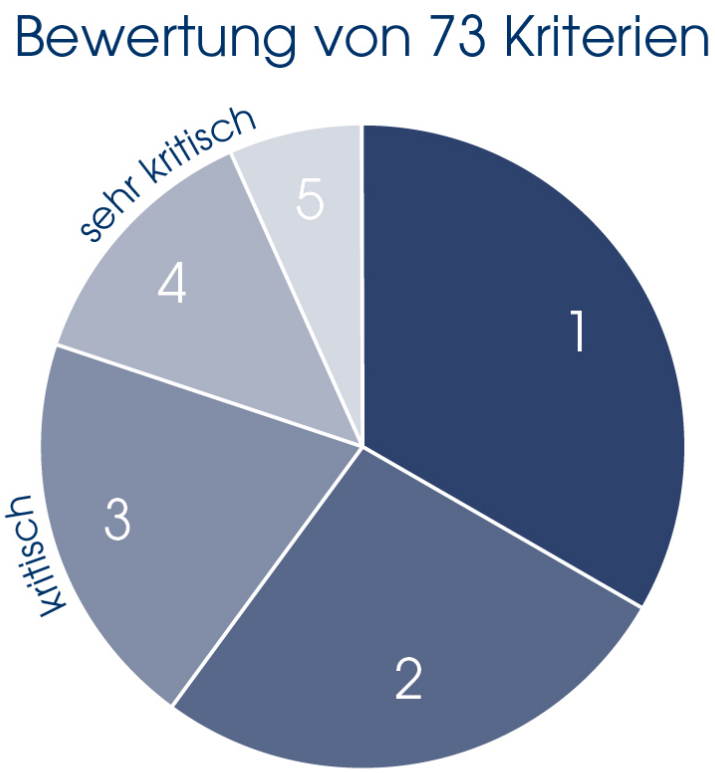
1. MANAGEMENT SUMMARY

Gemeinsam mit Ihrem Team haben wir mehr als 70 Kriterien der NIS2-Richtlinie in 5 Hauptkategorien analysiert. Die folgende Grafik gibt Ihnen einen Überblick über den aktuellen IST-Stand Ihres Unternehmens im Hinblick auf die Erfüllung der NIS2-Vorgaben in den jeweiligen Haupt-Kategorien.



Wie Sie der Grafik entnehmen können, ist Ihr Unternehmen in einigen Bereichen bereits bestens für die Erfüllung der Richtlinie vorbereitet (z.B. Erkennung von Sicherheitsvorfällen, physische Sicherheit). In anderen Bereichen gibt es noch Handlungsbedarf, um vollständig NIS2-konform zu werden.

Sie finden im nachfolgenden Diagramm die Beurteilung der einzelnen Kriterien nach dem Schulnotensystem.



Im Detail finden sich 20 (von 73) Kriterien mit einem dringenden Handlungsbedarf (must-haves, Schulnoten 4 und 5). In diesen Bereichen ist die Umsetzung von Maßnahmen unbedingt notwendig, um NIS2-konform zu werden. Kriterien, die mit Schulnote 3 bewertet wurden sind ebenfalls als kritisch zu werten, können aber mit niedrigerer Priorität behandelt werden.

1.1 GESAMTBEWERTUNG DES AKTUELLEN NIS2-REIFEGRADS

Die generelle Sicherheitskultur im Unternehmen ist bereits ausgeprägt, und es existieren schriftlich dokumentierte Sicherheitsrichtlinien sowie etablierte Risikobewertungsprozesse. Ebenso wurden für die meisten Systeme vernünftige technische Basismaßnahmen umgesetzt (z. B. Firewalls, regelmäßige Backups).

Reifegrad des Unternehmens	3,2 (Schulnotensystem)

Insgesamt weist das Unternehmen einen beachtlichen Reifegrad auf, da viele organisatorische und prozessuale Anforderungen bereits erfüllt sind. Die NIS2-Compliance ist in weiten Teilen vorbereitet.

Gleichwohl existieren einige kritische Schwachstellen, die behoben werden müssen, um den Anforderungen vollständig gerecht zu werden.

