Bundesamt für Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 02/2022 | 23. März 2022

Betreff | Krieg in der Ukraine

Ausgangslage

Die Kampfhandlungen in der Ukraine dauern an. Das militärische Vorgehen Russlands wird nach wie vor durch Cyberangriffe und Versuche der Einflussnahme begleitet. Aufgrund der andauernden deutschen Unterstützung für die ukrainische Seite ist das Risiko, dass auch deutsche Stellen – direkt oder indirekt – zu Zielen werden, weiterhin hoch. Zudem verzeichnet Deutschland einen anhaltenden Zustrom an Geflüchteten.

Sachverhalte

Anhaltend hohe Cyberaktivitäten

Das Kriegsgeschehen in der Ukraine wird weiterhin von umfangreichen Aktivitäten im Cyberraum begleitet. Die Angriffe richten sich vor allem gegen ukrainische Ziele. IT-Sicherheitsdienstleister berichten unter anderem von erneuten Angriffen mit einer Wiper-Malware. Weiterhin positionieren sich auch bekannte Cybergruppierungen und Hacktivisten öffentlich auf Seiten beider Kriegsparteien.

GHOSTWRITER mit neuer Domain

Nachdem bereits Anfang März erneute Angriffe von GHOSTWRITER gegen deutsche *t-online.de*-E-Mail-Adressen festzustellen waren, konnte dem Akteur nun die neu registrierte Domain *dienste-email.eu* zugeordnet werden. Bislang sind noch keine konkreten Angriffsaktivitäten unter Nutzung dieser Domain festzustellen.

Ein IT-Sicherheitsdienstleister berichtet, dass kompromittierte E-Mail-Accounts ukrainischer Militärangehöriger genutzt werden, um Phishing-Angriffe gegen Politikerinnen und Politiker verschiedener europäischer Regierungen durchzuführen. Die dabei verwendete Schadsoftware weise Ähnlichkeiten zur GHOSTWRITER-Kampagne auf.

#bloodytrade

Unter dem Hashtag #bloodytrade bauen aktuell Twitter-Accounts Druck auf Unternehmen auch in Deutschland auf, sich aus dem Russland-Geschäft zurückzuziehen. Dabei werden die Unternehmensnamen genannt oder verlinkt.

Russische Unternehmensbeteiligung

Die deutsche Tochtergesellschaft eines russischen Konzerns ist Opfer eines Angriffs durch eine internationale pro-ukrainische Cybergruppierung geworden. Das betroffene Unternehmen ist Teil der Kritischen Infrastruktur (KRITIS).

Andauernde Einflussnahmeversuche

Russische Akteure sind weiterhin bestrebt, die politische und öffentliche Meinung in Deutschland durch die Verbreitung von Propaganda, Desinformation sowie durch weitere Einflussnahmeversuche zu Russlands Gunsten zu steuern. Ziel der Bemühungen ist es, westliche Staaten und Bündnisse zu diskreditieren, den politischen Diskurs polarisierend zuzuspitzen und das Vertrauen in staatliche Stellen zu untergraben. Trotz der Sperrung der russischen Staatsmedien in Deutschland sind weiterhin Aktivitäten, insbesondere auf den Social-Media-Accounts dieser Medien zu beobachten.

„SOS"-Postfach der Russischen Botschaft

Kürzlich hat die Russische Botschaft in Deutschland das E-Mail-Postfach *sos@russische-botschaft.de* eingerichtet. Das Postfach richtet sich an „Landsleute", die auf diesem Weg Informationen über „Fälle von Mobbing, Belästigung, Drohungen, Angriffen oder physischer Gewalt" melden können. Die gemeldeten Fälle werden auf der Website öffentlich aufgelistet. Wo ein Unternehmensbezug besteht, wird auch der Name des Unternehmens genannt.

Engagement für Geflüchtete in Unternehmensbelegschaften

In Deutschland gibt es derzeit eine Vielzahl von Unterstützungs- und Hilfsaktionen für ukrainische Geflüchtete. Auch unter Mitarbeiterinnen und Mitarbeitern geheimschutzbetreuter Unternehmen gibt es eine hohe Bereitschaft, in der aktuell angespannten Situation humanitäre Unterstützung anzubieten und praktische Hilfe zu leisten.

Proliferation und Dual-Use-Güter

Seit geraumer Zeit liegen Hinweise auf illegale russische Beschaffungsaktivitäten unter Umgehung von Sanktionen und Verschleierung tatsächlicher Endverwender vor. Russland ist bei der Entwicklung und Herstellung militärischer Systeme weiterhin auf die Beschaffung von proliferationsrelevanten Gütern und sonstigen Rüstungsgütern auf den Weltmarkt angewiesen. Deutschland steht dabei als eine der führenden Industrienationen und Standort zahlreicher Unternehmen der Spitzentechnologie im Fokus. Bei den beschafften Produkten handelt es sich vorwiegend um Dual-Use-Güter, die militärisch bzw. proliferationsrelevant verwendet werden sollen.

