Bundesamt für Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 02/2024 | 1. Oktober 2024

Betreff | Nordkoreanische IT-Worker

Ausgangslage

Nordkoreanische Nachrichtendienste führen weltweit offensive Cyberoperationen zur Devisenbeschaffung durch. Dabei setzen sie unter anderem auf den Einsatz getarnter IT-Fachkräfte (IT-Worker), die ihre Dienstleistungen durch Telearbeit Unternehmen rund um den Globus anbieten. Die Erträge kommen dem nordkoreanischen Regime zugute. Auch deutsche Firmen standen bereits in Vertragsbeziehungen mit nordkoreanischen IT-Workern.

Sachverhalt

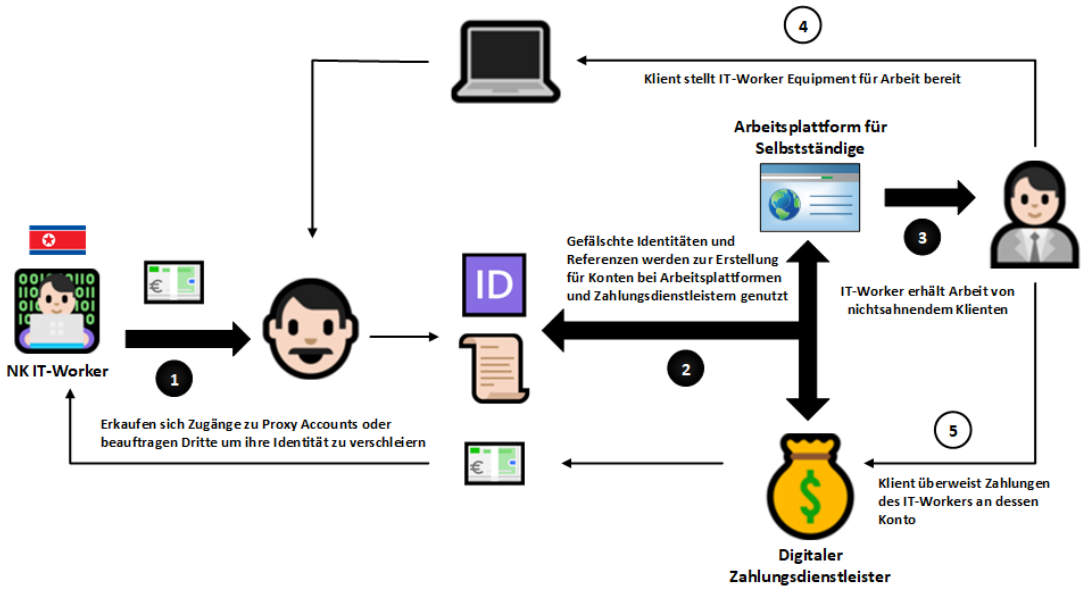
Auftragssuche als Selbständige und vielfältige Einsatzbereiche

Die IT-Worker arbeiten teils direkt aus Nordkorea heraus, teils aber auch außerhalb des Landes. Aufträge suchen sie sich hauptsächlich auf Vermittlungsplattformen für Selbstständige wie „Fiverr“, „Upwork“ und „freelancer.com“. Von generellem IT-Support über die Programmierung von Apps und Spielen bis hin zur Smart-Contract-Entwicklung decken sie vielfältige Einsatzbereiche ab. Zudem sind sie in diversen Branchen aktiv, z. B. im Gesundheitswesen, in der Unterhaltungsindustrie oder im Finanzsektor.

Verschleierung der Herkunft

Nordkoreanische IT-Worker verschleiern professionell ihre wahre Herkunft und verwenden sowohl frei erfundene als auch gestohlene Identitäten. Hierfür nutzen sie gefälschte oder gestohlene Dokumente wie Personalausweise, Reisepässe und Abschlusszeugnisse. Bewerbungsfotos werden teilweise mit KI-Programmen generiert. Alternativ werden gestohlene Bilder mittels Bildbearbeitungssoftware verändert. Die am häufigsten angegebenen Herkunftsländer sind Südkorea und Japan. Auch osteuropäische Nationalitäten werden immer wieder benannt. Die verwendeten falschen Namen werden mitunter an die vorgebliche Herkunft angeglichen. Auch der geographische Standort wird angepasst. Ein eventueller nordkoreanischer Standort wird gegenüber dem Auftraggeber durch die Nutzung von Virtual Private Networks (VPN) oder Proxy Accounts getarnt. Die gängigsten angegebenen Standorte sind Amerika, Japan oder China. Um ihre Glaubwürdigkeit

weiter zu erhöhen, verfügen nordkoreanische IT-Worker neben ihren Accounts auf den Vermittlungsplattformen oftmals auch über Profile auf den gängigen Social-Media-Plattformen und Messenger-Diensten. Die verschiedenen Accounts sind teilweise auf den jeweiligen Profilauftritten untereinander verlinkt. Zu den genutzten Plattformen und Diensten gehören insbesondere „LinkedIn“, „X“ (ehem. „Twitter“), „GitHub“, „Facebook“, „Telegram“ und „Skype“. Häufig wird mehrjährige Berufserfahrung im Bereich Informatik und insbesondere in der Softwareentwicklung vorgetäuscht. Umfangreiche mitgelieferte Referenzen sollen regelmäßig die angeblich vorhandene Expertise und Erfahrung untermauern.