Die must-haves die nach unserer Auffassung unbedingt umgesetzt werden müssen umfassen:

- regelmäßige Cyberübungen
- Umsetzung der NIS2-Anforderungen in Verträgen mit Lieferanten
- Prozess für Deaktivierung nicht mehr benutzter Konten
- Implementierung von Notfallplänen

Mehr Informationen dazu erhalten Sie aus dem beiliegenden Excel-Ergebnisdokument.

1.2 DETAILLIERTE ERGEBNISSE DES STATUS-CHECKS

In diesem Musterbericht finden Sie nur einen kleinen Auszug der detaillierten Bewertung. Ihr Unternehmen erhält von uns eine Aufstellung sämtlicher Ergebnisse in mehr als 70 Bereichen – in unserem Beispielreport finden Sie einen beispielhaften Auszug unseres fiktiven Musteruntenehmens.

Hauptkategorie	Beschreibung	Frage	Nachweis	Antwort des Kunden	Note	Anmerkungen von banet GmbH bezüglich Verbesserungspotential
Erkennung	Der Betreiber richtet ein Protokollierungssystem auf jedem kritischen Informationssystem (CIS) ein, um Ereignisse aufzuzeichnen, die sich mindestens auf die Benutzerauthentifizierung, die Verwaltung von Konten und Zugriffsrechten, Änderungen an Sicherheitsregeln sowie die Funktionsweise des CIS beziehen.	Wurden die Systeme so konfiguriert, dass eine automatische Registrierung und Eskalation von Vorfällen an die zuständigen Personen möglich ist?	Systeme, Werkzeuge und Verfahren zur Erkennung und Analyse von Vorfällen.	*Wir nutzen teilweise die Cloud-Lösung "Loggly", jedoch ist diese nicht für alle unsere Systeme umsetzbar. Dies liegt an der Heterogenität unserer Infrastruktur, die aus verschiedenen Plattformen besteht, darunter Windows, Linux, Steuerungssysteme, S4 und B&R.*	2	Verbesserungsmöglichkeit: einheitliches Logging mittels rsyslog und zentraler lokaler Loggingserver.
Erkennung	Der Betreiber erstellt ein System zur Protokollkorrelation und -analyse, das die von dem auf jedem CIS installierten Protokollierungssystem aufgezeichneten Ereignisse auswertet, um Ereignisse zu erkennen, die die Sicherheit des CIS beeinträchtigen.	Führen Sie Übungen zur Informationssicherheit durch?	Nachweise über durchgeführte Cyber-Übungen, einschließlich der Daten, an denen sie durchgeführt wurden.	*Cyberübungen wurden bislang nicht durchgeführt. Das Thema wurde zwar am Rande bereits angesprochen, jedoch weder konkret geplant noch umgesetzt oder simuliert.*	5	Es wird empfohlen, systematisch Nachweise über durchgeführte Cyber-Übungen zu dokumentieren. Dabei sollten die Übungen klar definiert und die relevanten Szenarien, Daten und beteiligten Systeme aufgeführt werden. Beispiele könnten sein: Disaster Recovery Szenarien (DRS), Playbooks für spezifische Vorfälle wie ein verlorenes Telefon oder einen Malware-Angriff auf einen Client-PC. Eine regelmäßige Überprüfung und Aktualisierung der Playbooks sowie die Evaluation der Ergebnisse der Übungen sollten ebenfalls festgelegt werden.
Ökosystemmanagement	Der Betreiber erstellt eine Richtlinie für seine Beziehungen zu seinem Ökosystem, um die identifizierten potenziellen Risiken zu mindern. Dies umfasst insbesondere, aber nicht ausschließlich, Schnittstellen zwischen den CIS und Dritten.	Sind die Sicherheitsanforderungen in den Verträgen mit Dritten enthalten?	Explizite Sicherheitsanforderungen in den Verträgen mit Dritten, die IT-Produkte, IT-Dienstleistungen, ausgelagerte Geschäftsprozesse, Helpdesks usw. liefern.	*Sicherheitsanforderungen sind in Verträgen mit Dritten teilweise enthalten, jedoch nicht durchgängig und standardisiert. Es gibt Bereiche, in denen diese Anforderungen klar definiert sind, während in anderen noch Optimierungsbedarf besteht.*	3	Es wird empfohlen, Sicherheitsanforderungen in Verträgen mit Dritten zu standardisieren und durchgängig festzulegen. Dabei sollten klare Richtlinien erstellt werden, die in allen relevanten Verträgen einheitlich umgesetzt werden. Eine regelmäßige Überprüfung der bestehenden Verträge sowie die Einbeziehung von Sicherheitskriterien in den Vertragsabschlussprozess könnten dazu beitragen, die Lücken zu schließen und die Anforderungen konsistent zu gestalten.
