Workstream
„Security“

Neue Bedrohungen, neue Aspekte: Sicherheit in Zeiten der Digitalisierung

Der Workstream „Security“ arbeitet an der systematischen Erfassung der Risiken, die mit der zunehmenden Digitalisierung auftreten. Mit der Digitalisierung von Produkten, Services und ganzen Produktionsanlagen weiten sich die Angriffsmöglichkeiten von Cyberkriminellen und -spionen deutlich aus. Darüber hinaus können sich Menge und Schwere von Schäden durch Angriffe und Datenverluste enorm steigern, weil nicht mehr „nur“ IT-Systeme, sondern sämtliche Assets bis hin zur physischen Infrastruktur von Unternehmen und Behörden betroffen sein können. Der Workstream betrachtet Security in diesem stark erweiterten Gesamtbild und fragt sowohl nach neu entstehenden Sicherheitsherausforderungen als auch nach der Neubewertung bestehender Herausforderungen.

Den Teilnehmern des Workstreams war von Anfang an klar, dass es unmöglich ist, alle in Zusammenhang mit der Digitalisierung relevanten Sicherheitsrisiken in allen Bereichen zu benennen und zu beschreiben.

Deshalb wurden aus einer Liste von zehn Themenbereichen, die in die engere Wahl genommen wurden, auf Basis der wesentlichen Digitalisierungstreiber (Technologie, Daten, Kunden und Mitarbeiter) drei Fokusthemen ausgewählt:

- **Agilität**
  Welche bestehenden Risiken verstärken sich und welche neuen Risiken tauchen auf durch die Agilisierung von IT, Geschäftsprozessen und Geschäftsmodellen?
- **Technologievielfalt**
  Wie kann den zusätzlichen Gefahren und erhöhten Risiken begegnet werden, die durch die Menge und Heterogenität der in Unternehmen eingesetzten Technologien entstehen?
- **IoT als Massenware**
  Welche Gefahren tauchen durch die vielen, oftmals nicht selbst abgesicherten IoT-Devices, Sensoren und Aktuatoren und deren Verknüpfung

Dr. Ilir Fetai
Workstreamleiter

Wie stellen wir sicher, dass Security auch im agilen Umfeld priorisiert wird?

mit dem Internet und der klassischen IT auf?

In Bezug auf Agilität erscheinen dem Workstream vor allem drei Fragen wichtig: Wie wirken sich agile Vorgehensweisen auf die Themen Transparenz, Governance, Qualität und Skalierbarkeit aus? Wie wirkt sich Agilität auf die konsequente Implementierung von Security aus? Und wie können Unternehmen sicherstellen, dass diese Themen trotz Agilisierung den Unternehmens- und Compliance-Anforderungen gemäß behandelt werden? Workstreamleiter Dr. Ilir Fetai von der SBB erläutert: „Dabei geht es uns nicht nur um die spezifischen technischen Themen, sondern auch um Organisationsfragen. Wie stellen wir zum Beispiel sicher, dass Security auch im agilen Umfeld priorisiert wird?“. Wenn zum Beispiel die Schnelligkeit ein entscheidendes Kriterium bei der Produktentwicklung sei, werde Security wahrscheinlich nicht automatisch Priorität eingeräumt. Der Workstreamleiter betont, dass man dieses Thema auch unter Weiterbildungsaspekten betrachtet. „Wir müssen das in die Schulung der Mitarbeiter verstärkt einfließen lassen.“

Im Bereich Technologievielfalt befasst sich der Workstream in erster Linie mit der Heterogenität der eingesetzten Technologien und mit den Auswirkungen neuer Technologien auf die Sicherheit. So werden bei großen Unternehmen viele Technologieentscheidungen dezentral getroffen, weil bestimmte Business Units ihre Entwicklungen und Produkte schnell auf den Markt bringen wollen. Das stellt die Security vor besondere Herausforderungen beispielsweise in Bezug auf Open-Source-Produkte oder ungetestete Produkte.

Zusätzlich wird der Einfluss neuer Technologien auf die Security betrachtet: Wie wirkt sich Künstliche Intelligenz auf die Sicherheitsrisiken aus, wenn man bedenkt, dass durch KI viele neue Angriffsmöglichkeiten entstehen (z. B. automatisierte Suche nach Schwachstellen in der Software, automatisierte Social-Engineering-Angriffe, manipulierte Sprach- und Gesichtserkennung usw.)?

Die Auswirkungen der Digitalisierung auf Kernapplikationen sieht der Workstream ebenfalls als einen wichtigen Aspekt im Bereich der Technologievielfalt. „Wir wollen herausbekommen, wie Kernanwendungen im Kontext der Agilität zu schützen sind“, formuliert der Workstreamleiter den Anspruch des Workstreams in diesem Bereich.

Beim Fokusthema „IoT als Massenware“ konzentriert sich der Workstream auf die Sicherheit der IoT-Devices, Sensoren und Aktuatoren und auf die Verknüpfung der IoT-Devices mit Web und IT sowie auf die Sicherheit von Entscheidungen, die auf der Analyse der von den Devices gelieferten Daten basieren. „Wie stellen wir sicher, dass die Resultate der Verknüpfungen von Devices mit der klassischen IT und dem Internet sicher sind? Wenn zum Beispiel Sensoren dafür verantwortlich sind, dass ein Zug in einer bestimmten Situation fährt oder anhält, können das lebenswichtige Entscheidungen sein. In diesen Fällen muss man hundertprozentig sicher sein können, dass die Sensordaten nicht manipuliert sind“, erklärt Dr. Fetai. Im Allgemeinen bieten viele IoT-Geräte keine Möglichkeit für Updates, was eine ganze Reihe von Security-Fragestellungen aufwirft.