

Inetum Cybersecurity ServicePack

Cyber Compass Workshop

Standort bestimmen. Risiken erkennen. Prioritäten setzen.

Cybersecurity ist heute weit mehr als eine technische Disziplin. Menschen, Prozesse und Technologien müssen ineinandergreifen, damit Risiken wirksam reduziert und Sicherheitsvorfälle verhindert werden können.

Viele Unternehmen investieren bereits in Sicherheitsmassnahmen, verfügen jedoch nicht über eine klare Sicht auf ihren tatsächlichen Sicherheitsstatus. Häufig fehlen Transparenz über bestehende Risiken, klare Verantwortlichkeiten oder eine Priorisierung der nächsten Schritte.

Mit unserem **Cyber Compass Workshop** erhalten Sie innerhalb eines halben Tages eine strukturierte Standortbestimmung Ihrer Cybersecurity. Gemeinsam analysieren wir die wichtigsten Sicherheitsaspekte entlang der Bereiche Mensch, Prozesse und Technologie, identifizieren Risiken und zeigen konkrete Verbesserungsmöglichkeiten auf.

Der Workshop liefert ein verständliches Lagebild Ihrer aktuellen Sicherheitsreife sowie pragmatische Handlungsempfehlungen mit unmittelbarem Mehrwert.

Unser Service

Der **Cyber Compass Workshop** ist ein kompakter Security Health Check für Unternehmen, die ihre Sicherheitslage realistisch und ohne aufwendiges Audit beurteilen möchten.

In einem moderierten Workshop betrachten wir die organisatorischen, prozessualen und technischen Grundlagen Ihrer Cybersecurity. Dabei bewerten wir gemeinsam relevante Themenfelder, identifizieren Schwachstellen und diskutieren bereits während des Workshops konkrete Massnahmen und Quick Wins.

Das Ergebnis ist eine übersichtliche Security Heatmap mit einer priorisierten Übersicht der wichtigsten Risiken und Handlungsfelder.

Zielgruppe

Der **Cyber Compass Workshop** richtet sich an Geschäftsleitungen, Verwaltungsräte, CIOs, IT-Leitungen sowie IT- und Sicherheitsverantwortliche, die einen fundierten Überblick über die aktuelle Sicherheitslage ihrer Organisation gewinnen möchten. Insbesondere für KMU mit steigenden Anforderungen an Cybersecurity, Governance, Compliance und Risikomanagement bietet der Workshop eine pragmatische und unabhängige Standortbestimmung.

Ihr Nutzen

Mit dem **Cyber Compass Workshop** schaffen Sie Transparenz über Ihre aktuelle Sicherheitslage:

- **Klarheit über den aktuellen Security-Reifegrad** – verstehen Sie, wo Ihr Unternehmen heute steht und welche Bereiche besonderen Handlungsbedarf aufweisen.
- **Identifikation der grössten Risiken** – erkennen Sie organisatorische, prozessuale und technische Schwachstellen frühzeitig.
- **Konkrete Quick Wins** – erhalten Sie sofort umsetzbare Empfehlungen mit hoher Wirkung und überschaubarem Aufwand.
- **Priorisierte Handlungsempfehlungen** – fokussieren Sie Investitionen und Ressourcen auf die Massnahmen mit dem grössten Nutzen.
- **Fundierte Entscheidungsgrundlage** – Management und IT erhalten ein gemeinsames Verständnis über den Handlungsbedarf.

Wie gehen wir vor?

Mensch

Der Mensch ist ein zentraler Erfolgsfaktor für eine wirksame Cybersecurity. Deshalb betrachten wir gemeinsam, wie Sicherheitsbewusstsein, Verantwortlichkeiten und sicherheitsrelevante Abläufe in Ihrer Organisation verankert sind. Dabei analysieren wir unter anderem die Rollen und Zuständigkeiten im Bereich Informationssicherheit, die Durchführung von Awareness-Massnahmen sowie bestehende Onboarding- und Offboarding-Prozesse. Ziel ist es, mögliche Risiken durch fehlende Sensibilisierung, unklare Verantwortlichkeiten oder unzureichend etablierte Sicherheitspraktiken frühzeitig zu erkennen und geeignete Verbesserungsmöglichkeiten aufzuzeigen.