Identitäts- und Zugriffsmanagement	Für die Identifizierung richtet der Betreiber eindeutige Konten für Benutzer oder automatisierte Prozesse ein, die auf Ressourcen seines CIS zugreifen müssen. Nicht verwendete oder nicht mehr benötigte Konten sind zu deaktivieren. Ein regelmäßiger Überprüfungsprozess sollte eingerichtet werden.	Werden ungenutzte oder nicht mehr benötigte Konten deaktiviert?	Regeldefinition für das Löschen nicht mehr genutzter Konten nach einem kurzen Zeitraum.	*Ungenutzte oder nicht mehr benötigte Konten werden nur teilweise deaktiviert, meistens dann, wenn darauf hingewiesen wird oder es auffällt. Ein strukturierter Ansatz mit Checklisten und klaren Freigabeprozessen ist nicht nachvollziehbar etabliert.*	5	Es wird empfohlen, einen strukturierten Prozess für die Deaktivierung ungenutzter oder nicht mehr benötigter Konten einzuführen. Dies sollte durch die Verwendung von Checklisten und klar definierten Freigabeprozessen unterstützt werden. Regelmäßige Überprüfungen der Konten sowie ein automatisiertes Monitoring könnten zusätzlich helfen, ungenutzte Konten frühzeitig zu identifizieren und zeitnah zu deaktivieren.
IT-Sicherheitswartung	Der Betreiber entwickelt und implementiert ein Verfahren zur Sicherheitswartung in Übereinstimmung mit seiner Informationssicherheitsstrategie (ISSP). Zu diesem Zweck definiert das Verfahren die Bedingungen, die es ermöglichen, das minimale Sicherheitsniveau für CIS-Ressourcen aufrechtzuerhalten.	Werden Software- und Hardware-Ressourcen regelmäßig gewartet und aktualisiert?	Formal dokumentierte Software- und Hardwareanforderungen zur Sicherstellung der Kompatibilität. Das Asset-Management für Software und Hardware ist formal dokumentiert und wird regelmäßig gepflegt.	*Software- und Hardware-Ressourcen werden zwar regelmäßig gewartet und aktualisiert, jedoch nicht nach einem festen Plan und auch nicht vollständig. Häufig erfolgen Updates situativ, wenn Probleme oder Notwendigkeiten erkannt werden. Dabei kommt es gelegentlich vor, dass ein Update Auswirkungen auf das Tagesgeschäft hat, da anschließend weitere Software angepasst oder aktualisiert werden muss.*	2	Verbesserungsmöglichkeit: geplanten Wartungszyklus zu etablieren, der dokumentiert und durch Checklisten unterstützt wird. Dadurch können potenzielle Auswirkungen auf das Tagesgeschäft minimiert und eine koordinierte Aktualisierung aller abhängigen Systeme sichergestellt werden.
Physische Sicherheit	Der Betreiber verhindert unbefugten physischen Zugang, Beschädigung und Störung der Informations- und Datenverarbeitungsanlagen der Organisation.	Hat nur eine begrenzte Anzahl autorisierter Personen mit berechtigtem Zugang und entsprechenden Berechtigungsnachweisen Zugang zu Räumlichkeiten, die Informationssysteme enthalten?	Liste des Personals mit berechtigtem Zugang und Berechtigungsnachweisen	*Ja, der Zugang zu Räumlichkeiten, die Informationssysteme enthalten, ist auf eine begrenzte Anzahl autorisierter Personen beschränkt. Es wird ein elektronisches Schließsystem genutzt, und zusätzlich sorgen Überwachungskameras für eine verstärkte Sicherheitsüberwachung.*	1	-
Betriebskontinuität	In Übereinstimmung mit seiner Informationssicherheitsstrategie (ISSP) definiert der Betreiber Ziele und strategische Leitlinien für das Business Continuity Management im Falle eines IT-Sicherheitsvorfalls.	Sind Notfallpläne für die Systeme, die wesentliche Dienste unterstützen, in der Organisation implementiert?	Notfallpläne für kritische Systeme, einschließlich klarer Schritte und Verfahren für gängige Bedrohungen, Auslöser für die Aktivierung, Maßnahmen und Wiederherstellungszeitziele (RTO).	*Notfallpläne für die Systeme, die wesentliche Dienste unterstützen, sind in der Organisation teilweise implementiert. Allerdings sind diese Pläne veraltet, enthalten Lücken und beinhalten keine aktuellen Zugangsdaten oder Kennwörter.*	3	Es wird empfohlen, die bestehenden Notfallpläne umfassend zu überarbeiten und zu aktualisieren. Dabei sollten sämtliche Lücken geschlossen und aktuelle Zugangsdaten sowie Kennwörter integriert werden. Zusätzlich sollte ein regelmäßiger Überprüfungsprozess etabliert werden, um sicherzustellen, dass die Pläne stets auf dem neuesten Stand sind und den Anforderungen der wesentlichen Dienste entsprechen.

