IT-IMPROVEMENT
run your business smarter

# NIS2-UMSETZUNG IN 4 SCHRITTEN: **ALLES FÜR IHRE UNTERNEHMENS- & CYBERSICHERHEIT**

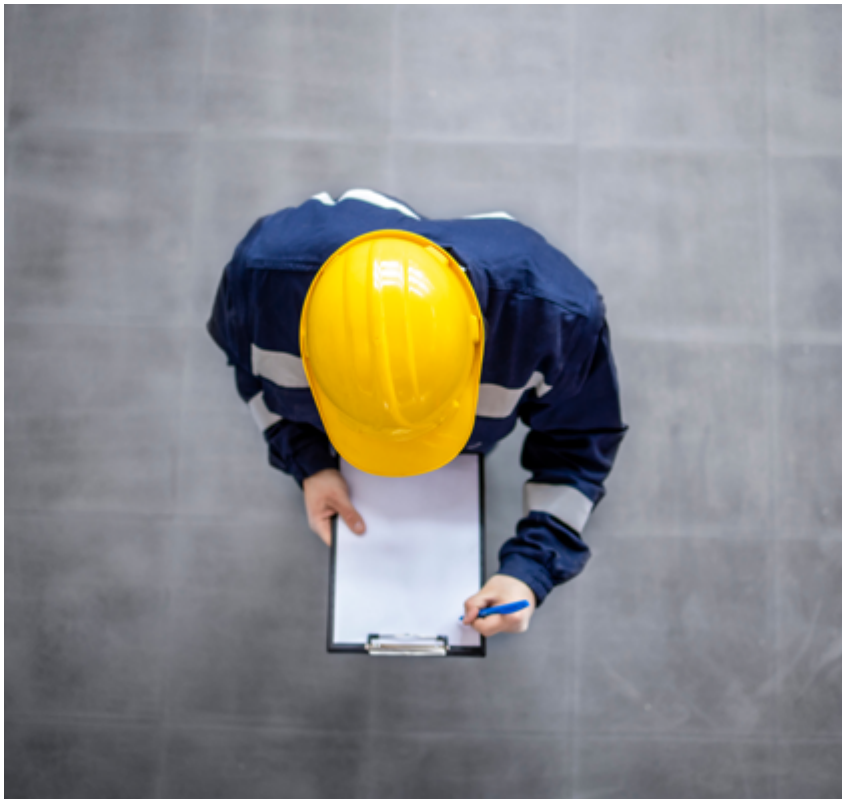
IT-IMPROVEMENT
run your business smarter

# INHALT

# MIT NIS2 IHR CYBER-SECURITY-NIVEAU **OPTIMIEREN & HARMONISIEREN**

NIS2 ist Europas Antwort auf die allgegenwärtigen Cyberbedrohungen, denen Unternehmen zunehmend ausgesetzt sind. **Gerade auch kleine und mittlere Unternehmen (KMUs) werden immer häufiger zum Ziel von Cyberattacken –** laut dem BSI-Lagebericht 2023 steigen die Zahlen betroffener Betriebe stetig an. Diese Angriffe führen häufig zu immensen wirtschaftlichen Schäden und schwächen die Unternehmensreputation. Vielfach werden **Daten** von KundInnen und GeschäftspartnerInnen sowie andere sensible Informationen **abgegriffen, manipuliert, gelöscht, verschlüsselt, im Darknet zum Kauf angeboten oder gar für weitere Hackerangriffe und andere Straftaten verwendet.**

Untersuchungen zeigen, dass KMUs in der Regel zwar nicht zielgerichtet als Opfer ausgewählt, sondern vielmehr von **großvolumigen und automatisiert durchgeführten Angriffen getroffen** werden. Vor diesem Hintergrund kommen den Maßnahmen und Vorgaben aus der NIS2-Richtlinie, die ab Oktober 2024 verpflichtend eingehalten werden müssen, besondere Bedeutung zu: Es geht darum, die **Cyberresilienz für all diejenigen Unternehmen zu stärken, die GeschäftspartnerInnen von Unternehmen sind, die zu den 18 „wesentlichen" und „wichtigen" Sektoren gehören.** Damit gehören mit NIS2 weitaus mehr Unternehmen zum Kreis der besonders schützenswerten Organisationen.



**18 KRITIS SEKTOREN**

**WESENTLICHE**
Unternehmen & Organisation

**in 11 Sektoren mit hoher Kritikalität**

- Energie
- Gesundheit
- Transport
- Trinkwasser
- Bankwesen
- Abwasser
- Finanzmärkte
- Weltraum
- ICT Service Management
- Öffentliche Verwaltung
- Digitale Infrastruktur

**WICHTIGE**
Unternehmen & Organisation

**in 7 Sonstigen kritischen Sektoren**

- Post
- Industrie
- Abfall
- Forschung
- Chemikalien
- Lebensmittel
- Digitale Dienste

# NEU BEI NIS2:
# GESCHÄFTSPARTNERINNEN ENTLANG DER LIEFERKETTE

Neu ist auch, dass Betriebe in diesen Sektoren sicherstellen müssen, dass die **NIS2-Umsetzung auch entlang ihrer eigenen Lieferkette regelkonform** erfolgt. Und das aus gutem Grund: **98% der Unternehmen, die von Ransomware – Attacken betroffen sind, arbeiten mit Geschäftspartnern** zusammen, die innerhalb der letzten Jahre **Datenlecks** aufgedeckt haben. Abgesehen davon haben die multiplen Krisen der letzten Jahre gezeigt, wie schwerwiegend die Konsequenzen von gestörten Lieferketten sein können.

Kurzum: Selbst, wenn Sie mit Ihrem Unternehmen nicht die NIS2-Schwellenwerte von mehr als 50 Mitarbeitenden und zehn Millionen Euro Jahresumsatz erreichen, sind Sie nicht unbedingt außen vor. Sofern Ihr Unternehmen in einer **relevanten Geschäftsbeziehung** als LieferantIn, System- oder EntwicklungspartnerIn steht, können Sie durchaus von Ihren KundInnen in die Pflicht genommen werden, **die Erfüllung der NIS2-Kriterien nachzuweisen.**

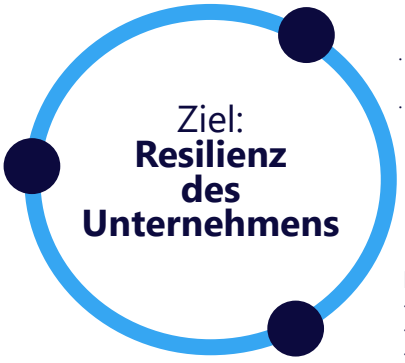
Abgesehen von der Pflicht ist NIS2 vor allem eines: **Die Chance für den Aufbau Ihrer Cyberresilienz.** Das Regelwerk beinhaltet alle wichtigen Aspekte und Mindeststandards der IT- und Cybersicherheit, die heute jedes Unternehmen erfüllen sollte – allein schon für die eigene Unternehmenszukunft.

Darüber hinaus wappnen Sie sich auch gleich für weitere Gefahren, indem Sie **Umweltkatastrophen wie Hochwasser in einem Allgefahrenplan berücksichtigen** und entsprechende **Maßnahmen für die Fortführung des Geschäftsbetriebs** planen und umsetzen.

**Im Fokus bei NIS2:**
**Ihre Lieferkette:**
Ein komplexes Thema ist die Sicherheit in der Lieferkette. Denn NIS-2 verlangt deren Absicherung in Bezug auf die Netz- und Informationssysteme und die physische Umwelt dieser Systeme. Somit können selbst kleinere Betriebe „NIS2-pflichtig" werden, wenn größere Player ihre Lieferkette absichern wollen und von ihnen als Zulieferer entsprechende Nachweise verlangen.

