> Die Zusammenarbeit zwischen privatem und öffentlichem Sektor ist unerlässlich. Nicht umsonst heißt es „Es braucht ein internationales Netzwerk, um ein internationales Netzwerk zu besiegen.

Philipp Amann
Group CISO,
Österreichische Post AG

Praxistipps

- **Kennen Sie Ihre wachsende Angriffsfläche und priorisieren Sie sie:** Verstehen Sie, welche Elemente in Ihrer Kontrolle liegen und welche nicht. Gehen Sie technische, menschliche und Drittrisiken durch entsprechende Nachverfolgung, sorgfältige Prüfung und den Einsatz von Ressourcen basierend auf Ihrem Ausmaß an Bedrohungen an.
- **Vereinfachen Sie Prozesse im Sinne der Agilität und Kostensenkung:** Jede zusätzliche Layer, jeder Prozess und jedes System steigert die Komplexität im Alltag und erschwert eine schnelle Reaktion im Fall eines Angriffs. Konsolidieren Sie Zulieferer und Systeme und etablieren Sie Geschäftsbereiche, um sicherzustellen, dass sie alle ihre Prozesse vereinfachen.
- **Stärken Sie Ihre operationale Resilienz:** Arbeiten Sie Hand in Hand mit den Verantwortlichen für Geschäftsprozesse, um sicherzustellen, dass wichtige Aufgaben auch im Falle eines Cyberangriffs fortgesetzt werden können – unter anderem auch durch analoge Abläufe. So gewährleisten Sie, dass Ihre Organisation in jeder Lage ein Minimum Viable Product oder Service bereitstellen kann.
- **Verteilen Sie die Verantwortung auf Abteilungen:** Vermeiden Sie, dass mangelnde Qualitätskontrollen in anderen Bereichen der Organisation auf das Sicherheitsteam zurückfallen. Weisen Sie die Zuständigkeit für OS-Patching, Code-Härtung und das Aufspüren veralteter Systeme den entsprechenden Teams zu, die dann auch für entstehende Risiken verantwortlich sind.