Warnhinweis an Länder, Unternehmen und andere Akteure betreffend nordkoreanische IT-Fachkräfte

31.7.2026 - | Auswärtiges Amt

Gemeinsamer Warnhinweis Japans, der Vereinigten Staaten von Amerika, der Republik Korea, Australiens, Deutschlands, Frankreichs, Italiens, Kanadas, Neuseelands, der Niederlande und des Vereinigten Königreichs.

Nordkorea stützt sich auf ein Netzwerk qualifizierter IT-Fachkräfte, die innerhalb und außerhalb Nordkoreas eingesetzt werden, um sich falsche Identitäten zu beschaffen und in Remote-Arbeit Einkommen zu erzielen, mit dem die rechtswidrigen Kernwaffen- und Raketenprogramme Nordkoreas finanziert werden.

Nordkoreanische IT-Fachkräfte geben sich als Staatsangehörige anderer Länder aus, um über Online-Plattformen, die private Unternehmen zur Mitarbeitersuche, Beschaffung sowie Beauftragung von Dienstleistungen betreiben, Arbeit und Einkommen zu erhalten. Diese Personen versuchen, Verträge abzuschließen und ihre Gehälter an ihre übergeordneten nordkoreanischen Agenturen weiterzugeben. Zudem bedrohen sie Unternehmen von innen und sind an Datenabfluss sowie dem Diebstahl von Kryptowährungen und sensiblen Informationen beteiligt. Nordkoreanische IT-Fachkräfte setzen immer raffiniertere Methoden ein, auch unter Nutzung von KI, um ihre Identitäten zu verschleiern und ihre Aktivitäten weltweit auszuweiten.

Unsere Länder haben wiederholt Informationen veröffentlicht, um die internationale Staatengemeinschaft und den Privatsektor vor der Bedrohung durch nordkoreanische IT-Fachkräfte zu warnen. Japan, die Vereinigten Staaten und die Republik Korea gaben im August 2025 eine „Gemeinsame Erklärung zu nordkoreanischen IT-Fachkräften“ ab, und das multilaterale Sanktionsüberwachungsteam (MSMT) veröffentlichte im Oktober 2025 seinen zweiten Bericht über die Verletzung und Umgehung von VN-Sanktionen durch Nordkorea mittels Cyber-Aktivitäten und IT-Fachkräften. Die Vereinigten Staaten, Japan, die Republik Korea, das Vereinigte Königreich, Australien und Kanada haben jeweils Leitfäden bezüglich der Risiken veröffentlicht, die von nordkoreanischen IT-Fachkräften für private Unternehmen, Regierungen und einzelne Bürgerinnen und Bürger ausgehen. Die Bedrohung durch nordkoreanische IT-Fachkräfte wird durch uns weiterhin aktiv beobachtet und bekämpft.

Nach Maßgabe von Resolution 2397 des VN-Sicherheitsrats müssen alle VN-Mitgliedstaaten alle nordkoreanischen Staatsangehörigen, die im Hoheitsgebiet des jeweiligen Mitgliedstaats Einkommen erzielen, nach Nordkorea repatriieren, vorbehaltlich begrenzter Ausnahmen. Darüber hinaus verstößt der Abschluss von Verträgen mit nordkoreanischen IT-Fachkräften und ihre Bezahlung für erbrachte Leistungen möglicherweise gegen die innerstaatlichen Gesetze vieler Länder, darunter Japan, die Vereinigten Staaten und die Republik Korea, und kann rechtliche Konsequenzen oder Geldstrafen nach sich ziehen.

Die Arbeitsgruppe zur Geldwäschebekämpfung (FATF) stuft Nordkorea als Hochrisiko-Land (high-risk jurisdiction) ein, für das ein Aufruf zum Handeln besteht (schwarze Liste). Die FATF bekräftigt kontinuierlich die Notwendigkeit, robuste und zielgerichtete Finanzsanktionen im Einklang mit den einschlägigen Resolutionen des VN-Sicherheitsrats umzusetzen, und fordert alle Staaten und Gebiete auf, Gegenmaßnahmen zu ergreifen, um ihre Finanzsysteme vor den Risiken der

nordkoreanischen Geldwäsche sowie Terrorismus- und Proliferationsfinanzierung zu schützen. Dessen ungeachtet vernetzt sich Nordkorea durch diversifizierte Maßnahmen zur Generierung von Einkommen, unter anderem das IT-Fachkräfte-System, immer stärker mit dem internationalen Finanzsystem. Wie im Bericht der FATF zu Typologien der komplexen Proliferationsfinanzierung und Sanktionsumgehung (Complex Proliferation Financing and Sanctions Evasion typologies report) hervorgehoben wird, nutzt Nordkorea häufig sein IT-Fachkräfte-System, um Einnahmen zur Finanzierung seines Programms für Massenvernichtungswaffen zu generieren.