Prozesse

Sichere und klar definierte Prozesse bilden die Grundlage für den nachhaltigen Schutz von Informationen und Systemen. Im Workshop bewerten wir gemeinsam die wichtigsten organisatorischen und operativen Sicherheitsprozesse Ihres Unternehmens. Dazu gehören beispielsweise das Benutzer- und Berechtigungsmanagement, Patch- und Change-Management-Prozesse, Notfall- und Incident-Response-Verfahren sowie Backup- und Recovery-Konzepte. Durch die strukturierte Betrachtung dieser Bereiche identifizieren wir Schwachstellen, Verbesserungspotenziale und konkrete Massnahmen zur Erhöhung der organisatorischen Resilienz.

Technologie

Neben Menschen und Prozessen analysieren wir die wesentlichen technologischen Sicherheitsbausteine Ihrer Organisation. Dabei betrachten wir die Absicherung von Identitäten und Zugängen, den Schutz von Endgeräten, Monitoring- und Überwachungsmöglichkeiten sowie Cloud- und Datensicherheitsaspekte. Der Fokus liegt nicht auf einer detaillierten technischen Prüfung oder einem Audit, sondern auf einer praxisnahen Einschätzung der vorhandenen Sicherheitsmassnahmen und möglicher Risiken. Dadurch entsteht ein realistisches Bild über den aktuellen technischen Sicherheitsstatus Ihres Unternehmens.

Bewertung und Empfehlungen

Die Erkenntnisse aus den Bereichen Mensch, Prozesse und Technologie werden in einer übersichtlichen Security Heatmap zusammengeführt und gemeinsam bewertet. Bereits während des

Workshops diskutieren wir identifizierte Risiken, mögliche Optimierungsmassnahmen und konkrete Quick Wins. Auf dieser Grundlage priorisieren wir die Handlungsfelder nach Nutzen, Risiko und Umsetzbarkeit und erarbeiten praxisnahe Empfehlungen für die nächsten Schritte. Das Ergebnis ist eine verständliche und nachvollziehbare Standortbestimmung, die Management und IT als Entscheidungsgrundlage für die Weiterentwicklung der Cybersecurity dient.

Lieferergebnisse

Nach dem Workshop erhalten Sie eine kompakte und verständliche Zusammenfassung der Ergebnisse. Diese umfasst eine **Security Heatmap**, welche den aktuellen Reifegrad Ihrer Organisation entlang der Dimensionen **Mensch, Prozesse und Technologie** visualisiert und Handlungsfelder auf einen Blick sichtbar macht. Ergänzend erstellen wir ein **Management Summary** mit den wichtigsten Erkenntnissen, einer Bewertung der identifizierten Risiken sowie einer Einordnung des aktuellen Sicherheitsstatus.

Darüber hinaus dokumentieren wir die während des Workshops identifizierten **Quick Wins**, die mit überschaubarem Aufwand kurzfristig umgesetzt werden können und einen direkten Sicherheitsgewinn erzielen. Abschliessend erhalten Sie eine **priorisierte Übersicht** mit **konkreten Handlungsempfehlungen** und einer **pragmatischen Roadmap**, welche die nächsten sinnvollen Schritte zur Weiterentwicklung Ihrer Cybersecurity aufzeigt. Dadurch verfügen Management und IT über eine fundierte Entscheidungsgrundlage, um Sicherheitsmassnahmen gezielt zu planen und umzusetzen.

Rahmenbedingungen

Dauer: 4 Stunden

Format: Vor Ort oder Remote

Durchführung: Workshop mit relevanten Fachbereichen und Entscheidungsträgern

Ergebnisse des Workshops: Security Heatmap, Management Summary, Quick Wins und priorisierte Roadmap

Fixpreis: CHF 2'000.00 exkl. MwSt.

Ihr Kontakt

Raphael Ruch

Cybersecurity Advisor

raphael.ruch@inetum.com

+41 44 405 21 00

