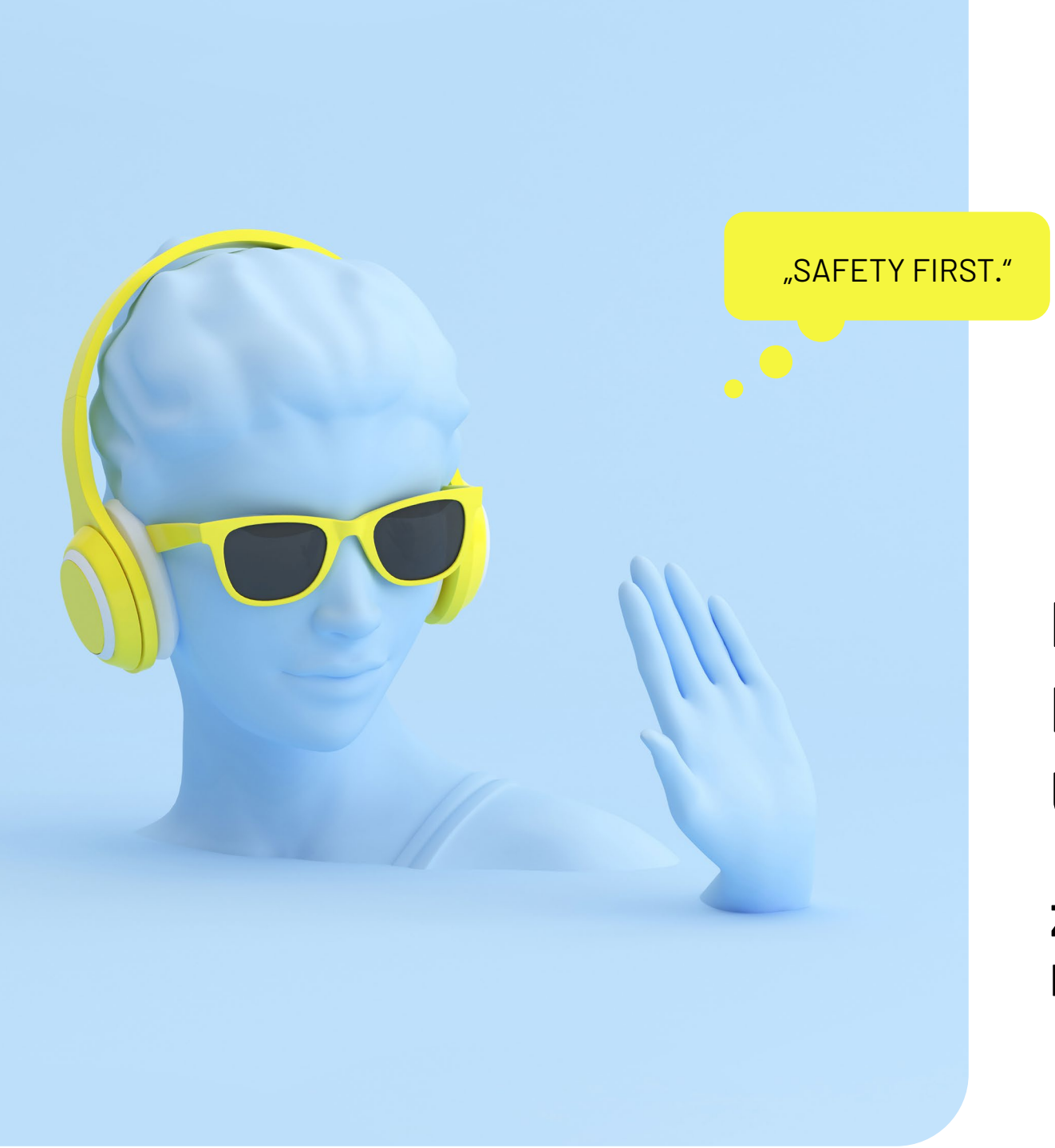


PROVECTUS

NIS2 & DORA ERFOLGREICH UMSETZEN

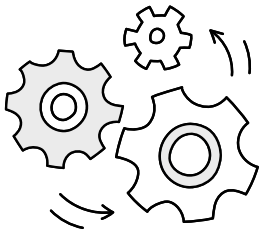
Zero Trust als Fundament, Microsoft als Enabler

