Bundesministerium
Inneres

Direktion Staatsschutz
und Nachrichtendienst

VS-H0

Sensibilisierungsbericht

Spione im Bewerbungsprozess – Einschleusen von nachrichtendienstlichen Akteuren in österreichische Organisationen und Unternehmen

GZ:
Datum: Juni 2026
Urheber: Direktion Staatsschutz und Nachrichtendienst
Seiten: 11
Klassifizierungsstufe: VS-H0

Inhalt

1 Allgemeines

Globalisierung und Digitalisierung öffnen eine Vielzahl von Möglichkeiten für österreichische Unternehmen, insbesondere in der Personalrekrutierung. Offene Stellen, die über das Internet und soziale Medien bekannt gegeben werden, erlauben aus einem globalen Pool von Bewerberinnen und Bewerbern zu schöpfen. Auch ermöglichen Online-Bewerbungen einen schnellen und niederschwelligen Bewerbungsprozess für Interessentinnen und Interessenten. Eine korrekte und umsichtige Nutzung dieser modernen Möglichkeiten erlaubt es, die Qualität der neu eingestellten Mitarbeiterinnen und Mitarbeiter signifikant zu verbessern und so die internationale Wettbewerbsfähigkeit zu steigern. Gleichzeitig ergeben sich hieraus neue Risikofaktoren. Das Bekanntwerden einer offenen Stelle in einem globalen Umfeld erlaubt es einer großen Anzahl von Akteuren mit rechtswidrigen Interessen, in den Bewerbungsprozess einzusteigen. Dies kann mannigfaltige Folgen nach sich ziehen, darunter „Fake-Bewerbungen“, die einen Ransomware-Angriff zufolge haben, oder Wirtschafts- und Wissenschaftsspionage durch neue Mitarbeitende, die von privaten oder staatlichen Akteuren angeleitet werden. Dieser Sensibilisierungsbericht soll diese Problematik adressieren, anhand von Beispielen Bewusstsein für gängige Methoden schaffen und Maßnahmen des Eigenschutzes erläutern.

2 Modus Operandi

Im Folgenden wird der Einsatz verdeckter Bewerberinnen und Bewerber durch Nachrichtendienste unterschiedlicher Staaten dargestellt. Dazu werden ihre strategischen Absichten und typischen Vorgehensweisen sowie die daraus resultierenden Gefährdungen beschrieben. Anzumerken ist, dass unspezifische Teilaspekte auf alle angeführten Staaten anwendbar sind.

2.1 Nordkorea: Generieren von Devisen

Neben klassischen Cybermethoden schleust Nordkorea Beschäftigte in IT-Abteilungen zur Devisenbeschaffung ein, die Lohn und System-Zugänge zur Zielerreichung nutzen.

Ein Hauptziel nordkoreanischer Cyberaktivitäten ist die Beschaffung von Devisen zur Finanzierung des nordkoreanischen Regimes. Dazu unterhält Nordkorea mehrere schlagkräftige Cybereinheiten. Diese stehen in Konkurrenz zu einander und sind beauftragt, möglichst viel Geld zu lukrieren. Neben Ransomware-Angriffen und dem Diebstahl von Kryptowährungen hat sich das Einschleusen von Beschäftigten in Unternehmen als drittes Standbein entwickelt. Diese Beschäftigten bewerben sich in der Regel auf Remote Only IT-Rollen und liefern ihren so erworbenen Lohn an den nordkoreanischen Staat ab. Zusätzlich ziehen sie Informationen ab, die entweder direkt vom nordkoreanischen Regime verwertet oder als Druckmittel für Erpressungshandlungen gegen die betroffenen Unternehmen genutzt werden.

Nordkoreanische IT-Fachkräfte verwenden aufwendig gefälschte Identitäten, um sich bei Unternehmen zu bewerben und verrichten ihre Arbeit remote über konspirative Wohnungen. Vielfach kommt bei der Erstellung der gefälschten Identitäten und Lebensläufe mittlerweile Künstliche Intelligenz (KI) zum Einsatz. Diese gefälschten Profile werden auf Freelance- und Bewerbungsplattformen hochgeladen. Mitunter bewerben sie sich auch direkt bei Unternehmen. Die Arbeit erfolgt ausschließlich remote. Vorzugsweise werden dazu Geräte verwendet, die der Bewerberin oder dem Bewerber vom Unternehmen überlassen werden. Nordkoreanische Stellen unterhalten dazu in mehreren

Ländern konspirative Wohnungen, in denen eine Vielzahl dieser Geräte betrieben werden. Die IT-Fachkräfte greifen dann meist über VPN-Verbindungen aus China darauf zu, um ihre Arbeit zu verrichten. Im gesamten Prozess kommt ein Konglomerat an Tarnfirmen und legitimen New Work-Unternehmen zum Einsatz.

