Bundesamt für
Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 03/2022 | 17. Mai 2022

Betreff | Krieg in der Ukraine

Ausgangslage

Der russische Angriffskrieg in der Ukraine wird nach wie vor durch Cyberangriffe und Versuche der Einflussnahme begleitet. Die Bundesregierung intensiviert ihre Unterstützung der Ukraine, indem künftig auch schwere Waffen geliefert und ukrainisches Personal daran ausgebildet werden sollen. Zudem sind vermehrt auch russische Staatsangehörige an einer Ausreise nach Deutschland interessiert.

Sachverhalte

KILLNET

Aktuell führt die pro-russische Cybercrime-Gruppierung KILLNET eine Kampagne von Überlastungsangriffen (DDoS-Angriffen) gegen diverse deutsche Webseiten aus Privatwirtschaft und Forschung. Verbunden sind die Angriffe mit dem Aufruf, die Unterstützung für die Ukraine einzustellen. Bei KILLNET handelt es sich um eine russische Hacktivisten-Gruppierung, die sich in Reaktion auf den Ausruf der „Ukrainian Cyber Army“ nach Kriegsbeginn formiert hat und die russische Regierung unterstützt.

REvil

Nach Berichten von IT-Sicherheitsforschern ist auch die Cyberkriminellen-Gruppierung REvil (alias Sodinokibi) wieder aktiv. Seit Oktober 2021 waren die Infrastruktur von REvil vom Netz genommen und einige mutmaßliche Mitglieder festgenommen worden. Nun sind neue Malware und Infrastruktur bekanntgeworden, die mutmaßlich REvil zugeordnet werden können. REvil war unter anderem für den Ransomware-Angriff auf Kunden von *Kaseya* im Juli 2021 verantwortlich, von dem weltweit mehr als 1 500 Unternehmen betroffen waren.

Beschäftigte mit russischem Hintergrund

Im Zusammenhang mit dem Krieg in der Ukraine verlassen vermehrt russische Staatsangehörige ihre Heimat in Richtung Deutschland. Das schließt Oppositionelle ein, aber auch Beschäftigte von deutschen oder europäischen Unternehmen, die ihre geschäftlichen Aktivitäten in Russland zurückfahren oder ganz einstellen. Die meisten dieser Personen sind bestrebt, sich in Deutschland eine (vorübergehende oder dauerhafte) berufliche Existenz aufzubauen. Insbesondere Unternehmen, bei denen ein hoher Bedarf an Fachkräften besteht, sind daran interessiert,

Beschäftigten einen schnellen und unbürokratischen Einstieg beziehungsweise Standortwechsel zu ermöglichen.

Datenbanken zu Russland-geschäften

Im Internet sind inzwischen verschiedene Datenbanken zu finden, die teilweise tagesaktuell nachvollziehen, ob beziehungsweise inwiefern ausländische – auch deutsche – Unternehmen noch in Russland aktiv sind oder sich von dort zurückgezogen haben.

Bewertung

KILLNET, REvil und andauernde Cyber-gefährdung

Bei den DDoS-Angriffen von KILLNET handelt es sich um vergleichsweise harmlose Störangriffe, die die Erreichbarkeit von Online-Präsenzen beeinträchtigen. Aktivitäten, die über DDoS-Angriffe hinausgehen, sind aktuell nicht festzustellen. Vor dem Hintergrund der politischen Lage ist mit weiteren DDoS-Angriffen gegen deutsche Webseiten durch pro-russische Hacktivisten zu rechnen. Es ist anzunehmen, dass auch REvil zukünftig wieder westliche Ziele angreifen wird.

Gefahr der nachrichten-dienstlichen Anbahnung

Russland ist durch die in Reaktion auf den Krieg in der Ukraine verhängten Sanktionen zusehends isoliert und seine Wirtschaft von Know-how und Technologien aus dem westlichen Ausland abgeschnitten. Entsprechend dürfte der Druck auf die Nachrichtendienste zunehmen, Zugang zu Menschen mit einschlägigen Kenntnissen und zu Technologien von Bedeutung für die russische Wirtschaft zu gewinnen. Somit besteht die Gefahr, dass es vermehrt zu Anbahnungsversuchen insbesondere von Beschäftigten in für Russland relevanten Wirtschafts- und Forschungszweigen auch in Deutschland kommt. Beschäftigte mit russischer Staatsangehörigkeit sind besonders gefährdet. Die Kontaktaufnahme kann völlig beiläufig und mit langfristiger Perspektive erfolgen. Gelegenheiten der Ansprache bieten sich den russischen Nachrichtendiensten vor allem im Rahmen von – häufig notwendigen – Kontakten russischer Staatsangehöriger zu diplomatischen Einrichtungen oder Behörden ihres Heimatlandes sowie bei Reisen nach Russland. Sie können aber auch versuchen, über Repressalien gegenüber in Russland gebliebenen Verwandten oder Bekannten Druck auszuüben. Generell scheuen die russischen Nachrichtendienste bei Bedarf auch vor Methoden wie Bedrohung und Erpressung nicht zurück.

Ableitung von Zielen aus Datenbanken

Es erscheint denkbar, dass Akteure auf Seiten beider Kriegsparteien Datenbanken, die Auskunft über das Russlandgeschäft von Unternehmen geben, auswerten und daraus Ziele zum Beispiel für Desinformations- oder Sabotageaktivitäten ableiten.

Handlungsempfehlungen

Cybersicherheit

Maßnahmen für Anwenderinnen und Anwender:

- 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, Bekannten oder Arbeitgeber(in). Deren E-Mail-Konten könnten ebenfalls gehackt worden sein.

Maßnahmen für IT-Verantwortliche:

- Verfolgen Sie die Entwicklungen weiter aufmerksam und passen Sie Ihre Schutzmaßnahmen bei Bedarf an. Das Bundesamt für Verfassungsschutz aktualisiert laufend seine Übersicht über die ihm vorliegenden Indicators of Compromise (IoCs). Die Liste stellt der Wirtschaftsschutz Ihnen auf Anfrage digital zur Verfügung, damit Sie Ihre Systeme selbständig auf mögliche Kompromittierung prüfen können.
- Von DDoS-Angriffen betroffene Unternehmen 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.

Verdacht von Ausforschungs- und Anbahnungsversuchen

Maßnahmen für Personalverantwortliche:

- Weisen Sie insbesondere neu eingestellte Beschäftigte mit russischer Staatsangehörigkeit auf die Möglichkeit von Anbahnungsversuchen hin und etablieren Sie Meldewege für Verdachtsfälle.
- 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. Das gilt insbesondere, wenn es zu konkreten Bedrohungen kommt.

Maßnahmen für Beschäftigte:

- Gehen Sie grundsätzlich diskret mit Informationen über Ihr Unternehmen, über Kolleginnen und Kollegen sowie über geschäftliche Zusammenhänge um. Besondere Vorsicht ist im Kontakt mit Ihnen unvertrauten Ansprechpartnerinnen und -partnern geboten.

- Nutzen Sie die Meldewege in Ihrem Unternehmen, wenn Sie den Verdacht haben, dass Sie Ziel eines Ausforschungs- oder Anbahnungsversuchs werden sollen oder bereits geworden sind. Das gilt insbesondere, wenn Sie konkreten Bedrohungen ausgesetzt sind.

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