EINLEITUNG

NIS 2 & DORA MANAGEN MIT ZERO TRUST ALS STARTPUNKT

Die NIS2-Richtlinie hebt die Anforderungen an die IT-Sicherheit auf ein neues Niveau und verpflichtet Unternehmen dazu, ihre Infrastrukturen noch robuster gegenüber Cyberangriffen aufzustellen. Mit der fortschreitenden Digitalisierung und der zunehmenden Vernetzung wachsen auch die potenziellen Angriffsflächen. Rein reaktive Maßnahmen genügen längst nicht mehr – gefragt und dringend erforderlich sind gezielte Investitionen in präventive und ganzheitliche Sicherheitsstrategien. Ein Kernelement dabei stellt eine Infrastruktur nach dem Zero Trust Modell dar.

ZERO TRUST



ZERO TRUST IST KEINE SICHERHEITSLÖSUNG, SONDERN EIN PROZESS

NIS2 und DORA sind Regularien, die Unternehmen dazu verpflichten Ihre IT-Sicherheit kontinuierlich zu verbessern. Auch das Zero Trust Konzept ist ein Prozess und keine einmalige Einführung.
Es umfasst vielmehr verschiedenen Grundprinzipien, die dazu führen, die IT-Sicherheit kontinuierlich zu verbessern und Angriffsvektoren sukzessive zu reduzieren. Mit wachsenden Angriffsszenarien muss also auch das Konzept weiterentwickelt werden.

DAS ZERO TRUST MODELL

Zero Trust ist ein modernes Sicherheitskonzept, das einem radikal neuen Denkansatz folgt: „Vertraue niemandem – weder innerhalb noch außerhalb des Netzwerks."
Statt sich auf Perimeterschutz („Vertrauensgrenzen") zu verlassen, geht Zero Trust davon aus, dass jeder Zugriff – egal von wem oder woher – zunächst als potenziell unsicher behandelt werden muss. Sicherheit wird dadurch zu einem kontinuierlichen Prüfprozess, nicht zu einer einmaligen Entscheidung.

PRINZIPIEN

↓

GRUNDPRINZIPIEN

VON ZERO TRUST

1.

NEVER TRUST, ALWAYS VERIFY

Jeder Zugriff – egal ob von einem internen oder externen Benutzer, Gerät oder Dienst – muss konsequent überprüft werden. Es wird niemals automatisch Vertrauen gewährt, nur weil sich etwas „innerhalb" des Unternehmensnetzwerks befindet.

2.

LEAST PRIVILEGE ACCESS

Benutzer und Systeme erhalten nur die minimal notwendigen Zugriffsrechte – also genau das, was sie zur Erfüllung ihrer Aufgabe benötigen, nicht mehr. Dadurch wird das Risiko im Falle eines Sicherheitsvorfalls stark reduziert.

3.

KONTINUIERLICHE AUTHENTIFIZIERUNG UND ÜBERWACHUNG

Zero Trust setzt auf Multi-Faktor-Authentifizierung (MFA), kontinuierliche Identitätsprüfungen und das Monitoring aller Aktivitäten, um verdächtiges Verhalten frühzeitig zu erkennen.

4.

SEGMENTIERUNG VON NETZWERKEN

Das Netzwerk wird in kleinere, isolierte Zonen unterteilt (Mikrosegmentierung), damit sich Angreifer nicht ungehindert seitlich im System bewegen können, falls sie einmal eindringen.

5.

