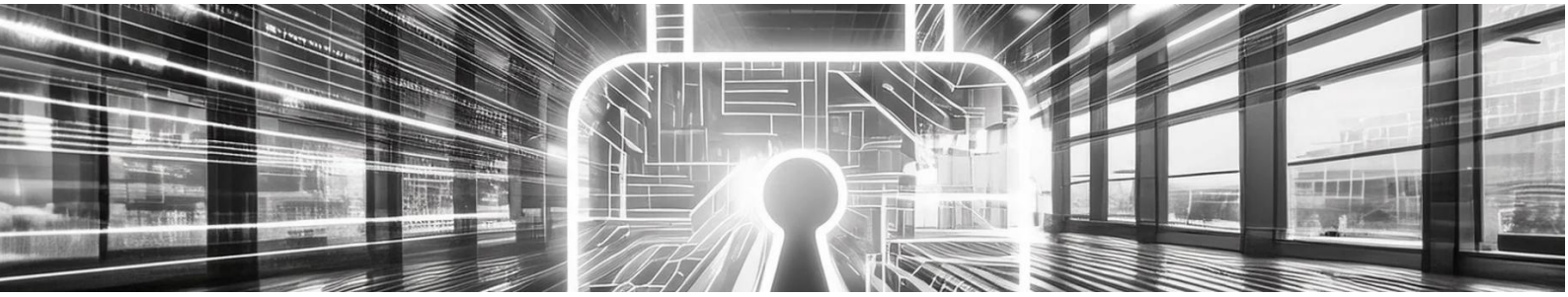


Cyber Security Readiness

Risiken erkennen. Sicherheitsmaturität verstehen. Gezielt handeln.

Cyberbedrohungen nehmen kontinuierlich zu und betreffen längst nicht mehr nur grosse Unternehmen. Gleichzeitig fehlt vielen Organisationen eine klare Sicht darauf, wie gut sie tatsächlich auf Cyberangriffe vorbereitet sind. Technische Massnahmen, organisatorische Regelungen und menschliches Verhalten greifen oft nicht ineinander, wodurch ein trügerisches Sicherheitsgefühl entsteht.

Unser Service **Cyber Security Readiness** schafft Transparenz. Wir analysieren Ihre aktuelle Sicherheitslage ganzheitlich und zeigen auf, wo reale Risiken bestehen, wie hoch Ihre Sicherheitsreife ist und welche Massnahmen notwendig sind, um Ihr Unternehmen gezielt und wirksam zu schützen.

Unser Service

Cyber Security Readiness unterstützt Sie dabei, Ihre Sicherheitslage ganzheitlich und verständlich zu beurteilen. Wir analysieren technische Systeme, organisatorische Strukturen, Prozesse sowie den menschlichen Faktor und setzen diese in Relation zu anerkannten Standards und Best Practices.

Neben einer strukturierten Bewertung Ihrer Cyber-Sicherheitsreife identifizieren wir dabei auch konkrete Quick Wins, mit denen sich das Sicherheitsniveau kurzfristig und mit überschaubarem Aufwand verbessern lässt. Ergänzend zeigen wir mittel- und langfristige Handlungsfelder auf und priorisieren Massnahmen zur nachhaltigen Steigerung Ihrer Sicherheitsmaturität. Das Ergebnis ist ein realistisches, nachvollziehbares Lagebild Ihrer Cyber Security Readiness – als fundierte Entscheidungsgrundlage für Management, IT und Governance.

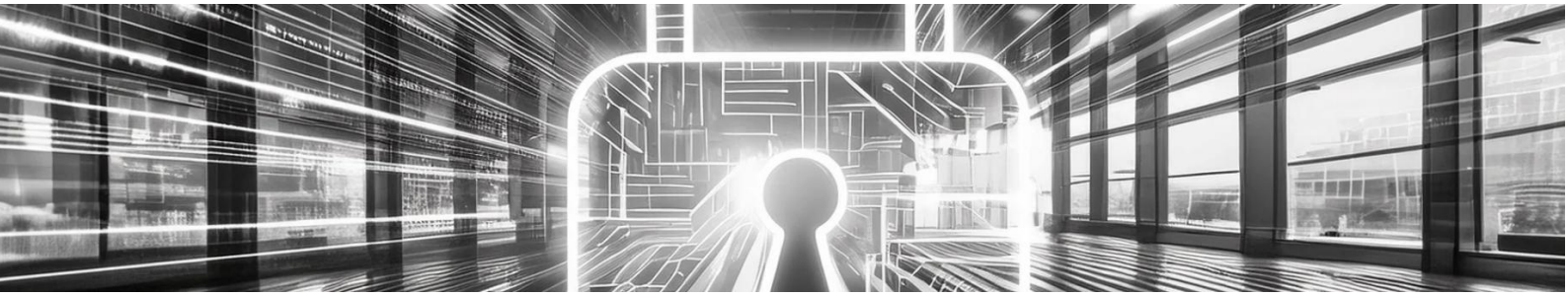
Zielgruppe

Der Service richtet sich an Geschäftsleitungen, Verwaltungsräte, IT- und Sicherheitsverantwortliche sowie Organisationen, die ihre Cyber-Sicherheitslage realistisch einschätzen und gezielt verbessern möchten. Besonders geeignet ist Cyber Security Readiness für Unternehmen mit steigenden regulatorischen oder versicherungsrelevanten Anforderungen.

