Bundesamt für Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 01/2025 | 11. Juli 2025

Betreff | Konflikt im Nahen Osten

Ausgangslage

Der Konflikt zwischen Israel und Iran ist seit dem terroristischen Überfall der HAMAS auf Israel am 7. Oktober 2023 deutlich eskaliert. Die langfristigen Folgen der Militärschläge Israels und der USA gegen das iranische Atom- und Raketenprogramm und führende Köpfe des Regimes sind noch nicht absehbar. Auch wenn die Geschehnisse sich bisher primär auf die Region beschränken, können sie doch negative Auswirkungen auf die Sicherheitslage in Deutschland haben. Abhängig von der weiteren Dynamik können verschiedene Stellen mittelbar oder unmittelbar betroffen sein.

Sachverhalte

Gestiegene Aktivitäten iranischer Nachrichtendienste

In den letzten Jahren ist das Hinweisaufkommen zu Aktivitäten iranischer Nachrichtendienste und irannaher Akteure in Europa gestiegen. Auch die Hinweise auf staatsterroristische Gefährdungssachverhalte nehmen zu. Besonders im Fokus stehen dabei Oppositionelle und (vermeintliche) Staatsfeinde im Ausland (sogenannte Transnationale Repression). Dort greifen iranische Nachrichtendienste für Ausspähversuche sowie für die Vorbereitung und Durchführung von Anschlägen regelmäßig auf stellvertretende Strukturen (sogenannte Proxys) einschließlich der Organisierten Kriminalität zurück. Derzeit liegen keine Hinweise auf entsprechende konkrete Gefährdungen von Stellen in Deutschland vor.

Festnahmen ausländischer Staatsangehöriger

Aktuell mehren sich Meldungen über Festnahmen ausländischer Staatsangehöriger durch den Sicherheitsapparat im Iran. Den Betroffenen wird regelmäßig Spionage u. a. gegen militärische oder atomare Einrichtungen und/oder Kollaboration mit Israel vorgeworfen. Eine von der Politik unabhängige gerichtliche Prüfung der Vorwürfe durch die Gerichte findet dabei nicht statt.

Aktivitäten im Cyberraum

Iranische Nachrichtendienste betreiben in westlichen Staaten weiterhin politisch motivierte Cyberspionage sowie digitale Ausspähung von Oppositionellen. US-Sicherheitsbehörden weisen aktuell auf eine erhöhte Gefährdung von US-

amerikanischen KRITIS-Unternehmen durch Cyberangriffe hin. Im Nahen Osten selbst prägen unterdessen derzeit hacktivistische Gruppierungen und deren Aktivitäten das Bild. Bislang sind weder direkte noch indirekte Betroffenheiten in Deutschland festzustellen.

Politisch motivierte Brandanschläge

Im Juni 2025 kam es in Berlin zu mehreren Brandstiftungen an Firmenfahrzeugen eines Onlineversandhändlers und eines Telekommunikationsanbieters. Ein Bekennerschreiben, das auf den linksextremistischen Plattformen „de.indymedia" und „Switch Off" veröffentlicht wurde, begründet die Taten mit der angeblichen „Militärkollaboration" der betroffenen Unternehmen u. a. mit den israelischen Streitkräften im Hinblick auf den „Genozid und Vernichtungskrieg in Gaza" sowie mit dem US-amerikanischen Militär und mit der Bundeswehr. In Korntal-Münchingen in Baden-Württemberg wurden bei einem Brandanschlag auf einen Baustoffhändler eine Halle sowie drei Lkw teilweise zerstört. Am Sitz des Unternehmens waren seit dem 7. Oktober 2023 aus Solidarität mit den Opfern des Terrorangriffs durch die HAMAS israelische Flaggen gehisst. Die Ermittler prüfen eine politische Motivation für die Tat.

Finanzierung u. Beschaffung für die Hizb Allah

Vor dem Hintergrund massiver finanzieller und militärischer Verluste der Hizb Allah durch den Nahostkonflikt kommt es zu erhöhten Finanzierungs- und Beschaffungsaktivitäten der Organisation im Ausland.

Bewertung

Erhöhte Gefährdung durch Staats-terrorismus

Im Falle einer weiteren Eskalation könnte das iranische Regime staatsterroristische Anschläge im Ausland – und möglicherweise auch in Deutschland - befehlen. Es muss insbesondere damit gerechnet werden, dass der Iran bzw. Proxys in seinem Auftrag gegen (pro-)israelische oder (pro-)jüdische bzw. (pro-)US-amerikanische Ziele außerhalb Israels vorgehen könnten. Insofern wird von einer erhöhten abstrakten Gefährdung insbesondere für entsprechende Einrichtungen in Deutschland ausgegangen. Auch Oppositionelle und andere Personen mit Verbindungen in den Iran könnten noch stärker ins Visier geraten. Grundsätzlich sind hierbei alle Iran bzw. seinen Proxys zur Verfügung stehenden Mittel einzukalkulieren.

