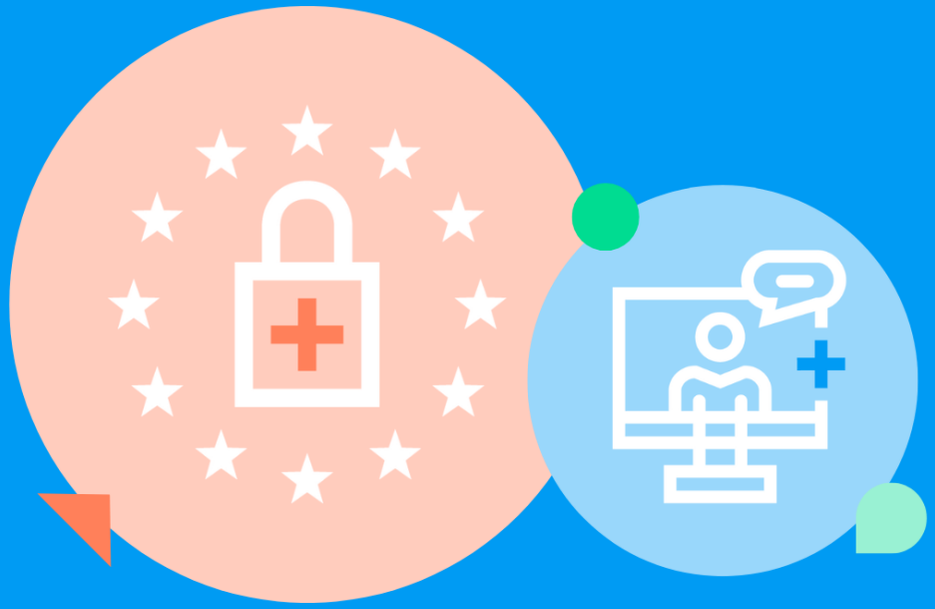
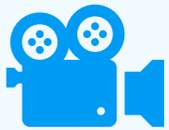
A Beginner's Guide to NIS2

NIS2 aus strategischer, juristischer und technischer Perspektive



Housekeeping Rules



Das Webinar wird aufgezeichnet

Teilnehmer sind während des Webinars stummgeschaltet

Fragen bitte während des Webinars in das Q&A-Fenster stellen

Herzlich willkommen

Ihre Experten

Daniel Graßer

Senior Director of Security Services

Peter Weber

Technical Account Manager Security

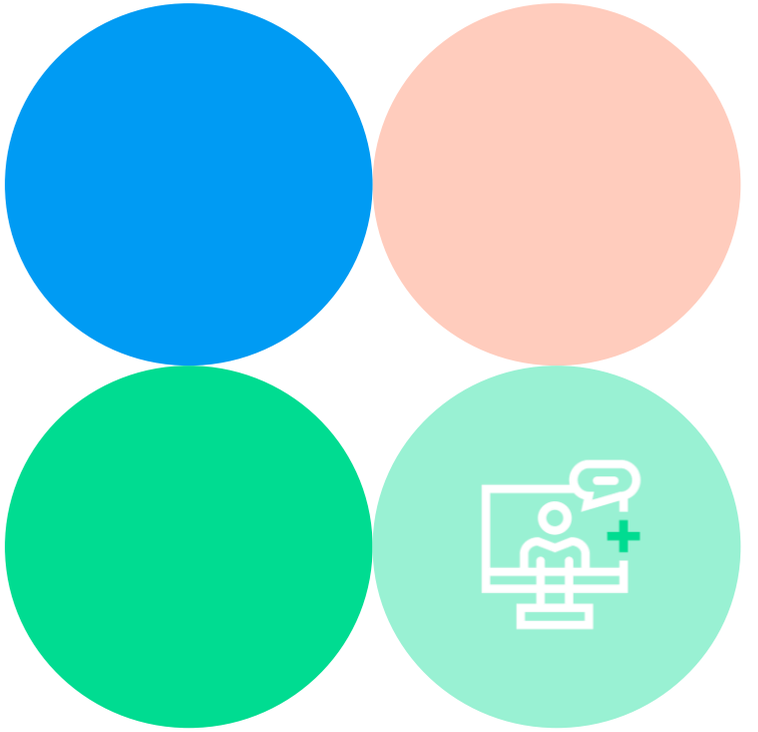
Dr. Thorsten Hennrich

General Counsel, Director Legal, Rechtsanwalt (Syndikusrechtsanwalt), Fachanwalt für IT-Recht

