Bundesamt für
Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 01/2023
Sicherheitshinweis für Politik & Verwaltung | 01/2023

30. Juni 2023

Betreff | Spionage gegen den Verteidigungssektor

Ausgangslage

Der Verteidigungssektor mit seinen Unternehmen, Forschungseinrichtungen und beteiligten staatlichen Stellen steht traditionell besonders im Fokus von Spionage durch ausländische Staaten und deren Nachrichtendienste. Zunehmende geopolitische Rivalitäten wie auch der russische Angriffskrieg gegen die Ukraine verschärfen die Gefährdungslage. Dabei geht es um strategische Aufklärung, die verdeckte Beschaffung von militärischen Technologien und Know-how sowie möglicherweise auch die Vorbereitung gezielter Sabotagehandlungen. Zum Einsatz kommen sowohl cybergestützte als auch realweltliche nachrichtendienstliche Methoden. Die meisten derartigen Aktivitäten gehen von Russland, China und Nordkorea aus.

Sachverhalte

RUSSLAND: Intensiviertes Aufklärungs-interesse

Deutschland ist aufgrund seiner Rolle als NATO-Bündnispartner sowie als EU-Mitglied seit langem ein vorrangiges Ziel russischer Nachrichtendienste. Angesichts der andauernden Unterstützung und insbesondere der Waffenlieferungen von deutscher Seite für die Ukraine hat sich deren Interesse an sicherheits- und verteidigungspolitischen Informationen sowie an rüstungsrelevanten Technologien nochmals intensiviert.

Ausspäh-versuche zu Sabotage-zwecken

In Polen wurde im Frühjahr 2023 ein mutmaßlicher Spionagering aufgedeckt. Bei den Tatverdächtigen soll es sich um Staatsbürger von Ländern „jenseits der Ostgrenzen Polens“ handeln. Ihnen wird vorgeworfen, Bahn- und Luftverkehrsinfrastruktur ausgespäht und Sabotageakte vorbereitet haben, um die Lieferung von Ausrüstung, Waffen und Hilfsgütern in die Ukraine zu stören. Dafür haben sie den Berichten zufolge elektronische Geräte und GPS-Sender bei sich gehabt, die sie an Hilfskonvois in die Ukraine befestigen wollten, um deren Routen nachzuvollziehen.

Verdeckte Beschaffungsversuche zur Sanktionsumgehung

Um die umfassenden EU-Sanktionen zu umgehen, setzt Russland verstärkt auf einen verschleierten Erwerb sogenannter „Dual-Use"-Güter, die sowohl zu zivilen als auch zu militärischen Zwecken nutzbar sind. Diese Güter werden mithilfe von Tarnunternehmen über verschiedenste Umgehungsländer ausgeführt. Im Mittelpunkt der Beschaffungsbemühungen stehen Halbleitertechnologien und verwandte Produkte wie Testequipment oder Produktionsanlagen sowie Ausrüstungsgegenstände für die Luftfahrt und den maritimen Bereich.

Vielfältige Cyberakteure und Angriffsvektoren

Mutmaßlich von russischen staatlichen Stellen gesteuerte Cybergruppierungen nahmen in der Vergangenheit bereits Personen aus der Verteidigungspolitik, die Bundeswehr und ihre Angehörigen sowie Unternehmen der Verteidigungswirtschaft ins Visier. Dabei kamen Spear-Phishing-Angriffe zum Einsatz, aber auch selbstentwickelte (und mitunter hochspezialisierte) Software oder frei verfügbare (Open-Source-)Tools. Seit Beginn des Angriffskrieges gegen die Ukraine sind zudem vermehrt Hacktivismus-Gruppierungen, die sich mit der russischen Regierungslinie solidarisieren, u. a. mit DDoS-Angriffen gegen deutsche Ziele aktiv.

CHINA: Hauptaugenmerk auf Hochtechnologie

China will zu einer globalen Führungsmacht aufsteigen und baut seit Jahren auch seine militärischen Fähigkeiten aus, um diesen Anspruch zu untermauern. Die Zentralregierung verfolgt dafür eine aggressive Strategie der „zivil-militärischen Fusion", die darauf ausgerichtet ist, Wirtschaft und Militär enger zu verzahnen und die rüstungsbezogene Entwicklung und Nutzung von zivilen Technologien/Know-how stärker zu integrieren. Benötigte Hochtechnologie wird dabei gezielt auch durch die Nachrichtendienste beschafft.

