



SAM Cybersecurity Engagement.

Weltweit verursachen Cyberangriffe auf Unternehmen einen jährlichen Schaden von mehr als 400 Mrd. \$¹. Studien prognostizieren bis 2019 einen Anstieg auf bis zu 2.1 Billionen \$². Viel zu viele Unternehmen schützen sich nicht ausreichend vor diesen Angriffen: Apps können ohne Zustimmung heruntergeladen werden, im Unternehmensnetzwerk können nicht verwaltete Geräte verwendet werden, der Passwortschutz ist unzulänglich und vieles mehr. Durch den digitalen Wandel benötigen nun immer mehr Unternehmen eine verbesserte Transparenz und Kontrolle ihrer IT-Infrastruktur, um die damit verbundenen Chancen und Möglichkeiten voll und ganz nutzen zu können.

SAM Cybersecurity Engagement

Das Software Asset Management (SAM) Cybersecurity Engagement bietet Ihnen eine umfassende Analyse Ihrer Cybersecurity-Infrastruktur inklusive Ihrer aktuellen Softwarebereitstellung und -nutzung sowie Ihrer Lizenzierungsdaten. Wir helfen Ihnen aber nicht nur dabei, die richtigen Vorkehrungen zu treffen, damit Sie Cyberrisiken vermeiden, sondern bieten Ihnen auch Leitlinien und Best Practices zum Thema Cybersecurity in der digitalen Welt an. So können Sie sich stärker auf Ihr Kerngeschäft konzentrieren, da für den Schutz gesorgt ist.

Nutzen des SAM Cybersecurity Engagements

- | Verringerung von Datenverlusten, Betrugsrisiken und Ausfallzeiten von Mitarbeitern
- | Kostenvermeidung durch die Abwehr von Cyberangriffen und durch die Steigerung der Effizienz
- | Sichere Verwaltung der Softwarebestände und Förderung verlässlicher Cybersecurity-Vorgehensweisen
- | Aufbau einer stabilen und flexiblen IT-Infrastruktur, die schnell auf Bedrohungen reagieren kann
- | Gewährleistung einer sicheren IT-Infrastruktur, die Ihnen gegen Angriffe wirksamen Schutz bietet

Was Sie von einem SAM-Engagement erwarten können. 4-Phasen-Projekt:

Planung

- | Ermittlung Ihrer Erfordernisse und Ziele
- | Einholen von Informationen zu Ihren Lizenzen, Ihrer IT-Infrastruktur und Ihrer Unternehmensorganisation
- | Besprechung und Festlegung der Zugänge und Ressourcen

Datenerhebung

- | Inventarisierung der Hardware- und Softwarebestände sowie der Lizenzen mittels Inventarisierungstools, Fragebögen und Interviews mit Stakeholdern
- | Einholen von Informationen zu den Prozessen und Verfahren

Datenanalyse

- | Prüfung und Validierung aller erhobenen Daten
- | Vergleich der eingesetzten Assets mit Ihrer aktuellen Nutzung
- | Erarbeitung eines Plans zur Optimierung der aktuellen Umgebung im Hinblick auf Ihre Ziele

Schlusspräsentation

- | Vorstellung der Endergebnisse und Empfehlungen mit anschließender Diskussion auf Grundlage detaillierter Berichte, um sicherzustellen, dass Ihre geschäftlichen Erfordernisse erfüllt sind und Ihre Ziele erreicht werden

Im Jahr 2016 waren 53 Prozent aller Unternehmen von mindestens einer Datenschutzverletzung im Laufe der letzten beiden Jahre betroffen³.

¹<http://www.cyberinsurance.co.uk/cybernews/loyds-ceo-cyber-crime-cost-businesses-up-to-400-billion-a-year/>

²Juniper Research, Cybercrime and the Internet of Threats, May 2015

³The 2016 Cyber Resilient Organization Executive Summary, Ponemon Institute and IBM, <http://info.resilientsystems.com/ponemon-institute-study-the-2016-cyber-resilient-organization>

Comsoft direct AG

Telefon +41 848 820 420

sam@comsoft.ch, comsoft.ch



Weitere Informationen:
comsoft.ch/valueengagement

COMSOFTdirect

Bechtle's Software Specialist