BLUE CONSULT.

Cyber-Resilienz Workshop

Wieso ist Cyber-Resilienz ein besonders wichtiges Thema für Unternehmen?

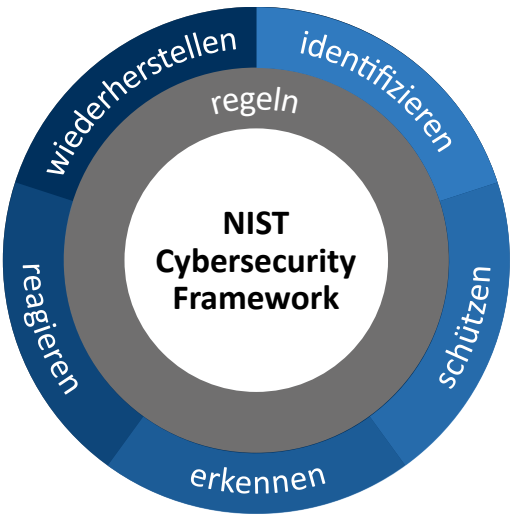
Die aktuelle Bedrohungslage macht deutlich: Cyber-Resilienz ist für Unternehmen längst keine Wahlmöglichkeit mehr, sondern eine zwingende Voraussetzung. Hackerangriffe haben inzwischen ein globales Ausmaß erreicht – verschärft durch geopolitische Spannungen und staatlich unterstützte Angreifergruppen – und können enorme Schäden verursachen.
Gleichzeitig wächst auch der regulatorische Druck: Vorgaben wie NIS-2, DORA oder die DSGVO verpflichten Unternehmen zu strengeren Sicherheitsmaßnahmen und erweiterten Melde- pflichten. Insbesondere durch NIS-2 rückt die Geschäftsführung stärker in die Verantwortung – bis hin zur persönlichen Haftung für Risikomanagement und die Umsetzung geeigneter Schutzmaßnahmen.

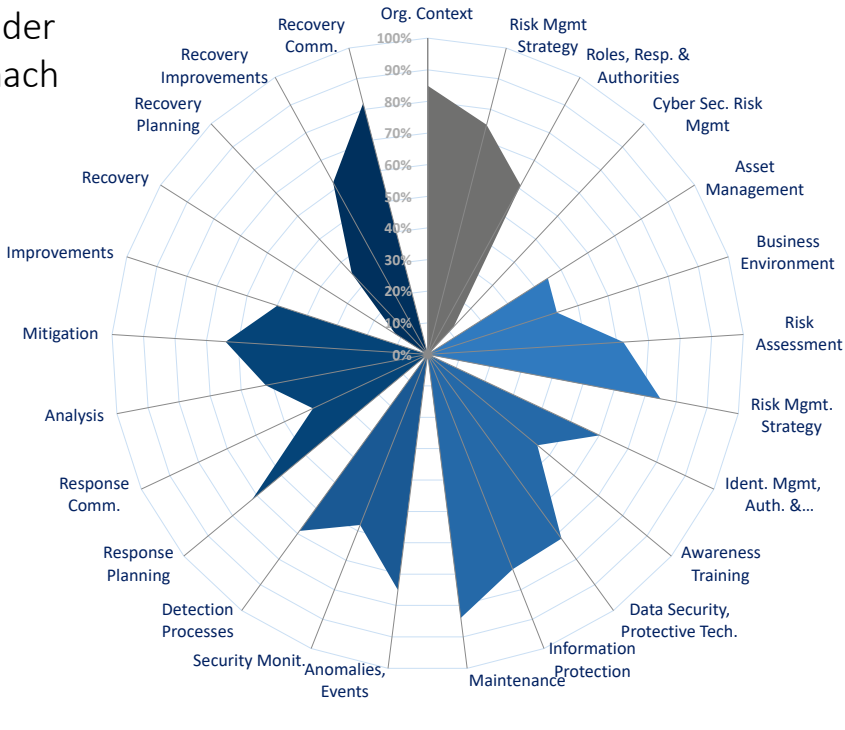
Fakten-Check: Studienergebnisse des Digitalverbandes Bitkom e. V.

- 8 von 10 Unternehmen von Datendiebstahl, Spionage oder Sabotage betroffen
- Rekordschaden von rund 267 Milliarden Euro
- China wird immer mehr zum Standort Nr. 1 für Angreifer
- Cyberangriffe: Zwei Drittel der Unternehmen fühlen sich in ihrer Existenz bedroht

Umso wichtiger ist es, rechtzeitig aktiv zu werden und die eigene Widerstandsfähigkeit gegenüber Cyber-Bedrohungen zu stärken. Ein gezielter Cyber-Resilienz Workshop, auf Basis des NIST-Frameworks, bietet hier eine praxisnahe Möglichkeit.