Wir fordern alle Länder, Unternehmen und andere Akteure dringend auf, sich eingehender mit dem nordkoreanischen IT-Fachkräfte-System zu befassen und Maßnahmen zur Bekämpfung der unten aufgeführten Taktiken zu ergreifen. Unternehmen, die Online-Plattformen betreiben, sollten ihre Gegenmaßnahmen weiter verstärken, etwa durch die Verbesserung von Identitätsprüfungsverfahren (strenge Prüfung von Ausweisdokumenten, Bestehen auf persönlichen Vorstellungsgesprächen usw.) und die Erkennung verdächtiger Konten (Einführung von Systemen, die bei anomalen Dateneingaben benachrichtigen usw.). Die folgenden Informationen werden von den Staaten bereitgestellt, die diesen Warnhinweis herausgeben.

[Vorgehensweise nordkoreanischer IT-Fachkräfte]

- Viele nordkoreanische IT-Fachkräfte melden sich unter falscher Staatsangehörigkeit oder falscher Identität auf Online-Plattformen an. Typisch ist beispielsweise, dass sie mit gefälschten Ausweisdokumenten arbeiten und sich für eine andere Person ausgeben. Nordkoreanische IT-Fachkräfte nutzen zur Registrierung von Konten Bilder von Ausweisdokumenten, die von Dritten – etwa Mittelsmänner in Drittstaaten – bereitgestellt werden, führen die eigentliche Arbeit jedoch selbst aus.
- Nordkoreanische IT-Fachkräfte nutzen zunehmend Mittelsmänner, um die Erstellung von Online-Konten zu erleichtern, an Vorstellungsgesprächen teilzunehmen und sogar persönlichen Kontakt herzustellen, um ein trügerisches Vertrauen herzustellen und sich Arbeitsverträge zu sichern.
- Nordkoreanische IT-Fachkräfte versuchen oft, direkte Banküberweisungen zu vermeiden und bitten stattdessen um Zahlungen über Geldtransferdienste oder Kryptowährungen. In vielen Fällen geben sie gegenüber den Arbeitgebern das Bankkonto eines Dritten als Zahlungsempfänger an; von diesem Dritten wird dann erwartet, dass er die Gelder auf ein bestimmtes Auslandskonto überweist, wofür er einen Teil der Zahlung als Gebühr für die Nutzung seines Bankkontos erhält.
- Nordkoreanische IT-Fachkräfte verfügen häufig über sehr gute Kenntnisse in IT-Tätigkeiten und suchen über Online-Plattformen und andere Kanäle Arbeit in einem breiten Spektrum, von der Website-Entwicklung über mobile Anwendungen und Software bis hin zu Blockchain-Anwendungen. In manchen Fällen erhalten sie Arbeitsverträge direkt von Unternehmen oder Privatpersonen.
- Viele nordkoreanische IT-Fachkräfte halten sich in Nordkorea, China und Russland sowie in südostasiatischen und afrikanischen Ländern auf, verschleiern aber möglicherweise die Tatsache, dass sie aus dem Ausland arbeiten, durch Verwendung von Proxyservern von Drittanbietern, VPN, Remote-Desktop-Software und ähnlichen Tools.
- Es ist bekannt, dass nordkoreanische IT-Fachkräfte Dritte als Mittelsmänner im Ausland, etwa in den Vereinigten Staaten, zum Betreiben sogenannter „Laptop-Farmen“ nutzen. Diese erhalten von Unternehmen bereitgestellte Laptops, auf die die nordkoreanischen IT-Fachkräfte remote zugreifen können, um ihren tatsächlichen Standort zu verschleiern.
- Neben der Arbeit im IT-Bereich können sich nordkoreanische IT-Fachkräfte durch betrügerischen Devisenhandel unter Nutzung selbst entwickelter automatisierter Handelssysteme Fremdwährung verschaffen.

