Bundesamt für Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 01/2024 | 26. Juli 2024

Betreff | Schutz vor Sabotage (Nr. 2)

Ausgangslage

Sabotageakte durch fremde Staaten oder von extremistischer Seite können weitreichende Auswirkungen haben und zu schwerwiegenden Schäden führen. Das gilt besonders mit Blick auf Kritische Infrastrukturen (KRITIS) und KRITIS-nahe Unternehmen, die essenziell für ein funktionierendes Gemeinwesen sind. Der Sabotageschutz zählt daher zu den Kernaufgaben der Verfassungsschutzbehörden. Im Zuge ihrer Gefährdungsanalyse fallen regelmäßig Erkenntnisse über Einfallstore an, die der Vorbereitung und Unterstützung von Angriffen dienlich sind oder diese überhaupt erst ermöglichen. Es ist davon auszugehen, dass unter anderem ausländische Nachrichtendienste diese gezielt auskundschaften und zur Vorbereitung weiterer Maßnahmen ausnutzen. Das Ausmaß der Gefahr russischer Sabotageakte in Europa und Deutschland ist abhängig von der Lageentwicklung um den russischen Angriffskrieg gegen die Ukraine sowie von der Entwicklung des Konflikts zwischen Russland und dem Westen. Die seit 2023 europaweit beobachteten Fälle sowie vermehrte Hinweise auf mögliche Aktivitäten in Deutschland führen aktuell zu einer angepassten Bewertung: Es besteht eine erhöhte Gefährdung in Bezug auf Sabotageaktivitäten bzw. entsprechende Vorbereitungshandlungen in Deutschland.

Sachverhalte

Auf folgende potenzielle Einfallstore und Vorgehensweisen ist besonders zu achten:

Öffentlich zugängliche Informationen

Öffentlich zugängliche interne Dokumente, wie Anweisungen, Leitfäden und Gebäudepläne, geben zum Teil detailliert Auskunft über Abläufe, Kommunikationswege und weitere Unternehmensinterna. Flyer, Stellenausschreibungen, Broschüren und Websites enthalten zudem Hinweise auf eingesetzte Hard- und Software sowie häufig auch über das gesetzlich erforderliche Maß hinausgehende Kontaktinformationen. Profile von Beschäftigten in sozialen Netzwerken und insbesondere Karriere-

plattformen nennen Arbeitsschwerpunkte und Qualifikationen. Regelmäßig werden hier auch Anschriften und private Telefonnummern aufgeführt.

Ausspähung in Social Media

Es liegen Hinweise vor, wonach russische Nachrichtendienste gezielt Social-Media-Profile von Mitarbeitenden deutscher Unternehmen im Hinblick auf Meinungsäußerungen zum russischen Angriffskrieg gegen die Ukraine sowie zu anderen polarisierenden Themen ausgewertet haben sollen. Ziel soll es gewesen sein, Personen zu identifizieren, die für russische Einflussnahme- oder Anbahnungsversuche empfänglich sein könnten.

Port-, Service- und Schwachstellen-Scans

IP-Adressen oder IP-Adressbereiche eines Unternehmens sind kein Geheimnis und lassen sich oftmals allein durch Recherchen in öffentlichen Datenbanken ermitteln. Im Rahmen von Scans kann anschließend festgestellt werden, ob schwachstellenbehaftete oder schlecht konfigurierte Dienste auf dem System des Unternehmens ausgeführt werden.

Hacktivistische Cyberangriffe

Es sind weiter anlassbezogen Cyberangriffe von pro-russischen Hacktivismus-Gruppierungen auf Websites deutscher Behörden und Unternehmen festzustellen. Die Auswirkungen waren bis dato meistens zeitlich begrenzt und die betroffenen Websites nur vorübergehend nicht erreichbar.

Brandstiftung und Vandalismus durch Low-Level-Agents

Im europäischen Ausland wird derzeit in mehreren Fällen versuchter bzw. erfolgter Brandstiftung sowie in Bezug auf Vandalismus und Propagandaaktivitäten ermittelt, die auf russische Nachrichtendienste zurückzuführen sein könnten. Auch Sprengmittel scheinen als Einsatzmittel herangezogen zu werden. Die hierfür angeworbenen „Low-Level-Agents“ scheinen überwiegend jung, russischsprachig, ideologisch prorussisch und ungeschult zu sein sowie Interesse daran zu haben, durch die Ausübung einfacher Tätigkeiten schnell Geld zu verdienen. Die Rekrutierung erfolgt über soziale Medien und Messenger-Dienste kurzfristig zur Erfüllung konkreter Aufträge.

