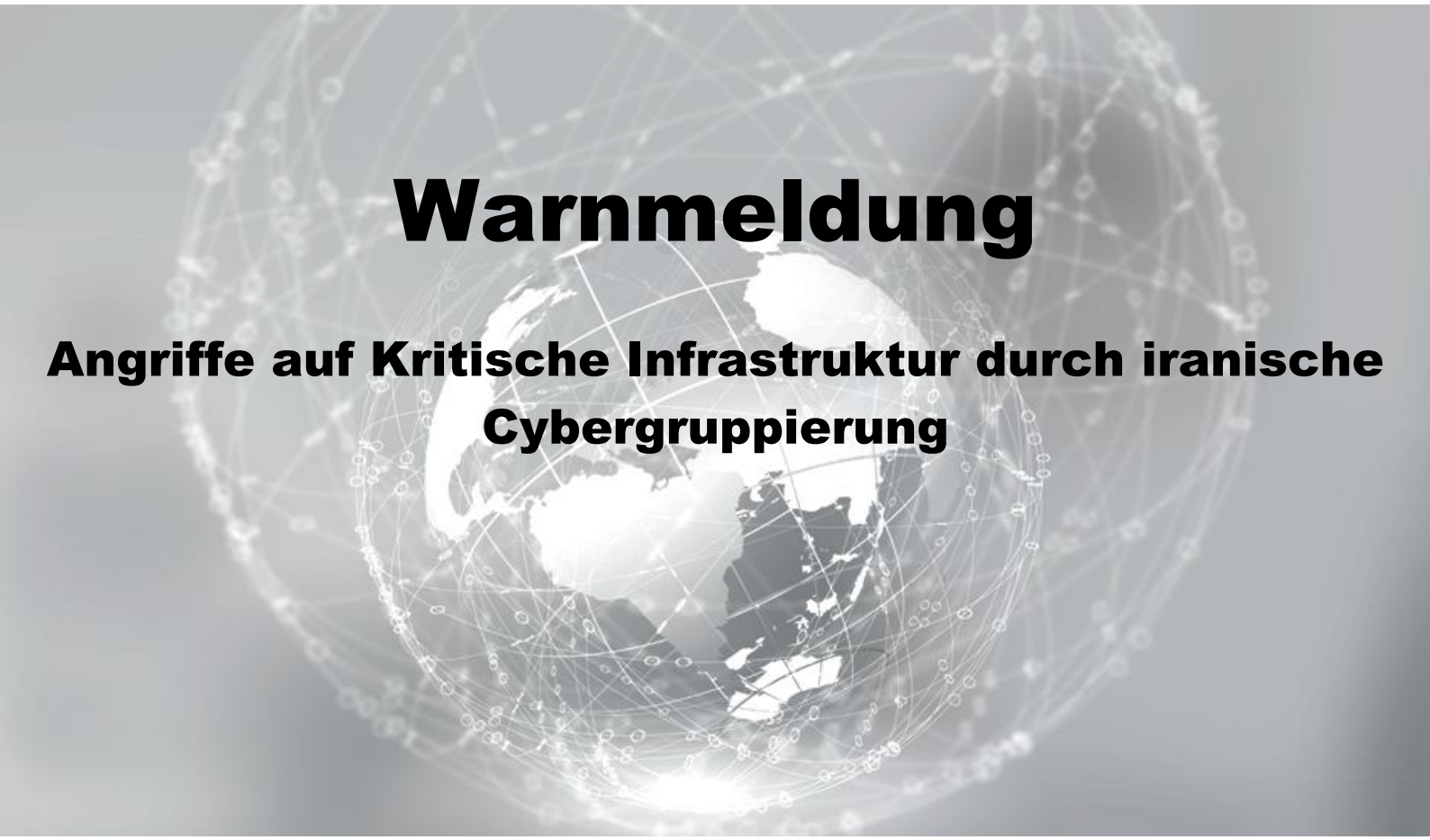
TLP:CLEAR

Verfassungsschutz
Baden-Württemberg

Beobachten.
Informieren.
Schützen.

