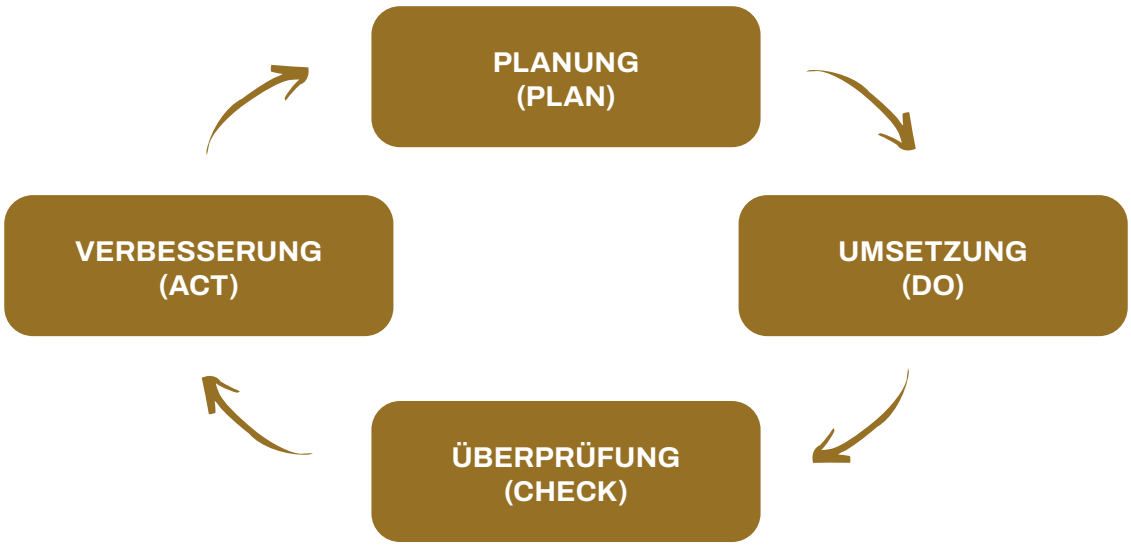
HARDMAN SECURITY
WE GET IT DONE

Informationen zum Sicherheitsprozess

Informationssicherheit ist kein statischer Zustand, der einmal erreicht wird und dann für immer besteht. Es handelt sich vielmehr um einen kontinuierlichen Prozess, der fortlaufend angepasst werden muss. Veränderungen in den Verfahren und Prozessen einer Institution, rechtliche Rahmenbedingungen, neue Technologien sowie bislang unbekannte Schwachstellen und damit verbundene Bedrohungen stellen immer wieder neue Anforderungen. Daher ist es nicht automatisch gewährleistet, dass die angemessene und effektive Sicherheit dauerhaft gewährleistet ist. Der gesamte Sicherheitsprozess durchläuft einen Lebenszyklus, der aus folgenden Phasen besteht:



- **Planung (Plan)**: In dieser Phase werden Sicherheitsmaßnahmen geplant.
- **Umsetzung (Do)**: Hier erfolgt die praktische Umsetzung der geplanten Maßnahmen.
- **Überprüfung (Check)**: Es werden Erfolgskontrollen durchgeführt, um die Zielerreichung zu überwachen.
- **Verbesserung (Act)**: Anhand der Ergebnisse der Überprüfung werden Mängel behoben und Verbesserungen vorgenommen.

Dieser PDCA-Zyklus (Plan-Do-Check-Act) nach William Edwards Deming ist ein bewährter Bestandteil vieler Managementsysteme, einschließlich des Qualitäts- und Umweltmanagements.

Insbesondere die regelmäßige Überprüfung und kontinuierliche Verbesserung sind entscheidende Managementprinzipien im Sicherheitsprozess. Ohne regelmäßige Überprüfung kann die Wirksamkeit der organisatorischen und technischen Schutzmaßnahmen langfristig nicht gewährleistet werden.

Die Dokumentation ist kein Selbstzweck, aber eine gute Dokumentation trägt dazu bei, den Sicherheitsprozess und getroffene Entscheidungen nachvollziehbar zu gestalten und Missverständnisse zu vermeiden. Die Dokumentation kann sowohl in elektronischer Form als auch in Papierform vorliegen. Die elektronische Form bietet den Vorteil der leichten Aktualisierbarkeit und schnellen Verfügbarkeit, wobei die Zugriffsrechte sorgfältig geregelt werden müssen.

Um Informationen angemessen schützen zu können, ist es wichtig, ihre Bedeutung für die Institution klar zu erkennen. Eine Möglichkeit hierfür ist die Klassifizierung von Informationen, bei der Dokumente je nach Vertraulichkeit eingestuft und entsprechende Regeln für ihren Umgang festgelegt werden. Durch einen Klassifizierungsvermerk kann jeder Mitarbeiter sofort erkennen, wie er mit den eingestuften Informationen umgehen sollte.

Alle Leistungen müssen in den vorgegebenen Richtlinien gemäß den Anforderungen des Kunden ausgeführt werden. Es ist wichtig, jeden einzelnen Schritt genau aufzuführen und sicherzustellen, dass er sich an die festgelegten Parameter anpasst. Das System erkennt Muster nur dann, wenn die Variablen mit den Parameterdaten übereinstimmen. Sollte ein unbekannter Ablauf auftreten, wird das System diesen analysieren und isolieren, um die Schwachstelle zu identifizieren und zu beheben.

Um den angestrebten „SOLL“-Zustand zu erreichen, ist es notwendig, alle potenziellen Schwachstellen in den Prozess einzubeziehen. Selbst scheinbar unwichtige Details können die größten Sicherheitslücken darstellen. Daher ist es wichtig, alle Aspekte des Vorgangs im Blick zu behalten.

Dies ist nur ein kurzer Überblick darüber, wie ein Sicherheitskonzept aufgebaut ist und funktioniert. Das gesamte Verfahren wird von unserem professionellen Sicherheitsanalytikerteam gewährleistet.

Mit freundlichen Grüßen,

Ihr Hardman Security Team