Digital auf wackeligen Beinen

Die ATHENE-Studie zur IT-Sicherheit der Länder

(BS/Haya Schulmann/Michael Waidner) Digitalisierung ist Voraussetzung für eine moderne Verwaltung, Innovationsfähigkeit und digitale Souveränität. Seit über einem Jahrzehnt gibt es Strategien und teure Investitionsprogramme. Das Ziel: besserer Service und effizientere Prozesse durch mehr digitale Dienste.

Die Länder investieren in Online-Dienste, Plattformen und Cloud-Lösungen. Das aktuelle Lagebild des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE zeigt, dass die aus dem Internet erreichbare Länder-IT zwischen 2023 und 2025 um 53 Prozent gewachsen ist. Die Zahl der Services stieg auf über 115.000, verteilt auf rund 25.000 Internet-Domains. Cloud-Nutzung hat sich verfünffacht, externe Hosting-Lösungen wuchsen um 88 Prozent.

Doch die IT wächst schneller als die Fähigkeit, sie zu kontrollieren. Neue Systeme ersetzen alte nicht, sondern kommen hinzu. Das Ergebnis ist Wildwuchs statt Modernisierung – die IT wird so fehleranfälliger und verwundbarer.

Das offenbart ein fundamentales Problem: Digitalisierungsinitiativen setzen stillschweigend voraus, dass die bestehende IT-Infrastruktur tragfähig ist. Das ist sie nicht. Neues wird auf einem sanierungsbedürftigen Fundament gebaut. Veraltete Systeme, Wildwuchs und fehlende Steuerungsfähigkeiten untergraben den Fortschritt.

Was ist ein Lagebild – und was nicht?

Lageberichte zur IT-Sicherheit wie der des Bundesamts für Sicherheit in der Informationstechnik (BSI) analysieren nicht die strukturellen Ursachen und Governance-Probleme der IT-Landschaften, sondern beschreiben primär Statistiken zu Bedrohungen und Vorfällen. Ein Lagebild sollte jedoch nicht die Fähigkeiten der Angreifer, sondern die strukturelle Verwundbarkeit der IT analysieren: Wie groß und fragmentiert sind die IT-Landschaften? Welche Teile laufen in eigenen Netzen, bei externen Dienstleistern oder in der Cloud? Sind Dienste aktuell oder „end of life“, wie alt sind Schwachstellen und können sie überhaupt behoben werden?

So wird sichtbar, wo Digitalisierung professionell betrieben wird, wo Unterschiede in Governance und Sicherheitsreife bestehen und wo sich Risiken aufbauen – durch Wildwuchs, fehlende Zuständigkeiten, Lieferketten-Abhängigkeiten oder mangelhaftes Lifecycle-Management.

Die Länder-IT ist historisch gewachsen, fragmentiert und alt

Das ATHENE-Lagebild der Länder-IT untersuchte die externe Angriffsfläche aller 16 Bundesländer zwischen 2023 und 2025. Die Ergebnisse belegen strukturelle Defizite, die mit Compliance-Maßnahmen allein nicht zu beheben sind.

Erstens: Die Länder-IT wächst vorrangig durch Addition, nicht durch Modernisierung. Das Ergebnis ist Parallelbetrieb alter und neuer IT – mit steigender Fragmentierung und wachsender Angriffsfläche.

Zweitens: End-of-Life-Systeme dominieren die Sicherheitsprobleme. Über 75 Prozent der kritischen Schwachstellen sind älter als ein Jahr, einige sogar älter als Zehn Jahre. Ein großer Teil der Angriffsfläche ist nicht mehr patchbar – unabhängig von der Qualität der Governance-Prozesse. Wo Hersteller den Support eingestellt haben und Fachverfahren an veraltete Laufzeitumgebungen gebunden sind, läuft die Empfehlung „zeitnah patchen" ins Leere.

Drittens: Kein Bundesland hat die Voraussetzungen geschaffen, seine gesamte Behörden-IT zentral zu steuern. Landes-CERTs, SOCs oder zentrale IT-Dienstleister dürfen nachgelagerte Behörden oft nicht verpflichten. Es fehlen vollständige Asset-Register, verbindliche technische Baselines und Dekommissionierungsvorgaben sowie Lagebilder wie das von ATHENE.

Compliance ist ein Lenkrad ohne Motor

Das ATHENE-Lagebild zeigt nachdrücklich, dass Digitalisierung nicht nur neue digitale Dienste braucht, sondern auch die Professionalisierung der vorhandenen IT-Infrastrukturen. Typische Empfehlungen wie „Patchen“ und „höhere ISMS-Reifegrade“ setzen voraus, dass die zugrunde liegende IT patchbar, inventarisiert und steuerbar ist. Genau das ist sie aber nicht.