Agenda

A Beginner's Guide to NIS2

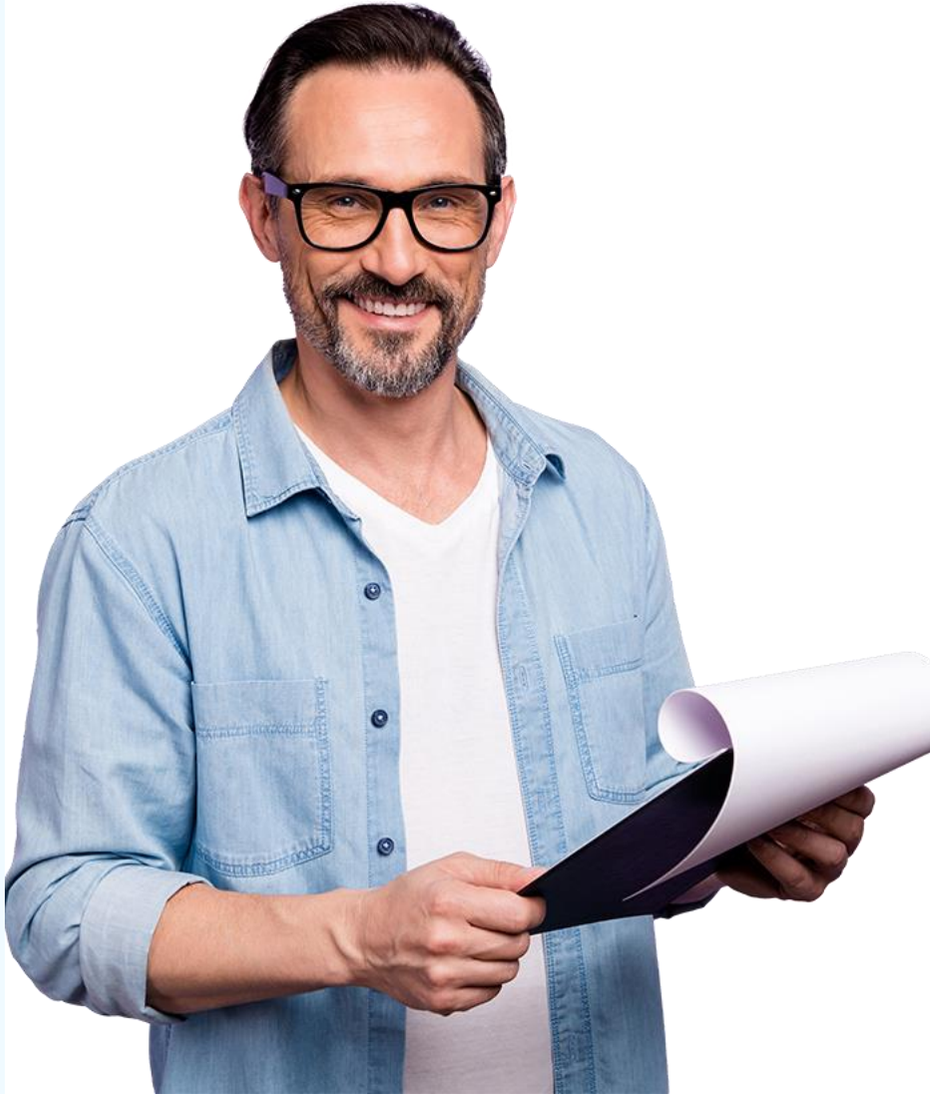
- Einleitung & Vorstellung
- Grundlage: Was ist NIS2?
- Motivation, Inhalte und Hintergründe
- Konsequenzen für IT-Security
- Handlungsempfehlungen
- Q & A



Warum Cybersecurity?

