Vom Lagebericht...

...zur Handlungsgrundlage

(BS/Haya Schulmann/Michael Waidner) Berichte zur IT-Sicherheits-Lage wie der des Bundesamt für Sicherheit in der Informationstechnik (BSI) schauen auf die Angreifenden, aber für wirksame Sicherheitsstrategien braucht es den Blick auf uns selbst. Die zentrale Frage der IT-Sicherheit ist nicht, was die Angreifenden können, sondern wie gut wir geschützt sind.

Verantwortungsvolle Digitalisierung setzt sichere IT-Infrastrukturen voraus. Dank Künstlicher Intelligenz (KI) schreitet die Digitalisierung so schnell voran wie nie – und je schneller sie voranschreitet, desto kritischer wird die Fähigkeit unserer IT, Cyber-Angriffe abzuwehren. Entscheiderinnen und Entscheider in Politik, Verwaltung und Wirtschaft brauchen dafür eine faktenbasierte Antwort auf die einfache Frage: Sind wir ausreichend vorbereitet oder müssen wir mehr tun?

Aktuelle Lagebilder helfen wenig

Lageberichte zur IT-Sicherheit sollen helfen, diese Frage zu beantworten – tun dies aber nur sehr unzureichend. Schaut man etwa in den Bericht des BSI "Die Lage der IT-Sicherheit in Deutschland 2025", so erfährt man viel dazu, welche Schwachstellen dem BSI gemeldet wurden und wie und von wem unsere IT angegriffen wird. Unbeantwortet bleibt aber, wie gut unsere IT auf diese Schwachstellen und Angriffe vorbereitet war und wie resilient wir gegenüber künftigen Angriffen sind. Ähnliches gilt für andere bekannte Lageberichte, etwa die "ENISA Threat Landscape" oder den "Microsoft Digital Defense Report".

Wer seine Sicherheitsstrategie nur an der aktuellen Bedrohungslage ausrichtet, kommt nie "vor die Lage", er wird immer wieder aufs Neue überrascht. Beispiele für solche Überraschungen gibt es mehr als genug: Isolierte industrielle Kontrollsysteme galten als für Cyber-Angriffe unerreichbar – bis Stuxnet 2009 die iranischen Urananreicherungsanlagen traf. Vom Hersteller signierte Updates galten als sicher – bis Sunburst 2020 genau diesen Mechanismus für einen Angriff gegen die Kunden von Solarwinds missbrauchte. In der Praxis hatte niemand mit diesen Angriffen gerechnet, kein Lagebericht, keine Threat Landscape hatte vor ihnen gewarnt. Für eine solide und objektive Antwort auf unsere obige Frage braucht es also deutlich mehr als nur eine Auflistung aktueller Gefährdungen. Es braucht eine Analyse, wie gut unsere IT gegen diese geschützt ist, und wie gut sie darauf vorbereitet ist, auf künftige Gefahren schnell und professionell zu reagieren. Wir brauchen ein Resilienz-Lagebild.

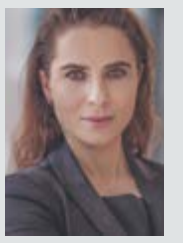
Resilienz-Lagebilder sind zwar dringend notwendig, aber bislang mehr als rar – es gibt sie praktisch nicht. Der Grund ist, dass sie technisch komplex und damit deutlich schwerer zu erheben sind als die üblichen Lageberichte. Für eine Threat Landscape kann man auf bekannte Quellen zurückgreifen – CVE-Datenbanken, CERT-Berichte, Datensammlungen von Firmen wie Mandiant und CrowdStrike. Das geht schnell und einfach. Für ein Resilienz-Lagebild etwa eines Landes oder eines Sektors muss man die notwendigen Daten selbst erheben und dafür eine große Anzahl an Organisation einzeln betrachten, und das ist aufwändig und technisch komplizierter. Repräsentative Befragungen der Organisationen könnten einen ersten Eindruck vermitteln, haben aber den Schönheitsfehler, dass viele Organisationen ihre eigene Resilienz überhaupt nicht objektiv einschätzen können. Studien von ATHENE belegen, dass die meisten Organisationen keinen wirklichen Überblick über ihre IT haben, überall gibt es vergessene Server, ungewartete Systeme, seit Jahren offene Schwachstellen.