SCHUTZ VON DATEN – NICHT NUR VOM PERIMETER

Im Fokus steht der Schutz sensibler Daten, unabhängig davon, wo sie sich befinden – lokal, in der Cloud oder auf mobilen Geräten.

ZERO TRUST & NIS2/DORA: WELCHE PRINZIPIEN WORAUF EINZAHLEN

ZERO TRUST PRINZIP	Zahlt ein auf...	NIS2	DORA
Identitätsbasierte Zugriffskontrolle	Starke Authentifizierung, Schutz vor unbefugtem Zugriff	Art. 21 Abs. 2a	Art. 9 Abs. 2a
Multi-Faktor-Authentifizierung (MFA)	Zugangsschutz, Angriffserkennung	Pflicht für privilegierte Konten	Grundschutz für kritische Systeme
Least Privilege Access	Minimierung von Zugriffsrechten	Sicherheitsmaßnahmen allgemein	Incident-Vermeidung
Netzwerksegmentierung / Mikrosegmentierung	Eindämmung von Angriffen, Lateralbewegung verhindern	Art. 21 Abs. 2d	Operative Resilienz

ZERO TRUST PRINZIP	Zahlt ein auf...	NIS2	DORA
Bedingter Zugriff (Conditional Access)	Zugriff nur unter sicheren Bedingungen	Risikobasiertes Management	Echtzeitschutz vor Angriffen
Sicherer Fernzugriff (ZTNA)	Absicherung von Remote Work & Externen	Art. 21 Abs. 2e	Absicherung externer Dienstleister
Datenklassifizierung & -verschlüsselung	Schutz sensibler & personen-bezogener Daten	DSGVO + NIS2	Verfügbarkeit & Ver-traulichkeit
Kontinuierliches Monitoring & Logging	Erkennung & Reaktion auf Vorfälle	Art. 23 + Meldepflicht	Art. 11, 12 (Überwa-chung & Reaktion)
Automatisierte Bedrohungs-erkennung (SIEM/SOAR)	Reaktionsfähigkeit, Frühwarnsystem	Incident Response & Resilienz	Business Continuity
Zero Trust für Dritte & Lieferanten	Kontrolle über Drittanbieterzugriffe	Art. 21 Abs. 2g	Art. 28 (Third-Party Risk Management)

ZUSAMMENGEFASST:

NIS2 will...

- Zugriffskontrollen und Sicherheitsrichtlinien auf dem Stand der Technik
- Schutz vor Cybervorfällen & schnelle Reaktion
- Risikoanalyse & Prävention als kontinuierlichen Prozess

Zero Trust deckt das durch Identitätskontrollen, Kontextanalyse und Netzwerksegmentierung ab.

DORA will...

- Resiliente Systeme, die auch unter Angriffen weiterarbeiten
- Testbarkeit von Cyberabwehrmaßnahmen
- Absicherung der gesamten Lieferkette

Zero Trust liefert durch Mikrosegmentierung, SIEM-Integration und Least Privilege Zugang die technische Grundlage.

