Was folgt aus "Assume-Breach" im Cyber Security Management??

Fragestellung und Ausgangspunkt

Der Assume-Breach-Ansatz verschiebt den Schwerpunkt der Cyber-Sicherheitsanalyse von der ausschließlichen Verhinderung eines Einbruchs auf die kontrollierte Beherrschung seiner Folgen. Ausgangspunkt ist die Annahme, dass eine Komponente, ein Asset, ein Benutzerkonto oder ein technischer Dienst bereits kompromittiert ist. Die zentrale Fragestellung lautet damit, welche Wirkung eine angenommene Kompromittierung auf technische Systeme, Datenbestände, Schnittstellen, Segmentierungsgrenzen und Geschäftsprozesse entfaltet.
Diese Perspektive adressiert eine notwendige Detaillierung klassischer Schutzkonzepte: Ein Asset kann isoliert betrachtet eine mittlere Kritikalität besitzen, im Verbund mit Identitäten, Datenflüssen, APIs, Backend-Systemen und Prozessabhängigkeiten jedoch einen direkten Zugang zu geschäftskritischen Funktionen eröffnen. Die Kritikalität eines Assets ergibt sich daher nicht allein aus seinem Eigenwert, sondern aus seiner Position im Systemverbund und aus den erreichbaren Folgewirkungen.

Kompromittierungs-Ausbreitungs-Analyse

Eine Kompromittierungs-Ausbreitungs-Analyse könnte eine systematische Ermittlung der technischen und geschäftlichen Auswirkungen einer angenommenen Kompromittierung unterstützen. Mittels Analyse kann transparenter werden, welche Funktionen ein (kompromittiertes) Asset für das Gesamtsystem erfüllt, welche Daten und Informationen erreichbar sind, welche Schnittstellen genutzt werden können und welche Segmentierungsgrenzen überwunden werden können. Ergänzend sind Identitäten, Berechtigungen, Vertrauensbeziehungen, ausführbare Aktionen, Detektionsmöglichkeiten und Reaktionspunkte zu erfassen.
Das Ergebnis wäre letztlich ein Wirkungsmodell auf die Geschäftsprozesse. Es beschreibt mittels Ausbreitungspfade erreichbare Zielobjekten wie Datenbanken, Administrationsschnittstellen, Service-Accounts, Cloud-Ressourcen, ERP-Systemen, Zahlungsfunktionen oder produktionskritischen Diensten. Als kritische Pfade könnten solche Pfade identifiziert werden, die mit wenigen Übergängen hohe Schadenswirkungen, geringe Detektionswahrscheinlichkeit oder nachhaltige Persistenz ermöglichen.

Methodischer Kern

Methodisch ist eine Modellierung des betrachteten Gesamtsystems als gerichteter Graph möglich. Knoten repräsentieren Assets, Identitäten, Datenobjekte, Schnittstellen, Geschäftsprozessschritte und Segmentierungszonen. Kanten beschreiben technische Erreichbarkeit, Berechtigungsverhältnisse, Datenflüsse, API-Beziehungen, Trust-Beziehungen oder Prozessabhängigkeiten. Die angenommene Kompromittierung bildet den Startknoten. Von diesem Startknoten aus werden alle technisch und organisatorisch plausiblen Ausbreitungsmöglichkeiten rekonstruiert.
Die Analyse umfasst mindestens sechs Bewertungsebenen: Erstens die funktionale Rolle des Assets im Gesamtsystem. Zweitens die erreichbaren Daten einschließlich Schutzbedarf, Vertraulichkeit, Integrität und Verfügbarkeit. Drittens die erreichbaren Schnittstellen und deren Berechtigungsmodell. Viertens die überwindbaren Grenzen zwischen Netzsegmenten, Datenräumen, Systemdomänen und Verantwortungsbereichen. Fünftens die möglichen Angreiferaktionen wie Lesen, Verändern, Löschen, Ausführen, Weiterleiten oder Tarnen. Sechstens die geschäftliche Wirkung auf Prozessverfügbarkeit, Ergebnisqualität, Compliance, Kundenbeziehung, Umsatz und Reputation.

Die Ableitung der Kritikalität erfolgt aus der Kombination von Reichweite, Wirkung und Beherrschbarkeit. Hohe Kritikalität liegt vor, wenn ein Asset sensible Daten erschließt, privilegierte Identitäten nutzt, Segmentierungsgrenzen überwindet, geschäftskritische Transaktionen beeinflusst oder Persistenz in der Systemlandschaft ermöglicht. Die Methode ergänzt damit klassische Schwachstellenbewertungen, weil nicht der einzelne Fehler, sondern die Wirkungskette bewertet wird.

Mittels einer Visualisierung besteht die Möglichkeit einer transparenten Darstellung. Geeignet wären gerichtete Graphen, Flow-Charts und mehrschichtige Architekturmodelle. Eine zweckmäßige Darstellung unterscheidet technische Assets, Identitäten, Datenobjekte, Schnittstellen, Segmentierungsgrenzen und Geschäftsprozessschritte. Kritische Pfade können farblich hervorgehoben und mit Kriterien wie Angriffsdistanz, Datenkritikalität, Berechtigungsniveau, Geschäftsfolgen und Detektionsgrad annotiert werden.

Einordnung gegenüber der Risikoanalyse

Die Kompromittierungs-Ausbreitungs-Analyse ersetzt eine Risikoanalyse nicht vollständig. Sie präzisiert jedoch deren technische und prozessuale Grundlage. Während die Risikoanalyse Eintrittswahrscheinlichkeit, Schadenshöhe, Risikoakzeptanz und Maßnahmenwirtschaftlichkeit bewertet, liefert die Ausbreitungsanalyse eine belastbare Sicht auf Wirkungsketten nach einer angenommenen Kompromittierung. Sie macht sichtbar, welche Assets aufgrund ihrer Position im Systemverbund, ihrer Berechtigungen und ihrer erreichbaren Ziele besonders kritisch sind.

Der wesentliche Beitrag liegt in der Maßnahmenpriorisierung. Sicherheitsmaßnahmen werden nicht allein nach Schwachstellenanzahl oder abstraktem Schutzbedarf festgelegt, sondern entlang konkreter kritischer Pfade. Dazu gehören Segmentierung, Least Privilege, starke Identitätskontrollen, API-Härtung, Secrets-Management, Monitoring, Detektion, Response-Fähigkeit und technische Validierung.

Fazit

Die Kompromittierungs-Ausbreitungs-Analyse wäre ein geeigneter methodischer Baustein einer resilienten Cyber-Sicherheitsarchitektur. Sie verbindet Assume-Breach-Denken, Angriffspfadmodellierung, Systemarchitekturanalyse und Business-Impact-Bewertung. Ihr Nutzen liegt in der transparenten Ableitung von Asset-Kritikalität, der Identifikation kritischer Pfade und der gezielten Platzierung wirksamer Sicherheitsmaßnahmen.
Welche Tools und Methoden wären geeignet hier praktikable Lösungsansätze zu liefern?

<Ein Beitrag von Security-System Engineering>

Security-System Engineering; Security-System Buch