Eine objektivere Methode besteht darin, für die Resilienz relevante IT-Indikatoren der ausgewählten Organisationen direkt und von außen zu erfassen. Diesen Weg geht ATHENE mit seinen Lagebildern zur IT-Sicherheit. Datengrundlage für ATHENE sind Informationen zur Struktur und Sicherheit der aus dem Internet erreichbaren IT-Infrastrukturen sowie Informationen zu Datenlecks und kompromittierten Anmeldedaten – gewonnen aus den Datenbanken von Internet-Registraren, öffentlichen Scans und vergleichbaren Quellen. Zwei typische Indikatoren sind die Anzahl und das Alter der offenen kritischen Schwachstellen. Die Anzahl ist ein Indiz für die aktuelle Verwundbarkeit, das Alter ein Indiz für die Professionalität des technischen Sicherheitsmanagements, also die Fähigkeit, auf künftige Gefahren schnell reagieren zu können. Von außen erfassbar sind zwar nur die Schwachstellen in den von außen erreichbaren IT-Systemen, aber erstens sind es genau diese Schwachstellen, die Angreifenden ein Eindringen erlauben, und zweitens unterliegen typischerweise alle IT-Systeme einer Organisation einem gemeinsamen IT-Management, so dass Probleme im von außen sichtbaren Teil sich typischerweise auch im inneren Teil wiederfinden. Wer seine externe Angriffsoberfläche nicht im Griff hat, der hat im Allgemeinen auch seine innere nicht im Griff. Weitere Indikatoren sind zum Beispiel Systeme, die jenseits ihres End-of-Life betrieben werden oder die Fragmentierung zwischen Rechenzentren, Fachverfahren und Cloud-Anbietern.

Eine ernüchternde Bilanz

Das Bild, das die ATHENE-Lagebilder zeichnen, ist über alle Sektoren ernüchternd: Die Lage ist schlecht und sie verbessert sich nicht. Die IT wächst, die Digitalisierung kommt voran – aber neue Dienste ersetzen nicht die alten, sondern kommen einfach hinzu. Alte Strukturen laufen unverändert weiter, die Fragmentierung steigt, der Wildwuchs nimmt zu. Schwachstellen bleiben jahrelang ungepatcht, Systeme laufen nach ihrem End-of-Life ohne Wartung weiter. Kaum eine Organisation scheint die volle Übersicht und Kontrolle über ihre IT zu haben. Kurz: Deutschlands IT wird immer größer – Digitalisierung kommt voran – aber sie wird immer weniger resilient und immer unsicherer, weil neue IT und Dienste auf historisch gewachsene und marode IT Infrastruktur aufgebaut werden.

Die Antwort auf die Eingangsfrage ist damit klar: Nein, wir sind nicht vorbereitet. Was aber folgt daraus? Erstens, Modernisierung ist der Schlüssel zur Verbesserung unserer IT-Sicherheit. Neue digitale Dienste auf existierenden Plattformen zu betreiben, ist wie ein Neubau auf morschem Fundament. Ebenso wenig hilft es, neue Plattformen aufzubauen, die alten aber unangetastet weiterlaufen zu lassen. Modernisierung ohne Konsolidierung und Außerbetriebnahme führt zu mehr Betriebsproblemen und einer größeren Angriffsfläche. Zweitens, wir brauchen ein Resilienz-Lagebild als Grundlage von Investitionsentscheidungen. Threat Landscapes alleine helfen nicht weiter, denn die Gefährdungslage können wir nicht kontrollieren, wohl aber den Zustand unserer eigenen IT-Infrastruktur.



Haya Schulmann ist ist Professorin für Cybersicherheit 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 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/privat