Bundeskriminalamt

BKA

ST14 Gefährdung –
Zusammenarbeit mit der Wirtschaft
ST14@bka.bund.de

Information für die Wirtschaft 19.12.2024

Sensibilisierungsschreiben im Kontext potenzieller russischer Ausspähung und Sabotage

1. Ausgangslage

Seit geraumer Zeit stellt das Bundeskriminalamt (BKA) eine erhöhte Gefährdung durch Ausspähungs- und Sabotageaktivitäten in Deutschland fest.
Diese lässt sich insbesondere durch ein zunehmendes Aufkommen an (potenziellen) Ausspähungs- und Sabotageaktivitäten, vor allem zum Nachteil von Kritischen Infrastruktureinrichtungen in Deutschland und anderen Staaten begründen, die (mutmaßlich) durch russische Nachrichtendienste oder durch sog. Proxies bzw. „Low-Level-Agents“ initiiert oder durchgeführt werden.

Bei sog. Proxies bzw. „Low-Level-Agents“ handelt es sich um Personen, die von russischen Stellen bzw. Mittelspersonen bspw. über soziale Medien oder Sofortnachrichtendienste zunächst gegen kleine Geldbeträge für die Durchführung von niederschwelligen Ausspähungs- bzw. Sabotageaktionen angeworben werden, mit der Möglichkeit im „Erfolgsfall“ gegen höhere Geldzahlungen auch mit „höherwertigen“ Aufgaben betraut zu werden. Der in Frage kommende Personenkreis ist dabei nicht abschließend darstellbar. Neben Personen aus dem kriminellen Milieu können grundsätzlich auch Mitarbeitende sowohl im eigenen Unternehmen als auch bei externen Dienstleistern aus den unterschiedlichsten Berufsgruppen, Tätigkeitsfeldern und Positionen sowie Personen, die keinen Bezug zum Unternehmen haben, rekrutiert werden.
Neben dem vorgenannten Modus Operandi sind weiterhin klassische Spionageaktivitäten wie die Anwerbung und Rekrutierung von Innentätern bzw. die Manipulation von Firmenmitarbeitenden im Kontext Wirtschaftsspionage und -sabotage zur Anwendung einzukalkulieren.

Das Agitationsspektrum solcher im Auftrag russischer Stellen handelnder Personen reicht von Ausspähungs- und Propagandadelikten bis hin zu Sabotagehandlungen, die bspw. die

Betriebsabläufe von Kritischer Infrastruktur und Unternehmen stören und dadurch bestimmte Leistungen bzw. Produkte verhindern oder verzögern, etwa durch bewusstes Beschädigen oder in Brand setzen.
Dabei dürfte ein möglicher nachrichtendienstlicher Hintergrund für die beauftragten Täterinnen bzw. Täter selbst häufig nicht offensichtlich sein. Auch können derartige Taten und die entsprechenden Auswirkungen mitunter vom ersten bzw. äußeren Anschein und dem Schadensbild nach, vermeintlich gewöhnlichen Defekten, Unfällen, Vandalismus oder Straftaten der Allgemeinkriminalität gleichen.

Im Hinblick auf potenzielle Ausspähungshandlungen wurde in den vergangenen Monaten bspw. eine erhöhte Anzahl an unerlaubten Drohnenüberflügen oder auch Personen bei augenscheinlichen Video- und Fotoaufnahmen von Kritischen Infrastruktureinrichtungen festgestellt, u. a. im Zusammenhang mit militärischen Einrichtungen, LNG-Terminals, Tanklagern, Umspannwerken, Seehäfen und Logistikunternehmen.

In London/GBR wurde eine Lagerhalle in Brand gesetzt, in der sich – wie sich erst später herausstellte – für die Ukraine bestimmtes militärisches Gerät befand. Hierbei konnten mehrere für den Brand verantwortliche Personen festgestellt werden, die unter anderem im Auftrag eines russischen Nachrichtendienstes gehandelt haben sollen.
Des Weiteren gerieten einzelne Paketsendungen, die von Privatpersonen an Standorten in Europa aufgegeben wurden, auf dem Weg zu ihren Adressaten in mehreren europäischen Ländern in Brand. Eine dieser Luftfrachtsendungen verursachte ein Feuer auf dem Logistikgelände des Flughafens Leipzig. Es besteht der Verdacht, dass die Pakete im staatlichen Auftrag aufgegeben wurden, um Frachtdienstleistungsunternehmen und weitere logistische Infrastruktur zu schädigen. Die Ermittlungen hierzu dauern an.
Weiterhin kam es in Deutschland in Bayreuth/BY zur Festnahme von zwei Personen mit deutsch-russischer Staatsangehörigkeit, die im Verdacht stehen, im Auftrag staatlicher russischer Stellen Informationen zu militärischen Liegenschaften, Infrastruktureinrichtungen und Industriestandorten gesammelt und an einen russischen Geheimdienst übermittelt zu haben. Mit diesen Informationen sollte die Vorbereitung von Sabotageakten in der Bundesrepublik Deutschland ermöglicht werden. Auch hier dauern die Ermittlungen an.