Fortdauernder Einsatz von Geisel-diplomatie

Es ist anzunehmen, dass das iranische Regime weiterhin unter vorgeschobenen Spionagevorwürfen ausländische Staatsangehörige verhaften wird. Diese können dann als Druckmittel im Rahmen der „Hostage Diplomacy" (Geiseldiplomatie) missbraucht werden, um von den Regierungen der Heimatländer politische Zugeständnisse zu erpressen. Besonders gefährdet sind Personen mit doppelter Staatsangehörigkeit, die der Iran grundsätzlich als Inländer behandelt.

Vermehrte Angriffs-vorbereitungen im Cyberraum

Die Entwicklungen im Nahen Osten dürften die Bereitschaft von Akteuren auf Seiten der beteiligten Konfliktparteien weiter erhöhen, Vorbereitungshandlungen im Cyberraum zu intensivieren und Angriffsaktivitäten zu initiieren. Es könnte auch zu direkten Angriffen gegen Stellen in Deutschland oder zu Spill-over-Effekten auf diese kommen.

Zusätzlicher Mobilisierungs-schub für extremistische Akteure

Es ist davon auszugehen, dass die Entwicklungen im Nahen Osten eine mobilisierende Wirkung auf extremistische Akteure aus verschiedenen Phänomenbereichen haben und dass es vermehrt zu Protest- bis hin zu Gewaltaktionen kommen kann. Mit Blick auf den Linksextremismus könnten vor dem Hintergrund des Begründungszusammenhangs „Antimilitarismus" insbesondere die Sicherheits- und Verteidigungsindustrie sowie Stellen mit USA-Bezug vermehrt zur Zielfläche werden. Im Bereich des auslandsbezogenen Extremismus und des Islamismus kann mit Aktionen insbesondere gegen (pro-)israelische und (pro-)jüdische Einrichtungen gerechnet werden, z. B. ausgehend vom entsprechenden Demonstrationsgeschehen.

Verstärkter Ankauf von Dual-Use-Gütern durch die Hizb Allah

Vor dem Hintergrund ihres erhöhten Nachbeschaffungsbedarfs wird die Hizb Allah wahrscheinlich versuchen, auch in Deutschland verstärkt militärisch nutzbare Güter (sogenannte Dual-Use-Güter) wie z. B. unbemannte Fluggeräte (Unmanned Aerial Vehicles/UAV) oder entsprechende Bauteile anzukaufen.

Handlungsempfehlungen

Verdacht von Ausforschungs- und Anbahnungs- sowie physischen Sabotageversuchen

Maßnahmen für Personalverantwortliche:

- Weisen Sie Beschäftigte auf die Möglichkeit von nachrichtendienstlichen Ausforschungs- und Anbahnungsversuchen hin. Das gilt insbesondere für Personal mit (doppelter) iranischer Staatsangehörigkeit oder sonstigen Verbindungen in den Iran. Etablieren Sie interne Meldewege für Verdachtsfälle. Kommunizieren Sie an die Beschäftigten, was im Verdachts- oder Notfall zu tun ist.
- Informieren Sie Beschäftigte auch über physische Sabotagehandlungen und darüber, dass diese mit Cyberangriffen abgestimmt durchgeführt werden können. Berücksichtigen Sie dabei vor allem solche Betriebsabläufe, deren Ausfall besonders schwerwiegende und/oder langfristige Folgen hätte.
- Stellen Sie in Ihrer Social-Media-Policy sicher, dass Beschäftigte besondere Zurückhaltung bei Bezügen zu KRITIS-Bereichen üben.
- Zögern Sie nicht, Kontakt zum Verfassungsschutz aufzunehmen, wenn Sie den Verdacht haben, dass Beschäftigte Ziel von Ausforschungs- oder Anbahnungsversuchen werden sollen oder bereits geworden sind.
- Wenden Sie sich bei konkreten Bedrohungen gegen Beschäftigte und bei sonstigen Notfällen direkt an Ihre örtliche Polizeidienststelle.