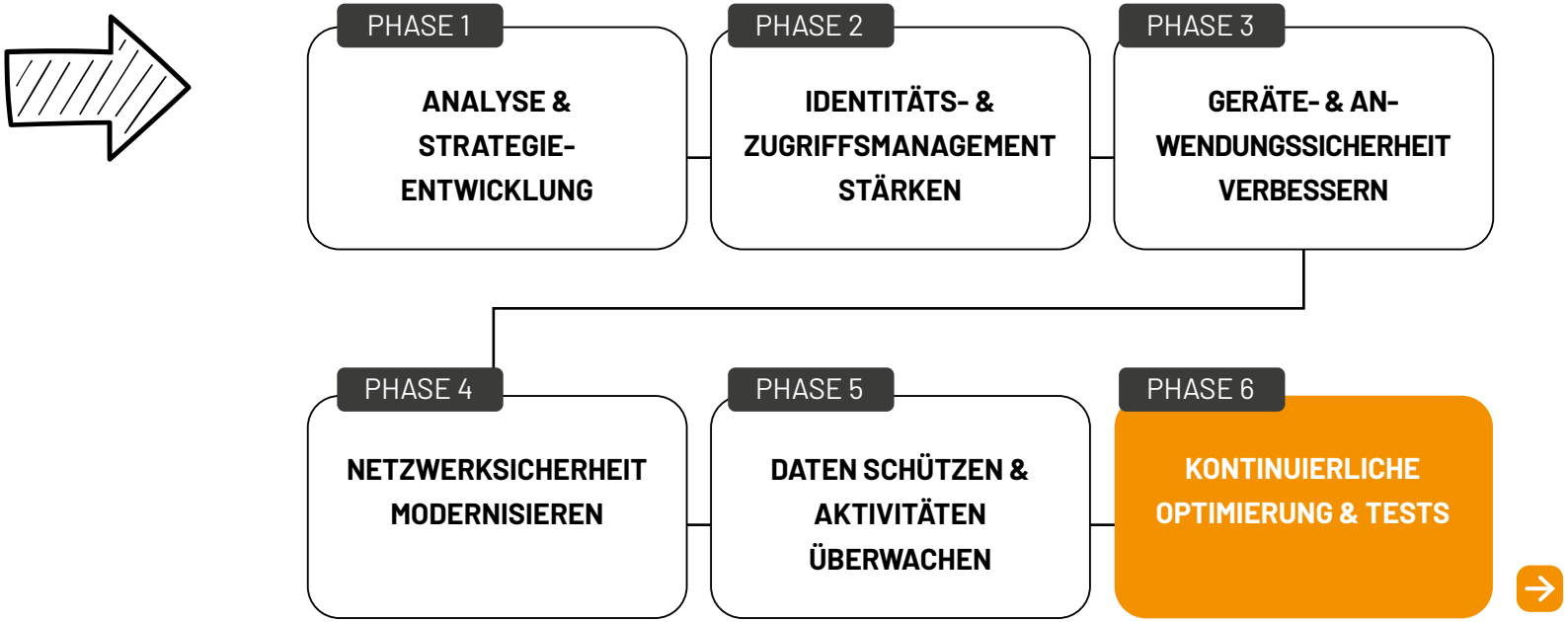
ZERO TRUST JOURNEY

↓

WIE SOLLTEN UNTERNEHMEN IHRE ZERO TRUST JOURNEY STARTEN?

Der Weg zu Zero Trust ist ein strategischer Transformationsprozess, kein Sprint. Aus unserer Sicht lässt es sich gut in Phasen gliedern, die sich an realistischen Unternehmensbedürfnissen und regulatorischen Anforderungen wie NIS2 oder DORA orientieren.

Wir teilen diese Journey daher in 6 Phasen:



PHASE 1

ANALYSE & STRATEGIE-ENTWICKLUNG (Startpunkt)

Ziel: Status quo verstehen, Risikofelder erkennen & Prioritäten setzen

Aktivitäten:

- IT-Asset-Inventur (Identitäten, Geräte, Anwendungen, Daten)
- Risikoanalyse in Bezug auf NIS2/DORA
- Reifegradbewertung der aktuellen Security-Architektur
- Definition von Zero-Trust-Zielen (z. B. Schutz sensibler Daten, Segmentierung)
- **Microsoft-Tools:** Microsoft Secure Score, Microsoft Purview, Defender Vulnerability Management

PHASE 2

IDENTITÄTS- & ZUGRIFFSMANAGEMENT STÄRKEN (Trust beginnt bei der Identität)

Ziel: Nur autorisierte Nutzer und Geräte bekommen Zugriff – und nur so viel wie nötig.