Aufgrund der neuen Sanktionen ist nun die Lieferung sämtlicher Güter und Technologien verboten, die zur militärischen und technologischen Stärkung Russlands oder zur Entwicklung des Verteidigungs- und Sicherheitssektors beitragen könnten (EU-Verordnungen 2022/328 vom 25. Februar 2022, 2022/394 vom 9. März 2022 und 2022/428 vom 15. März 2022). Zudem sind Finanzierungsmöglichkeiten stark eingeschränkt (EU-Verordnungen 2022/262 vom 23. Februar 2022, 2022/328 vom 25. Februar 2022, 2022/345 vom 1. März 2022, 2022/394 vom 9. März 2022 und 2022/428 vom 15. März 2022).

Bewertung

Weiter hohe Gefahr von Cyberangriffen

Angesichts der fortwährenden Unterstützung Deutschlands für die Ukraine ist auch das Risiko russischer Cyberangriffe gegen deutsche Stellen, einschließlich Unternehmen, als anhaltend hoch einzuschätzen. Cybersabotageakte gegen Unternehmen in den KRITIS-Sektoren, aber auch gegen den politischen Raum sowie gegen militärische Einrichtungen, sind jederzeit möglich.

Die andauernden Aktivitäten des Akteurs GHOSTWRITER verdeutlichen, dass weiterhin besondere Vorsicht geboten ist. Wortwahl und Endung der von GHOSTWRITER neu verwendeten Domain *dienste-email.eu* lassen es wahrscheinlich erscheinen, dass diese Domain für zukünftige Angriffe gegen deutsche und europäische Ziele angelegt wurde. Möglicherweise wird sie auch bereits verwendet.

Die Warnungen aus dem Sicherheitshinweis 01/2022 vor „Hack and Leak"- bzw. „Hack and Publish"-Operationen haben weiter Bestand. Auch ist angesichts der großen Zahl von Akteuren, die sich auf Seiten beider Konfliktparteien engagieren, weiterhin mit Spill-Over-Effekten und Kollateralschäden auf deutsche Stellen zu rechnen. Dies betrifft insbesondere die Sektoren Energie, Telekommunikation, Transport, Finanzen, Medien und Rüstung, kann sich aber sanktionsreziprok auf weitere Branchen ausdehnen.

Die Aufrufe über Twitter unter dem Hashtag #bloodytrade zeigen, dass auch auf pro-ukrainischer Seite mobilisiert wird. Es ist daher nicht auszuschließen, dass Akteure im Cyberbereich Angriffe auf Unternehmen vornehmen, weil diese sich nicht aus ihrer Geschäftstätigkeit in Russland zurückgezogen hätten.

Mögliche Nutzung von Unternehmensentscheidungen zu Propagandazwecken

Es ist anzunehmen, dass die Einrichtung des „SOS"-Postfachs der russischen Botschaft in Deutschland zur öffentlichkeitswirksamen Verbreitung russischer Narrative beitragen soll. Auch kann nicht ausgeschlossen werden, dass die russischen Nachrichtendienste die erhaltenen Informationen gezielt für operative Zwecke, etwa der Anbahnung, nutzen. Ebenfalls ist nicht auszuschließen, dass Entscheidungen von Unternehmen über die Einschränkung oder Einstellung von Geschäftstätigkeiten in Russland als russlandfeindliche Handlungen ausgelegt und für Propagandazwecke verwendet werden. Dies gilt auch für Äußerungen von russischen Mitarbeiterinnen und Mitarbeitern sowie Geschäftskontakten, die als russlandfeindlich gedeutet werden könnten.

Proliferationsrelevante Güter

Illegale russische Beschaffungsbemühungen in Deutschland werden sich mit hoher Wahrscheinlichkeit intensivieren. Betroffen sind insbesondere Güter der Branchen der maritimen Wirtschaft, Luft- und Raumfahrt, Halbleiterproduktion, Werkzeugmaschinen sowie der Sicherheits- und Rüstungsindustrie. Angesichts der verschärften Sanktionen muss davon ausgegangen werden, dass sich die russischen Methoden der Verschleierung und Umgehung verfeinern. Das kann beispielsweise

die Gründung neuer Tarnfirmen sowie den Aufbau neuer Beschaffungsnetzwerke über Drittstaaten und neue Endverwender umfassen.

Handlungsempfehlungen

Cybersicherheit

- Blocken Sie die Domain *dienste-email.eu*.