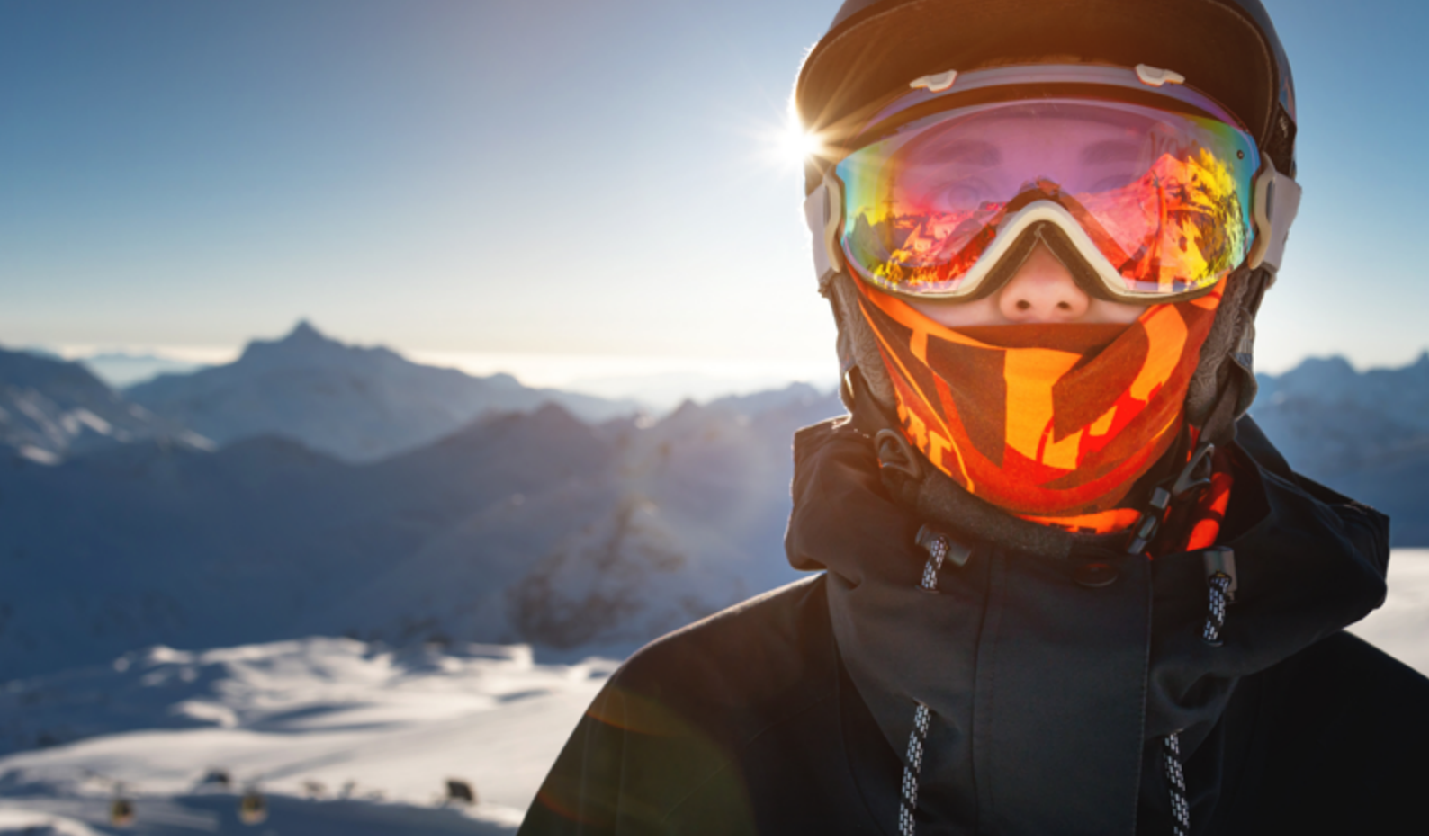
**Organisation**
- Einführung eines **Information Security Management Systems** ISMS (ggf. spätere DIN ISO 27001 Zertifizierung)
- Aufbau eines umfassesnden Risikomanagements
- Etablierung eines **Geschäftsfortführungsplans Business Continuity**

**Geschäftsführung & Mitarbeitende**
- **Sensibilisierung** der Mitarbeitenden
- **Schulungen** für Mitarbeitende UND Geschäftsführung
  - Einkauf (Supply Chain)
  - Geschäftsbereiche (Risikomanagement)
  - IT-Sicherheit
  - Geschäftsführung
- **Haftung** des Unternehmens UND der Geschäftsführung




**IT-Landschaft**
- **Schutz** vor Cyberangriffen
- **Management** von Cyberrisiken
- **Früherkennung** von Cybersicherheitsvorfällen
- **Minimierung** der Auswirkungen von Cybersicherheitsvorfällen

Die gute Nachricht ist: **Die Einführung der Mindeststandards braucht nur ein paar kleine Schritte und Maßnahmen.** Auf dem Weg begleiten wir Sie wie gewohnt mit unserem Know-How und entlasten Sie mit unseren Services entsprechend Ihren Vorstellungen.



# IN 4 PHASEN
# SICHER ZUR NIS2-UMSETZUNG

Die NIS2-Richtlinie verlangt nicht nur mehr Maßnahmen als ihre Vorgängerin, die Network-and-Information-Security-Richtlinie aus dem Jahr 2016, sondern übersteigt auch die Vorgaben des deutschen IT-Sicherheitsgesetzes 2.0. Sie umfasst sowohl **technische als auch organisatorische Mindeststandards,** sodass Sie sich **ganzheitlich** mit Ihren **eingesetzten Technologien, Prozessen, Governance-Strukturen, rechtlichen Rahmenbedingungen und Mitarbeitenden** beschäftigen müssen.

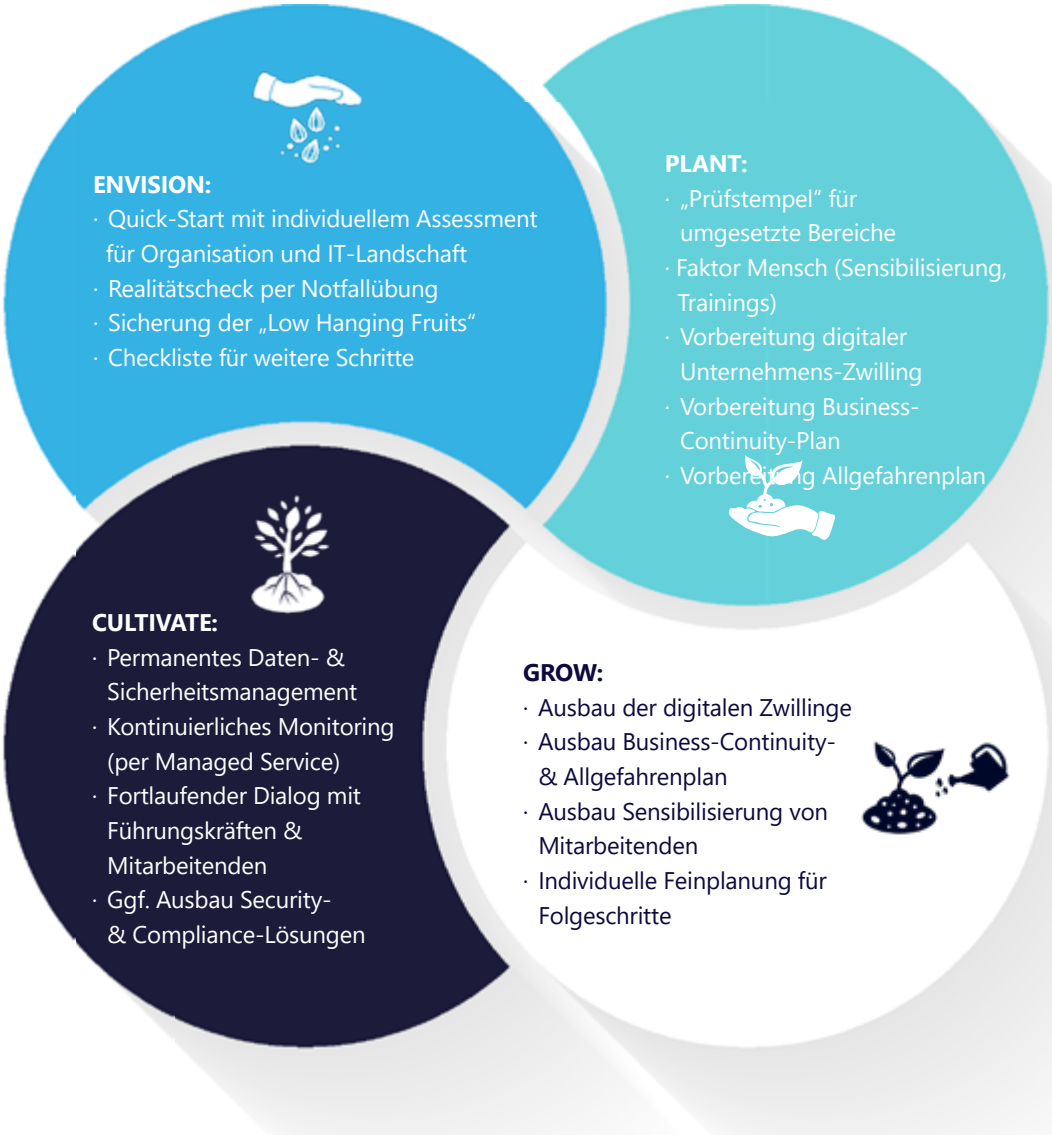
Die zentrale Anforderung der künftig verpflichtenden EU-Richtlinie ist das **Einbeziehen der IT-Sicherheit in die globale Unternehmenssteuerung.** Weitere Vorgaben betreffen ein stringentes **Risikomanagement, die Sensibilisierung und Schulung von Mitarbeitenden,** Regelungen für das **Melden von Vorfällen** sowie das Vorhalten von **Notfallplänen** für den Ernstfall.

