Junge Welt / 27.08.2026 / Inland / Seite 4

Die üblichen Verdächtigen

Geheimdienst und Lobbyverband Bitkom stellen Umfrage unter Unternehmen zu IT-Angriffen vor. Selen und Wintergerst betonen enge Kooperation.

Von Marc Bebenroth

Wohin anders als nach Osten können die Spuren schon weisen, wenn deutsche Geheimdienste und Kapitalisten Hand in Hand die Schuldigen für IT-Sicherheitsvorfälle suchen? Am Mittwoch hat der Präsident des Digitalbranchenverbands Bitkom, Ralf Wintergerst, an der Seite seines Amtskollegen Sinan Selen vom Bundesamt für Verfassungsschutz (BfV) in Berlin seinen sogenannten Wirtschaftsschutzbericht 2026 vorgestellt. Und wer hätte es gedacht: Neben der organisierten Kriminalität werden deutsche Firmen offenbar am häufigsten von Tätern aus dem Territorium der drei erklärten Hauptfeinde der NATO digital ausspioniert oder gar sabotiert: China, Russland und Iran. Als ob es noch eines Vorwandes bedurft hätte, um die von der Bundesregierung bereits beschlossene folgenschwere Ermächtigung der Geheimdienste als dringend geboten darstellen zu können.

37 Prozent der laut Bitkom 671 befragten Unternehmen, die in den vergangenen zwölf Monaten Fälle von »Datendiebstahl, Industriespionage oder Sabotage« verzeichnet hatten, vermuten dahinter demnach »ausländische Nachrichtendienste«. Ein Jahr zuvor habe der Anteil 28 Prozent betragen. 52 Prozent der befragten Unternehmen gaben an, von IT-Angriffen aus China betroffen gewesen zu sein – dem Bitkom zufolge eine Steigerung um sechs Prozentpunkte. 49 Prozent der Firmen nannten Russland, demnach ein Plus von drei Prozentpunkten. Nur neun Prozent nannten Iran als Ursprungsland, dies seien aber fünf Prozentpunkte mehr als im Jahr zuvor. Drittgrößte Herkunftsregion sei »Osteuropa (nicht EU und RU)«.

Von einem Journalisten auf den Anteil von ebenfalls 27 Prozent angesprochen, der den USA zugeschrieben wird, erklärte Wintergerst ausweichend, dass die BRD durchaus ein »attraktiver Forschungs- und Technologiestandort« sowie »die drittgrößte Volkswirtschaft« sei. »Und daher kommt natürlich das Interesse.« Weitere 27 Prozent jener Vorfälle konnten laut Bitkom-Umfrage keiner bestimmten Weltregion zugeordnet werden. Insgesamt habe der Verband 1.003 Unternehmen »der deutschen Wirtschaft« mit mindestens zehn Beschäftigten befragt. Der Bitkom vertritt gegenwärtig nach eigenen Angaben mehr als 2.200 Firmen der sogenannten Digitalwirtschaft.

Doch wie konnten die befragten Unternehmen überhaupt sagen, wer ihre IT-Systeme angegriffen hatte? Schließlich ermöglichen beispielsweise VPN-Anbieter, den eigenen Standort zu verschleiern. Angreifer könnten zudem fremde Geräte in anderen Ländern kapern und für ihre Operationen nutzen.

Eine konkrete Antwort auf die Nachfrage von *junge Welt* blieb Wintergerst schuldig. Dies könne er »nicht genau sagen«, weil diese Frage den Unternehmen gar nicht »ganz genau« gestellt worden sei. Aus den veröffentlichten Umfrageergebnissen geht lediglich hervor, dass 68 Prozent der 667 befragten Firmen, die zuletzt von »Datendiebstahl«, Industriespionage oder Sabotage betroffen gewesen seien »und Erkenntnisse über Herkunft oder Täterkreis« hätten, auf die Analyse von Logdateien verweisen. Zur Hälfte gaben die Firmen an, durch »Informationen von Behörden« auf die entsprechende Spur gebracht worden zu sein. Geringer ist der Anteil derer, die auf interne oder externe Untersuchungen (37 bzw. 21 Prozent), spezifische Muster der Angriffstechnik (20 Prozent), den Austausch mit anderen Firmen (16 Prozent) oder gar »Hinweise/Geständnisse von Beteiligten« (sechs Prozent) verwiesen.

Hinzu kommt, dass Bitkom selbst davon spricht, 29 Prozent der 1.003 befragten Firmen seien einem der genannten IT-Delikte »vermutlich« zum Opfer gefallen. Wintergerst: »Es gibt eigentlich nur noch zwei Arten von Unternehmen: die, die gehackt worden sind, und die, die es noch nicht wissen.« Dabei seien die häufigsten Schadensursachen bei IT-Sicherheitsvorfällen »keine besonders ausgefeilten oder exotischen Angriffe, sondern blinde Flecken im eigenen System«, teilt Bitkom zur Erhebung mit. Diese gelte es, mit Hilfe modernster KI-Systeme aufzudecken, entgegnete Wintergerst auf die Frage von *jW*, wer aus seiner Sicht für Schäden durch das Ausnutzen von Sicherheitslücken in Software haften solle.

Auch Selen wollte von einer etwaigen Herstellerhaftung nichts wissen. Ebenso wenig sei der Einsatz von Open-Source-Software die Lösung. Er betonte statt dessen wiederholt, wie eng seine »Abwehrbehörde« mit der Privatwirtschaft kooperiere. Er wies auf Nachfrage zudem den Verdacht zurück, sein Amt wolle unveröffentlichtes Wissen über Sicherheitslücken in Software für eigene Zwecke geheimhalten. »Der Auftrag ist ein eindeutiger, und das ist der Schutz der Wirtschaft«, sagte Selen.

https://www.jungewelt.de/artikel/528654.bitkom-bericht-zur-it-sicherheit-die-üblichen-verdächtigen.html