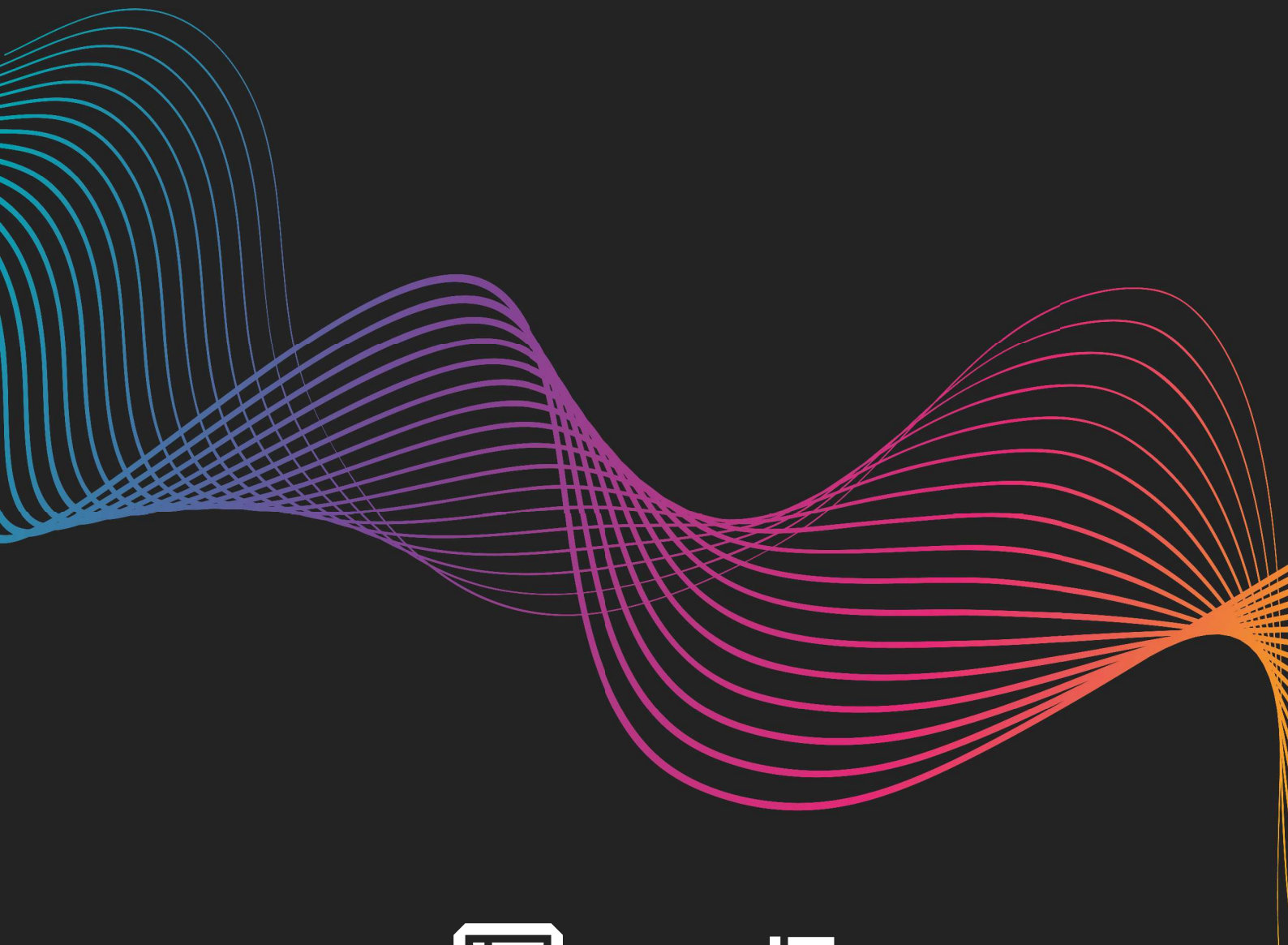
Stay ahead of the Wave

Cyber Security Assessment



omniIT
INNOVATIVE TECHNOLOGY

Optimieren Sie Ihr CyberSecurity und bringen Sie es in Einklang mit best practices der Branche

Wie steht es um Ihre Sicherheitsstrategie?
Was sind Ihre größten Risiken?
Worauf sollten Sie Ihre Aufmerksamkeit richten?

Die zunehmend professionelle Bedrohungen und ein immer komplexeres Umfeld für CyberSicherheit stellen Unternehmen vor neuen Herausforderungen.

