BSI

Analyse zu KRITIS-Angriffen

[15.12.2025] Prorussische Hacktivisten setzen laut einer neuen internationalen Analyse zunehmend auf einfache Angriffsmethoden, um Kritische Infrastrukturen zu stören. Die Gemeinschaftspublikation mehrerer Sicherheitsbehörden zeigt, wo Betreiber besonders wachsam sein müssen.

Einfache technische Mittel reichen mitunter aus, um erhebliche Schäden in Kritischen Infrastrukturen anzurichten. Wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) in einem gemeinsam mit US-Behörden und weiteren internationalen Partnern herausgegebenen Papier zeigt, nutzen prorussische Hacktivisten im Rahmen der hybriden Kriegsführung auch wenig komplexe Vorgehensweisen, um in Systeme einzudringen und Abläufe zu stören.

Dem Dokument zufolge agieren verschiedene Gruppierungen mit unterschiedlichen Zielen, häufig jedoch mit Blick auf Fernwartungszugänge oder ungeschützte Steuerungs- und Automatisierungssysteme der Operational Technology. Beschrieben werden Fälle, in denen Angreifer über solche Schnittstellen tief in Anlagen gelangten und damit ein beträchtliches Gefährdungspotenzial erzeugten. Die Publikation bietet zudem Hinweise für Betreiber und Hersteller, wie sich typische Angriffspfade frühzeitig erkennen lassen und welche organisatorischen sowie technischen Maßnahmen dabei unterstützen.

Auch außerhalb des KRITIS-Sektors geraten Unternehmen und öffentliche Einrichtungen ins Visier. Den beteiligten Behörden zufolge sollten Institutionen ungewöhnliche Systemaktivitäten ernst nehmen und ihre Infrastruktur konsequent absichern. Dazu gehören segmentierte Netzwerke, Firewalls, Intrusion-Detection-Systeme und vor allem eine lückenlose Aktualisierung von Hard- und Software. Ebenso betont wird die Notwendigkeit von Notfall- und Wiederherstellungsplänen, um nach einem Vorfall rasch wieder handlungsfähig zu sein.

(th)

Stichwörter: Informationstechnik, Bundesamt für Sicherheit in der Informationstechnik (BSI), KRITIS