Cyber-Angriffe auf deutsche Energieversorger

Demnach nutzen die Angreifer unterschiedliche Methoden, die ihnen in einigen Fällen Zugriff auf Büro-Netzwerke der Unternehmen ermöglicht haben. In mehreren Fällen konnten zudem Spuren der Angreifer nachgewiesen werden, die auf Angriffsvorbereitungen zur späteren Ausnutzung hindeuten. Derzeit liegen keine Hinweise auf erfolgreiche Zugriffe auf Produktions- oder Steuerungsnetzwerke vor.

Dazu erklärt BSI-Präsident Arne Schönbohm:

> *„Diese Angriffe zeigen, dass Deutschland mehr denn je im Fokus von Cyber-Angriffen steht. Dass bislang keine kritischen Netzwerke infiltriert werden konnten, zeigt, dass das IT-Sicherheitsniveau der deutschen KRITIS-Betreiber auf einem guten Level ist. Das ist auch ein Verdienst des IT-Sicherheitsgesetzes. Die bekanntgewordenen Zugriffe auf Büro-Netzwerke sind aber ein deutliches Signal an die Unternehmen, ihre Computersysteme noch besser zu schützen. Diese Entwicklung offenbart, dass es womöglich nur eine Frage der Zeit ist, bis kritische Systeme erfolgreich angegriffen werden können. Wir müssen daher das IT-Sicherheitsgesetz fortschreiben, so wie es bereits im Koalitionsvertrag der Bundesregierung festgehalten wurde. Die Bedrohungslage im Cyber-Raum hat sich in den vergangenen Monaten deutlich zugespitzt und es gibt keinen Grund zur Annahme, dass sie sich entspannen wird“.*

Bereits im Juni 2017 hatte das BSI eine Warnung an mehrere hundert Unternehmen aus der Energiebranche herausgegeben, die Handlungsempfehlungen zum Schutz der Netzwerke enthalten hatte. Zum damaligen Zeitpunkt waren noch keine erfolgreichen Angriffe in Deutschland bekannt. Über das Nationale Cyber-Abwehrzentrum findet derzeit die koordinierte Fallbearbeitung mit anderen Behörden auf Bundes- und Landesebene statt.

Anmerkung der Redaktion: Man mag sich gar nicht ausdenken, welche weichen Ziele die sog. Smart Meter bieten, wenn deren Einbau erstmal großräumig vollzogen ist. Marc Elsbergs Bestseller „Blackout“ bietet dazu spannende Aufklärung an. Hier bestellen