Aktivitäten:

- Einführung von **Multi-Faktor-Authentifizierung (MFA)** überall
- Umstellung auf **bedingten Zugriff (Conditional Access)** basierend auf Risiko, Standort, Gerät etc.
- Einrichtung von rollenbasierten Zugriffskontrollen (RBAC)
- **Microsoft-Tools:** Azure Active Directory (Microsoft Entra ID), Conditional Access, Identity Protection

PHASE 3

GERÄTE- & ANWENDUNGS-SICHERHEIT VERBESSERN

Ziel: Sicherstellen, dass nur vertrauenswürdige Geräte und Apps mit Unternehmensressourcen kommunizieren.

Aktivitäten:

- Endpoint Security (Antivirus, Patching, App Control)
- Geräte-Compliance-Richtlinien einführen
- Anwendungen mit Schutzmechanismen wie App Wrapping oder Sandbox absichern
- **Microsoft-Tools:** Microsoft Defender for Endpoint, Microsoft Intune, App Control, Endpoint Manager

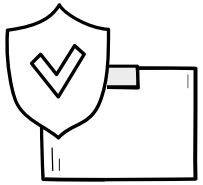
PHASE 4

NETZWERKSICHERHEIT MODERNISIEREN

Ziel: Segmentierung und Minimierung von Bewegungsfreiheit für Angreifer.

Aktivitäten:

- Mikrosegmentierung (z. B. nach Abteilungen, Datenarten)
- Einführung von VPN-Alternativen wie Secure Access Service Edge (SASE) oder ZTNA; Provectus Modern Application Portal
- Absicherung von Remote-Zugängen
- **Microsoft-Tools:** Microsoft Entra Private Access (ehemals Azure AD Application Proxy), Microsoft Defender for Network, Azure Firewall, Microsoft Tunnel



PHASE 5

DATEN SCHÜTZEN & AKTIVITÄTEN ÜBERWACHEN

Ziel: Schutz sensibler Daten und Überwachung aller Aktivitäten in Echtzeit

Aktivitäten:

- Klassifizierung und Verschlüsselung sensibler Daten
- Data Loss Prevention (DLP) einführen
- Ein zentrales SIEM/SOAR für Ereignisanalyse und Incident Response etablieren
- **Microsoft-Tools:** Microsoft Purview, Defender for Cloud Apps, Microsoft Sentinel (SIEM), DLP Policies

PHASE 6

KONTINUIERLICHE OPTIMIERUNG & TESTS

Ziel: Zero Trust ist ein dynamisches Modell, das sich stetig weiterentwickeln muss.

Aktivitäten:

- Penetration Tests / Red Teaming / Simulationen
- Schulung der Mitarbeitenden (Security Awareness)
- Regelmäßige Reviews & Anpassungen der Policies
- **Microsoft-Tools:** Microsoft Defender Attack Simulation, Microsoft Sentinel, Secure Score Monitoring

MICROSOFT TOOLS

↓

MIT MICROSOFT 365 NIS 2 & DORA MEISTERN

Viele Unternehmen, die Microsoft-Produkte im Einsatz haben, wissen oft nicht genau, für welche Sicherheitsdienste sie bereits lizenziert sind – und damit auch bezahlen –, diese jedoch nicht oder nur teilweise nutzen. Genau hier schlummert ein großes Potenzial – gerade auch im Kontext von NIS2 und DORA.

Denn Microsoft bietet eine breite Palette an leistungsstarken Sicherheitslösungen, von denen viele bereits vollständig oder anteilig mit bestehenden Lizenzen abgedeckt sind – und somit nur darauf warten, gezielt eingesetzt zu werden.

Darüber hinaus stellt Microsoft ausgewählten Unternehmen im Rahmen spezieller Programme wie dem **Threat Protection Envisioning Workshop** die Möglichkeit zur Verfügung, bestimmte Security-Features kostenlos und unverbindlich zu testen. Wir prüfen gerne, ob Ihr Unternehmen für dieses Angebot berechtigt ist.