Es ist also höchste Zeit für Sie und Ihr Unternehmen, sich mit den NIS2-Vorgaben vertraut zu machen und die IT- und Cybersicherheit auf den neuesten Stand zu bringen. Getreu unseres Mottos „Starten statt Warten" möchten wir Ihnen auf den folgenden Seiten ein 4-Phasen-Modell vorstellen, mit dem wir Ihre NIS2-Umsetzung kontinuierlich begleiten:

„Mit Cybersecurity verkaufen Unternehmen erstmal kein Stück mehr. Ohne Cybersecurity verkaufen Unternehmen allerdings überhaupt kein Stück mehr."

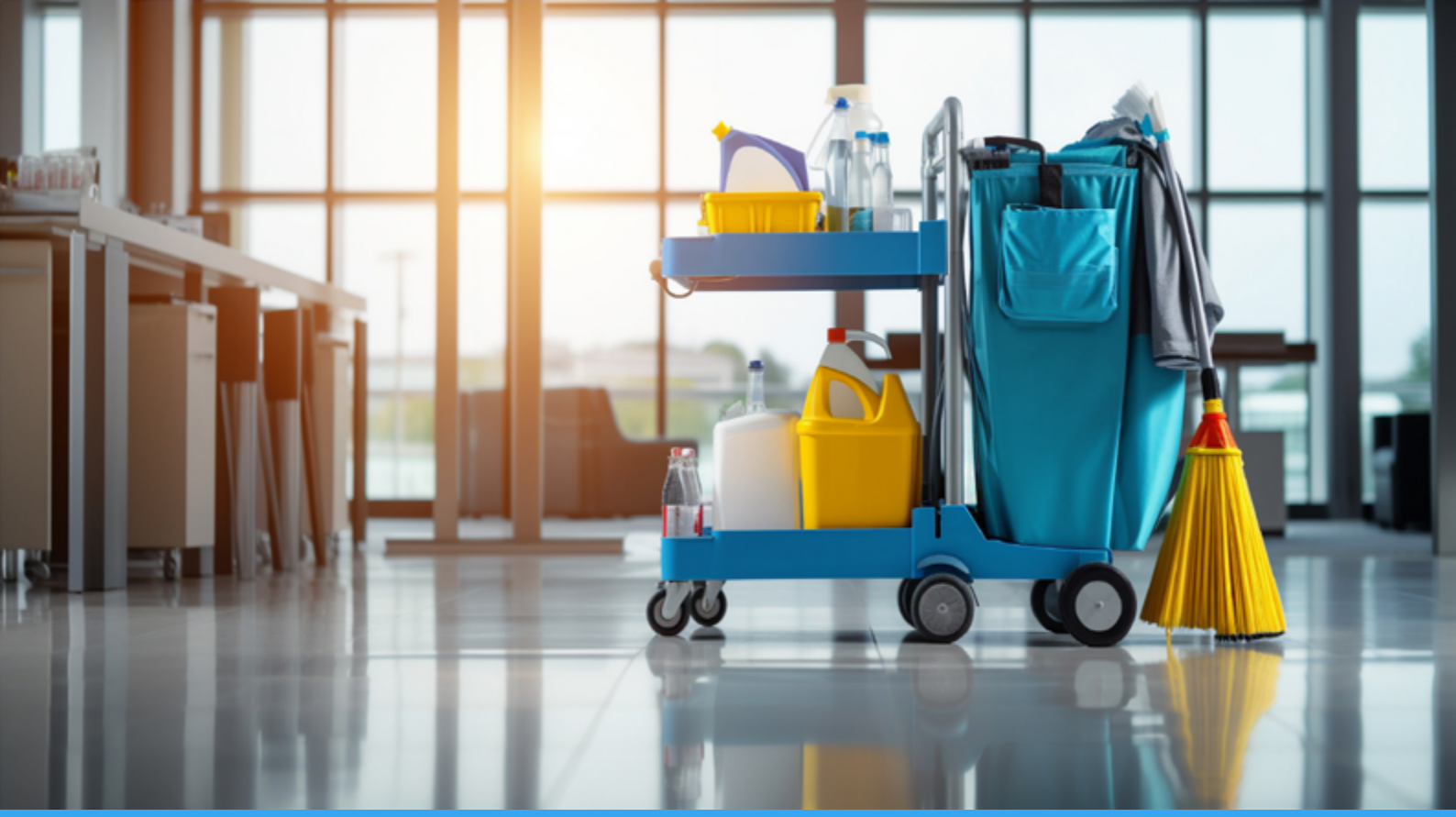
Rainer Rehm
Präsident (ISC)² Chapter Germany

# DIE 4 PHASEN
# ENVISION, PLANT, GROW & CULTIVATE




**Klare Grenzen für NIS2 – oder doch nicht? Fallbeispiel 1**

Ein inhabergeführter Sanitärbetrieb möchte sich bei der Ausschreibung für einen neuen Wartungsauftrag an die Spitze setzen – die kommunale Kläranlage soll betreut werden. Der Auftraggeber gilt als KRITIS-Betreiber und verlangt somit, dass auch die beauftragten Firmen die NIS2-Richtlinie erfüllen, um seinen eigenen Lieferkettenverpflichtungen nachzukommen. Denn bei Compliance-Verstößen drohen hohe Bußgelder und Sanktionen.



# PHASE 1: ENVISION - **GRUNDLEGENDE CYBERHYGIENE**

In der heutigen Zeit kann praktisch jedes Unternehmen ins Visier von Cyberkriminellen geraten. Die Folgen solcher Angriffe sind nicht nur ein **finanzieller Schaden und Reputationsverluste,** sondern auch ganz konkrete **„Datenlecks" und Systemausfälle,** durch die der laufende **Betrieb massiv beeinträchtigt** wird. Die gute Nachricht lautet jedoch, dass Sie genau diese Risiken mit einigen zentralen Maßnahmen minimieren können. Und damit schützen Sie zugleich Ihr Unternehmen und Ihre KundInnen.