Maßnahmen für Beschäftigte:

- Gehen Sie diskret mit Informationen über Ihr berufliches Umfeld, Kolleginnen und Kollegen sowie geschäftliche Zusammenhänge um.
- Besondere Zurückhaltung ist im Kontakt mit Ihnen unvertrauten Ansprechpartnerinnen und -partnern geboten.
- Treten Sie in sozialen Netzwerken und Karriereplattformen möglichst datensparsam auf und üben Sie besondere Zurückhaltung, wenn es um Bezüge zu KRITIS-Bereichen innerhalb Ihres Unternehmens geht.
- Nutzen Sie die internen Meldewege, wenn Sie den Verdacht haben, dass Sie Ziel eines Ausforschungs- oder Anbahnungsversuchs werden sollen – oder es bereits geworden sein sollten.
- Achten Sie auf Anzeichen physischer Sabotage und melden Sie ungewöhnliche Beobachtungen über die dafür vorgesehenen Wege.

Sicherheit auf Geschäftsreisen

- Vermeiden Sie Reisen in den Iran. Besondere Vorsicht gilt, wenn Sie (auch) die iranische Staatsangehörigkeit besitzen. Beachten Sie bei unverzichtbaren Reisen die Reise- und Sicherheitshinweise des Auswärtigen Amtes und halten Sie sich über die aktuelle Lage auf dem Laufenden.
- Tragen Sie sich in die Krisenvorsorgeliste ELEFAND ein. Reisen Sie möglichst in Begleitung.
- Seien Sie skeptisch bei der Kontaktaufnahme durch Ihnen unbekannte Personen, um kompromittierende Situationen zu vermeiden.
- Vermeiden Sie jedes Verhalten, aus dem Spionagevorwürfe konstruiert werden könnten (z. B. Bild- oder Tonaufnahmen).
- Planen Sie Transportmittel und -routen vorab. Halten Sie sich von potentiell sensiblen Orten (z. B. Militäreinrichtungen) und gefährlichen Situationen (z. B. Protesten) fern.

Cybersicherheit

Maßnahmen für (IT-)Sicherheitsverantwortliche:

- Sensibilisieren und schulen Sie Beschäftigte regelmäßig mit Blick auf aktuelle Cybergefährdungen. Etablieren Sie klare Meldewege. Kommunizieren Sie, was im Verdachts- oder Notfall zu tun ist.
- Bewerten Sie – bestehende und geplante – Veröffentlichungen neu und prüfen Sie diese hinsichtlich des Adressatenkreises kritisch. Hinterfragen Sie insbesondere Veröffentlichungen, die über das gesetzlich erforderliche Maß hinausgehen und unterlassen Sie diese im Zweifel. Sofern keine rechtlichen Veröffentlichungspflichten entgegenstehen, geben Sie sensible Inhalte nur restriktiv und an einen auf das notwendige Minimum beschränkten Adressatenkreis heraus („Need-to-know"-Prinzip).

- Schaffen Sie für sensible Informationen geeignete Übermittlungswege mit den jeweils notwendigen Vorkehrungen – zum Beispiel Zwei-Faktor-Authentifizierung (2FA) und verschlüsselte E-Mail-Kommunikation.
- Führen Sie in geeigneten Abständen Penetrationstests durch, um ein Feedback zum Umsetzungsstand der IT-Sicherheit aus Angreifer-Sicht zu erhalten. Sorgen Sie dafür, dass interne Serverdienste grundsätzlich nicht ohne Weiteres aus dem Internet erreichbar sind. Es bietet sich an, einen Zugriff lediglich aus dem Unternehmensnetzwerk oder über Virtual Private Network (VPN) zuzulassen. Wägen Sie ab, ob eine Verschleierung der eigenen IP-Adressen/-Adressbereiche durch Reseller möglich ist.
- Von DDoS-Angriffen betroffene Stellen finden auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine Liste qualifizierter DDoS-Mitigation-Dienstleister.

Verdacht von (Dual-Use-)Beschaffungsaktivitäten für terroristische/militärische Zwecke

- Nehmen Sie Kontakt zu uns auf, wenn bei Ihnen Dual-Use-Güter in auffällig hoher Stückzahl in kurzer Zeit und/oder durch Einzelpersonen (mit libanesischem Hintergrund) oder kurzfristig erst gegründete und unbekannte Unternehmen gekauft/bestellt werden.

So erreichen Sie uns

Für Informationen zu Bedrohungen für Ihre Branche durch Spionage und Sabotage, Terrorismus oder gewaltbereiten Extremismus sowie für konkrete Sicherheitsanfragen oder Verdachtsfälle kontaktieren Sie den Bereich Wirtschaftsschutz:

wirtschaftsschutz@bfv.bund.de
+49 30 18792-3322

Natürlich steht Ihnen auch Ihre Landesbehörde für Verfassungsschutz als Ansprechpartner zur Verfügung. Sollte Ihnen der Kontakt nicht bekannt sein, vermitteln wir Ihnen diesen gerne.

Ihre Angaben werden in jedem Fall vertraulich behandelt.

PRÄVENTION
WIRTSCHAFTSSCHUTZ