Ein weiterer Mehrwert: Microsoft unterstützt Sie aktiv dabei, den Reifegrad Ihrer IT-Sicherheit zu analysieren – beispielsweise über den Microsoft Secure Score sowie die NIS2-Reifegradbewertung mit dem Purview Compliance Manager. Damit erhalten Sie wertvolle Einblicke, wo Ihr Unternehmen in Sachen Cybersicherheit und Compliance aktuell steht.

IHR KOSTENLOSER SECURITY-WORKSHOP WARTET!

Nutzen Sie die Chance auf den Microsoft Threat Protection Envisioning Workshop – **komplett kostenfrei und unverbindlich.**

Jetzt Berechtigung prüfen!

MICROSOFT PRODUKTE UND WELCHE NIS2 ANFORDERUNGEN SIE ADRESSIERE

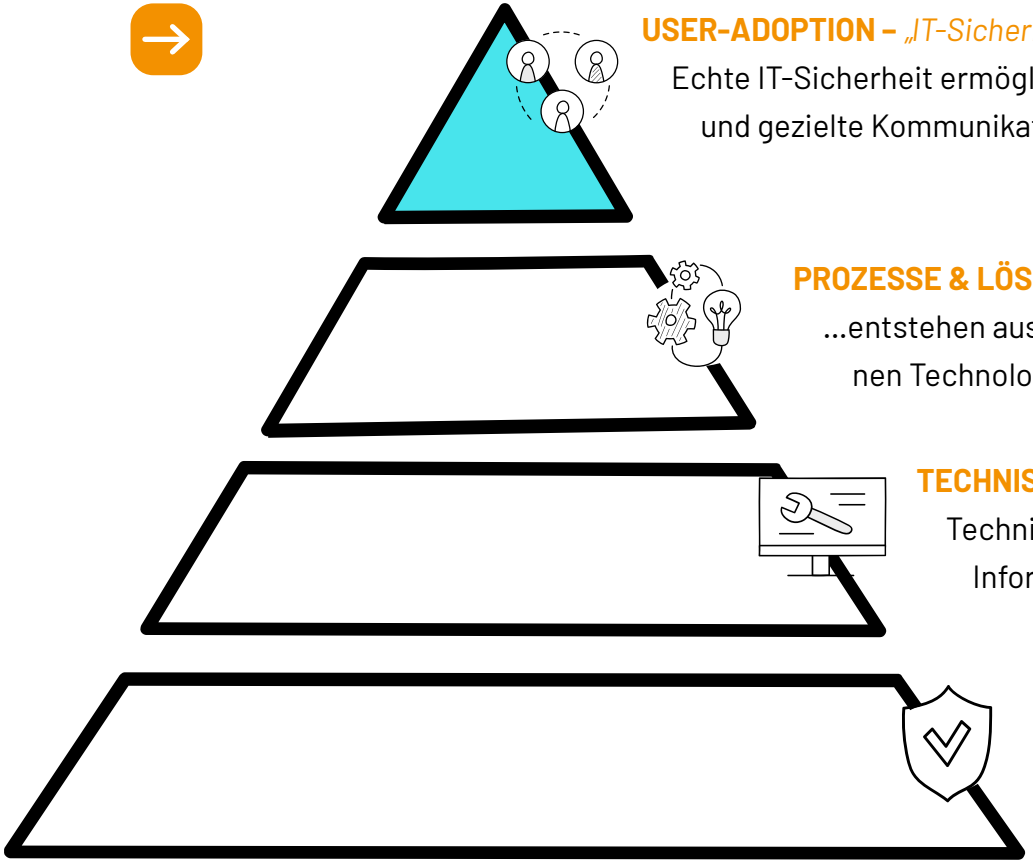
MICROSOFT TOOL	Zero Trust Prinzip	NIS2 Anforderung	DORA Anforderung
Microsoft Entra ID (Azure AD)	Identität & Zugriffskontrolle	Art. 21 Abs. 2a - Identitätsprüfung	Art. 9 Abs. 2a - Authentifizierung
Conditional Access	Kontextbasierter Zugriff	Zugriffskontrolle	Echtzeit-Risikoanalyse
Microsoft Defender for Endpoint	Geräteschutz & Monitoring	Art. 21 Abs. 2e - Gerätesicherheit	Kritische Infrastruktur absichern
Microsoft Intune	Geräte-Compliance & Richtlinien	Art. 21 Abs. 2e - Compliance	Betriebskontinuität bei Störungen
Microsoft Purview	Datenschutz & Governance	Datenschutz / DSGVO	Vertraulichkeit & Integrität
Microsoft Sentinel	SIEM & Incident Response	Art. 23 - Incident Response	Art. 11/12 - Monitoring
Defender for Cloud Apps	Cloud-Zugriffskontrolle	Art. 21 - Cloud-Absicherung	Absicherung externer Dienste
Microsoft Secure Score	Sicherheitsbewertung & Reifegrad	Art. 21 - Sicherheitsmaßnahmen	Plattformweite Sichtbarkeit
Defender Vulnerability Management	Schwachstellenmanagement	Risiko- & Schwachstellenanalyse	Vulnerability Management
Microsoft Entra Private Access	Zugriffssteuerung für Private Apps	Art. 21 Abs. 2e - Remote Access	Absicherung von Remote-Zugängen
Microsoft Tunnel	Mobiler Zugriffsschutz	Art. 21 Abs. 2e - Mobilgeräte	Secure Mobile Access
Microsoft Defender for Network	Netzwerksegmentierung	Art. 21 Abs. 2d - Segmentierung	Segmentierung & Kontrolle
Microsoft Defender Attack Simulation	Simulation & Awareness	Security Awareness & Testing	Cyber Resilience Testing