Nordkorea bedroht dadurch die Cybersicherheit von Unternehmen aller Sektoren. Schätzungen gehen davon aus, dass mehrere tausend IT-Fachkräfte auf diese Art in westlichen Unternehmen Devisen für Nordkorea beschaffen. Der Fokus liegt hier auf der kontinuierlichen Erwirtschaftung des Arbeitslohns. Darüber hinaus setzen nordkoreanische Nachrichtendienste einige dieser IT-Fachkräfte auch ein, um frühzeitig Informationen zu exfiltrieren oder Schadsoftware bei Dritten aufzubringen. Grundsätzlich sind alle Sektoren vom beschriebenen Vorgehen betroffen.

2.2 Iran: Wirtschaftsspionage zur Sanktionsumgehung

Um geopolitische Machtansprüche zu behaupten und durchzusetzen, strebt die Islamische Republik Iran nach umfassender Aufrüstung.

Dieses Bestreben wird durch aufliegende Sanktionen durch den Westen erschwert. Auf Anordnung des iranischen Regimes beschaffen seine Dienste deshalb verdeckt Technologien und Materialien – auch in Form von Dual-Use-Gütern – sowie Fachwissen zum Bau von Massenvernichtungswaffen und deren Trägersystemen, um geopolitische Ambitionen der Islamischen Republik zu unterstützen. Insbesondere das Beschaffen von Fachwissen erfolgt über die Einschleusung von (wissenschaftlichen) Mitarbeitenden in Forschung und Industrie. Die Themenschwerpunkte Drohnentechnologien, Metallverarbeitung, Bio- und Lifesciences sowie IT und Elektrotechnik sind hier besonders hervorzuheben. Diese Technologien werden oft direkt in kriegerischen Auseinandersetzungen angewendet. Beispielhaft ist hier die Unterstützung der Russischen Föderation im Ukrainekrieg durch Know-how im Bereich Drohnentechnologien.

Jede Ausreise von iranischen Studierenden/Forschenden oder Arbeitnehmerinnen und Arbeitnehmern ist den dortigen Behörden bekannt. Die Islamische Republik Iran unterzieht jeden Ausreiseantrag einer strengen nachrichtendienstlichen Prüfung. Eine Ausreise wird nur genehmigt, wenn diese vorteilhaft für das Regime ist. Im Rahmen der Prüfung muss der oder die Ausreisende eine detaillierte Begründung darlegen. Sofern es sich bei der

Bewerbung nicht ohnehin um eine von einem iranischen ND geführte Operation handelt, wird diese spätestens zu diesem Zeitpunkt den Behörden bekannt. Sollte der angestrebte Arbeitgeber von Bedeutung für das iranische Regime sein, kann durch Druck eine Kooperation mit dem Staat erzwungen werden. Hierzu werden zumeist die Verweigerung der Ausreise oder zurückbleibende Familienangehörige als Druckmittel benutzt. Auch werden Heimaturlaube genutzt, um im Rahmen von Verhören Informationen zu beschaffen, sollte die Kooperation nicht auf vollumfassender Freiwilligkeit basieren.

2.3 China: Wissenschaftliche Mitarbeitende zum Ausbau des Informationsvorsprungs

In den letzten Jahrzehnten trug der Wissenstransfer aus westlichen Ländern wesentlich zu Chinas Aufstieg bei.

Dieser Wissenstransfer ist Teil einer gesamtstaatlichen Vorgehensweise, um gegenüber dem „Westen“ technologisch und geopolitisch aufzuholen und diesen letztendlich zu überholen. China gelangt über verschiedene, oft legale oder semilegale Kanäle an das gewünschte Wissen. Zentrale Interessensfelder des von China betriebenen Know-how-Transfers sind sogenannte Emerging Technologies wie Quantentechnologie, Halbleiter(prozess)technik, Künstliche Intelligenz, Robotik, Biotechnologie und Überwachungstechnologie. Die Informationsbeschaffung umfasst sowohl Wissenschafts- als auch Wirtschaftsspionage.

