LEANmade
PRIVATE | SECURE | COMPLIANT

Kundensegment:
Mittelstand

Schweizer Produktionsunternehmen
Metalloberflächen-Veredelungen

Situation

- **Wachsende Besorgnis hinsichtlich des Umgangs mit und des Schutzes von folgenden Informationstypen:**
  - Geistiges Eigentum (IP)
  - Persönlich identifizierbare Daten (PID) von Kunden, Partnern und Mitarbeitern
  - Finanz- und Betriebsdaten

- **Wollte eine unabhängige Bestätigung über ausreichende Schutz und Sicherheitsmaßnahmen für IT-Infrastruktur, -Prozesse und -Governance,** und zwar in folgenden Bereichen:
  - Strukturierte Daten (ERP, CRM, Fertigungssysteme, usw) sowie
  - Unstrukturierte Daten (Email, Fileshares)

- **Limitierte interne und externe Ressourcen, denen die Kapazität und teilweise die erforderlichen Fachkenntnisse fehlen**

Lösung

Durchführung ein zweitägigen, standardisierten und technischen IT-Sicherheits-Assessment, um die größten Risiken und Möglichkeiten zu ermitteln und einen schlanken und überschaubaren Arbeitsumfang zu definieren. Dies beinhaltete:

- **Datensicherheit**
  Überprüfung der vorhandenen Zugriffsrichtlinien, um sicherzustellen, dass nur autorisierte Benutzer auf vertrauliche Informationen zugreifen können. Dies führte zu Empfehlungen für Änderungen, die sich speziell auf den Remotezugriff von Drittanbietern beziehen

- **IT Security**
  - Überprüfung der bestehenden Risikomanagement-Kontrollen im Falle einer Datenpanne.
  - Durchführung eines vollständig skriptbasierten und automatisierten technischen Erkennungs-service, um ein technisches Bild der Cyberrisiken zu erhalten, mit denen die Organisation konfrontiert ist.
    Dies umfasste die folgenden Bereiche:
    - Risikomanagement (NIST)
    - Bestandsverwaltung (Hardware) (CIS 1)
    - Bestandsverwaltung (Software) (CIS 2)
    - Kontinuierliches Schwachstellenmanagement (CIS 3)
    - Kontrolle über Administratorrechte (CIS 4)
    - Sichere Konfiguration - Endpunkte (CIS 5)
    - Überwachung (CIS 6)
  - Zusätzlich haben wir einen grundlegenden Penetrationstest für einige der wichtigsten Assets der Organisation durchgeführt.

Ergebnisse

- Durch unsere Bewertung stellten wir fest, dass die vorhandenen Prozesse und Compliance-Maßnahmen als Ausgangspunkt solide sind (u.a. durch IT-Spezialisten von Drittpartnern), **jedoch mehrere Aktualisierungen und Verbesserungen erforderten, um den gesamten IT-Betrieb in einer immer vernetzteren Welt heute und auch morgen garantieren zu können.**

- LEANmade war in der Lage, sowohl schnelle Erfolge als auch langfristige Verbesserungsvorschläge zu identifizieren, die **kostengünstig und effizient** umgesetzt werden können

- **Einige Verbesserungsbereiche waren:**
  - Übergang von einem passiven zu einem aktiven Schutzmodell, bei dem Sicherheitskontrollen geprüft und im Laufe der Zeit verbessert werden
  - **Optimierung der aktuellen Sicherheitsinfrastruktur**, um die verfügbaren Funktionen voll nutzen zu können
  - **Vorschlag zusätzlicher Kontrollen**, inkl. einer Roadmap für einen essentiellen Business-Service, der auf eine End-of-Life-Plattform (EoL) baut.