CSMS & SUMS – Cybersecurity- und Software-Update-Managementsysteme

Die Sicherstellung von IT-Sicherheit und Integrität erfordert heute mehr als nur technische Schutzmaßnahmen. Mit der Einführung eines **Cybersecurity-Managementsystems (CSMS)** und eines **Software-Update-Managementsystems (SUMS)** können Unternehmen ihre Sicherheitsprozesse systematisch stärken und Risiken nachhaltig reduzieren.
Während das CSMS organisatorische und technische Maßnahmen zur Absicherung von IT-Systemen umfasst, sorgt das SUMS für eine strukturierte Verwaltung und Verifizierung von Software-Updates. Zusammen bilden sie eine entscheidende Grundlage für den Schutz gegen Cyberangriffe und die Einhaltung regulatorischer Anforderungen.

Hauptfunktionen von CSMS & SUMS

- **Cybersecurity-Managementsystem (CSMS)**: Risikoanalysen, Sicherheitsrichtlinien, Incident-Response-Prozesse und Mitarbeiterschulungen.
- **Software-Update-Managementsystem (SUMS)**: Überwachung, Planung, Installation und Verifizierung von Updates.
- **Risikomanagement**: Laufende Bewertungen und Maßnahmen zur Reduzierung von Bedrohungen.
- **Compliance & Standards**: Erfüllung internationaler Vorgaben wie ISO 27001 und DSGVO.
- **Qualitätssicherung**: Regelmäßige Prüfungen, um die Wirksamkeit der Sicherheits- und Update-Prozesse sicherzustellen.

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

Vorteile der Einführung von CSMS & SUMS

- **Verbesserte Sicherheit** durch strukturierte Prozesse und definierte Richtlinien.
- **Reduzierung von Cyberrisiken** durch präventive Analysen und kontrollierte Updates.
- **Steigerung der Effizienz** durch Automatisierung und klare Verantwortlichkeiten.
- **Erfüllung von Compliance-Anforderungen** und Unterstützung bei Audits.
- **Höhere Resilienz** gegenüber Ausfällen und Angriffen.

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

CSMS & SUMS – Checkliste für Unternehmen

Ziel: Herausfinden, ob die Einführung eines CSMS und SUMS für Ihr Unternehmen notwendig ist.

1. Cyberbedrohungen & Sicherheitsrichtlinien

Fragen:	**Ja**	**Nein**
Sind unsere IT-Systeme gegen externe Angriffe wie Hacking abgesichert?	☐	☐
Verfügt unser Unternehmen über dokumentierte Sicherheitsrichtlinien?	☐	☐
Finden regelmäßige Sicherheitsschulungen für Mitarbeitende statt?	☐	☐
Wissen wir, wie wir unsere Daten wirksam vor Verlust schützen?	☐	☐

---

2. Software-Updates & Prozesse

Fragen:	**Ja**	**Nein**
Führen wir regelmäßig Updates für alle Systeme und Anwendungen durch?	☐	☐
Überwachen wir verfügbare Updates kontinuierlich?	☐	☐
Werden Installation und Verifizierung von Updates standardisiert durchgeführt?	☐	☐
Gibt es Pläne für Notfälle bei fehlgeschlagenen oder kritischen Updates?	☐	☐

---

3. Risikoanalyse & Reduzierung

Fragen:	**Ja**	**Nein**
Wird regelmäßig eine umfassende Risikobewertung durchgeführt?	☐	☐
Sind alle relevanten IT-Systeme und Daten Teil der Analyse?	☐	☐
Existieren konkrete Maßnahmen zur Risikoreduzierung?	☐	☐
Wissen wir, wie wir Auswirkungen eines Cyberangriffs minimieren können?	☐	☐

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

4. Compliance & Standards

Fragen:	Ja	Nein
Sind wir nach gängigen Sicherheitsstandards (z. B. ISO 27001) zertifiziert?	☐	☐
Erfüllen wir die Vorgaben der DSGVO?	☐	☐
Sind Sicherheitsrichtlinien allen Mitarbeitenden bekannt?	☐	☐
Berücksichtigen wir interne Risiken wie Fehlverhalten von Mitarbeitenden?	☐	☐

---

5. Effizienz & Produktivität

Fragen:	Ja	Nein
Haben wir analysiert, wie CSMS & SUMS unsere Produktivität verbessern können?	☐	☐
Gibt es Pläne zur Umsetzung notwendiger IT-Änderungen?	☐	☐
Wird die Qualitätssicherung regelmäßig überprüft?	☐	☐

Auswertung der Checkliste

Anzahl „Ja“ Antworten	Einschätzung
0–2	Wahrscheinlich nicht notwendig, alternative Maßnahmen prüfen.
3–5	Möglicherweise sinnvoll – detaillierte Bedarfsanalyse empfohlen.
6 oder mehr	Sehr wahrscheinlich sinnvoll – Einführung von CSMS & SUMS dringend empfohlen.

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg

Cyber Complete GmbH
Weststraße 4
57392 Schmallenberg