**Ministerium des Innern
des Landes Nordrhein-Westfalen**

Ministerium des Innern des Landes NRW, Postfach 103013, 40021 Düsseldorf

Unternehmen und Einrichtungen
im Bereich KRITIS

Aktenzeichen
(bei Antwort bitte angeben)
613/31 - 71.35.02 - 109517 -
313378/2023

Telefon 0211 871-2899

Mögliche Cyberangriffe auf PLC-Infrastruktur im Bereich von KRITIS
Cyberabwehr des Verfassungsschutzes Nordrhein-Westfalen

Sehr geehrte Damen und Herren,

im Rahmen unserer gesetzlichen Aufgabenerfüllung warnen wir vor Cyberangriffen, die vermutlich von ausländischen Staaten gesteuert werden. Die Angreifer verfolgen in der Regel keine finanziellen Interessen, agieren höchstprofessionell und handeln unauffällig, eher lang- als kurzfristig. Da eine Kompromittierung durch die Betroffenen oftmals über einen großen Zeitraum unbemerkt bleibt, werden die Angreifer auch als fortgeschrittene, andauernde Bedrohen - „Advanced Persistent Threat“ oder „APT“ bezeichnet.

Aus aktuellem Anlass warnen wir Sie vor der Gruppierung „CyberAv3ngers“, einer vermutlich den Islamischen Revolutionsgarden des Iran nahestehenden Hacktivismus-Gruppierung. Besagte Gruppierung führt mindestens seit November 2023 Cyberangriffe auf speicherprogrammierbare Steuerungen (PLC) des israelischen Herstellers „Unitronics“ aus. Die in diesem Kontext bereits entdeckten Angriffe zielen primär auf KRITIS-Einrichtungen im Bereich des Wasser- und Abwasser-Sektors ab. Bei bisher erfolgten Angriffen hinterließen die Angreifer folgendes Defacement:

*„You have been hacked, down with Israel.
Every equipment ‚made in Israel‘ is CyberAv3ngers legal target.“*

Dienstgebäude:
Friedrichstraße 62-80
40217 Düsseldorf

Lieferanschrift:
Fürstenwall 129
40217 Düsseldorf

Telefon 0211 871-2821
Telefax 0211 871-2980
kontakt.verfassungsschutz@im1.nrw.de
www.im.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 732, 736, 835, 836, U71, U72, U73, U83
Haltestelle: Kirchplatz

Im Anhang finden Sie den den Joint Cybersecurity Advisory der US-Amerikanischen Cybersecurity and Infrastructure Security Agency (CISA) mit präventiven Handlungsempfehlungen und einer detaillierten Beschreibung des Angreifervorgehens.

Weitere Informationen zu dem Sachverhalt erhalten Sie ebenfalls auf der Webseite des britischen National Cyber Security Centre [*https://www.ncsc.gov.uk/news/ncsc-statement-following-exploitation-of-unitronics-programmable-logic-controllers]* sowie auf der Webseite des estnischen Rundfunks ERR [*https://news.err.ee/1609181887/paper-cyber-attack-targets-israeli-made-tech-used-by-estonian-boiler-houses*].

Falls Sie Hinweise zu diesem Sachverhalt haben, sind wir für eine Rückmeldung dankbar. Bei Fragen stehen wir gerne zur Verfügung.

Cyberabwehr des Verfassungsschutzes Nordrhein-Westfalen
cyberabwehr@im1.nrw.de
0211/871-2899

Anlage:
CISA_Advisory_AA23-335A.pdf