COMSOFT direct

Bechtle's Software Specialist

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 SAM (Software Asset Management) Cybersecurity Engagement bietet Ihnen eine umfassende Analyse Ihrer Cybersecurity-Infrastruktur inkl. 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 Förderungverlässlicher 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

Im Jahr **2016** waren **53 Prozent** aller Unternehmen von mindestens einer Datenschutzverletzung im Laufe der letzten beiden Jahre betroffen.[3]

[1]http://www.cyberinsurance.co.uk/cybernews/lloyds-ceo-cyber-crime-cost-businesses-up-to-400-bilion-a-year/
[2]Juniper Research, Cybercrime and the Internet of Threats, May 2015
[3]The 2016 Cyber Resilient Organization Executive Summary, Ponemon Institute and IBM, http://info.resilientsystems.com/ponemon-institute-study-the-2016-cyber-resilient-organization

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 deren aktueller Nutzung
- Erarbeitung eines Plans zur Optimierung Ihrer 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

Competence Center SAM · sam@comsoft.ch · www.comsoft.ch · +41 848 820 421