Ukraine-Krieg: Erhöhte Bedrohungslage im Cyberraum

Warum ein Cyberangriff auf die Ukraine die Fernwartungssysteme von Windkraftanlagen in Europa lahmlegen kann. Worauf Betriebe nun achten sollten.

23.03.2022, 14:50

© ISSARONOW, ADOBESTOCK

Aktuell gibt es eine Zunahme der Aktivitäten von unterschiedlichen Gruppierungen im Cyberraum.

Es war der Hack eines Kommunikationssatelliten eines US-amerikanischen Satelliteninternetbetreibers, der gleich am ersten Tag des Ukraine-Krieges die Kommunikation ukrainischer Armee- und Sicherheitsbehörden stören sollte. Betroffen war aber nicht nur die Kommunikation der Ukraine, sondern auch zehntausender Satellitenmodems von Kunden in ganz Europa – von Frankreich bis Tschechien – , die über den betroffenen Satelliten mit Breitbandinternet versorgt werden. So wurden beispielsweise Modems für die Fernwartung von Windkraftanlagen außer Gefecht gesetzt. „Das zeigt aufs Deutlichste, wie vernetzt und verletzlich unsere Kommunikations- und IT-Systeme sind“, so Gerald Kortschak, Sprecher der IT-Security-Experts-Group der Fachgruppe UBIT der WKO.

Starke Vernetzung birgt Gefahren

Die Bundessparte Information und Consulting warnt derzeit vor einer sehr hohen allgemeinen Gefährdungslage im Cyberraum. Denn aktuell sei eine starke Zunahme von Meldungen zu Aktivitäten unterschiedlichster Gruppierungen im Internet zu beobachten und zahlreiche bekannte Cybergruppen wie etwa Anonymous positionieren sich öffentlich auf Seiten einer der beiden Kriegsparteien. Die ukrainische Regierung hat außerdem ausdrücklich zur Cyberverteidigung des Landes aufgerufen und es werden im Netz vermehrt Angriffstools sowie gehackte Daten veröffentlicht, die zur Durchführung von Cyberangriffen dienen. „Auch der kriminelle Cyberuntergrund sowohl in der Ukraine als auch in Russland, der bisher mit Internet-Betrug und Phising Geld erbeutete, wendet sich nun verstärkt den Kriegsparteien zu", berichtet Kortschak. In der Folge habe der klassische Internetbetrug abgenommen. Nun beobachte man aber vielfach Phising-Mails mit betrügerischen Spendenaufrufen oder auch Aufrufe, sich online am Krieg zu beteiligen. Derartige Aktivitäten können strafrechtlich relevant sein (z.B. Hacking oder DDoS-Angriffe) oder zu ungeahnten Folgen führen (z.B. Infiltration des Firmennetzwerkes durch Schadsoftware bis hin zu Vergeltungsmaßnahmen der Kriegsparteien).

Prävention & Konsequenzenmanagement

„Unternehmen sollten verdächtige IT-Kommunikation verstärkt beobachten und Mitarbeiter im Umgang mit derartigen E-Mails und Nachrichten schulen", so Kortschak. „Wichtig ist es aber auch, nicht nur an die Prävention zu denken, sondern auch verstärkt ans Konsequenzenmanagement – wie kann ein Betrieb weitergeführt werden, wenn die IT oder die Server trotz aller Vorsorgemaßnahmen dennoch ausfallen?"

Tipps für die Sicherheit

- Antivirusprogramme
- Firewall
- Multi-Faktor-Authentifizierung
- zügiges Patchen und automatische Updates
- aktuelle Software
- Backup-/Restore-Prozesse und offline Backups
- erweitertes Logging

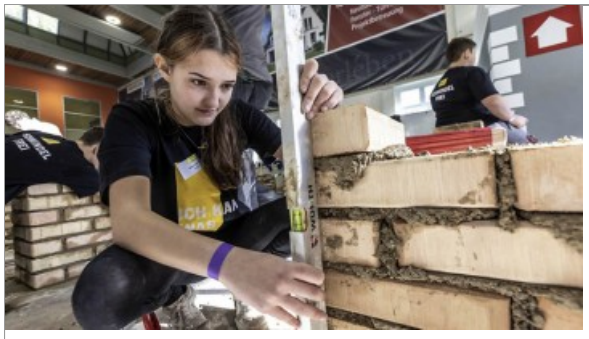
WKO-Cyber-Security-Hotline: 0800 888 133

Von Petra Mravlak

Das könnte Sie auch interessieren

Blackout: Was passiert, wenn's passiert

Jürgen Roth, Bundesobmann des Energiehandels, im Interview über Präventionsmaßnahmen und Notfallpläne für Unternehmen im Falle eines Blackouts. › mehr



Rekord-Teilnahme beim Bau-Lehrlingscasting

145 Jugendliche kamen am 24. November 2022 in die Bauakademie Übelbach, um beim „Lehrlingscasting“ mit anschließendem Firmen-Speed-Dating ihr Talent unter Beweis zu stellen.

› mehr

Spannende Einblicke ins Online-Marketing

Rund 100 HAK-Schüler aus der ganzen Steiermark bekamen kürzlich an der FH Campus 02 neue Blick- winkel auf die Welt des digitalen Marketings. › mehr