Bundesamt für
Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 04/2022 | 02.12.2022

Betreff | Schutz vor Sabotage

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. In der Vergangenheit waren bereits zahlreiche Aktivitäten festzustellen, bei denen es sich um Ausspähungen durch ausländische Nachrichtendienste handeln kann.

Sachverhalte

Auf folgende potenzielle Einfallstore ist besonders zu achten:

Präsentationen und Karten-material

Veröffentlichungen, die frei im Internet abrufbar sind, bieten häufig sehr detaillierte Informationen. Das gilt zum Beispiel für Präsentationen, die sich ursprünglich an Behörden und Marktteilnehmer richten, aber auch für Kartenmaterial, das Standorte von Anlagen oder Trassenverläufe abbildet.

Leitfäden und Ablaufpläne

Öffentlich zugängliche interne Dokumente wie Anweisungen und Leitfäden beschreiben detailliert Abläufe, Informationspflichten und Kommunikationswege. So finden sich in diesen Dokumenten zum Beispiel Vordrucke oder auch Funktionspostfächer, die im Störfall genutzt werden sollen.

Kontakt-informationen und Profile

Flyer, Broschüren und Websites enthalten Kontaktinformationen – häufig auch über das gesetzlich erforderliche Maß hinaus. Profile von Beschäftigten in sozialen Netzwerken und insbesondere Karriereplattformen nennen Arbeitsschwerpunkte und Qualifikationen. Regelmäßig werden zudem Anschriften und private Telefonnummern aufgeführt.

Port-, Service- und Schwach-stellen-Scans

IP-Adressen oder IP-Adressbereiche eines Unternehmens sind kein Geheimnis und lassen sich oftmals allein durch Recherche 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.

Stellenaus-schreibungen

Stellenausschreibungen für IT-Personal geben regelmäßig Auskunft über eingesetzte Hard- und Software, zum Beispiel Netzwerkkomponenten und Firewalls.

Bewertung

Auswertung offener Informationen durch Nachrichten-dienste

Nachrichtendienste werten gezielt offen zugängliche Informationen aus und lassen sie in Handlungsempfehlungen an ihre operativen Kräfte einfließen – zum Beispiel zu Sabotagezwecken. 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 Kontakt-informationen und Online-profilen

Detaillierte Informationen über Erreichbarkeiten ermöglichen das Erstellen glaubhafter Spear-Phishing-E-Mails. Mittels E-Mail-Spoofing können zudem E-Mails mit maliziösem Anhang von vermeintlich vertrauenswürdigen Absenderadressen verbreitet werden. Beschäftigte, die detaillierte Informationen in sozialen Netzwerken veröffentlichen, laufen Gefahr, zum Ziel von Cyberangriffen und realweltlicher Kontaktaufnahme zu werden.

Einfallstore 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.

Handlungsempfehlungen

Maßnahmen für (IT-)Sicherheitsverantwortliche:

- Sensibilisieren und schulen Sie Ihre Mitarbeiterinnen und Mitarbeiter regelmäßig mit Blick auf aktuelle Gefahren im Cyberraum. Ziel muss es sein, 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.
- 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.

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 des Bundesamtes für Verfassungsschutz (BfV):

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