Bundesamt für Verfassungsschutz

Sicherheitshinweis für die Wirtschaft | 01/2022 | 04.03.2022

Betreff | Krieg in der Ukraine

Ausgangslage

Im Zuge des Krieges in der Ukraine ist neben den militärischen Auseinandersetzungen auf ukrainischem Staatsgebiet auch im Cyberraum eine zunehmende Eskalation zu verzeichnen. Es besteht ein erhöhtes Risiko von Cyberangriffen gegen deutsche Stellen – insbesondere in Reaktion auf die jüngsten Sanktionen und militärischen Unterstützungszusagen.

Sachverhalte

Bedrohungen im Cyberraum

Seit dem 24. Februar 2022 gehen russische Streitkräfte gegen die Ukraine vor. Bereits im Vorfeld des militärischen Angriffs kam Schadsoftware gegen Ziele in der Ukraine zum Einsatz.

Im Januar 2022 gab das Microsoft Threat Intelligence Center eine Warnung vor der Malware *WhisperGate* heraus. Diese sei gegen Ziele in der Ukraine eingesetzt worden. Laut Microsoft soll *WhisperGate* infizierte Geräte funktionsuntüchtig machen.

Am 23. Februar 2022 haben mehrere Cybersicherheitsexperten bekanntgegeben, dass die Malware *HermeticWiper* gegen Ziele in der Ukraine eingesetzt werde. Laut SentiLabs greift die Malware Windows-Geräte an und manipuliert den Master Boot Record (MBR). Im Ergebnis könnten die Geräte nicht mehr gestartet werden.

Verschärfte Bedrohungslage

Aktuell ist eine rapide Zunahme von Meldungen zu Aktivitäten unterschiedlichster Gruppierungen im Cyberraum zu beobachten. Immer mehr bekannte Cybergruppierungen und sogenannte Hacktivisten positionieren sich öffentlich auf Seiten einer Kriegspartei. Die ukrainische Regierung rief explizit zur Cyberverteidigung des Landes auf.

Vermehrt werden im Netz sowohl Angriffstools als auch gehackte Daten veröffentlicht, die die Durchführung von Cyberangriffen unterstützen. Im Hinblick auf Operationen zur Veröffentlichung und/oder Manipulation erbeuteter Daten

geht insbesondere von russischen Cybergruppierungen eine Bedrohung aus. Insbesondere GHOSTWRITER hat in der Vergangenheit erfolgreich Daten von Mandatsträgerinnen und Mandatsträgern und sonstigen politischen Zielen erbeutet, um damit möglicherweise „Hack and Leak"-Operationen (erbeutete Daten werden – teils in manipulierter Form – öffentlich gemacht) und/oder „Hack and Publish"-Operationen (Falschinformationen werden über gekaperte reichweitenstarke Kommunikationskanäle veröffentlicht) vorzubereiten.

Desinformation

Das militärische Vorgehen Russlands wird zudem massiv von russischen Desinformationskampagnen begleitet. Staatliche Kommunikationskanäle verbreiten fortlaufend pro-russische und antiwestliche Narrative sowie Fake-News.

Bewertung

Es ist davon auszugehen, dass *WhisperGate* und *HermeticWiper* nicht die einzigen Fälle von Malware sind bzw. bleiben, die im Zuge des militärischen Vorgehens Russlands gegen die Ukraine zum Einsatz kommen. Bei länger anhaltenden und/oder sich verschärfenden Kampfhandlungen, muss davon ausgegangen werden, dass vermehrt auch Cyberwerkzeuge eingesetzt werden.