Warnmeldung

Angriffe auf Kritische Infrastruktur durch iranische Cybergruppierung



Datum
13. Dezember 2023

Ausgabe
Dezember 2023

Einstufung
TLP:CLEAR

Landesamt für Verfassungsschutz
Baden-Württemberg
Cyberabwehr
Taubenheimstraße 85A • 70372 Stuttgart
Telefon 0711 9544 4985
E-Mail Cyberabwehr@lfvbw.bwl.de

TLP:CLEAR

Verfassungsschutz
Baden-Württemberg

Beobachten.
Informieren.
Schützen.

Warnmeldung zu einer aktuellen Angriffskampagne der Gruppierung CyberAv3ngers

1. Sachverhalt

Seit mindestens November 2023 greift die iranische Cyber-Gruppierung CyberAv3ngers Einrichtungen aus dem Bereich der Kritischen Infrastruktur an. Der staatlich gesteuerte Akteur wird den iranischen Revolutionsgarden zugeordnet. Ziel der Angriffe sind dabei speicherprogrammierbare Steuerungen (programmable logic controller) des israelischen Herstellers Unitronics. Die hier bekannt gewordenen Angriffe zielen auf KRITIS Einrichtungen ab. Insbesondere auf Unternehmen der Wasser- und Abwasserwirtschaft, die entsprechende IT-Komponenten des israelischen Herstellers im Einsatz haben.

CyberAv3ngers greift zunächst die über das Internet verfügbaren Systeme mittels Brute-Force-Attacken an. Meist sind die Systeme nur mittels Standardnutzerdaten und Passwörter geschützt. Aufgrund dessen kann die Sicherheitsbarriere schnell und mit einfachsten Mitteln überwunden werden. Haben die Angreifer die Kontrolle übernommen, wird die Benutzeroberfläche des Steuerungssystemes verändert. Durch die Veränderung der Oberfläche erscheint beim Aufruf der Seite der folgende Schriftzug: „You have been hacked, down with Israel. Every equipment ‘made in israel‘ is CyberAv3ngers legal target.“
Zwar sind mit dem so gewonnen Zugang auch tiefergreifende Manipulationen am System möglich, jedoch wurden solche bislang nicht festgestellt.

Die Gruppierung hat bereits Unternehmen in Israel, den Vereinten Staaten und auch in Europa erfolgreich angegriffen. Alle Unternehmen hatten Komponenten des oben genannten Herstellers verbaut. Zum aktuellen Zeitpunkt liegen der Cyberabwehr keine Informationen vor, dass durch solche Cyberangriffe auch deutsche Stellen betroffen sind, auszuschließen ist es jedoch nicht.

2. Handlungsempfehlungen

Da sich CyberAv3ngers nicht zwingend auf die Produkte von Unitronics beschränkt und auch Angriffe auf andere KRITIS-Sektoren möglich sind, empfehlen wir folgende Schutzmaßnahmen:

- Vermeiden Sie es Standardpasswörter zu verwenden.
- Nutzen Sie Multifaktorauthentifizierung, wo immer es möglich ist
- Sichern Sie Remote-Zugriffe ab.
- Halten Sie Software auf dem aktuellen Stand und spielen Sie regelmäßige Sicherheitsupdates auf.

Über unsere Cloud stellen wir Ihnen ein ausführliches Joint Cybersecurity Advisory zur Vorgehensweise der Angreifer und entsprechende IoCs zur Verfügung. Darüber hinaus sind im Schreiben auch Beschreibungen zu empfohlenen Mitigationsmaßnahmen enthalten.

https://cloud.landbw.de/index.php/s/8sAzaJNg2SZbD9P

3. Kontakt

Sollten Sie entsprechende Anhaltspunkte bzw. eine Betroffenheit feststellen, steht Ihnen die Cyberabwehr des Landesamtes unter den genannten Erreichbarkeiten zur Verfügung. Bei Kontaktaufnahme kann Ihnen seitens des Verfassungsschutzes Vertraulichkeit zugesichert werden.

Telefon 0711 9544 4985

E-Mail Cyberabwehr@lfvbw.bwl.de

Zum Senden verschlüsselter E-Mails finden Sie **hier** unseren öffentlichen PGP-Schlüssel.

Verfassungsschutz
Baden-Württemberg

Beobachten.
Informieren.
Schützen.

4. Weitergabevorbehalt

TLP:CLEAR Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Hinweis:
TLP:CLEAR entspricht der Kennzeichnung TLP:WHITE der früheren Version 1.0 des TLP.