Neue Wege der Spionage

Neben Spionage mit menschlichen Quellen und Cyberangriffen setzt China zuallererst auf legale und legitime Methoden wie z. B. Forschungskooperationen, Joint Ventures oder Unternehmensaufkäufe, um Know-how nach China zu transferieren. Eine Vielzahl staatlich geförderter Talentprogramme spannt gezielt Gastwissenschaftlerinnen und -wissenschaftler oder Werksstudierende zur Beschaffung ein. Solche „Non-Professionals" verfügen regelmäßig über weitreichende Zugangsmöglichkeiten, ohne Verdacht zu erregen.

Aktive Rolle nichtstaatlicher Akteure

Von China gehen seit Jahren zahlreiche und massive Cyberangriffe gegen westliche Rüstungsunternehmen aus, insbesondere in den Bereichen Luftfahrt und maritime Technologien. Ein Großteil geht auf mutmaßlich staatlich gesteuerte Gruppierungen zurück. Darüber hinaus liegen auch Erkenntnisse vor, die eine aktive Rolle nichtstaatlicher Akteure vermuten lassen. Demnach spionieren chinesische Cybercrime-Gruppierungen vermutlich ebenfalls gezielt westliche Technologien und Unternehmen aus. Die erbeuteten Daten werden dann aus patriotischen oder finanziellen Motiven an chinesische Rüstungsunternehmen oder staatliche Stellen übergeben bzw. verkauft.

NORDKOREA: Beschaffung von Know-how und Devisen

Nordkorea ist bei der Modernisierung seines veralteten militärischen Arsenals und insbesondere bei der Weiterentwicklung seines Nuklearwaffenprogramms auf Güter und Wissen aus dem Ausland angewiesen. Ein Beschaffungsinteresse an Technologien und Know-how auch aus Deutschland liegt daher nahe. Das Gleiche gilt für Informationen zu Schwachstellen bzw. Leistungs- und Baubeschreibungen von Systemen, die in diversen Rüstungsgütern integriert sind. Das nordkoreanische Regime leidet weiterhin unter den umfassenden Sanktionen der Vereinten Nationen. Cyberspionage spielt daher auch eine wichtige Rolle bei der Devisenbeschaffung, indem z. B. Kryptowährungen erbeutet oder gestohlenes Wissen an Dritte weiterverkauft wird.

Karriere-plattformen als Einfallstor

Eine wahrscheinlich staatlich gesteuerte Cybergruppierung fällt seit Jahren durch weltweite Cyberangriffe gegen Unternehmen der Verteidigungswirtschaft auf. In den festgestellten Fällen ging es vor allem um die Erbeutung geschützter Informationen. Angehörige der Zielunternehmen wurden auf Karriereplattformen über gefälschte Profile vermeintlicher Headhunter namhafter Konkurrenzunternehmen angesprochen. Anschließend wurden vorgebliche Stellenangebote mit integriertem Schadcode übermittelt. Im Erfolgsfalle erlaubte der Schadcode dem Angreifer umfangreichen Zugriff auf das gesamte Unternehmensnetzwerk.

Bewertung

Ausblick

Angesichts des russischen Angriffskrieges gegen die Ukraine und aktueller geopolitischer Umwälzungen insgesamt ist von einer anhaltenden, wenn nicht sogar steigenden nachrichtendienstlichen Gefährdung des deutschen Verteidigungssektors auszugehen.

RUSSLAND

Die russischen Nachrichtendienste sind infolge der diplomatischen Ausweisungen von Mitarbeiterinnen und Mitarbeitern aus verschiedenen europäischen Ländern zwar herausgefordert. Sie werden aber auf neue Beschaffungswege umschwenken und jedes Mittel sowie jede Gelegenheit nutzen, um ihren Informations- und Technologiebedarf zu decken. Es ist z. B. davon auszugehen, dass russische Aktivitäten im Cyberraum künftig noch zunehmen werden. Der Fall des Spionagerings in Polen deutet zudem darauf hin, dass künftig vermehrt auch mit Sabotageversuchen zu rechnen ist. Offenbar setzen russische Nachrichtendienste dabei auch auf nicht-hauptamtliche Akteure. Darüber hinaus sind verstärkt Umgehungsversuche mit Blick auf die EU-Sanktionen zu erwarten, insbesondere bei Gütern, die das russische Militär für seinen Nachschub benötigt.