Digitale Bezahlung

Die Vergütung erfolgt bevorzugt über Kryptowährungen wie „Bitcoin“ und „Ethereum“ oder digitale Bezahldienste wie „PayPal“ und „Wise“. Transfers lassen sich damit unkompliziert bewerkstelligen und nur schwer zurückzuverfolgen. Zur zusätzlichen Verschleierung kommen zum Teil Accounts zum Einsatz, die von dritten Personen bereitgestellt werden. Wenn Voraus- oder Extrazahlungen abgelehnt werden, führt dies regelmäßig zu aggressiven und verärgerten Reaktionen. Zudem wird häufig damit gedroht, unternehmensinternen Quelltext zu veröffentlichen, wenn Forderungen nicht erfüllt werden.

Unpersönliche Kommunikation

Die Kommunikation findet vorzugsweise schriftlich über Kurznachrichten statt. Dabei kommen sowohl die Chatfunktion der Vermittlungsplattformen als auch eigenständige Anwendungen wie „Telegram“ zum Einsatz. Video- und Telefonanrufe sowie persönliche Treffen werden in den meisten Fällen vermieden. Die bevorzugte Sprache ist Englisch. Allerdings wird – unabhängig von der angeblichen Herkunft – häufig angeboten, auf Koreanisch zu kommunizieren.

Inkonsistente Lebensläufe

Persönliche Daten und Angaben zum beruflichen Werdegang, wie z. B. Namensschreibweisen, Arbeitserfahrung, Bildungsabschlüsse und gesprochene Sprachen, sind oftmals inkonsistent. Wenn z. B. die angebliche universitäre Ausbildung in China, Japan, Malaysia, Singapur oder anderen asiatischen Ländern

absolviert worden ist, die Person aber bisher nur Anstellungen in den USA, Korea oder Kanada vorzuweisen hat, kann dies auf eine Bewerbung aus Nordkorea hindeuten.

Auffälligkeiten bei Social-Media-Profilen und Adressen

Angegebene Profile in sozialen Netzwerken stimmen regelmäßig nicht mit dem eingereichten Lebenslauf überein. Teils existieren auch mehrere Profile mit demselben Namen, aber unterschiedlichen Bildern. Wohn- und Versandadressen für den Erhalt von Arbeitsausstattung wie z. B. Laptops und anderer Hardware ändern sich oftmals in schneller Folge. Accounts weisen regelmäßig hohe Zeiten der Onlineaktivität auf. Zudem stechen sie durch äußerst positive Kundenbewertungen hervor. Die geforderten Vergütungen liegen dagegen eher im unteren Preissegment.

Platzierung von Schadsoftware

In bestätigten Fällen wurde aufgedeckt, dass nordkoreanische IT-Worker sofort nach dem Erhalt der Arbeitsmittel begonnen haben, Schadsoftware im Unternehmensnetzwerk zu platzieren.

Bewertung

Potentiell schwerwiegende Konsequenzen

Unternehmen, die nordkoreanische IT-Worker beauftragen, helfen dem Regime bei der Devisenbeschaffung und tragen so mittelbar dazu bei, dessen Nuklearwaffen- und Raketenprogramm zu finanzieren. Dies kann nicht nur zu Reputationsrisiken infolge von Compliance-Verstößen, sondern auch zu Sanktionsverletzungen und entsprechenden juristischen Konsequenzen führen. Darüber hinaus besteht die Gefahr, dass geistiges Eigentum und firmeninterne Daten abfließen.

Handlungsempfehlungen

Maßnahmen für Personalverantwortliche:

- Halten Sie Bewerbungsgespräche persönlich oder als Videoanruf ab, um die Identität von selbstständigen Arbeitskräften zu verifizieren.
- Achten Sie im Videoanruf auf Augenbewegungen oder lange Redepausen, die auf ein Ablesen der Antworten hindeuten.
- Vermeiden Sie es, Vergütungen ausschließlich in Kryptowährungen zu bezahlen.
- Stellen Sie sicher, dass Angaben wie die Namensschreibweise, Nationalität, Aufenthaltsort, Kontaktinformationen, Bildungsweg, frühere Arbeitgeber usw. über alle Profile und Konten hinweg konsistent sind.
- Seien sie skeptisch, wenn Ihr Gegenüber die Kommunikation auf separate Plattformen (außerhalb der Vermittlungs- oder Arbeitsplattform) verlagern will.
- Lassen Sie sich die angegebenen Qualifikationen direkt von den Stellen bestätigen, die sie bescheinigt haben. Nutzen Sie dabei nur Kontaktdaten, die Sie unabhängig von Angaben von Bewerberinnen und Bewerbern verifiziert haben.

Maßnahmen für IT-(Sicherheits-)Verantwortliche:

- Verschicken Sie Arbeitsausstattung nur an die Adresse, die in den Ausweisdokumenten angegeben ist. Werden Sie hellhörig, wenn unter der angegebenen Adresse angeblich keine Lieferungen angenommen werden können.
- Stellen Sie sicher, dass Telearbeitende nicht ohne Genehmigung eigene Programme wie Fernwartungssoftware auf zur Verfügung gestellte Arbeitsgeräte herunterladen und installieren können.
- Kontrollieren Sie die Zugriffsrechte von neuen Beschäftigten. Stellen Sie sicher, dass diese nur Zugriff auf Dateien haben, die sie für Ihre Arbeit benötigen.
- Nutzen Sie einen Endgeräteschutz. Spielen sie neue Updates zeitnah ein.

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 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