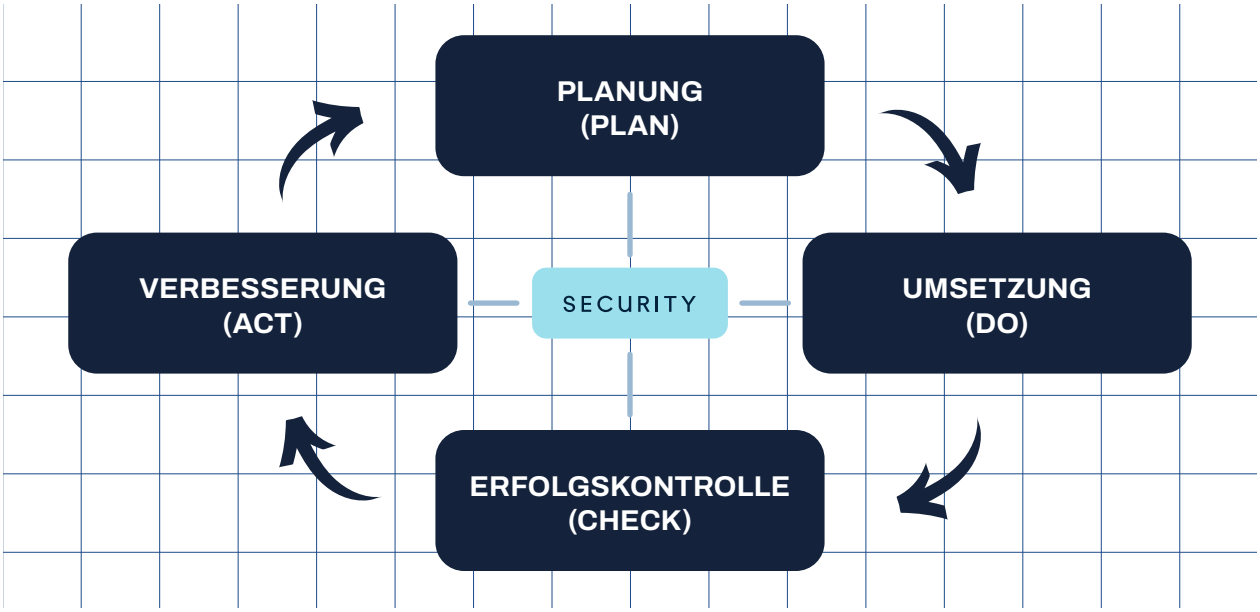
MOMENTUM
SECURITY

Informationen zum Sicherheitsprozess

Informationssicherheit ist ein dynamischer Prozess und keine statische Zustandsgröße. Es erfordert kontinuierliche Anpassungen an veränderte Verfahren, Prozesse in Institutionen, rechtliche Rahmenbedingungen, neue Technologien sowie bisher unbekannte Schwachstellen und daraus resultierende Bedrohungen. Die nachhaltige Angemessenheit und Wirksamkeit der Informationssicherheit sind daher nicht automatisch gewährleistet. Der gesamte Sicherheitsprozess durchläuft einen Lebenszyklus, der aus den folgenden Phasen besteht:



- **Planung (Plan)**: In dieser Phase werden Sicherheitsmaßnahmen geplant.
- **Umsetzung (Do)**: Hier werden die geplanten Maßnahmen praktisch umgesetzt.
- **Erfolgskontrolle (Check)**: Es erfolgen Erfolgskontrollen zur Überwachung der Zielerreichung.
- **Verbesserung (Act)**: Basierend auf den Überprüfungsergebnissen werden Mängel behoben und Verbesserungen vorgenommen.

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

Besonders die regelmäßige Überprüfung und kontinuierliche Verbesserung sind wesentliche Managementprinzipien im Sicherheitsprozess. Ohne regelmäßige Überprüfung kann die langfristige Wirksamkeit organisatorischer und technischer Schutzmaßnahmen nicht gewährleistet werden.

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

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

Alle Leistungen müssen gemäß den Anforderungen des Kunden in den vorgegebenen Richtlinien ausgeführt werden. Es ist wichtig, jeden Schritt detailliert 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 Sicherheitsanalyseteam gewährleistet.

Mit freundlichen Grüßen,

Ihr Momentum Security Team