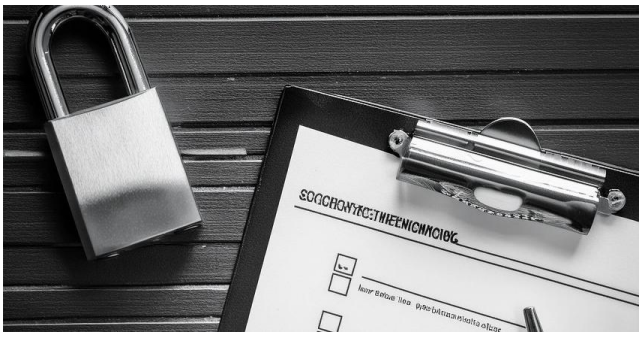
Ihr Nutzen

Mit Cyber Security Readiness verbessern Sie Ihre Sicherheitslage gezielt und nachvollziehbar. Der konkrete Nutzen für Ihr Unternehmen zeigt sich insbesondere in folgenden Punkten

- **Klarheit über die aktuelle Sicherheitsmaturität** ihrer Organisation.
- **Früherkennung von Schwachstellen und Risiken,** bevor Angreifer diese ausnutzen.
- **Konkrete, umsetzbare Handlungsempfehlungen,** abgestimmt auf Ihr Unternehmen.
- **Verbesserte Entscheidungsgrundlage für Geschäftsleitung und IT,** verständlich aufbereitet.
- **Prävention statt Reaktion,** um Zeit, Kosten und Reputationsschäden im Ernstfall zu vermeiden.



Wie gehen wir vor?



Organisatorische und prozessuale Sicherheitsaspekte

Neben der Technik analysieren wir Ihre internen Prozesse und Strukturen. Dazu gehören unter anderem vorhandene IT-Sicherheitsrichtlinien, klar definierte Rollen und Verantwortlichkeiten sowie Prozesse für Zugriffs- und Benutzerverwaltung. Auch das Patch- und Schwachstellenmanagement sowie das Notfall- und Incident-Management werden bewertet, um aufzuzeigen, wie gut Ihre Organisation auf Sicherheitsvorfälle vorbereitet ist.

Technische Sicherheit

Im technischen Teil bewerten wir die Sicherheitsarchitektur Ihres Unternehmens umfassend. Wir prüfen Netzwerke, Firewalls und Remote-Zugänge, die Absicherung Ihrer Endgeräte sowie Cloud-Umgebungen wie Microsoft 365 oder Azure. Ergänzend analysieren wir Konfigurationen, Berechtigungen und Schutzmechanismen und identifizieren potenzielle Angriffsflächen.

Menschliches Verhalten und Awareness

Ein zentraler Faktor für die Cyber-Sicherheitslage ist das Verhalten der Mitarbeitenden. Deshalb betrachten wir auch, wie Sicherheitsbewusstsein in Ihrem Unternehmen verankert ist und im Alltag gelebt wird. Wir prüfen, ob regelmässige Schulungen stattfinden, wie Mitarbeitende auf Phishing und Social Engineering vorbereitet sind und inwiefern Awareness-Massnahmen bereits Wirkung zeigen.

Zusammenführen und Risikobeurteilung

Alle gewonnenen Erkenntnisse werden in einem strukturierten Gesamtbild zusammengeführt. Sie erhalten eine klare Bewertung Ihrer Cyber-Sicherheitsreife sowie priorisierte Empfehlungen zur Verbesserung Ihrer Sicherheitsmaturität. Neben mittel- und langfristigen Massnahmen identifizieren wir dabei auch konkrete Quick Wins, mit denen sich die Sicherheit Ihres Unternehmens kurzfristig und mit überschaubarem Aufwand spürbar erhöhen lässt. Der Bericht ist so aufgebaut, dass er sowohl für Geschäftsleitung als auch für IT-Verantwortliche verständlich, nachvollziehbar und direkt umsetzbar ist.

Vorgehensweise

Wir erfassen Ihre aktuelle Sicherheitslage in Interviews und Workshops mit relevanten Fach- und Führungspersonen. Ergänzend prüfen wir vorhandene Sicherheitsdokumente, Richtlinien und Verantwortlichkeiten. Technische Analysen in Form von Schwachstellenscans ermöglichen eine realistische Einschätzung von Systemen, Netzwerken und Konfigurationen. Anschliessend gleichen wir den Ist-Zustand mit anerkannten Standards ab, bewerten identifizierte Risiken nach Kritikalität und Wirkung und fassen die Ergebnisse in einem übersichtlichen Bericht inklusive Ergebnispräsentation zusammen.

Optional: Begleitung bei der Umsetzung

Auf Wunsch unterstützen wir Sie bei der Umsetzung der empfohlenen Massnahmen oder begleiten Sie bei der Weiterentwicklung Ihrer Sicherheitsstrategie. So stellen wir sicher, dass aus der Analyse konkrete Verbesserungen entstehen und Ihre Cyber Security Readiness nachhaltig erhöht wird.

Ihr Kontakt
Raphael Ruch
Senior Cyber Security Consultant
raphael.ruch@netrics.ch
+41 31 531 32 08