Deutschland als mögliches Ziel

In Reaktion auf die jüngsten Sanktionen und militärischen Unterstützungszusagen Deutschlands wächst auch das Risiko für russische Cyberangriffe gegen deutsche Stellen einschließlich Unternehmen. Es ist möglich, dass sich Cyber-Sabotageakte nicht nur gegen Unternehmen in den KRITIS-Sektoren, sondern auch gegen den politischen Raum sowie gegen militärische Einrichtungen, richten. Russische Dienste verfügen zweifelsohne über entsprechende Fähigkeiten und Tools, die genannten Bereiche erheblich und nachhaltig zu sabotieren. Cyberangriffe des Akteurs GHOSTWRITER gegen deutsche Abgeordnete belegen, dass es im Vorfeld des eigentlichen Angriffs Vorbereitungshandlungen gab, wie breit angelegtes Credential-Phishing über Phishing-Mails. Aufgrund erneuter, aktueller Angriffe von GHOSTWRITER im März 2022 gegen Personen in Deutschland ist besondere Vorsicht geboten. Derzeit werden private T-Online-Konten u.a. von der Absenderadresse *t-online.de@comcast.net* angephisht.

Im Rahmen sogenannter „Hack and Leak"-Operationen könnten erbeutete Daten, etwa von politischen Zielen, veröffentlicht oder manipuliert werden und für bevorstehende Desinformationskampagnen genutzt werden. Zudem besteht die Gefahr, dass Nachrichtenportale im Internet oder reichweitenstarke Social-Media-Konten etwa von Journalistinnen und Journalisten kompromittiert und Falschmeldungen darüber verbreitet werden könnten („Hack and Publish"-Operationen).

Gefahr von Spill-Over-Effekten und Kollateral-schäden

Die steigende Zahl an Cybergruppierungen und sogenannte Hacktivisten, die sich auf beiden Seiten des Konflikts positionieren, erhöht die Anzahl der beteiligten und fähigen Akteure im Cyberraum deutlich, wodurch die Wahrscheinlichkeit für Kollateralschäden erhöht wird. Es kann nicht ausgeschlossen werden, dass Ziele in Deutschland auch indirekt im Zuge von Spill-Over-Effekten und Kollateralschäden betroffen werden. Dies trifft insbesondere auf die Sektoren Energie, Telekommunikation, Transport, Finanzen, Medien und Rüstung zu.

Aktuelle IoCs

Unternehmen sollten die entsprechenden Entwicklungen aufmerksam beobachten und ihre IT-Sicherheitsmaßnahmen entsprechend 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.

Handlungsempfehlungen

Da die benannte Wiper-Malware nur kurze Zeit benötigt, um ein System zu zerstören, ist Prävention besonders wichtig:

- Weil der Angreifer für das Platzieren und die Ausführung der Malware eine Zugriffsmöglichkeit auf das System besitzen muss, ist es dringend empfehlenswert, mögliche Angriffsvektoren zu minimieren. Es ist sorgfältig zu überlegen, welche Vorgänge und Systeme aktuell für die Gewährleistung der Funktionalitäten eines Unternehmens unbedingt erforderlich sind.
- Backups müssen in regelmäßigen Abständen angefertigt und anschließend von den betroffenen Systemen getrennt aufbewahrt werden.
- Bekannte Sicherheitslücken müssen durch das Einspielen vorhandener Update-Patches geschlossen werden und sind somit als Angriffsvektor verschlossen.
- Intrusion Detection Management Systeme (IDMS) sollten in der Lage sein, die Malware zu erkennen und zu blockieren. Dafür muss aber dem IDMS die Berechtigung gegeben werden, das Starten und Ausführen entsprechender Prozesse nicht nur zu protokollieren, sondern diese auch sofort zu stoppen und Dateien in Quarantäne verschieben zu können.
- Unbekannte oder nicht mehr verwendete Nutzer müssen entfernt und Berechtigungen für Nutzer auf ein Minimum reduziert werden.
- Zum Schutz vor (Credential-)Phishing-Angriffen müssen Konten nach Möglichkeit mit Multi-Faktor-Authentifizierung geschützt werden.
- 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.
- Die aktuelle Bedrohungslage muss den Mitarbeiterinnen und Mitarbeitern bekannt gemacht werden, um ein Gefährdungsbewusstsein zu schaffen.
- Etablierung und Bekanntmachung von Meldeprozessen bei Auffälligkeiten und Sicherheitsvorfällen innerhalb des Unternehmens sowie der Ansprechbarkeiten von Behörden.

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)228 – 99 – 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