In der NIS2-Richtlinie werden die entsprechenden technischen Maßnahmen zur Absicherung von Unternehmen als **„Cyberhygiene"** bezeichnet. Sie umfassen unter anderem eine **systematische Datensicherung, stichhaltige Konzepte für die Zugriffskontrolle, ein sicheres Management von Schwachstellen und die Verschlüsselung von Informationen. Risikoanalysen** helfen Ihnen darüber hinaus, **potenzielle Problembereiche zu erkennen und einzudämmen.**

Neben den technischen Maßnahmen sind auch organisatorische Schritte zu planen und umzusetzen. Alleine die Frage, **wieviel Zeit die Wiederherstellung Ihres Geschäftsbetriebs in Anspruch nimmt,** ist ein wichtiger Baustein Ihres **Business Continuity Plans**.

Die nachfolgenden Aufgabenpakete sollten Sie in dieser ersten Phase angehen:

**Die nachfolgenden Aufgabenpakete sollten Sie in dieser ersten Phase angehen:**

1. **Quick-Start mit individuellem Assessment**
Wie „NIS2-ready" ist Ihr Unternehmen? Mit unserem strukturierten Fragen- und Prüfkatalog, dem **Secure Score Quick Assessment**, finden Sie es heraus! Wir erheben gemeinsam mit Ihnen den **aktuellen Stand Ihrer IT-Infrastruktur und definieren kurz-, mittel- und langfristige Maßnahmen.** Dabei behalten wir immer das Ziel im Blick und gehen mit einem hohen Grad an Pragmatismus vor.

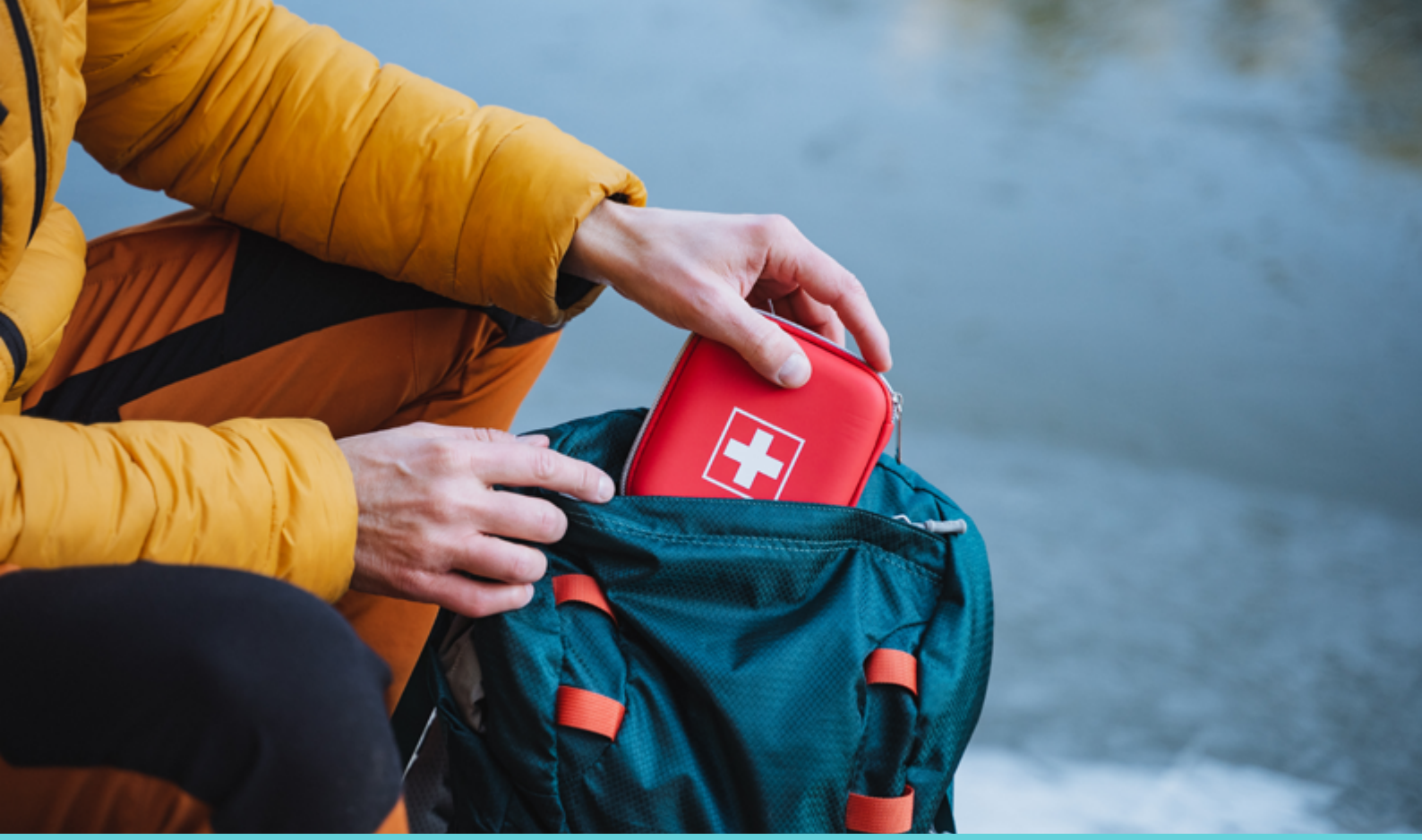
2. **Realitäts-Check per Notfallübung**
Die zweite Frage, die Sie sich stellen mögen ist: Wie effektiv und effizient ist unser Risikomanagement in einem echten Notfall? Die umfassendste Antwort darauf liefert Ihnen eine möglichst realitätsnahe Notfall-Übung. Setzen Sie sich selbst außer Gefecht und stellen Sie Ihr Risikomanagement auf den Prüfstand. Die wichtigste Frage wird sein: Wie lange benötigen Sie für die Wiederherstellung Ihres Geschäftsbetriebs? Wusste jeder Mitarbeitende, was zu tun ist? Welche Bereiche waren betroffen und inwieweit konnten Sie schwerwiegende Schäden vorab abwehren?

3. **Sicherung der „Low Hanging Fruits"**
Mit welchen Technologien und Prozessen sind Sie schon gut für die NIS2-Vorgaben aufgestellt? Hier setzen wir an, um **mit kleinen Optimierungen maximale Wirkung zu erzielen.** Sie arbeiten zum Beispiel mit Microsoft 365? Perfekt – damit lassen sich viele Vorgaben vergleichsweise rasch abbilden. Im gleichen Zuge vermerken wir offene Punkte und komplexere Aufgaben, um die wir uns in einer späteren Phase kümmern wollen.

4. **Checkliste für weitere Schritte**
Wo haben Sie noch Handlungs- oder Nachholbedarf, wo müssen Sie die richtigen Voraussetzungen schaffen, um NIS2 künftig zu erfüllen? Unsere Analyse zeigt Ihnen **Lücken** auf, und wir geben Ihnen eine **Checkliste** an die Hand, wie Sie diese **effektiv schließen** können. Ergänzend empfehlen wir Ihnen auch Security- und Compliance-Lösungen aus dem Microsoft Security Portfolio, die zu Ihren Anforderungen passen.

10.000 Microsoft

Security Spezialisten arbeiten an 365 Tagen 24 Stunden für die Sicherheit Ihres Unternehmens. Zum Vergleich: Das BSI hat 1750 Experten, das BKA 300 Cybercrime Experten und die Bitkom 100.