Compliance und Zertifizierung verwalten existierende IT-Sicherheit, aber sie können sie nicht schaffen. Audits prüfen im Allgemeinen punktuell Dokumentation und Prozessnachweise; sie messen aber nicht, ob die Angriffsfläche sinkt oder Legacy-Systeme abgebaut werden. Die ATHENE-Daten zeigen: In unseren Daten gibt es keinen signifikanten Unterschied in Angriffsfläche oder IT-Hygiene zwischen zertifizierten und nicht zertifizierten IT-Infrastrukturen.

Konsequenzen

Die eigentlichen Hindernisse für Digitalisierung und Cyber-Sicherheit sind strukturell: Legacy-Systeme, die niemand abschaltet, Wildwuchs, den niemand überblickt, und eine Infrastruktur, die schneller wächst als sie konsolidiert wird.

Digitalisierungs- und Cyber-Sicherheitsstrategien bauen mangels Lagebild auf falschen Annahmen auf. Ohne Dekommissionierungsvorgaben wächst die Angriffsfläche mit jedem neuen System. Geld fließt in Compliance-Programme, während technische Schulden akkumulieren.

Digitalisierung setzt eine moderne, konsolidierte und professionell betriebene IT-Infrastruktur voraus. Ohne eine strukturelle Erneuerung der IT-Basis erhöhen jedes neue Bürgerportal und jeder neue digitale Dienst potenziell das Sicherheitsrisiko. Solange Länder keinen Überblick über ihre eigene IT haben, IT-Architektur nicht systematisch planen und Legacy-Systeme nicht abbauen, werden auch die besten Strategien wirkungslos bleiben.

Den vollständigen ATHENE-Lagebericht zur Länder IT finden Sie unter: https://scienceshield.athene-center.de/studien/lagebild-bericht-bundeslaender

Haya Schulmann ist Professorin für Cyber-Sicherheit am Institut für Informatik der Goethe-Universität Frankfurt am Main und Mitglied im Direktorium des „Nationalen Forschungszentrums für angewandte Cybersicherheit“ ATHENE. Foto: BS/ATHENE

Michael Waidner ist Professor für Sicherheit in der Informationstechnologie im Fachbereich Informatik der TU Darmstadt, Leiter des Fraunhofer-Instituts für sichere Informationstechnologie SIT und CEO von ATHENE. Foto: BS/ATHENE

Wenn Berichte Pflicht werden

Zwischen Risikoprofil und Meldeplattform

(BS/Frederik Steinhage) Seit Januar steht die BSI-Plattform für die Umsetzung der NIS-2-Regeln offiziell zur Verfügung und markiert einen wichtigen Schritt bei der Digitalisierung und Zentralisierung für Cybersicherheits-Pflichten.

Mit dem neuen Portal zentralisiert das BSI erstmals Registrierung und Vorfallmeldungen nach NIS-2 an einer Stelle.

Foto: BS/ Maxim, stock.adobe.com

Mit dem Inkrafttreten des nationalen NIS-2-Umsetzungsgesetzes gelten für rund 29.000 bis 30.000 Unternehmen, Behörden und andere Einrichtungen deutlich erweiterte Anforderungen an die IT-Sicherheit, Registrierung und Vorfallmeldung, die über die bisherigen Vorgaben der ersten NIS-Richtlinie hinausgehen.

Betroffene Organisationen müssen sich künftig als sogenannte NIS-2-Einrichtungen beim Bundesamt für Sicherheit in der Informationstechnik registrieren und erhebliche IT-Sicherheitsvorfälle fristgerecht melden. Ziel ist es, die gesetzlichen Pflichten zentral zu bündeln.

Die Registrierung erfolgt in einem zweistufigen Verfahren. Voraussetzung ist zunächst die Authentifizierung über den Dienst „Mein Unternehmenskonto“ mit ELSTER-Organisationszertifikat. Anschließend kann die Anmeldung auf der BSI-Plattform abgeschlossen werden. Im Portal werden neben Basisinformationen auch sektorbezogene Angaben abgefragt, um das jeweilige Risikoprofil einordnen zu können. Die NIS-2-Vorgaben sehen hierfür feste Fristen vor: Spätestens drei Monate nach Feststellung der Betroffenheit müssen Einrichtungen registriert sein, andernfalls drohen aufsichtsrechtliche Konsequenzen.

Melden wird Pflicht

Zudem dient die Plattform als zentrale Meldeplattform für Sicherheitsvorfälle. Erhebliche Störungen sind unverzüglich anzuzeigen und durch weitere Meldungen zu ergänzen. Das BSI stellt hierzu unterstützende Informationen bereit, um die Umsetzung der gesetzlichen Vorgaben zu erleichtern. Ergänzend soll die Plattform dazu beitragen, Meldewege zu standardisieren und die Zusammenarbeit zwischen betroffenen Einrichtungen und Aufsichtsbehörden zu vereinfachen. Langfristig ist vorgesehen, Prozesse weiter zu automatisieren und die Bearbeitung von Sicherheitsvorfällen effizienter zu gestalten.