Beispiel einer Ist-Analyse bestehender Schutzmaßnahmen und Prozesse nach NIST (CSF)





Quelle Grafik: National Institute of Standards and Technology

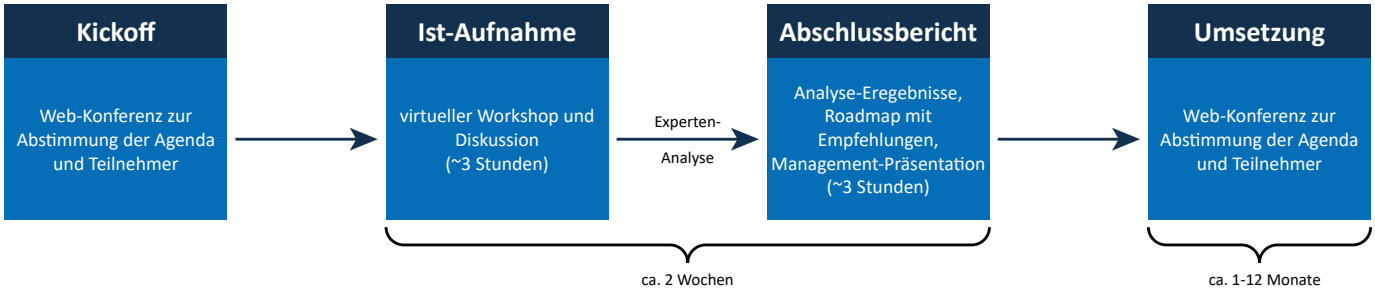
Um der zentralen Fragestellung, wie Ihr Unternehmen aktuell gegenüber Cyber-Angriffen aufgestellt ist und wie Sie es proaktiv weiter stärken können, nachzugehen, bieten wir Ihnen im Rahmen eines **Cyber-Resilienz Workshops** eine Einschätzung und Empfehlungen durch unsere Experten - basierend auf den Themenfeldern des NIST Cyber-Security Frameworks. Dieses bietet einen technologieneutralen Leitfaden für Cyber-Security Management, der sich in die Themenfelder Risikoidentifizierung, Sicherheitsmaßnahmen, Bedrohungserkennung, Reaktion auf Vorfälle und Wiederherstellung gliedert.

Angebot BLUE:

Unser Cyber-Resilienz-Workshop bewertet die aktuelle Widerstandsfähigkeit Ihres Unternehmens gegen Angriffe und liefert konkrete Empfehlungen zur Stärkung Ihrer Sicherheit. Gemeinsam mit einem renommierten Partner und Ihrem Team analysieren unsere Cyber-Resilienz Experten bestehende Schutzmaßnahmen und Prozesse. Auf Basis unserer Auswertung erhalten Sie einen aussagekräftigen Abschlussbericht sowie eine Management-Präsentation mit herstellerneutralen Handlungsempfehlungen. Im Anschluss priorisieren wir mit Ihnen die nächsten Schritte und präsentieren konkrete Lösungsvorschläge. So gewinnen Sie nicht nur eine klare Standortbestimmung, sondern auch einen praxisnahen Fahrplan zur gezielten Stärkung Ihrer Cyber-Resilienz.

Unser Angebot richtet sich an CISOs und CIOs in Zusammenarbeit mit Ihren Expertenteams für Business Continuity, Security und Storage.

Der Workshop gliedert sich in folgende Schritte:



Gemeinsam erarbeiten wir den Status quo, identifizieren Handlungsfelder und entwickeln konkrete Schritte, mit denen Ihr Unternehmen widerstandsfähiger und zukunftssicherer gegenüber Cyber-Bedrohungen aufgestellt wird.

Benefits

- Detaillierte Auswertung und herstellerneutrale Empfehlungen zur Stärkung der Cyber-Resilienz Ihres Unternehmens
- Vertrauliche Analyse und Berichte ohne Eingriffe in Ihre Umgebung
- Identifikation von Stärken und Schwachstellen Ihrer Schutzmaßnahmen und Prozesse ggü. Cyber-Angriffen
- Überprüfung Ihrer Verfahren zur Datensicherung, zum Schutz und zur Wiederherstellung
- Basierend auf Best-Practices für Cyber-Security, wie dem NIST Cyber-Security Framework oder EU DORA
- Nützliche Details zur Ausarbeitung und Umsetzung einer Cyber-Resilienz Strategie
- Verknüpfung Ihrer kritischen Geschäftsergebnisse mit gezielten Strategien für Cyber-Resilienz
- Förderung eines höheren Sicherheitsbewusstseins Ihres Teams gegenüber Cyber-Angriffen
- Ergänzende Leistungen durch unsere Partnerschaften mit erfahrenen Anbietern von Cyber-Resilienz Lösungen

Kontakt

Thomas Helget, BLUE Consult GmbH, Adolf-Dembach-Str. 2, 47829 Krefeld
Thomas.helget@blue-consult.de, Telefon: +49 2151 6500 10