Wissenschaftliche Kooperationen mit österreichischen Universitäten und Forschungseinrichtungen spielen eine essentielle Rolle beim Wissensabfluss nach China. Zentral ist die gezielte Entsendung und Instrumentalisierung von in Österreich tätigen chinesischen Forschenden und Studierenden für die nachrichtendienstliche Informationssammlung im akademischen Bereich („Non-Professionalisierung“ der Spionage). Hierbei sind staatlich vergebene Stipendien an chinesische Studierende in Österreich ein bevorzugtes Mittel. Für den Erhalt eines solchen Stipendiums müssen Wissenschaftlerinnen und Wissenschaftler ihre ideologische Treue zur Kommunistischen Partei Chinas (KPCh) demonstrieren und verpflichten sich zur Informationsweitergabe an chinesische Botschaften und Konsulate. Auch unterhält China spezielle Universitäten, die genutzt werden, um Personal und Wissen für sein Militär auszubilden bzw. zu generieren. Nach Abschluss werden die Absolventinnen und Absolventen oft direkt in den militärischen

Komplex übernommen oder in das Ausland entsandt, um dort über wissenschaftliche oder privatwirtschaftliche Anstellungen Wissen nach China zu transferieren.

Gesamtgesellschaftlicher Ansatz chinesischer Nachrichtendienste. Das im Jahr 2023 erneut verschärfte nationale Sicherheitsgesetz Chinas bietet chinesischen Nachrichtendiensten die rechtliche Grundlage für die gesamtgesellschaftlichen Spionagebemühungen: Dieses Gesetz verpflichtet sämtliche chinesische Firmen, Universitäten und auch Privatpersonen zur Kooperation mit chinesischen Nachrichtendiensten im In- und Ausland. In weiterer Folge besteht auch für chinesische Firmenniederlassungen in Österreich, chinesisch-stämmige Angestellte, Forschende sowie Studierende im Ausland oder aber international genutzte chinesische Apps die Obligation zur Informationsweitergabe an die Volksrepublik.

2.4 Russland: Erreichen der strategischen & geopolitischen Ziele mittels Einflussnahme und Informationsabfluss

Russlands Nachrichtendienste spielen bei der Erreichung der strategischen und geopolitischen Ziele Russlands eine maßgebliche Rolle.

Aus diesem Grund verfolgen sie mit unterschiedlichen Methoden das Ziel, politische und gesellschaftliche Prozesse zum Vorteil Russlands zu beeinflussen und Informationen aus relevanten Bereichen zu gewinnen. Besonderes Interesse herrscht dabei an Unternehmen, kritischen Infrastrukturen und deren sensiblen Informationen des jeweiligen Landes. Das Hauptaugenmerk liegt auf politischen, militärischen und wirtschaftlichen Gesichtspunkten.

Neben der diplomatischen Abdeckung nutzen russische Nachrichtendienste Tarntätigkeiten, um nachrichtendienstliches Personal einzusetzen. Diese Positionen werden als „Non-Official-Cover“, also „inoffizielle Abdeckungen“ bezeichnet, die unter dieser Abdeckung nachrichtendienstliche Tätigkeiten für Russland ausübten. Die Tarntätigkeit ermöglicht den gezielten Einsatz und Zugang von nachrichtendienstlichem Personal zu relevanten Bereichen und Unternehmungen, der in weiterer Folge zur nachrichtendienstlichen Informationsgewinnung genutzt wird. Neben dem direkten (proaktiven) Einsatz verfolgen russische Nachrichtendienste das Ziel, Kontakt zu Personen mit direktem oder indirektem Zugang zu klassifizierten Informationen und/oder Einrichtungen aufzubauen, diese in weiterer Folge anzusprechen und schließlich zu rekrutieren.