# PHASE 2: PLANT -
# **SCHRITT FÜR SCHRITT ZUR PLANUNG FÜR DEN NOTFALL**

Die Nachrichten der letzten Jahre beweisen es fast täglich: Cyberangriffe können heute jedes Unternehmen treffen, gleiches gilt für Umweltkatastrophen wie Überschwemmungen oder flächendeckenden Stromausfall. Eine 100% Absicherung gegen den Ernstfall gibt es nicht, deshalb ist die **Vorsorge für den Ernstfall genauso wichtig wie die Absicherung.**

Unsere Vorsorge für den Notfall umfasst gleich mehrere Schwerpunkte: Grundlage bildet ein **Allgefahrenplan,** der sämtliche Maßnahmen, Prozesse und Verantwortlichkeiten für den Notfall umfasst. Er gilt sowohl für Cyberangriffe als auch für sämtliche andere Katastrophen wie Hochwasser, Brand, Stromausfall etc.

Neben einem Allgefahren-Notfallplan muss auch Ihr Unternehmen möglichst unterbrechungsfrei weiterarbeiten können. Die entsprechenden Maßnahmen werden in einem **Business Continuity Plan - Geschäftsfortführungsplan** definiert. Ein wichtiger Teil dabei ist natürlich Ihre IT, genau hierfür haben wir Lösungen, die Ihnen eine **praktisch reibungslose Fortführung Ihrer Geschäftstätigkeit** ermöglichen.

1. **„Prüfstempel" für umgesetzte Bereiche**

Mit einigen bereits bei Ihnen vorhandenen Technologien und Prozesse entsprechen Sie nach unserer gemeinsamen Bewertung den Vorgaben? Glückwunsch, **die ersten Punkte für Ihre NIS2-Readiness sind erledigt.** Damit haben Sie bereits handfeste Beweise bei einer möglichen NIS2-Prüfung. Wir beraten Sie gern, wie Sie von hier aus am besten weiter vorgehen, die richtigen Prioritäten setzen und gegebenenfalls in passende Lösungen investieren können, die vor allem eines tun sollen: den Aufwand für Sie verringern.

2. **Faktor Mensch: Sensibilisierung und Trainings**

Nur wer weiß, wo die Gefahren und Stolperfallen in der digitalen Landschaft lauern, kann sich schützen: Nach diesem Ansatz ist es uns ein besonderes Anliegen, dass **alle Ihre Führungskräfte und Mitarbeitenden zu einer schlagkräftigen Mannschaft werden, die Cyberangriffe gemeinschaftlich vereitelt.** Im Schulterschluss mit dem Institute for Security and Safety UNISS und der Managementberatung VICCON bieten wir Ihnen Zugang zu maßgeschneiderten Aufklärungs- und Schulungskonzepten.

3. **Vorbereitung der digitalen Zwillinge**

Kennen Sie schon das Konzept eines **digitalen Zwillings?** Sie sind ein wesentlicher Bestandteil des **Desaster Recovery Plans**, und bilden Ihre **gesamte IT-Infrastruktur ebenso wie Ihre Endgeräte** in einer **sicheren Umgebung virtuell** nach und versorgen diese kontinuierlich mit genau den Aktualisierungen, die Sie auch an Ihren „realen" Systemen vornehmen.

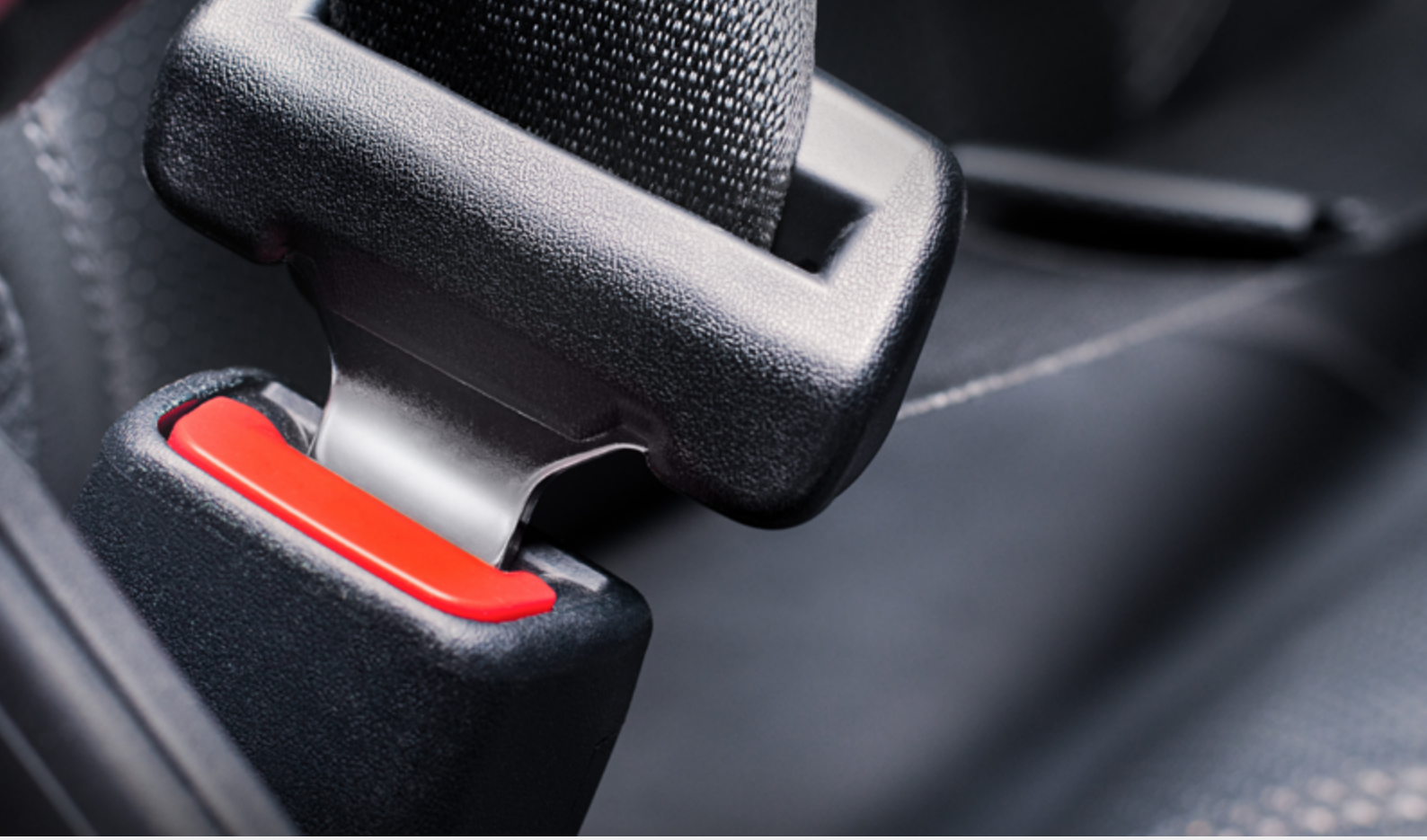
Der große Vorteil: Im Falle eines Systemausfalls – etwa aufgrund eines Cyberangriffs – lässt sich Ihre IT-Infrastruktur leicht wiederherstellen. Gleiches gilt für Ihre Endgeräte: Mit Windows365 oder Azure Virtual Desktop erhalten die Endgeräte Ihrer Mitarbeitenden einen virtuellen Zwilling und können nach einem Angriff praktisch unterbrechungsfrei weiterarbeiten.

4. **Vorbereitung Ihres Risikomanagements inkl. Business-Continuity-Plan**

Der Business Continuity Plan ist ein **praktischer Plan für die Aufrechterhaltung Ihrer Geschäftstätigkeit.** Denn im Fall aller Fälle müssen wichtige Funktionen auch bei Unterbrechungen der Betriebstätigkeit verfügbar sein – genau die gilt es in einem ersten Schritt zu definieren. Denn im Fall eines erfolgreichen Cyberangriffs oder einer Umweltkatastrophe zählt jede Minute und genau die gilt es mit einem professionellen Risikomanagement zu nutzen. Beispielsweise um neben den digitalen Zwillingen auch Ihre wichtigen Unternehmenssysteme und vor allem Ihre Daten nach einem Angriff schnell wieder herzustellen.

