# Verfassungsschutz warnt vor Cyberangriffen

**cebra GmbH - new technologies**
Sankt Martin Str. 9, 84539 Ampfing
Telefon: +49 8636 69 76 67
E-Mail: info@cebra.it
Webseite: https://www.cebra.it

## Allgemeines

| | |
|---|---|
| Autor: | Christian Sigl |
| Version: | 2.0 |
| Versionsdatum: | 2022-09-15 |

## Sicherheitshinweise

2022-03-04-Sicherheitshinweis.pdf

## Bedrohungslage

Die Bedrohungslage im Bereich von Cyberangriffen hat sich auch durch den Krieg in der Ukraine extrem verschärft. Die Lage um die Sicherheit in der Informationstechnik ist ernst. Aus diesem Grund hat der Verfassungsschutz Sicherheitshinweise veröffentlicht. Es besteht ein erhöhtes Risiko von Cyberangriffen gegen deutsche Einrichtungen und besonders auch gegen Unternehmen. Sie sollten die Entwicklungen aufmerksam beobachten und Ihre IT-Sicherheitsmaßnahmen entsprechend anpassen. Mehrere Schadprogramme (zum Beispiel WhisperGate, HermeticWiper) machen Geräte funktionsuntüchtig oder werden zur Manipulation von Daten verwendet.

Da die benannte Wiper-Malware nur kurze Zeit benötigt, um ein System zu zerstören, ist Prävention besonders wichtig – jeder kann betroffen sein.

Das Bundesamt für Verfassungsschutz gibt folgende Handlungsempfehlungen:

- 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.

Den kompletten Sicherheitshinweis des Bundesamtes für Verfassungssicherheit finden Sie im Anhang. Hier sind auch Kontaktdaten für Meldungen oder Rückfragen aufgeführt.

Nehmen Sie diesen Hinweis bitte sehr ernst und treffen Sie entsprechende Vorkehrungen.

---

Revision #2
Created 2022-09-15 14:19:49 UTC by Christian Sigl
Updated 2022-09-15 14:23:30 UTC by Christian Sigl