Beispielreport des fiktiven Musterunternehmens. Sie erhalten von uns ein Excel-Dokument mit allen Informationen zu Ihrem Fast-Track-Status-Check.

2. FAZIT UND NÄCHSTE SCHRITTE

Die Entsorgungsbetrieb Müller GmbH verfügt bereits über solide Grundstrukturen, um NIS2-Compliance zu erreichen. Organisatorische und prozessuale Anforderungen sind weitgehend erfüllt, ein Risikobewusstsein ist vorhanden. Wesentliche Verbesserungen liegen nun in der Beseitigung vorhandener Schwachstellen.

2.1 NÄCHSTE SCHRITTE

- Prioritäre Umsetzung der Sofortmaßnahmen:
  Kriterien mit Schulnote 4 & 5
- Planung für mittelfristige Maßnahmen (Schulnote 3), insbesondere ein umfassendes Lieferanten- und Schwachstellenmanagement.
- Langfristige Verfestigung der Sicherheitskultur durch regelmäßige Audits, (optional) Zertifizierungen und Schulungen.
- Mit diesen Schritten kann das Unternehmen die vorhandenen Stärken weiter ausbauen, die bestehenden technischen Lücken schließen und die Anforderungen der NIS2-Richtlinie nachhaltig erfüllen.

2. EMPFEHLUNG FÜR WEITERFÜHRENDE MAßNAHMEN

Unser NIS2-Fast-Track Roadmap-Paket mit Umsetzungsplan

Auf Basis des Status-Checks erstellen wir eine Roadmap für die noch offenen Compliance-Punkte, damit Sie schnell und effektiv ans Ziel gelangen.

Ergebnis: Eine klare, individuelle Roadmap zur NIS2-Compliance

Vorteile:

- Konkrete Antworten auf alle wichtigen Fragen zu Kostenrahmen, Ressourcen und Zeitplan
- Fokus auf die Must-haves, um schnell und zuverlässig NIS2-Compliance zu erreichen.
- Geringes Zeit- und Ressourceninvestment (typisch 8-16 Stunden Ihrer Fach- und Führungskräfte)
- Klare Entscheidungsgrundlage für schnelle Fortschritte
- Make or buy – Empfehlungen gemeinsam mit Ihrem Team erarbeitet

Aufgrund der Analyse stellen wir -gemeinsam mit Ihrem Team- mehrere Optionen entsprechend Ihrem gewünschten Risiko-Profil zur Verfügung: Must-haves-only, Quick Wins, Good Value, Maximum Security.

Daraus ergibt sich direkt ihre optimale kurzfristige und langfristige Roadmap