Die gute Nachricht ist: Mit Cloud-Technologien **stärken Sie Ihre Resilienz** und bleiben im **Notfall vor Informationsverlust oder -korrumpierung geschützt** – und sehen eventuellen Lösegeldforderungen gelassener entgegen.

Zudem schreibt die NIS2-Richtlinie verschiedene Vorgaben vor, unter anderem für das **Berichten von Sicherheitsvorfällen.** Einen Großteil der Arbeit nehmen Ihnen Werkzeuge wie Microsoft Defender und Microsoft Sentinel ab, und auch generative KI (wie Copilot for Security) spielt hier ihre Stärken aus, um Ihre Mitarbeitenden zu entlasten und ihnen mehr Zeit für andere wichtigere Aufgaben zu verschaffen. Denken Sie hier nochmal an die 10.000 Cybersecurity-Experten von Microsoft, die eine Menge Arbeit und ein gutes Stück Verantwortung abnehmen.



# PHASE 3: GROW - **ETABLIERUNG EINES UMFASSENDEN RISIKOMANAGEMENTS**

Die ersten wichtigen Schritte für Ihre Cyber-Resilienz sind getan. Jetzt geht es darum, alle Bereiche zu festigen und auszubauen. Denn wie auch Ihr Business sich weiterentwickelt, und jedes neue Geschäftsmodell abgesichert werden muss, erfinden Cyberkriminelle immer neue kreative Wege, um an Ihre Daten zu gelangen.

Dazu kommt, dass das die allgemeine Hektik des Arbeitsalltag die Wachsamkeit von uns allen beeinträchtigt. Deshalb ist es umso wichtiger, das Bewusstsein für die Cybergefahren regelmäßig zu schärfen und die Notfallmaßnahmen stets aktuell zu halten. Die entsprechenden Maßnahmen haben wir für Sie in unserer Phase Grow zusammengestellt:

**Klare Grenzen für NIS2 – oder doch nicht? Fallbeispiel 2**
Für Subunternehmer von Logistikpartnern und Speditionen ist zu erwarten, dass sie als kleinere Zustellbetriebe ebenfalls künftig die korrekte Umsetzung der NIS2-Vorgaben gegenüber ihren Auftraggebern nachweisen müssen. Insbesondere Anbieter von Gefahrguttransporten oder medizinische Lieferdienste sollten ihre IT-Systeme und Prozesse schon jetzt auf den Prüfstand stellen und auf die neuen Anforderungen abstimmen.


1. **Ausbau Ihrer digitalen Zwillinge**

Digitale Zwillinge ermöglichen Ihnen einen nahezu **unterbrechungsfreien Geschäftsbetrieb.** Voraussetzung hierfür ist, dass die digitalen Zwillinge den jeweils aktuellen Stand Ihrer Systeme, Daten und Geräte beinhalten. Dafür muss Ihre aktuelle IT-Landschaft nicht zwingenderweise komplett in die Cloud verlegt werden. Dennoch sorgen Cloud-Technologien dafür, dass durch **Virtualisierung der umfassende Schutz der IT-Infrastruktur** Ihres Unternehmens, einschließlich aller Netzwerke, Server, Endgeräte sowie On-Premises- und Cloud-Anwendungen gewährleistet wird. Für **On-Premises-Systeme** bietet sich beispielsweise die **Ausfallsicherung über Azure-Cloud-Rechenzentren** an, für Ihre Desktops und Mobilgeräte eine Vorbereitung mit **Virtual-Desktop-Verbindungen.** So bleiben Ihre Mitarbeitenden auch im Falle des Falles handlungsfähig.

Damit sind Sie nicht nur gegen Cybervorfälle bestens gerüstet, sondern können auch bei z.B. **Umweltkatastrophen wie Hochwasser, Feuer oder Einbruchdiebstahl** innerhalb weniger Minuten wichtige Teile des Geschäftsbetriebs wieder aufnehmen.

**Ein herausragender Vorteil der Cloud: Geteilte Verantwortung für Sicherheit & Datenschutz:** Ein bahnbrechender Vorteil der Microsoft Cloud im Vergleich zum eigenen Rechenzentrumsbetrieb ist die Verantwortung: Mit den Experten von Microsoft holen Sie sich nicht nur tatkräftige Unterstützung, sondern teilen auch die Verantwortung auf – die Sie beim eigenen Betrieb komplett alleine tragen.

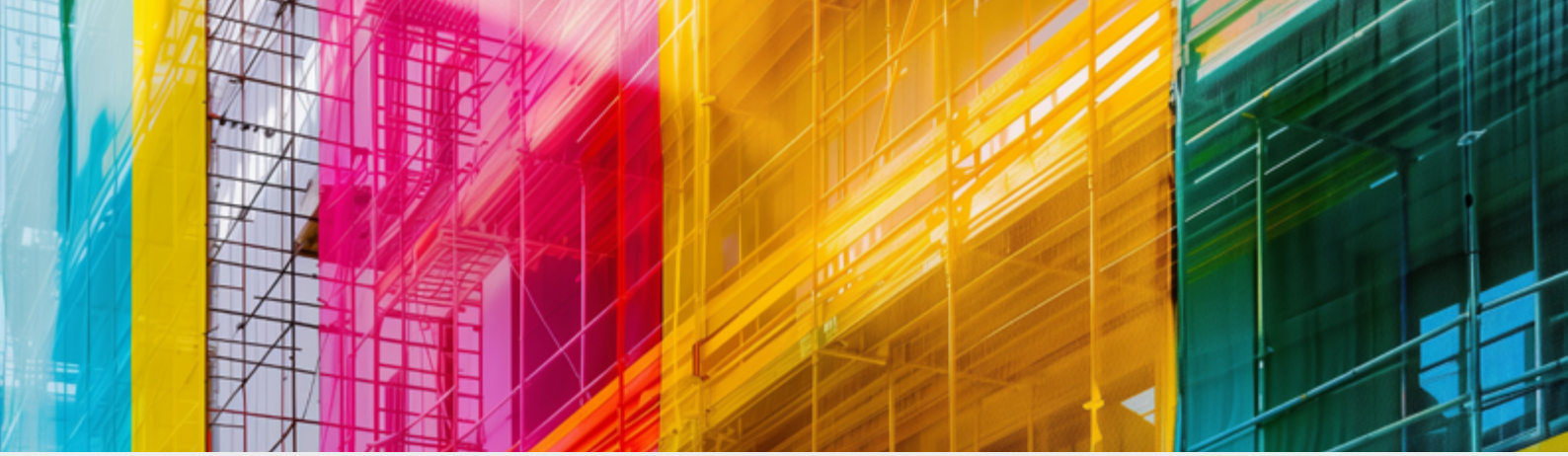
2. **Ausbau Ihres Business-Continuity- & Allgefahrenplans**

„Sorge in der Zeit, dann hast du in der Not" – denn in einer handfesten Krise ist rasches Handeln gefragt. Entwickeln Sie nun einen starken **Sicherheitsrahmen mit organisatorischen und technischen Maßnahmen,** die greifen, wenn Sie von einem Cybervorfall betroffen sind. Dazu zählen unter anderem die **Systemwiederherstellung (Desaster Recovery), Notfallverfahren, die Krisenorganisation und Meldeprozesse an Behörden.**

**Der Business-Continuity Plan BCP beinhaltet genau die drei wesentlichen Elemente:** Den Notfall-/Allgefahrenplan, das Risikomanagement inklusive Meldeprozesse sowie den Maßnahmenplan zur Wiederherstellung der Geschäftstätigkeit.

Der BCP bedarf **permanenter Aktualisierung.** Wichtig ist vor allem auch, dass Ihr verantwortliches Team im Notfall blitzschnell auf die entsprechenden Bereiche zugreifen kann.

Daher empfiehlt es sich, den **Plan nach verschiedenen Anforderungsbereichen zu strukturieren und den technologischen Rahmen zu gestalten.** Zudem sollte der Business-Continuity-Plan neben analogen Exemplaren an mehreren Stellen auch digital zentral zur Verfügung stehen, damit jederzeit von überall her egal mit welchem Endgerät darauf zugegriffen werden kann.