Was uns gerade beschäftigt!

+ Bedrohungslage
+ Digitalisierung & Cloud-Transformation
+ Wettbewerbsfähigkeit
+ Fachkräftemangel
+ Budget, Investitionsstau & Inflation
+ Komplexität (auch für Technologie)
+ Veränderte Gesetzeslage
+ Auswahl des richtigen Partners



70 neue Schwachstellen – jeden Tag. Software bleibt Einfallstor #1 für Cyberkriminelle.

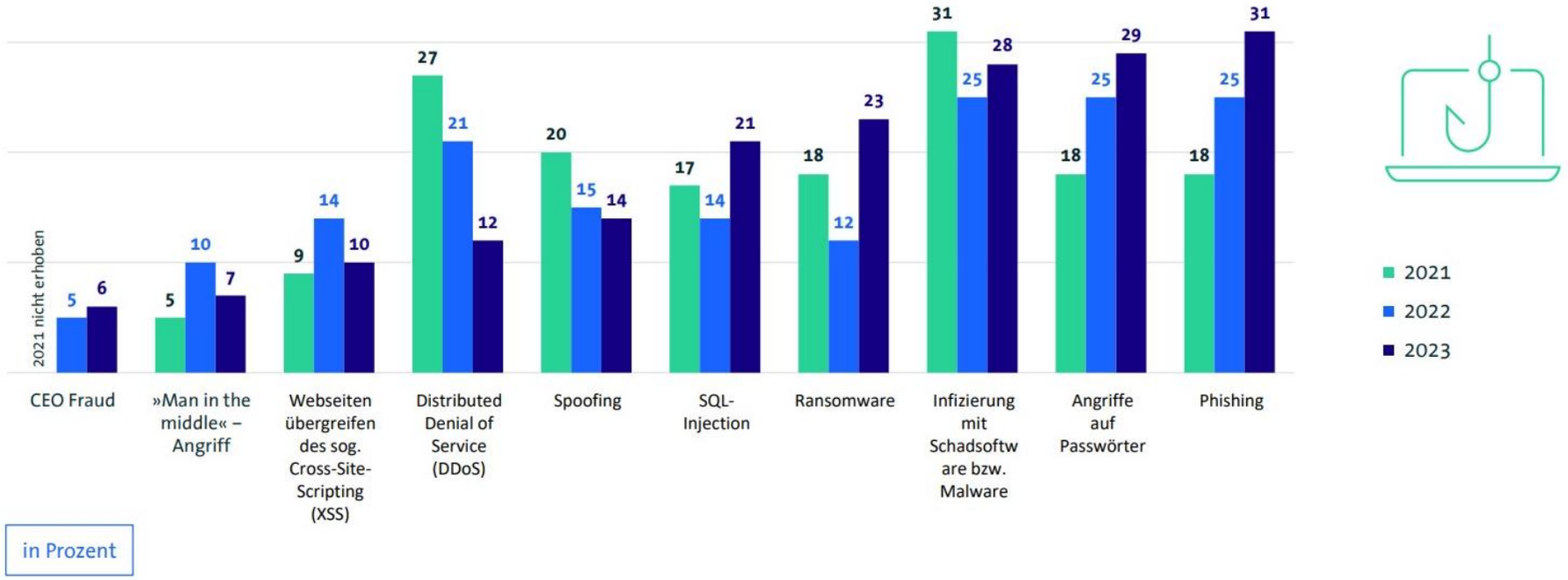
Quelle: BSI, Die Lage der IT-Sicherheit in Deutschland 2023

plusserver

Bedrohungslage und Themen

8 von 10 Unternehmen betroffen

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monaten in Ihrem Unternehmen einen Schaden verursacht?