Bewertung

Auswertung offener Informationen durch Nachrichtendienste

Nachrichtendienste werten gezielt offen zugängliche Informationen aus und lassen sie in Handlungsempfehlungen an ihre operativen Kräfte einfließen – zum Beispiel zu Sabotage- oder Anwerbungszwecken. Auch andere Tätergruppierungen gehen auf diese Weise vor. Mit Hilfe von Kartenmaterial sind zum einen die genauen Örtlichkeiten von Infrastrukturen nachzuvollziehen. Zum anderen kann mit technischer Expertise ein Verständnis über die Funktionsweise erworben werden. Hiermit wiederum lassen sich Schwachstellen und damit Ansatzpunkte identifizieren, um physische und cybergestützte Sabotagehandlungen durchzuführen.

Störung von Abläufen und Kommunikation

Kenntnisse über Abläufe, Informationspflichten und Kommunikationswege ermöglichen eine Prognose über das Vorgehen beteiligter Stellen im Krisenfall. Hierdurch besteht die Möglichkeit, Notfallabläufe zu unterbrechen oder zumindest zu stören, zum Beispiel durch gezielte Falschmeldungen oder durch Überlastung von E-Mail-Servern. Die Veröffentlichung von grundsätzlich nicht öffentlich bekannten E-Mail-Adressen macht es Angreifern leichter, die passenden Angriffspunkte zu identifizieren.

Missbrauch von Kontaktinformationen und Onlineprofilen

Beschäftigte, die detaillierte Informationen in sozialen Netzwerken veröffentlichen, laufen Gefahr, zum Ziel von Cyberangriffen und realweltlicher Kontaktaufnahme zu werden. Insbesondere russischsprachige oder pro-russische Beschäftigte und solche, die sich in den sozialen Medien öffentlich eindeutig für oder gegen die Ukraine-Unterstützung des Westens positionieren, können ins Blickfeld russischer Nachrichtendienste rücken und sich mit Rekrutierungsversuchen konfrontiert sehen. Detaillierte Informationen über Erreichbarkeiten ermöglichen außerdem das Erstellen glaubhafter Spear-Phishing-E-Mails. Mittels E-Mail-Spoofing können zudem E-Mails mit maliziösem Anhang von vermeintlich vertrauenswürdigen Absenderadressen verbreitet werden.

Ausnutzung von Schwachstellen für das Eindringen in Netzwerke

Durch schwachstellenbehaftete und im Internet für jeden erreichbare Serverdienste bieten sich vielfältige Möglichkeiten für Angreifer, in ein Zielnetzwerk einzudringen. Insbesondere Systeme, die nicht auf einem aktuellen Patch-Stand sind, können verwundbar sein. Angreifer könnten Server unter Ausnutzung bereits bekannter Sicherheitslücken kompromittieren und sich – je nach Sicherung des Netzwerks – im schlimmsten Fall vollständig im Unternehmensnetzwerk ausbreiten.

Missbrauch von Angaben in Stellenausschreibungen

Mit Hilfe von Informationen aus Stellenausschreibungen können Angreifer abschätzen, mit welcher Netzwerkumgebung – zum Beispiel Sicherheitssysteme, -software, industrielle Kontrollsysteme (ICS) – sie es zu tun haben und sich bei ihrem Angriff darauf einstellen.

Ausnutzung unzureichender Gebäudeschutzmaßnahmen

Gerade ungeschulte Akteure sind darauf angewiesen, dass die bestehenden Gebäudeschutzmaßnahmen leicht überwunden werden können. Mit russischen Nachrichtendiensten in Verbindung gebrachte Brandstiftungen verdeutlichen die Gefahr von Sabotagehandlungen, die mit relativ geringem Aufwand umsetzbar sind.

Nutzung der weitergehenden Effekte von disruptiven Maßnahmen

Neben wertigen Objekten, die einen Bezug zur (militärischen) Unterstützung der Ukraine aufweisen, können auch solche Objekte zum Ziel russischer Nachrichtendienste werden, deren strategische Bedeutung für Russland sich nicht unmittelbar erschließt. Dies begründet sich darin, dass disruptive Maßnahmen wie Sabotageakte und Brandanschläge auch weitergehende Effekte wie Verunsicherung und Angst in Politik und Öffentlichkeit, aber auch in bestimmten Personengruppen und Wirtschaftssektoren auslösen können.