Darüber hinaus weisen Konten, die mit nordkoreanischen IT-Fachkräften in Verbindung stehen, häufig die nachfolgenden Merkmale auf. Wenn mehrere dieser Merkmale auf eine Person zutreffen, die sich um eine Stelle bewirbt, handelt es sich möglicherweise um eine nordkoreanische IT-Fachkraft, die in betrügerischer Absicht nach Arbeit sucht.

(Für Unternehmen, die Online-Plattformen betreiben)

- Häufige Änderungen der registrierten Informationen (wie Kontoname, Kontaktdaten und Bankverbindungen für den Empfang des Gehalts)
- Der Name des Kontoinhabers stimmt nicht mit dem Namen des registrierten Zahlungskontos überein.
- Es wurden mehrere Konten unter Verwendung desselben Ausweisdokuments erstellt.
- Die zur Identitätsprüfung verwendeten Ausweisdokumente wirken gefälscht oder mit Bildbearbeitungssoftware manipuliert.
- Von derselben IP-Adresse wird auf mehrere Konten zugegriffen.
- Innerhalb kurzer Zeit wird von mehreren verschiedenen IP-Adressen auf ein einzelnes Konto zugegriffen.
- Die Person bleibt über einen ungewöhnlich langen Zeitraum im Konto eingeloggt.
- Die Gesamtarbeitsstunden oder damit zusammenhängende Kennzahlen sind ungewöhnlich hoch.
- Ein Kontonutzer postet gefälschte Rezensionen für sein Konto, vermutlich um die Bewertungen seines Kontos zu verbessern.

(Für Personal einstellende oder Dienstleistungen beschaffende Stellen)

- Im Kontoprofil sind Fehler enthalten oder werden unübliche Ausdrücke verwendet, die auf eine ungenaue maschinelle Übersetzung hindeuten. Dies lässt auf mangelnde Kenntnisse der Sprache des Landes schließen, aus dem die Person angeblich stammt. (Nordkoreaner können jedoch durch Übersetzungsdienste oder große Sprachmodelle in einer Fremdsprache Profile erstellen und kommunizieren, ohne Misstrauen zu erregen.)
- In Videokonferenzen treten Unstimmigkeiten auf, darunter Abweichungen vom Lichtbildausweis oder Video-Feeds, die manipuliert oder künstlich erzeugt wirken.
- Die Person weigert sich, an Videokonferenzen teilzunehmen.
- Die Person bietet an, für weniger Gehalt zu arbeiten als auf dem Markt üblich.
- Es gibt Anzeichen dafür, dass das Konto von mehreren Personen betrieben wird. Nordkoreanische IT-Fachkräfte arbeiten oft in Teams, d. h. je nach Tageszeit interagiert die einstellende oder beschaffende Stelle möglicherweise mit unterschiedlichen Personen.
- Es wird eine Bezahlung in Kryptowährung gefordert.

Unterzeichnet von:

- Japan: Ministerium für auswärtige Angelegenheiten, Nationale Behörde für Cybersicherheit, Nationale Polizeibehörde, Finanzministerium, Ministerium für Wirtschaft, Handel und Industrie
- USA: Außenministerium, Bundeskriminalpolizei
- Republik Korea: Ministerium für auswärtige Angelegenheiten, Nationale Polizeibehörde
- Australien: Ministerium für auswärtige Angelegenheiten und Handel
- Kanada: Ministerium für auswärtige Angelegenheiten und internationalen Handel, Royal Canadian Mounted Police

- Frankreich: Ministerium für Europa und auswärtige Angelegenheiten
- Deutschland: Auswärtiges Amt
- Italien: Ministerium für auswärtige Angelegenheiten und internationale Zusammenarbeit
- Niederlande: Ministerium für auswärtige Angelegenheiten
- Neuseeland: Ministerium für auswärtige Angelegenheiten und Handel
- Vereinigtes Königreich: Ministerium für Auswärtiges, Commonwealth und Entwicklung, Behörde für die Umsetzung von Finanzsanktionen

https://www.auswaertiges-amt.de/de/newsroom/2780756-2780756