in Prozent

Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2023

bitkom

80 %
der Unternehmen haben **Schaden** erlitten

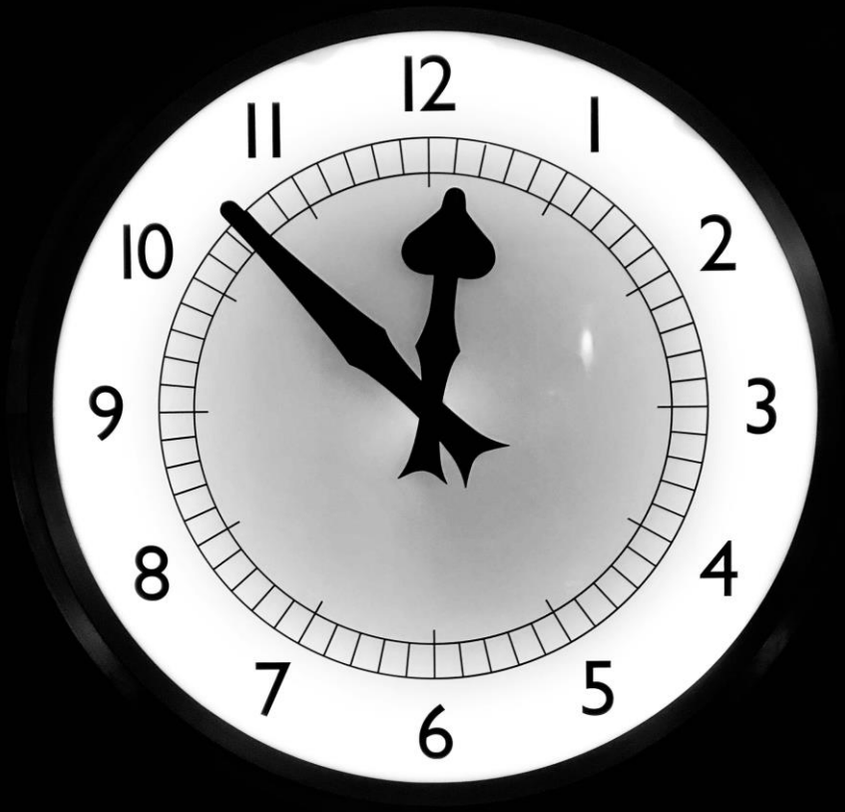
8 von 10
Unternehmen **häufiger** angegriffen

52 %
sehen Existenz bedroht

Cyberkriminalität ist ein Milliarden-Business

Haben wir noch Zeit?

....ist NIS2 die Lösung?



plusserver

Was ist NIS2?

Network and Information Security Directive 2 (NIS2)

Überführung in nationales Recht bis 17.10.2024

Angemessene Sicherheitsmaßnahmen für Organisationen in kritischen Sektoren

Bessere Zusammenarbeit der EU-Mitgliedsstaaten zur Stärkung der Cybersecurity in Europa

Sanktionen und hohe Geldstrafen bei Verstößen

Wen betrifft NIS2?

Organisationen, die Dienstleistungen in der EU erbringen

Größe/Umsatz

+ ab 50 Mitarbeitenden
+ ab 10 Millionen Euro Umsatz
+ Sonderfälle: Ein Ausfall hätte beispielsweise Auswirkungen auf die öffentliche Sicherheit/Gesundheit

Sektoren mit hoher Kritikalität

+ **Energie**
+ Verkehr & Transport
+ Bankwesen und Finanzmärkte
+ **Gesundheitswesen**
+ Trinkwasser
+ Abwasser
+ **Digitale Infrastruktur**
+ ITK-Services B2B
+ **Öffentliche Verwaltung**
+ Weltraum

Sonstige kritische Sektoren

+ Post- und Kurierdienste
+ Abfallwirtschaft
+ **Produktion & Handel** mit chemischen Stoffen
+ **Produktion, Verarbeitung** und Handel mit Lebensmitteln
+ Verarbeitendes Gewerbe, Herstellung von Waren
+ **Anbieter digitaler Dienste**
+ Forschung

plusserver

Was sind die Hintergründe zu NIS2?

plusserver

Was steht drin?

plusserver

Wie ist der aktuelle Stand?

plusserver

Ist plusserver auch von NIS2 betroffen?

plusserver

Welche Sanktionen sind möglich?