3. **Ausbau der Sensibilisierung der Menschen im Unternehmen**

Technologien leisten einen maßgeblichen Beitrag zur **erfolgreichen Cyberabwehr. Die Menschen in Ihrem Unternehmen leisten einen ebenso wichtigen Part.** Denn: Technologien unterstützen & entlasten Ihre Führungskräfte und Mitarbeitenden, eine möglichst ausgeprägte **Achtsamkeit schließt die kleinen Schlupflöcher.**

Wir kennen es alle aus dem eigenen Arbeitsleben: Achtsamkeit muss regelmäßig aufgefrischt werden. Das jährliche Cybersecurity-Training ist gut, **kurze monatliche Trainings mit praktischen Anwendungen sind weitaus wirksamer.**

Unterschiedlichste Fallstudien kommen zum Ergebnis, dass regelmäßige unterjährige Trainings & Awarenesskampagnen **einen Rückgang erfolgreicher Angriffe durch Pishing, Malware und Viren von bis zu 95%** erreichen. Auch hier helfen moderne Technologien, mit denen Online-Trainings regelmäßig aufgesetzt und von den Mitarbeitenden on demand absolviert werden können. Zudem helfen **gezielte Pishing Simulationen mit „Fake-Mails",** den Blick zu schärfen.

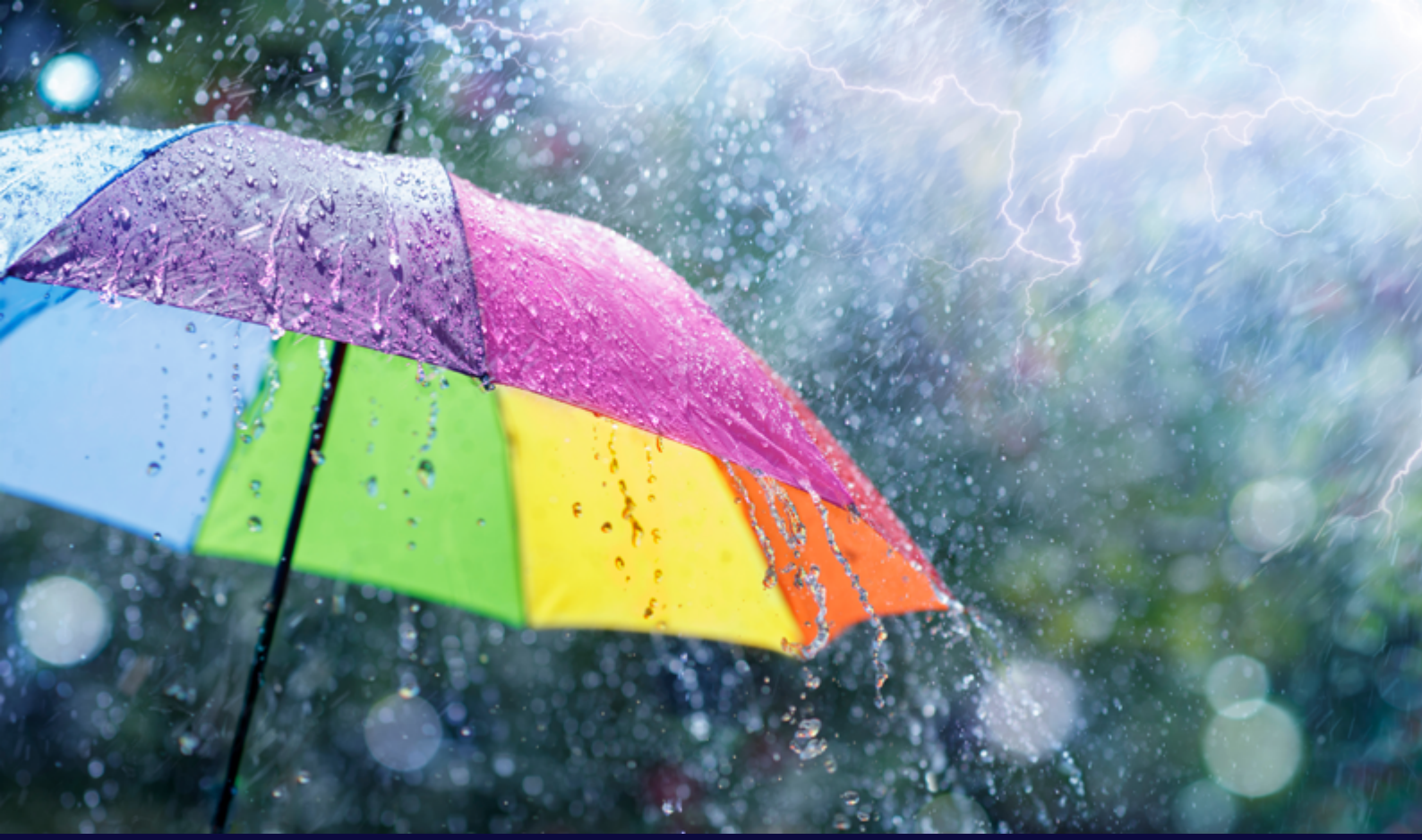
---

4. **Individuelle Feinplanung für Folgeschritte**

Fakt ist: Die Cyberkriminalität entwickelt sich in einem atemberaubenden Tempo weiter. Deshalb ist es umso wichtiger, beim **Ausbau der eigenen IT- und Cybersicherheit ständig am Ball zu bleiben** und die nächsten Schritte in Angriff zu nehmen. Viele Steps aus unserem ersten Secure Score Assessment haben wir bereits gemeinsam umgesetzt, jetzt geht es an die Feinplanung der Folgeschritte. Zudem werden unsere **Secure Score Assessments regelmäßig wiederholt,** ebenso weisen eingesetzte Technologien wie **Microsoft Defender und Sentinel** regelmäßig auf **neue lauernde Gefahren** hin.

**Klare Grenzen für NIS2 – oder doch nicht? Fallbeispiel 3**

Consultinghäuser und Anbieter für Softwareentwicklung sind vielfach für Unternehmen in Branchen tätig, die künftig zu den 18 Sektoren zählen, wie sie in der NIS2-Richtlinie definiert sind. Über kurz oder lang werden die auftraggebenden Unternehmen von diesen Dienstleistern ebenfalls einen Nachweis fordern, dass ihre Technologien und Prozesse „NIS2-compliant" sind.



# PHASE 4: CULTIVATE - **VON DER PFLICHT ZUR KÜR**

Die Umsetzung der für NIS2 erforderlichen Maßnahmen umfasst ein breites Aufgabenspektrum und sollte, wie auch das Thema Cybersicherheit selbst, als **elementarer Unternehmensprozess** verstanden werden.

In diesem Sinne sind Sicherheitsverantwortliche und AdministratorInnen dafür zuständig, die **eigenen Prozesse und Maßnahmen laufend zu prüfen und an eventuell neu entstehende Gegebenheiten anzupassen.** Denn durch die Dynamik und Komplexität in der IT-Welt ergeben sich für Organisationen und ihre internen IT-Sicherheitsmaßnahmen immer wieder andere oder weitreichendere Anforderungen.

Zusätzlich zu den technischen Aspekten gilt es, die notwendigen organisatorischen Standards weiter zu optimieren: Ein professionelles Risikomanagement ist zwar keine 100% Garantie, aber es sichert eine möglichst schnelle, reibungslose Wiederherstellung Ihres Geschäftsbetriebs. Und ist damit ein wichtiger Faktor für Ihre Wettbewerbsfähigkeit, denn bei Geschäftspartnern haben resiliente Lieferketten an Bedeutung gewonnen.