Darüber hinaus behalten die Handlungsempfehlungen aus dem Sicherheitshinweis 01/2022 ihre Gültigkeit:

- Beschränken Sie Zugriffsmöglichkeiten auf ein Minimum, um mögliche Angriffsvektoren zu reduzieren. Überlegen Sie sorgfältig, welche Vorgänge und Systeme aktuell für die Gewährleistung von Funktionalitäten erforderlich sind.
- Fertigen Sie in regelmäßigen Abständen Backups und bewahren Sie diese anschließend getrennt von den betroffenen Systemen auf.
- Schließen Sie bekannte Sicherheitslücken durch das Einspielen vorhandener Update-Patches.
- Geben Sie Ihrem Intrusion Detection Management System (IDMS) die Berechtigung, das Starten und Ausführen von Malware nicht nur zu protokollieren, sondern die entsprechenden Prozesse auch sofort zu stoppen und Dateien in Quarantäne verschieben zu können.
- Entfernen Sie unbekannte oder nicht mehr verwendete Nutzer und reduzieren Sie die Berechtigungen für Nutzer auf ein Minimum.
- Schützen Sie Ihre Konten nach Möglichkeit mit Multi-Faktor-Authentifizierung vor (Credential-)Phishing-Angriffen.
- Misstrauen Sie allen E-Mails, die Sie zu dringenden Handlungen auffordern. Geben Sie niemals Ihre Passwörter an und klicken Sie niemals auf Links oder Anhänge verdächtiger E-Mails. Dies gilt auch für E-Mails von Familie, Freunden oder dem Arbeitgeber. Deren E-Mail-Konten könnten ebenfalls gehackt worden sein.
- Informieren Sie Mitarbeiterinnen und Mitarbeiter über die aktuelle Bedrohungslage, um ein Gefährdungsbewusstsein zu schaffen.
- Etablieren und kommunizieren Sie Meldeprozesse innerhalb des Unternehmens sowie die Ansprechbarkeiten von Behörden bei Auffälligkeiten und Sicherheitsvorfällen.

Unternehmen sollten die Entwicklungen weiter aufmerksam verfolgen und ihre IT-Sicherheitsmaßnahmen bei Bedarf anpassen. Das Bundesamt für Verfassungsschutz aktualisiert laufend seine Übersicht über die ihm vorliegenden Indicators of Compromise (IoCs). Diese Liste stellt der Wirtschaftsschutz Unternehmen auf Anfrage digital zur Verfügung, damit

diese selbständig ihre Systeme auf mögliche Kompromittierung prüfen können.

Kommunikation mit Kontakten in Russland

Reduzieren Sie Ihre Kommunikation mit Niederlassungen oder Geschäftskontakten in Russland auf ein Minimum. Halten Sie Ihre Kommunikation sachlich. Insbesondere russische Mitarbeiterinnen und Mitarbeiter sollten nicht in die Lage gebracht werden, sich per Telefon oder E-Mail zum Krieg in der Ukraine äußern zu müssen.

Geheimschutz und Umgang mit Geflüchteten

Mitarbeiterinnen und Mitarbeiter geheimschutzbetreuter Unternehmen sollten im Falle einer etwaigen vorübergehenden Aufnahme von Geflüchteten aus der Ukraine und sonstigen Staaten im Sinne von
§ 13 Absatz 1 Nummer 17 SÜG äußerste Zurückhaltung bei Gesprächen zur beruflichen Tätigkeit wahren. Es dürfen keine Informationen preisgegeben werden, die auf die Tätigkeit in einem geheimschutzbetreuten Unternehmen, die übertragene Aufgabe oder die VS-Ermächtigung schließen lassen könnten.

Proliferationsrelevante Güter

Wenn Ihnen unübliche und/oder verdächtige Beschaffungsanfragen auffallen, zögern Sie bitte nicht, uns über die unten angegebenen Kontaktdaten anzusprechen. Wir stehen auch für Fragen in diesem Zusammenhang gerne zur Verfügung.

Mögliche Indizien für illegale Beschaffungsaktivitäten:

- Als Hersteller von zivilen Produkten erhalten Sie Anfragen von einem Kunden mit militärischen Betätigungsfeld.
- Namen von Unternehmen, Personal, Geschäftsführerinnen und Geschäftsführern passen in auffälliger Weise nicht zum Handelssitz des Unternehmens.
- Der Kunde wahrt zu weiteren Geschäftskontakten nach Deutschland eine auffällige Verschwiegenheit.
- Untypische Versandwege und Bestimmungsorte, z. B. Spedition als Endpunkt.
- Der Kunde wünscht außergewöhnliche Etikettierung oder Kennzeichnung/Beschriftung, die auf eine Verschleierung der Warengattung etc. hindeuten.
- Auffallende Zurückhaltung im Hinblick auf Informationen zur Endverwendung oder dem Endverbraucher.

- Anfrage für vorgebliches Inlandsgeschäft enthält Verweise auf möglichen Warenexport in ein weiteres Zielland.
- Käufer verzichtet auf Einweisungen, Service-Leistungen, Wartungsverträge oder Garantien.

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 (0)30 – 18 – 792 33 22

Für spezifische technische Hinweise oder Rückfragen zu einem konkreten Cyberangriff oder einer bestimmten Kampagne wenden Sie sich direkt an die Expertinnen und Experten der Cyberabwehr:

cyberabwehr@bfv.bund.de
+49 (0)30 – 18 – 792 26 00

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