



bechtle

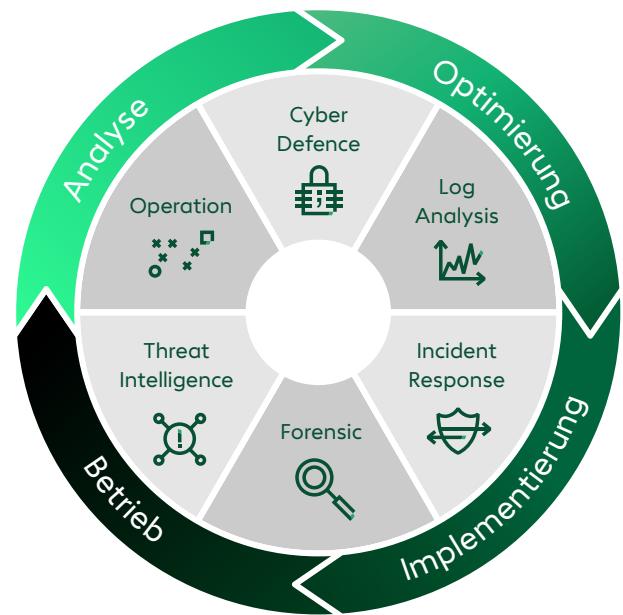


Cyber Security Assessment.

Welche Sicherheitsbereiche in Ihrem Unternehmen sind am meisten gefährdet? Ist Ihre Infrastruktur hinreichend gegen aktuelle Bedrohungen geschützt und auf dem aktuellsten Stand? Wie effizient nutzen Sie die Sicherheitsfeatures in Microsoft Azure? Gibt es möglicherweise unerkannte Risiken? Alle diese Fragen können durch ein Cybersecurity Assessment identifiziert, klassifiziert und beseitigt werden.

IT-Sicherheit ist ein komplexer Bereich geworden. Die Art, wie Angreifer agieren, verändert sich ständig: Über 50 verschiedene Angriffsarten sind bereits klassifiziert und es werden immer mehr. Unternehmen, die sich für alle Angriffsszenarien wappnen möchten, brauchen deshalb ausgefeilte Security-Lösungen und Dienstleistungen. Diese müssen natürlich auch regelmäßig aktualisiert und überwacht werden, damit unerkannte Sicherheitslücken kein Risiko für Ihr Unternehmen darstellen.

Bechtle Security bietet Ihnen ein umfangreiches Lösungspaket, um die maximale Sicherheit vor Cyberangriffen zu gewährleisten. Dabei kommt es auf eine ganzheitliche Ende-zu-Ende-Security-Lösung an – ganz gleich, ob es um Industrie 4.0, eine klassische IT-Infrastruktur, eine Cloud-Lösung oder um vernetztes mobiles Arbeiten geht.



Was bietet unser Cybersecurity Assessment?

Wie sicher ist Ihre IT-Infrastruktur? Gerade jetzt, wo viele Unternehmen von Ransomware, DDoS-Angriffen und Phishing-Mails betroffen sind, ist es wichtiger denn je, dass Sie überprüfen, wie effektiv Ihre Cybersicherheit ist. Idealerweise sollten Sie dies regelmäßig tun, da sich Cyber-Angriffstechniken und Malware ständig weiterentwickeln. Außerdem kann ein falscher Mausklick grosse Folgen haben, ohne dass Sie sich dessen bewusst sind. Eine regelmässige Überprüfung mit dem Cybersecurity Assessment Tool verschafft Ihnen schnell einen Einblick in mögliche Cyberrisiken und hilft Ihnen zu entscheiden, wie und wo Sie Ihre Sicherheitsmaßnahmen verbessern können.

Das Cybersecurity Assessment scannt Ihre gesamte Unternehmensinfrastruktur inklusive Microsoft 365 und Azure auf mögliche Schwachstellen. Wir scannen unter anderem Ihr Patch-Management für Geräte und kontrollieren, ob Windows korrekt konfiguriert ist. Außerdem überprüfen wir administrative Rechte und externe Nutzer in Microsoft 365, Teams und SharePoint. Auf diese Weise identifiziert das Assessment präzise die Schwachstellen in Ihrer Sicherheitskonfiguration.