§ 30 Abs. 1 NIS-2UmsuCG*

Maßnahmen nach Absatz 1 sollen den **Stand der Technik** einhalten, die einschlägigen europäischen und internationalen **Normen berücksichtigen** und müssen auf einem **gefahrenübergreifenden Ansatz beruhen**. Die Maßnahmen müssen zumindest Folgendes umfassen:

***aktueller Referentenentwurf**

plusserver

1. **Konzepte in Bezug auf die Risikoanalyse** und auf die Sicherheit in der **Informationstechnik**,
2. **Bewältigung von Sicherheitsvorfällen,**
3. Aufrechterhaltung des Betriebs, wie **Backup-Management und Wiederherstellung** nach einem Notfall, und Krisenmanagement,
4. **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. **Sicherheitsmaßnahmen** bei **Erwerb, Entwicklung und Wartung von informationstechnischen Systemen**, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der **Wirksamkeit von Risikomanagementmaßnahmen** im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Verfahren im Bereich der **Cyberhygiene und Schulungen** im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Verfahren für den Einsatz von **Kryptografie und Verschlüsselung**,
9. **Sicherheit des Personals**, Konzepte für die **Zugriffskontrolle** und für das Management von Anlagen,
10. Verwendung von Lösungen zur **Multi-Faktor-Authentifizierung** oder kontinuierlichen Authentifizierung, **gesicherte Sprach-, Video- und Textkommunikation** sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

plusserver

Technische und organisatorische Maßnahmen

...was ist zu tun?

plusserver

Was tun?

Security als Prozess – der 4-Punkte-Plan

Risiken im Unternehmen verstehen (Risikomanagement)

1

Schutzmaßnahmen nach Schutzbedarf (Prävention)

2

Wiederherstellung (Disaster Recovery)

4

Steigerung der Transparenz (24x7 Detektion & Reaktion)

3


NIS2 bildet die Leitplanken!


NIS2, eine
gemeinsame Reise!

plusserver

Wie kann plusserver unterstützen?

Security Services, gemeinsam mit unseren Partnern

Security-Beratung/ Consulting

+ Security Consulting
+ Security Assessments
+ NIS2 Assessments
+ Pentests und Audits

Security-Lösungen

+ SOC as a Service
+ EDR as a Service
+ Schwachstellenmanagement
+ Next Gen Firewall
+ DDoS-Schutz
+ Backup/Disaster Recovery

Zertifizierte Infrastruktur

+ Standorte in DE
+ ISO 27001
+ BSI C5 (Typ-II)

plusserver

Was tun?

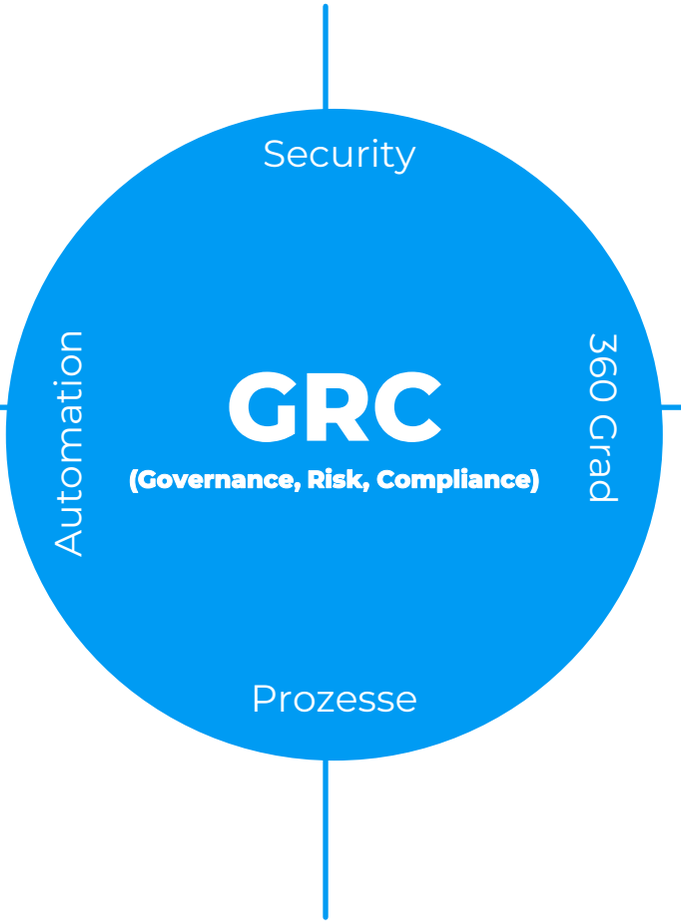
Security als Prozess – der 4-Punkte-Plan