PROVECTUS ANSATZ

↓

UNSERE GRUNDPRINZIPIEN

Compliance by Default. Security by Design. Adoption by Intention.



USER-ADOPTION – *„IT-Sicherheit endet nicht beim System – sie beginnt beim Nutzer."*
Echte IT-Sicherheit ermöglichen, durch verständliche Regeln, einfache Handhabung und gezielte Kommunikation.

PROZESSE & LÖSUNGEN – *„Pragmatisch, umsetzbar & modern ."*
...entstehen aus beiden Welten – rechtlich fundiert und basierend auf modernen Technologien.

TECHNISCHE SICHERHEITSARCHITEKTUR – *„Immer mitgedacht, von Anfang an."*
Technische Sicherheitsarchitekturen (Zero Trust, M365 Hardening, Informationsschutz, DLP etc.) setzen diese Anforderungen konkret um.

COMPLIANCE – *„Rechtskonformität als Standard – nicht als Ausnahme"*
Rechtliche Anforderungen und Standards (z. B. DSGVO, ISO 27001, NIS2, DORA) nehmen stetig zu.

Unsere Kunden schätzen insbesondere unsere pragmatische Herangehensweise mit der wir sinnvolle Compliance-Strategien entwickeln und diese mit technischer Expertise in sichere Lösungen übersetzen. **Unser höchstes Ziel ist** es modernes Arbeiten zu ermöglichen, ohne durch Regulatorik ausgebremst zu werden, dabei aber stets das Sicherheitsniveau zu gewährleisten, das heutige Cyberbedrohungen erfordern.

SIE WOLLEN IHRE IT-INFRASTRUKTUR SICHERER MACHEN?

Dann sprechen Sie mit uns! Und starten Sie mit unserem Zero-Trust Workshop!

Sprechen Sie mit uns!

IHR ANSPRECHPARTNER:

Jakob Beckmann | Sales Manager
jakob@provectus.de
+49 (0) 89 710 409 20

Kostenloses Beratungsbespäch →