Handlungsempfehlungen

Maßnahmen für Sicherheitsverantwortliche:

- Richten Sie das materielle Schutzniveau von Firmenobjekten an der Wertigkeit der in Frage stehenden Waren oder Dienstleistungen aus. Schon einfache Gegenmaßnahmen im Rahmen des Gebäudeschutzes (z. B. angemessene Zaunanlagen, Kameraüberwachung, Wachschutz) sind hilfreich und sollten getroffen werden.
- Sensibilisieren und schulen Sie Ihre für Anwerbungsversuche besonders gefährdeten Mitarbeitenden regelmäßig mit Blick auf aktuelle Gefahren durch ausländische Nachrichtendienste und – aufgrund ihrer aggressiven Vorgehensweisen – insbesondere durch die Nachrichtendienste Russlands.
- Schulen Sie Ihre Mitarbeitenden regelmäßig mit Blick auf aktuelle Gefahren im Cyberraum, um ein Problembewusstsein dafür zu entwickeln, welche Informationen sich offen im Internet recherchieren lassen und welche Möglichkeiten des Missbrauchs sich daraus ergeben.
- Informieren Sie im Zuge der Prävention Beschäftigte auch über physische Sabotagehandlungen sowie darüber, dass diese mit Cyberangriffen abgestimmt sein können. Berücksichtigen Sie dabei vor allem solche Betriebsabläufe, deren Ausfall besonders schwerwiegende und/oder langfristige Folgen hätte.
- Etablieren Sie klare Meldewege. Kommunizieren Sie an die Beschäftigten, was im Notfall zu tun ist. Stellen Sie sicher, dass relevante Vorkommnisse aufgenommen und gemeldet werden.
- Bewerten Sie – bestehende und geplante – Veröffentlichungen neu und prüfen Sie diese hinsichtlich des Adressatenkreises kritisch. Hinterfragen Sie insbesondere Veröffentlichungen, die über das gesetzlich erforderliche Maß hinausgehen und unterlassen Sie diese im Zweifel. Sofern keine rechtlichen Veröffentlichungspflichten entgegenstehen, geben Sie sensible Inhalte nur restriktiv und an einen auf das notwendige Minimum beschränkten Adressatenkreis heraus („Need-to-know“-Prinzip).
- Schaffen Sie für sensible Informationen geeignete Übermittlungswege mit den jeweils notwendigen Vorkehrungen – zum Beispiel Zwei-Faktor-Authentifizierung (2FA) und verschlüsselte E-Mail-Kommunikation.
- Führen Sie in geeigneten Abständen Penetrationstests durch, um ein Feedback zum Umsetzungsstand der IT-Sicherheit aus Angreifer-Sicht zu erhalten. Sorgen Sie dafür, dass interne Serverdienste grundsätzlich nicht ohne Weiteres aus dem Internet erreichbar sind. Es bietet sich an, einen Zugriff lediglich aus dem Unternehmensnetzwerk oder über Virtual Private Network (VPN) zuzulassen. Wägen Sie ab, ob eine Verschleierung der eigenen IP-Adressen/-Adressbereiche durch Reseller möglich ist.

Maßnahmen für Personalverantwortliche:

- Wägen Sie bei Stellenausschreibungen kritisch ab, welche Informationen zwingend veröffentlicht werden müssen, um qualifiziertes Personal anzusprechen. Beschreiben Sie hierbei möglichst generische Anforderungen. Verzichten Sie, wo möglich, auf Details zu eingesetzter Soft- und Hardware.
- Stellen Sie in Ihrer Social-Media-Policy sicher, dass Beschäftigte Zurückhaltung bei Bezügen zu KRITIS-Bereichen üben. Falls keine solche Policy existiert, prüfen Sie eine Einführung.

Maßnahmen für Beschäftigte:

- Treten Sie in sozialen Netzwerken und Karriereplattformen möglichst datensparsam auf und üben Sie Zurückhaltung, wenn es um Bezüge zu KRITIS-Bereichen innerhalb Ihres Unternehmens geht.
- Greifen Sie, wo möglich, auf alternative und sicherere Kommunikationswege zurück. Dafür bietet sich zum Beispiel der oben beschriebene geschützte Bereich auf der Website an.
- Achten Sie auf Anzeichen physischer Sabotage und bringen Sie ungewöhnliche Vorfälle wie zum Beispiel Manipulationen, Drohnenüberflüge oder sonstige Ausspähversuche über die dafür vorgesehenen Meldewege zur Anzeige.
- Seien Sie sich darüber bewusst, dass im Falle passender persönlicher Voraussetzungen und entsprechender öffentlicher Meinungsäußerungen auch Sie in den Fokus russischer Nachrichtendienste geraten und für die Durchsetzung von deren Interessen instrumentalisiert werden könnten. Dies kann auch ohne Ihr Wissen über die konkrete Involvierung eines ausländischen staatlichen Akteurs erfolgen.

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