Von der Antizipation der Resilienz

Cyber-Resilienz lässt sich als eine technisch gestaltete und organisatorisch gesteuerte Fähigkeit verstehen, durch die Organisationen ihre kritischen Funktionen unter Bedingungen nachteiliger Cyberaktivitäten aufrechterhalten. In den Leitlinien und Standards von MITRE und NIST wird Resilienz als die Fähigkeit definiert, widrige Bedingungen, Angriffe, Belastungen oder Kompromittierungen cyberoffener Systeme zu antizipieren, ihnen standzuhalten, sich davon zu erholen und sich an sie anzupassen. Diese Definition ist nicht lediglich beschreibend, sondern zugleich analytisch und operativ. Sie spiegelt eine ingenieurwissenschaftliche und lebenszyklusorientierte Perspektive auf Resilienz wider, in der organisatorische Praxis geplant, umgesetzt, aufrechterhalten und fortlaufend verbessert werden muss. Zugleich setzt sie ein Umfeld voraus, in dem Prävention allein nicht ausreicht und Kompromittierungen erwartet, gesteuert und systematisch ausgewertet werden müssen. Aus diesem Grund steht das Konzept nicht nur mit Security-System Engineering und Kontinuitätsmanagement in Einklang, sondern auch mit Angriffsmodellen wie der Cyber Kill Chain.

Das Konzept eignet sich zudem in besonderer Weise für gegenwärtige regulatorische Anforderungen. Regelwerke wie die NIS2-Richtlinie verpflichten Organisationen dazu, verhältnismäßige technische, operative und organisatorische Maßnahmen in Bezug auf Risikomanagement, Incident Handling, Business Continuity, Sicherheit der Lieferkette und Verbesserung nach Sicherheitsvorfällen umzusetzen. Diese Anforderungen korrespondieren eng mit den vier zentralen Resilienzmerkmalen: Antizipation ermöglicht eine bedrohungsinformierte Vorbereitung; Widerstandsfähigkeit reduziert die operative Beeinträchtigung während eines Angriffs; Wiederherstellung stellt vertrauenswürdige Funktionalität erneut her; und Anpassung gewährleistet, dass gewonnene Erkenntnisse in künftige Gestaltung und Governance einfließen.

Folglich bietet Cyberresilienz eine tragfähige konzeptionelle Grundlage, um Standards, Governance-Verpflichtungen und praktische operative Maßnahmen kohärent miteinander zu verknüpfen.

Innerhalb dieses übergeordneten Rahmens verdient insbesondere das Merkmal der Antizipation besondere Aufmerksamkeit, da an diesem Punkt Resilienz bereits vor dem Eintritt einer Störung operativ wirksam wird. MITRE strukturiert Antizipation anhand dreier miteinander verknüpfter Aktivitäten: Vorhersage, Prävention und Vorbereitung.

Vorhersage (Prediction) bezeichnet die strukturierte Einschätzung, welche Bedrohungen, Abhängigkeiten, Schwachstellen und Angriffsmöglichkeiten für die Organisation besonders relevant sind. Sie beruht auf aktuellem Wissen über Vermögenswerte und Systeme, auf Threat Intelligence, Angriffs-/Exposure-Analysen sowie szenariobasierten Risikobewertungen.

Prävention (Prevention) betrifft die Verringerung der Möglichkeiten zu einer Kompromittierung oder zu nicht hinnehmbaren Auswirkungen führen können. Erforderlich sind hierfür unter anderem die Härtung von Identitäten, das Least-Privilege-Prinzip, Segmentierung, sichere Konfigurationen, Cyber-Hygiene, Schwachstellenmanagement, Absicherung der Lieferkette sowie Secure-by-Design-Prinzipien.
Vorbereitung (Preparation) bezeichnet den Aufbau der Fähigkeit, wirksam zu handeln, wenn präventive Kontrollen umgangen werden oder sich die Betriebsbedingungen verschlechtern. Dazu gehören insbesondere die Planung des Incident Response, Kontinuitätsregelungen, Krisenkommunikation, die Priorisierung der Wiederherstellung, geschützte Backups sowie die Durchführung realistischer technischer und managementbezogener Übungen.

Um Antizipation zu operationalisieren, müssen Organisationen Governance, Intelligence, Architektur, Betrieb und Assurance integrieren. Durch Governance sorgen verantwortliche Entscheidungsträger dafür, Eskalationsschwellen und Risikotoleranzen eindeutig festlegen. Operative Teams steuern aktuelle Informationen über Vermögenswerte, Abhängigkeiten und geschäftskritische Dienste bei, damit Bedrohungs- und Expositionsdaten in zweckmäßige Maßnahmen übersetzt werden können. Die Sicherheitsarchitektur umfasst bedrohungsinformierte Reviews, Resilienz-Strukturen und kompensierende Kontrollen, um kritische (Business-)Assets zu schützen. Assurance-Aktivitäten, darunter Audits, Adversary Simulation, Wiederherstellungsübungen und Nachanalysen von Sicherheitsvorfällen, sind erforderlich, um festzustellen, ob Pläne und Kontrollen in der Praxis und nicht nur auf dem Papier wirksam sind. In dieser Hinsicht bieten Standards und Leitlinien wie NIST SP 800-160 Vol. 2 Rev. 1, ISO/IEC 27001, ISO 22301 sowie die NIS2-bezogenen Leitlinien der ENISA einen belastbaren Referenzrahmen für die Umsetzung.

Als nützliche Praxis ist Antizipation mit dem Konzept der Cyber Courses of Action (CCoA) zu verknüpfen. Ein CCoA ist eine strukturierte Abfolge von Entscheidungen und Aktivitäten, die darauf ausgerichtet ist, vor, während oder nach einer Cyberbeeinträchtigung eine bestimmte Wirkung zu erzielen. Chronologisch beginnt ein solcher Ansatz mit dem Situationsverständnis, gefolgt von der Entwicklung und Bewertung von Handlungsoptionen, der Autorisierung einer bevorzugten Option, ihrer Ausführung beim Eintritt definierter Auslösebedingungen sowie der anschließenden Anpassung auf Grundlage gewonnener Erkenntnisse. Dieses Konzept ist bedeutsam, weil es einen prozessorientierten Mechanismus bereitstellt, durch den sich Vorhersage, Prävention und Vorbereitung in konkretes organisatorisches Handeln übersetzen lassen. Anstatt Antizipation auf der Ebene konzeptioneller Analyse zu belassen, ermöglichen CCoA, im Voraus festzulegen, was unter welchen Bedingungen von wem und mit welcher beabsichtigten operativen Wirkung zu tun ist.

Zusammenfassend sollte Cyberresilienz nicht als bloße allgemeine Zielvorstellung, sondern als disziplinierte ingenieurwissenschaftliche Fähigkeit verstanden werden. Insbesondere das Merkmal der Antizipation ist von zentraler Bedeutung und muss durch Maßnahmen, Handlungen und Verfahren in den Bereichen Vorhersage, Prävention und Vorbereitung operationalisiert werden. Ein hilfreiches praktisches Instrument hierfür stellen CCoA dar, da sie organisatorische, technische und prozessuale Aspekte bündeln, strukturieren und insbesondere Schnittstellen adressieren.

<Ein Beitrag von Security-System Engineering>

Security-System Engineering; Security-System Buch