Risikomanagement 1

- ✚ NIS2 Assessment
- ✚ Security Consulting

Schutzmaßnahmen 2

- ✚ Endpoint Detection and Response
- ✚ Workload Protection
- ✚ Security Scanner



Wiederherstellung (Disaster Recovery) 4

- ✚ Backup as a Service
- ✚ Disaster-Recovery-Konzepte

Steigerung der Transparenz 3

(24x7 Detektion & Reaktion)

- ✚ Security Operations Center (SOC)

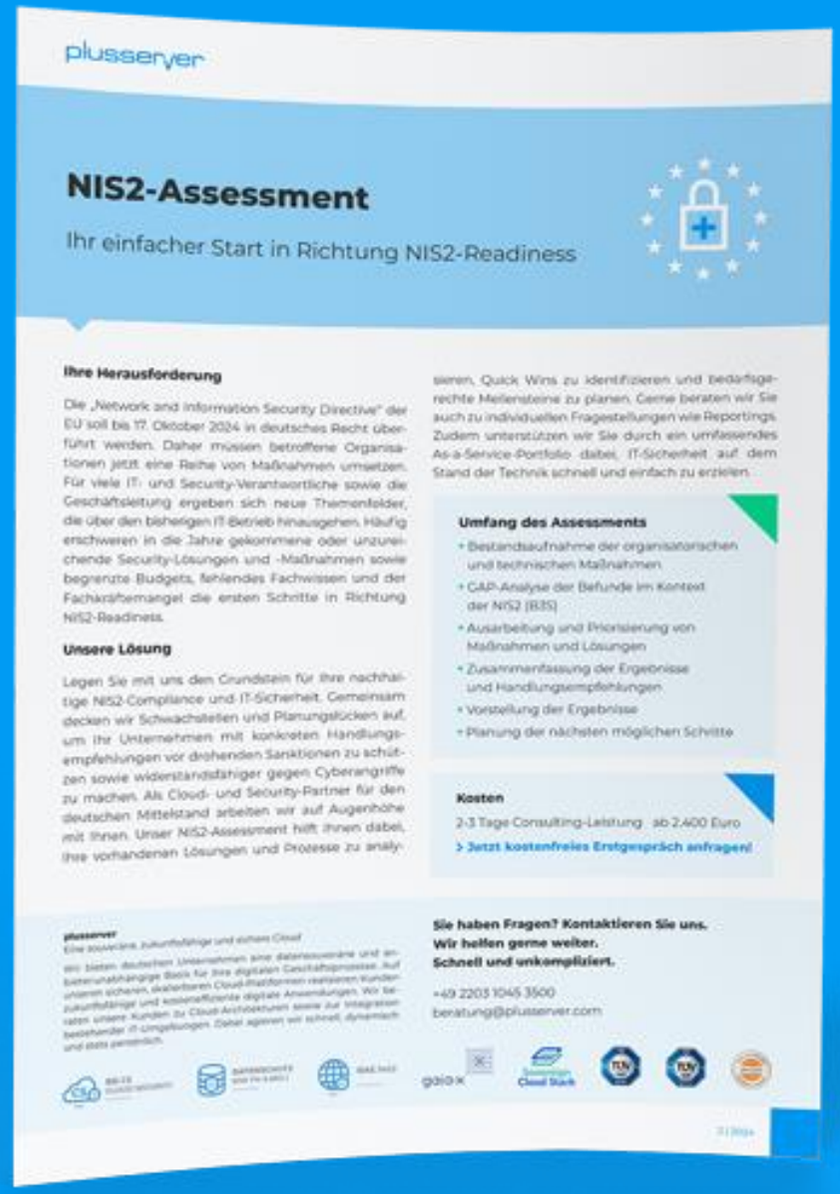
NIS2-Assessment

...den Einstieg finden!

+ Bestandsaufnahme der organisatorischen und technischen Maßnahmen
+ GAP-Analyse der Befunde im Kontext der NIS2 (B3S)
+ Ausarbeitung und Priorisierung von Maßnahmen und Lösungen
+ Zusammenfassung der Ergebnisse und Handlungsempfehlungen
+ Vorstellung der Ergebnisse
+ Planung der nächsten möglichen Schritte

Jetzt kostenfreies Erstgespräch anfragen

1 Risikomanagement


plusserver

NIS2-Assessment

Ihr einfacher Start in Richtung NIS2-Readiness

Ihre Herausforderung

Die „Network and Information Security Directive" der EU soll bis 17. Oktober 2024 in deutsches Recht überführt werden. Daher müssen betroffene Organisationen jetzt eine Reihe von Maßnahmen umsetzen. Für viele IT- und Security-Verantwortliche sowie die Geschäftsleitung ergeben sich neue Themenfelder, die über den bisherigen IT-Betrieb hinausgehen. Häufig erschweren in die Jahre gekommene oder unzureichende Security-Lösungen und -Maßnahmen sowie begrenzte Budgets, fehlendes Fachwissen und der Fachkräftemangel die ersten Schritte in Richtung NIS2-Readiness.

Unsere Lösung