2. Sensibilisierung

Wenngleich aus der Erkenntnislage eine abschließende Aufzählung möglicher Angriffsziele nicht ableit- bzw. darstellbar ist, fallen hierunter vornehmlich Kritische Infrastruktureinrichtungen und Wirtschaftsunternehmen aus den Bereichen Rüstungsindustrie,

Energie, Transport und Verkehr, Logistik sowie dem Bereich der Informations- und Kommunikationstechnik, bei denen aus russischer Sicht für deren Zwecke geeignete Informationen über bspw. Betriebsabläufe und Funktionsweisen, Sicherheitsvorkehrungen, Vulnerabilität sowie Angriffsvektoren erhoben werden können.

Neben der Erlangung vorgenannter Informationen ist es Ziel russischer Nachrichtendienste, militärische Unterstützungsleistungen für die Ukraine sowie (militärisch nützliche) Lieferungen an die Ukraine (bspw. Kommunikationstechnik) durch die Wirtschaft zu unterbinden oder zu erschweren.
Im Zielspektrum stehen insbesondere Örtlichkeiten, die für die Herstellung, Lagerung und den Transport von Bedeutung sein können.

Ausspähungs- und Sabotageaktivitäten können mittels unterschiedlichster Vorgehensweisen begangen werden. Dies umfasst Handlungen, die mit geringem Aufwand bzw. einfachen Mitteln zu realisieren sind und sowohl unternehmensinterne als auch -externe Wirkung entfalten können.
Ein besonderes Augenmerk sollte hierbei auf solche Ereignisse gerichtet werden, die bei näherer Betrachtung der Umstände russischen Interessen dienlich sein könnten. Hierzu zählen u. a. Vorkommnisse an und in Betrieben bzw. Einrichtungen wie unerlaubte Drohnenüberflüge, Anfertigungen von Foto- und Videoaufnahmen, Fälle unberechtigten Betretens von Firmengeländen, Farbschmierereien oder sonstige Schäden sowie plötzlich entstehende Brände bis hin zu Explosionen.

In diesem Kontext kann es auch zu Kontaktierungsversuchen einzelner Unternehmensangehöriger u. a. über soziale Medien kommen, mit dem Ziel der Einflussnahme und/oder Gewinnung möglicher Innentäter sowie sensibler Informationen. Des Weiteren könnte versucht werden, öffentlich zugängliche Informationen von Unternehmen, wie bspw. Gebäudepläne, Leitfäden, Arbeitsschwerpunkte, Qualifikationen, technisches Know-how, Prozessabläufe, Personalaufstellungen oder sonstige Unternehmensinterna, u. a. über deren Internetpräsenzen oder Social-Media-Profile, zu erheben und missbräuchlich zu verwenden. Vorgenannte Innentäter kommen insbesondere für Tätigkeiten in ihrem jeweiligen Zuständigkeits- und Einflussbereich in Frage, etwa um bspw. vertrauliche Informationen aus dem Unternehmen heraus zu erheben und/oder Betriebsabläufe zu stören bzw. zu verhindern.

Weiterhin ist hervorzuheben, dass sich russische Nachrichtendienste sowohl hinsichtlich des Modus Operandi als auch der Zielauswahl anpassungsfähig und innovativ zeigen, was sich nicht zuletzt im Einsatz der sog. Proxies aufzeigt.

Neben dem physischen Schaden wird die mögliche Erzeugung von (öffentlicher) Verunsicherung bewusst einkalkuliert.
Zumal auch Aktionen, die keinen (unmittelbaren) Schaden verursachen, in der Summe und Kombination mit anderen offenen wie verdeckten Maßnahmen (etwa Desinformation) Verunsicherung hervorrufen können.

3. Handlungsempfehlungen

Insgesamt gilt es wachsam zu sein und zu prüfen, ob verdächtige Feststellungen oder Auffälligkeiten im beschriebenen Kontext stehen könnten.

Dieses Schreiben dient insofern der Sensibilisierung, Feststellungen von verdächtigen Wahrnehmungen, die darauf hindeuten könnten, dass ggf. Einrichtungen ausgespäht bzw. sabotiert werden, der örtlich zuständigen Polizei zuzuleiten; auch wenn die Urheberschaft und Motivlage zunächst unklar sein sollten.

Des Weiteren wird angeregt, die Mitarbeitenden dahingehend zu sensibilisieren, potenzielle Kontaktierungsversuche, z. B. über Social-Media-Plattformen wie Facebook oder WhatsApp, im Lichte der vorgenannten Ausführungen zu prüfen und mögliche Anbahnungsversuche mitzuteilen.

Bezugnehmend auf potenzielle Ausspähungsversuche von öffentlich zugänglichen Informationen werden die Wirtschaftsunternehmen abschließend darauf aufmerksam gemacht, insb. Internetpräsenzen, wie eigene Webseiten oder Social-Media-Profile, auf potenziell sensible Informationen zu überprüfen, die von etwaigen Akteuren missbräuchlich eingesetzt werden könnten.

Ergänzend wird in diesem Zusammenhang auf den Sicherheitshinweis für die Wirtschaft 01/2024, „Schutz vor Sabotage (Nr. 2)“ des Bundesamtes für Verfassungsschutz vom 26.07.2024 hingewiesen.