CHINA

China hat infolge des Handelskonfliktes mit den USA und des Umbaus seiner Wirtschaft hin zu mehr Unabhängigkeit vom Westen einen akut erhöhten Bedarf an Know-how insbesondere im Halbleiterbereich, um seine ambitionierten industrie- und verteidigungspolitischen Ziele zu erreichen. Es ist davon auszugehen, dass das Land alle Mittel und Wege sowohl im Cyberraum als auch in der Realwelt nutzt, um

seinen Technologiebedarf zu decken. Es sind auch zukünftig Ausspähversuche gegen deutsche Ziele wahrscheinlich, insbesondere mit Blick auf militärisch nutzbare Hochtechnologie.

NORDKOREA

Nordkorea weist im Cyberraum seit Jahren eine wachsende Professionalisierung auf. Das Land verfügt über die Fähigkeiten, um selbst große – und auf dem Gebiet der IT-Sicherheit vergleichsweise versierte – Unternehmen erfolgreich angreifen zu können. Es ist davon auszugehen, dass auch Ziele in Deutschland verstärkt in das Visier nordkoreanischer Cybergruppierungen geraten.

Handlungsempfehlungen

Cybersicherheit

Maßnahmen für (IT-)Sicherheitsverantwortliche:

- Sensibilisieren und schulen Sie Ihre Mitarbeiterinnen und Mitarbeiter regelmäßig mit Blick auf aktuelle Gefahren im Cyberraum.
- Etablieren Sie klare Meldewege. Kommunizieren Sie an die Beschäftigten, was im Notfall zu tun ist.
- Überprüfen Sie in regelmäßigen Abständen die Notwendigkeit von Zugriffsberechtigungen, insbesondere bei neuen Mitarbeiterinnen und Mitarbeitern in administrativen Bereichen, aber auch bei externen Dienstleistern.
- Schaffen Sie für sensible Informationen geeignete Übermittlungswege mit den jeweils notwendigen Vorkehrungen – z. B. Multi-Faktor-Authentifizierung (MFA) und verschlüsselte E-Mail-Kommunikation.
- Führen Sie in geeigneten Abständen Penetrationstests durch, um ein Feedback zum Umsetzungsstand der IT-Sicherheit aus der Sicht von Angreifenden zu erhalten. Beachten Sie dabei auch mögliche Einfallstore in Ihre Netzwerke z. B. über Auslandsniederlassungen.
- Sorgen Sie dafür, dass interne Serverdienste grundsätzlich nicht aus dem Internet erreichbar sind. Es bietet sich an, einen Zugriff lediglich aus dem Unternehmensnetzwerk oder über Virtual Private Network (VPN) zuzulassen. Prüfen Sie ggf. auch bestehende Möglichkeiten, um die Zurechenbarkeit Ihrer öffentlichen IP-Adressen zu Ihrem Unternehmen zu reduzieren.
- Von DDoS-Angriffen betroffene Stellen finden auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine Liste qualifizierter DDoS-Mitigation-Dienstleister: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.html.

Maßnahmen für Anwenderinnen und Anwender:

- Schützen Sie Ihre Konten nach Möglichkeit mit Hilfe von MFA vor (Credential-)Phishing-Angriffen.
- Misstrauen Sie E-Mails, die Sie zu dringenden Handlungen auffordern. Geben Sie niemals Ihre Passwörter an.
- Klicken Sie niemals auf Links oder Anhänge verdächtiger E-Mails. Dies gilt auch für E-Mails von Familienangehörigen, Bekannten oder Ihrer Arbeitsstelle. Auch deren E-Mail-Konten könnten gehackt worden sein.
- Greifen Sie, wo möglich, auf alternative und sicherere Kommunikationswege zurück.

Verdacht von Ausforschungs- und Anbahnungs- sowie physischen Sabotageversuchen

Maßnahmen für Personalverantwortliche:

- Weisen Sie Beschäftigte auf die Möglichkeit von nachrichtendienstlichen Ausforschungs- und Anbahnungsversuchen hin und etablieren Sie interne Meldewege für Verdachtsfälle.
- Informieren Sie Beschäftigte auch über physische Sabotagehandlungen sowie 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.
- 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.

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.
- 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. Aufmerksam werden sollten Sie z. B. bei versteckt installierten Kameras oder Drohnenüberflügen.

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 Prävention/Wirtschaftsschutz:

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

Natürlich steht Ihnen auch die Landesbehörde für Verfassungsschutz in Ihrem Bundesland 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