Dabei geht Russland im Rahmen seiner nachrichtendienstlichen Aktivitäten sehr direkt vor und nutzt im Rekrutierungsprozess die Verbindung zu Doppelstaatsbürgerinnen und Doppelstaatsbürgern. Rekrutierung kann sowohl durch Befragungen von Doppelstaatsbürgerinnen und Doppelstaatsbürgern bei der Ein-/Ausreise nach bzw. aus Russland oder während konsularischen Besuchen in Botschaften erfolgen. Zwang, (Be-)Drohung der noch im Inland befindlichen Familie, Patriotismus, ideologische Motivation und weitere Faktoren spielen dabei eine Rolle.

„Citizenship by investment (CBI)“, auch „Goldene Pässe" genannt, wurde in der Vergangenheit gezielt durch Russland genutzt, um europäische Reisedokumente zu erwerben und so bestehende Sanktionen zu umgehen. Im Gegensatz zu „Goldenen Pässen" sind „Goldene Visa"-Programme („Residence by Investment, RBI“) in EU-Ländern weiterhin verfügbar. Nichtsdestotrotz sollte deshalb bei Personen mit dualen oder multiplen Staatsbürgerschaften das Risiko berücksichtigt werden, dass diese Personen Prozesse zum Vorteil Russlands beeinflussen und Informationen aus relevanten Bereichen gewinnen könnten.

3 Schutzmaßnahmen

3.1 Allgemein

Korrekte Einschätzung der eigenen Gefährdung

- Hohes Risiko: Quantentechnologie, Kryptographie, Drohnentechnologie, Metallverarbeitung, Halbleiterprozesstechnologie, KI, Sensorik, Avionik, Biotechnologie, Nuklearphysik, Radiochemie, Raumfahrt, Telekommunikation, IT Dienstleister, Softwareentwicklung

Achten Sie auf Gebäude- und Informationssicherheit

- Elektronische Kontrolle der Zugänge
- Protokollierung der Tätigkeit auf elektronischem Weg (Log-Files)
- Regelmäßige Schulung hinsichtlich Informationssicherheit
- Need-to-know Prinzip → Zugang zu internen Informationen bleibt auf den Bedarf der ausgeübten Tätigkeit beschränkt
- Zugang zu besonders sensiblen Informationen zeitlich und räumlich beschränken

3.2 Im Bewerbungsprozess

Achten Sie auf konsistente Lebensläufe

- Viele Angaben lassen sich durch Internetrecherche überprüfen
- Nutzen Sie Online Tools, um problematische Entitäten (z.B. Universitäten) zu erkennen → https://unitracker.aspi.org.au/
- Bitten Sie um Referenzkontakte
- Bitten Sie um Abschlussarbeiten und sichten Sie diese

Beantragen Sie eine Sicherheitsüberprüfung

- Bei Bewerberinnen und Bewerbern, die Zugang zu Informationen haben, deren missbräuchliche Verwendung zu einer nachhaltigen Funktionsstörung von kritischer Infrastruktur führt, sollten Sie eine offizielle Sicherheitsüberprüfung durch die Sicherheitsbehörden (§ 55a Abs 2 Z 3a Sicherheitspolizeigesetz (SPG)) beantragen.

Kontaktieren Sie bei Verdachtsfällen die DSN (post@dsn.gv.at)

- Wir melden uns zeitnah und besprechen mit Ihnen detailliert Ihre Bedenken
- Wir erarbeiten mit Ihnen eine konkrete Vorgehensweise, die Ihre wirtschaftlichen Interessen sowie sicherheitstechnische Aspekte einbezieht
- Bei hinreichend konkreten Verdachtsfällen wird der Verfassungsschutz im Rahmen seiner gesetzlichen Aufgaben aktiv

Seien Sie aufmerksam

- Perfekte Eignung oder Überqualifizierung ist als Warnzeichen zu verstehen
- Wunsch nach reiner Remotearbeit ist kritisch zu sehen
- Treffen Sie sich mit Bewerberinnen und Bewerbern vor der Anstellung persönlich

3.3 Während laufender Anstellung

Achten Sie auf Warnsignale

- Außergewöhnliche Arbeitszeiten (Wochenende, Feiertage, Nacht)
- Wissen und Fertigkeiten entsprechen im außergewöhnlichen Maß nicht der Ausbildung oder Erfahrung (positiv wie negativ)
- Beantragen von Home-Office über lange Zeit und/oder im Ausland

- Verändertes Verhalten vor oder nach Heimaturlauben
- Zugriff auf Daten oder Informationen, die für die eigene Tätigkeit nicht erforderlich sind