Das Cyber Security Maturity Assessment (CSMA) ist eine GAP-Analyse und Risikobewertung, bei der bewährte Verfahren der Cybersicherheit und anerkannte Frameworks wie Business Impact Analysis (BIA) und Threat Modelling (TM) eingesetzt werden, um die Fragen zu Ihrem bestehenden Sicherheitsprogramm zu beantworten.

Obwohl die CSMA besonders für mittlere und große Unternehmen von Nutzen ist, können Organisationen jeder Größe von der Bewertung profitieren.

Ziel der CSMA ist es, einen Überblick über die aktuelle Sicherheitslage, eine objektive Überprüfung der bestehenden Pläne und einen Leitfaden für die strategische Planung zu geben.

Die CSMA hilft Ihrem Unternehmen auch bei der Entwicklung taktischer und strategischer Richtungen, um Ihre CyberSecurity weiter auszubauen und zu stärken.

Mit dem Cyber Security Assessment von omniIT profitieren Sie von einem ganzheitlichen Ansatz, der Ihr IT-Sicherheitsniveau betrachtet und vollständig bewertet.

Das Assessment fokussiert auf verschiedene organisatorische und technische Bereiche. Dabei werden sowohl interne Richtlinien und Policies als auch branchenspezifische gesetzliche Anforderungen berücksichtigt.

Was ist Ihr Mehrwert?

- Aktuelle Sicht auf kritischen Geschäftsprozesse und Ressourcen
- Übersicht der potenziellen Bedrohungen für Ihr Unternehmen
- Bewertung der Angriffsvektoren und darauf abgestimmte Maßnahmenempfehlung
- Report der Aktivitäten inkl. Heatmap für die Umsetzung

Was enthält das Assessment?

- Begleitung aller Phasen durch CyberSicherheit und Governance Experten
- Prüfung der technisch-organisatorischen Risiken aller relevanten Fachbereiche
- Bewertung der aktuellen Lage im Bezug auf Risiken und Bedrohungen
- Maßnahmenplan

Wie gehen wir vor?

- Kickoff: Abstimmung mit den Teilnehmern, Festlegung von Terminen
- Workshop und Interviews mit den Fachbereichen
- Bewertung und Quantifizierung der Ergebnisse
- Präsentation der Resultate
- Gemeinsame Erarbeitung der Folgeschritte und Priorisierung der Maßnahmen.

Stay ahead of the wave

1.
Geschäftsprozesse bestimmen und ihrer Kritikalität priorisieren

Wesentliche Geschäftsprozesse stehen im Fokus - dabei wird die Kritikalität und Priorität der Prozesse festgelegt.

2.
Wiederanlaufparameter und Abhängigkeiten bestimmen:

Maximal tolerierbare Ausfallzeit, Wiederanlaufzeit und -Niveau werden festgelegt und ggf. Wiederanlaufparameter angepasst.

3.
Kritische Ressourcen

Kritischen Ressourcen zur Wiederherstellung bestimmen und priorisieren.

4.
Bedrohungsanalyse und Bewerten der Angriffsvektoren

Denken wie ein Angreifer - Analyse der identifizierten Prozesse auf mögliche Bedrohungen.

5.
Bewertung der Wirksamkeit von Sicherheitslösungen

Welche der aktuellen Abwehrmaßnahmen helfen präventiv die Risiken zu minimieren.

6.
Vorausschauende Plannung der Maßnahmen

Ein Plan um die Risiken zu minimieren und die Reife der Cybersicherheit zu erhöhen.

Für weitere Informationen oder Vertriebliche Fragen stehen wir gerne für Sie zur Verfügung:

Tel.: +49 (89) 998 241 920
Mail: secaas@omniit.de

omniIT GmbH
Georg-Hallmaier-Str. 6
81369 München
Telefon +49 89 998 24192 0
E-Mail: info@omniit.de
Web: www.omniit.de
Geschäftsführer: Patryk Wlodarczyk, Marek Chroust

Wir sind omniIT

Wir aktivieren Ihre digitale DNA!

Als Full-Service IT-Dienstleister erstreckt sich unser Angebot von IT-Sicherheit über die ITInfrastruktur bis hin zur Software-Entwicklung, Beratungsprojekten und Managed IT-Services. Nutzen Sie uns als verlängerte Werkbank, um Ihre Ziele zeitnah und mit den erwarteten Ergebnissen zu erreichen.

Unser Team arbeitet für den Erfolg nationaler und internationaler Unternehmen - egal ob Mittelstand oder Großkonzern aus der Technologie-, Automobil-, Finanz- oder Telekommunikationsbranche. Wir agieren stets transparent und kommunizieren auf Augenhöhe.

Unser Portfolio