Legen Sie mit uns den Grundstein für Ihre nachhaltige NIS2-Compliance und IT-Sicherheit. Gemeinsam decken wir Schwachstellen und Planungslücken auf, um Ihr Unternehmen mit konkreten Handlungsempfehlungen vor drohenden Sanktionen zu schützen sowie widerstandsfähiger gegen Cyberangriffe zu machen. Als Cloud- und Security-Partner für den deutschen Mittelstand arbeiten wir auf Augenhöhe mit Ihnen. Unser NIS2-Assessment hilft Ihnen dabei, Ihre vorhandenen Lösungen und Prozesse zu analysieren, Quick Wins zu identifizieren und bedarfsgerechte Meilensteine zu planen. Gerne beraten wir Sie auch zu individuellen Fragestellungen wie Reportings. Zudem unterstützen wir Sie durch ein umfassendes As-a-Service-Portfolio dabei, IT-Sicherheit auf dem Stand der Technik schnell und einfach zu erzielen.

Umfang des Assessments

- Bestandsaufnahme der organisatorischen und technischen Maßnahmen
- GAP-Analyse der Befunde im Kontext der NIS2 (B3S)
- Ausarbeitung und Priorisierung von Maßnahmen und Lösungen
- Zusammenfassung der Ergebnisse und Handlungsempfehlungen
- Vorstellung der Ergebnisse
- Planung der nächsten möglichen Schritte

Kosten

2-3 Tage Consulting-Leistung ab 2.400 Euro

> Jetzt kostenfreies Erstgespräch anfragen!

Sie haben Fragen? Kontaktieren Sie uns. Wir helfen gerne weiter. Schnell und unkompliziert.

+49 2203 1045 3500

beratung@plusserver.com

Q&A

Wir helfen gerne!

plusserver

Vielen Dank für Ihre Aufmerksamkeit!

Es geht weiter am 4. Juni:

Auf die Plätze, fertig, NIS2!

Jetzt zum Webinar registrieren

Unsere Security-Initiative wird unterstützt von

VEEAM