(Kein) Vertrauen

Das Schlagwort „Zero Trust" ist in aller Munde. Als eine Art „Heilsbringer" wird es im Zusammenhang mit den Vorzügen einer ganzen Reihe von IT-Produkten erwähnt, der die Herausforderungen eines modernen IT-Betriebs – allen voran die im Bereich der Informationssicherheit – zu lösen verspricht.

Doch die Grundidee hinter Zero Trust ist alles andere als neu. Bereits Anfang der 2000er Jahre wurden die ersten Ideen dazu vom Jericho Forum, dem „Vorgänger" der Open Group, präsentiert. Der Begriff Zero Trust selbst datiert ebenfalls bereits auf das Jahr 2009 und damit fast 15 Jahre zurück. Das erklärt, warum sich unter dem Sammelbegriff Zero Trust auch heute noch viele technologische Ansätze verbergen, die alles andere als neu sind.

Während das Konzept laufend erweitert wurde, blieb der Grundgedanke stets erhalten: so wenig Vertrauen wie notwendig, so viel Kontrolle wie möglich. Dies umzusetzen, stellt Unternehmen allerdings vor eine enorme Herausforderung. Denn aktuell basieren viele „Prozesse" auf Vertrauen, insbesondere etwa im Bereich des Outsourcings, bei dem häufig schlichtweg keine Kompetenzen beim Auftraggeber vorhanden sind, den Dienstleister angemessen zu kontrollieren.

Hier versucht Zero Trust vor allem durch das Prinzip eines zeitlich eingeschränkten „*least privilege access*" mögliche Schäden zu begrenzen. Dies erfordert aber zum einen eine grundlegende Umstellung der IT-Prozesse und geht zum anderen vor allem auch mit einer umfangreichen Kontrolle eines jeden einzelnen Datenzugriffs einher – was wiederum neue Problemstellungen aufwirft.

Die einzelnen Beiträge im Überblick

Die insgesamt acht Schwerpunktbeiträge widmen sich dem Themengebiet aus unterschiedlichen Blickwinkeln und diskutieren, ob und wie Zero Trust wirksam und zielführend umsetzbar ist:

- Der Beitrag *„Zero Trust für eine robuste Cyberresilienz"* von Paul Bauer beleuchtet die Relevanz und Notwendigkeit von Zero Trust auf dem Weg zu einer verbesserten Cybersicherheit.
- Steffen Ullrich stellt im Beitrag *„Zero Trust im Gesundheitswesen"* das Thema Zero Trust im Kontext der aktuellen Entwicklung im Bereich der Digitalisierung im Gesundheitswesen dar.
- Silvia Knittl hinterfragt im Beitrag *„Zero Trust: Die letzte Bastion für die IT-Sicherheit deutscher Behörden"*, ob und ggf. wie Zero Trust Kommunen vor typischen Cyberangriffe schützen kann.
- Marit Hansen und Thomas Probst beleuchten im Beitrag *„Souveräne Sicherheit, Zero Trust und das Datenschutzrecht"* das datenschutzrechtliche Spannungsfeld der umfassenden Kontrollmöglichkeiten im Rahmen von Zero Trust.
- Im Beitrag *„Zero Trust"* zum Thema *„Technische Möglichkeiten und Grenzen"* zeigt Stefan Strobel die technischen Möglichkeiten und Herausforderungen beim Einsatz von Zero Trust auf.
- David Fuhr und Dror-John Röcher thematisieren im Beitrag *„Zero-Trust-Architekturen: Herausforderung für die Kryptographie?"* die möglichen Probleme, die sich beim Einsatz von Zero Trust durch die Nutzung von kryptographischen Mechanismen ergeben können.
- Im Beitrag *„Confidential Computing: Zero Trust in der Public Cloud"* diskutiert Felix Schuster einen potentiellen Lösungsansatz für Vertrauen in typischerweise nicht vertrauenswürdigen Cloud-Umgebungen.
- Abschließend widmet sich Thomas Milde im Beitrag *„Macht Zero Trust wirklich sicher? Und falls ja: Zu welchem Preis?"* der Frage, ob und ggf. welche betriebswirtschaftlichen Auswirkungen die Einführung und Nutzung von Zero Trust mit sich bringen.

Ergänzt wird dieser Schwerpunkt diesmal durch den Beitrag *„Föderale Cybersicherheitsarchitektur und Informationssicherheitsmanagement im Kontext der NIS-2-Richtlinie"* von Thomas Rehbohm und Frank Moses.

Nun hoffe ich, dass Ihnen die Beiträge viele Anregungen für Ihre eigenen Projekte geben, und wünsche Ihnen als Gastherausgeber zusammen mit dem gesamten Herausgeberteam eine spannende Lektüre.

Christoph Wegener