Zukunftsfeld Sicherheitsvorsorge

Österreichs Wirtschaft auf dem Weg zu einem gemeinsamen Cyberlagebild

Von Dr. Heiko Borchert und Mag. Wolfgang Gattringer

Diebstahl, Fälschung, Betrug, Spionage, Sabotage – die Gefahren des Umgangs mit digitalen Technologien sind in der Medienberichterstattung allgegenwärtig. Beinahe entsteht der Eindruck, der „Cyberspace" sei der gefährlichste Raum, in dem sich Menschen bewegen. Der sprunghafte Anstieg des Interesses an Cyber(un)sicherheit ist die logische Folge der digitalen Vernetzung. Der Einsatz digitaler Technologien ist zentrale Voraussetzung für effiziente Wirtschaftsprozesse, bürgernahe staatliche Dienstleistungen und die Pflege des „always on"-Lebensstils. Dem stehen die Risiken gegenüber: Auf mehrere hundert Milliarden Euro belaufen sich die Kostenschätzungen für weltweit begangene Cyberstraftaten (Cybercrime). Nicht überraschend spricht das Österreichische Bundesamt für Verfassungsschutz und Terrorismusbekämpfung in seinem Jahresbericht 2011 sogar davon, dass die Cyberrisiken „einen bisher nicht bekannten Reifegrad" erreicht haben.

Kann nur gemeinsam gelingen

Die Diskussion über Risiken ist wichtig für die Bewusstseinsbildung und für die Erkenntnis, dass neue Wege beschritten werden müssen, um Cyberunsicherheit zu bekämpfen. Ein Beispiel, wie Staat und Wirtschaft gemeinsam die Cybersicherheit verbessern können, ist die „Cybersecurity-Initiative" (CSI), die das Bundesministerium für Inneres und das Kuratorium Sicheres Österreich (KSÖ) lanciert haben. Sie basiert auf der Einsicht, dass Cybersicherheit nur gelingt, wenn Staat und Wirtschaft gemeinsam die erforderlichen Konzepte erarbeiten, den Bedarf an regulatorischen Maßnahmen erörtern, sich auf die benötigten Prozesse und Strukturen einigen sowie konkrete Kooperationsfelder identifizieren und bearbeiten.

In diesem Kontext stellt die mediale Konzentration auf Cyberunsicherheit auch ein Risiko dar: Öffentliche „Stigmatisierung" reduziert die Bereitschaft zur Zusammenarbeit und blockiert den Informationsaustausch zwischen Unternehmen, zwischen Unternehmen und Behörden sowie zwischen den Behörden. Die negativen Folgen wirken umso stärker, wenn das Vertrauen zwischen den staatlichen und den privatwirtschaftlichen Partnern erst ansatzweise vorhanden sind und wenn klare rechtliche Grundlagen fehlen, die für jeden verständlich regeln, wer welche Information unter welchen Bedingungen mit wem austauschen kann.

Der Informationsaustausch ist deshalb so zentral, weil Führungsentscheidung auf gemeinsamem Lagebewusstsein und einem Lageverständnis basieren. Daher thematisiert die CSI seit Beginn die erforderlichen Rahmenbedingungen, Spielregeln, Instrumente und Verfahren sowie den institutionellen Rahmen zur Förderung des öffentlich-privaten Informationsaustauschs im Cyber-Kontext.

Informationsaustausch

Die 2011/12 im CSI-Rahmen durchgeführte Cyberrisikoanalyse für die Energie-, Informations-/Kommunikations-, Finanz-, Transport/Logistik- und Behördensektoren Österreichs unterstrich den hohen Stellenwert des Informationsaustauschs. Zudem schuf der partnerschaftlich aufgesetzte CSI-Prozess ein Umfeld des Vertrauens, in dem staatliche und privatwirtschaftliche Akteure die Chance genutzt haben, erste Ideen zur Ausgestaltung dieses Informationsaustauschs zu entwickeln und zu präzisieren. Das Cyberlagebild spielt dabei eine zentrale Rolle.

SI-Autor Dr. Heiko Borchert (l.) ist Inhaber und Geschäftsführer des sicherheitsstrategischen Beratungsunternehmens Sandfire AG in Luzern.

Mag. Wolfgang Gattringer ist Inhaber und Geschäftsführer der Repuco Unternehmensberatung GmbH in Wien, die sich auf die Konzeption, Begleitung und Moderation komplexer Stakeholder-Prozesse spezialisiert hat. Gemeinsam unterstützen sie mit ihrem Team seit Mitte 2011 die BM.I/KSÖ-Cybersicherheits-Initiative.

Abstrakt gesprochen, bereitet das Cyberlagebild die Informationen staatlicher und privatwirtschaftlicher Akteure auf, um die cyberspezifische Lage und ihre Entwicklung zu erfassen, zu bewerten und zu verfolgen. Konkret geht es unter anderem um folgende Punkte:

- Bedrohungsbild: Zu erkennen, worin die Gefahr besteht und welche alternativen Entwicklungen möglich sind, ist entscheidend, um Vorsorge und Krisenmanagement dynamisch zu konzipieren.
- Opferbild: Wen eine Cybergefahr betrifft, ist vor allem relevant für die koordinierte Planung und Durchführung von Vorsorge-, Abwehr- und Gegenmaßnahmen, die sektorübergreifend abgestimmt werden müssen.
- Täter-/Angreiferbild: Von wem die Gefahr ausgeht, ist für die Zurechenbarkeit von Handlungen entscheidend, Grundlage der Strafverfolgung und relevant für Haftungs- sowie Versicherungsfragen.
- Wirkungsbild: Das Verständnis der Konsequenzen, die sich aus Cybergefahren ergeben, ist unerlässlich. Entscheidend ist die Simulation alternativer Gefahrenvektoren, um zu überprüfen, wie robust bestehende Schutzkonzepte/-maßnahmen sind.
- Erfahrungsbild: Antworten auf die Frage, wie in vergleichbaren vergangenen Situationen reagiert wurde, berücksichtigen idealerweise Stärken und Schwächen früherer Handlungen und dienen der Prüfung, ob diese überhaupt geeignet sind, um die erkannten Gefahren zu bewältigen.

Es fehlt die übergreifende Architektur

Staat und Wirtschaft verfügen in Österreich ansatzweise über Fähigkeiten und Mittel, um ein solches Cyberlagebild bereitzustellen. Was fehlt, sind die übergreifende Architektur und die grundlegende Konzeption, vor allem mit Blick auf die Schnittstellen zu den Partnern. Die im Entwurf vorliegende neue nationale Cybersicherheitsstrategie Österreichs geht auf diesen Aspekt ein. Darin liegt die Chance für Österreichs Unternehmen. Indem sie eigene Vorstellungen zur Cyberkooperation entwickeln, stärken sie ihre Rolle als Partner der Behörden. In den nächsten Monaten wird genau daran gearbeitet. Indem dieser Ansatz auch Aspekte der aktuellen Diskussion in Deutschland aufnimmt, bietet er die Gelegenheit, dass Staat und Wirtschaft ein Zukunftsfeld der Sicherheitsvorsorge gemeinsam und grenzüberschreitend bearbeiten – eine neue und vielversprechende Perspektive!