Wir möchten nochmals betonen: Insgesamt ist die NIS2-Richtlinie für Ihr Unternehmen keine erneute „EU-Knute“, sondern ein Rahmenwerk, das Ihnen mit einer gewissen Dringlichkeit nahelegt, sich selbst zu helfen und die interne Sicherheit zu erhöhen. Bauen Sie darauf auf:

1. **Permanentes Daten- und Sicherheitsmanagement**

An dieser Stelle möchten wir nochmal Ihr Bewusstsein schärfen: **JEDES Unternehmen ist der Gefahr von Cyberangriffen ausgesetzt.** Im Visier der Hacker sind **sensible Daten** und die hat jedes Unternehmen in Form von Kunden- und Mitarbeitenden-Daten wie z.B. Bankverbindungen. Vor allem kleinere und mittlere Unternehmen bemerken oft viel zu spät, dass sie bereits angegriffen wurden: Praktisch alle Angriffsstatistiken zeigen, dass gerade bei **KMUs Angriffe erst nach rund 80 Tagen** erkannt werden, manche werden erst nach knapp 1500 Tagen – sprich fast 5 Jahre später – erkannt.

Umso wichtiger ist, dass Sie das Thema **Datensicherheit** auch über die DSGVO hinaus als **elementaren Unternehmensprozess** betrachten, damit weder KundInnen noch Mitarbeitende Opfer eines Angriffs werden und finanziellen Schaden erleiden.

Auch hier können Microsoft Technologien wie Purview einen wertvollen Beitrag leisten wie z.B. der Schutz von Dokumenten und die Rückverfolgung von Dokumenten, die innerhalb sowie über Unternehmensgrenzen hinweg entstehen und von Teams bearbeitet werden.

**Cloud-IT: Mehr Nachhaltigkeit bei höchsten Sicherheitsstandards zu 80% geringeren Kosten**
Ob digitale Zwillinge oder Datenspeicherung, mit einem virtuellen Rechenzentrum in der Cloud setzen Sie nicht nur auf **höchste Sicherheitsstandards** durch 10.000 Security ExpertInnen, sondern sparen im Vergleich zu einem traditionellen physischen Rechenzentrum bis zu **80% der Betriebskosten.** Und nicht nur das: Die Cloud punktet in Sachen Nachhaltigkeit in vielfacher Hinsicht wie z.B. durch erhebliche **Einsparung von CO2-Emissionen** und der **Vermeidung von Elektronikschrott.**

---

2. **Kontinuierliches Monitoring (per Managed Service)**

Ohne Kontrolle keine Sicherheit: Nur durch eine **kontinuierliche Ermittlung und Analyse aktueller Risiken** – sowohl außerhalb als auch innerhalb des Unternehmens – **können Sicherheitslücken schnell geschlossen und neue Bedrohungen effizient abgewehrt werden.**

Hervorragende Unterstützung bieten auch hier wieder die Microsoft Security Lösungen an. Für mittelständische Unternehmen, die kein eigenes größeres Cyber-Security Team aufbauen können, bieten wir unterschiedliche individuell zusammenstellbare Pakete in Form von Managed Services an, über die Sie je nach Ausbaustufe Ihre Teams beim Monitoring und Reporting maßgeblich entlasten können.

3. **Fortlaufender Dialog mit Führungskräften und Mitarbeitenden**

Zugegeben: IT- und Cybersicherheit sind für die meisten Menschen im Unternehmen per se nicht sehr spannend. Dazu kommt, dass Maßnahmen wie die Multifaktor-Authentifizierung, der Schutz von Dokumenten und verpflichtende Trainings schlicht Zusatzaufwand mit sich bringen.

Deshalb ist es umso wichtiger, dass das Sicherheitsbewusstsein von allen Ebenen gelebt wird. Von der **Geschäftsleitung und sämtlichen Führungskräften muss schlichtweg eine Vorbildfunktion gelebt werden, damit jeder Mitarbeitende ebenfalls Verantwortung übernimmt.**

Einen erheblichen Beitrag können **Gamification Ansätze** leisten: **Spannende Schulungen mit Spaßfaktor bleiben definitiv länger im Kopf, Auszeichnungen und kleinere Mitarbeiter-Benefits für erfolgreiche Trainings und bei vorbildlichem Verhalten regen zusätzlich den Ehrgeiz an.** Der Kostenfaktor ist dank heutiger Technologien wie Microsoft Teams und entsprechende Apps überschaubar. Gemeinsam mit unseren Partnern, dem Institut für Security & Safety UNISS und Managementberatung VICCON können wir Ihnen unterschiedliche Lösungsansätze aufzeigen.

---

4. **Perspektivischer Ausbau Ihrer Security- und Compliance-Lösungen**

NIS2 ist eine Chance, die Themen Sicherheit und Compliance für Ihre Organisation strukturierter und erfolgreicher als bisher anzugehen. Mit passgenauen Technologien können **Sie Abläufe verschlanken und automatisieren**, um beispielsweise die **Bedrohungsabwehr und Cyberresilienz** zu stärken, das **Risikomanagement zu verbessern** und **Reporting-Verpflichtungen zu erleichtern.** Setzen Sie auf **höchste Sicherheitsstandards** für Ihre Infrastruktur, und lassen Sie sich eingehend beraten, wie Sie dennoch Kosten sparen, die Flexibilität steigern und für mehr Nachhaltigkeit sorgen.

# GEMEINSAM SIND **WIR STARK**

**Gehen Sie jetzt mit uns in die NIS2-Umsetzung!**

Keine Frage: Mit den NIS2-Anforderungen stehen Sie als Geschäftsführung, Ihre Sicherheitsverantwortlichen ebenso wie Ihre Mitarbeitenden vor einer großen Aufgabe. Mit dem Institute for Security and Savety uniss und der VICCON nen wir Ihnen ein Rundumpaket anbieten, das sowohl die technologischen Rahmenbedingungen und Maßnahmen beinhaltet, als auch alles rund um die Unternehmensorganisation und den Menschen. Mit der Direktorin Frau Dr. Swantje Westphal haben wir zudem eine weltweit anerkannte Expertin an Bord, die absolute Notwendigkeit und mittelstandsgerechten Pragmatismus in Einklang bringt. Damit unterstützen Sie dabei, IT- und Cybersecurity nachhaltig aufzubauen und die Aufgabe in sinnvolle und leichter handhabbare Schritte zu unterteilen. Wir beginnen mit dem, was ab Oktober 2024 absolut unerlässlich ist, und entwickeln dann gemeinsam mit Ihnen einen zukunftsfähigen, maßgeschneiderten Plan für eine kontinuierliche NIS2-Compliance. Und auch im Falle eines Sicherheitsverstoßes können Sie auf uns zählen.

**Wir begleiten Sie auf dem Weg zu mehr IT-, Cyber- und letztlich Unternehmenssicherheit – und das bedeutet Zukunftssicherheit.**

**Sprechen Sie uns einfach an:**

verkauf@it-improvement.com
Telefon: 0203 / 440 968 30

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Security

**Sind Sie bereit?**

Künstliche Intelligenzen wie Microsoft Copilot bringen bahnbrechende Potentiale im Arbeitsalltag. Gemeinsam mit weiteren digitalen Technologien bieten sie vielfältige Antworten und Lösungen auf die Herausforderungen der Zeitenwende. Wenn die Rahmenbedingungen wie Datenschutz, Cyberabwehr und Veränderungsmanagement ebenso sorgfältig im Unternehmensalltag integriert werden, bieten digitale Technologien das wesentliche Fundament für Wettbewerbsfähigkeit und Widerstandsfähigkeit von mittelständischen Unternehmen. Wir begleiten Sie auf dem Weg in die digitale Zukunft, lassen Sie uns gemeinsam die Chancen und Herausforderungen meistern!

**Kennen Sie schon unsere Webinare?**

Auf unserer Eventseite finden Sie alle Termine inklusive Anmeldung:

events.it-improvement.com

powered by

INSTITUTE FOR SECURITY AND SAFETY
AT THE UAS MANNHEIM

VICCON
CONSULTING