Das Cybersecurity Assessment wird mit einem klaren Plan zur Verbesserung der Cybersicherheit in Ihrem Unternehmen geliefert, und zwar genau dort, wo es nötig ist. Er umfasst klare technische und organisatorische Massnahmen, so dass Sie direkt mit der Arbeit beginnen und Ihre Ressourcen effektiv nutzen können.

Mit folgenden Dienstleistungen können wir Sie hier unterstützen:

Einmaliges Cybersecurity Assessment Ihrer Infrastruktur.

Einmaliges Cybersecurity Assessment¹



Aufnahme und Installation:

- Installation der Software (CSAT) auf einem Windows-Server
- Konfiguration CSAT (Accounts/Gruppen/Rechte)
- Erhebung der technischen Infrastruktur
- Kontrolle Endpunkte und Netzwerkzugänge (Discovery)



Durchführung des technischen Scans der Infrastruktur sowie der Microsoft Technologien:

- Durchführung Scan auf Endpunkten
- Durchführung Scan auf Active Directory
- Kontrolle Office 365-Lizenzen
- Durchführung Scan auf Office 365 und Azure Active Directory



Durchführung der organisatorischen Auditierung anhand des CIS Frameworks:

- Erläuterung aller 18 Disziplinen im Framework
- Interview und Selbstevaluierung anhand des bestehenden Fragekatalogs zu den einzelnen Disziplinen



Erstellung Report:

- Analysieren der Ergebnisse
- Erstellung Report und Empfehlungen
- Ausarbeiten der Quickwins
- Ausarbeiten der dringlichsten Massnahmen



Präsentation der Ergebnisse und des Reports:

- Bereitstellung eines Abschlussberichtes sowie Präsentation über die identifizierten Findings
- Festhalten der nächsten Schritte
- Handlungsempfehlung basierend auf Microsoft Technologien

Cybersecurity Assessment im Subscription Modell (ab 12 Monate Laufzeit).

Kontinuierlicher Zugang zum Cybersecurity Assessment¹

Alle Dienstleistungen inkludiert wie im einmaligen Cybersecurity Assessment plus folgende Vorteile:

- Jährliche/halbjährliche Sicherstellung des aktuellen Reifegrades
- Darstellung der Verbesserungen einzelner Disziplinen über die Laufzeit des Assessments
- Fester Ansprechpartner für alle relevanten Fragen über die komplette Laufzeit
- Vollautomatisierte Scans in Ihrer Infrastruktur, um Änderungen schnell erkennen zu können
- Aufzeigen einer Entwicklung des Unternehmensrisikos über den Nutzungszeitraum

¹Die tatsächlichen Kosten der Lösung sind immer abhängig von der Anzahl der zu scannenden Assets sowie der Komplexität der Umgebung. Für jedes Kundenszenario erfolgt eine dedizierte Bestandsaufnahme sowie Dienstleistungsabschätzung.

Weitere Vorteile für Sie:

Hilfreiche Funktionen für Ihr Unternehmen.

Installation der Software in Ihrer eigenen Infrastruktur	Alle Endpunkte in Ihrem Unternehmensnetzwerk werden gescannt (Laptops, Server, virtuelle Instanzen)	Überprüfung aller Microsoft 365 und Office 365 Ressourcen	Überprüfung aller Azure Ressourcen
Komplette Überprüfung Azure Active Directory	Technische und organisatorische Reifegradbestimmung anhand des CIS Frameworks	Endpunktagenten deinstallieren sich nach dem Assessment vollautomatisch	Überprüfung Lizenzierung in Azure

Sie haben Fragen zum Thema Security?

Bechtle Schweiz AG
Kontaktieren Sie Ihren Key Account Manager oder einfach:

security.ch@bechtle.com
Telefon +41 848 820 420

Basel | Bern | Mägenwil | Morges | Petit-Lancy | Pratteln | Rotkreuz | St. Gallen

