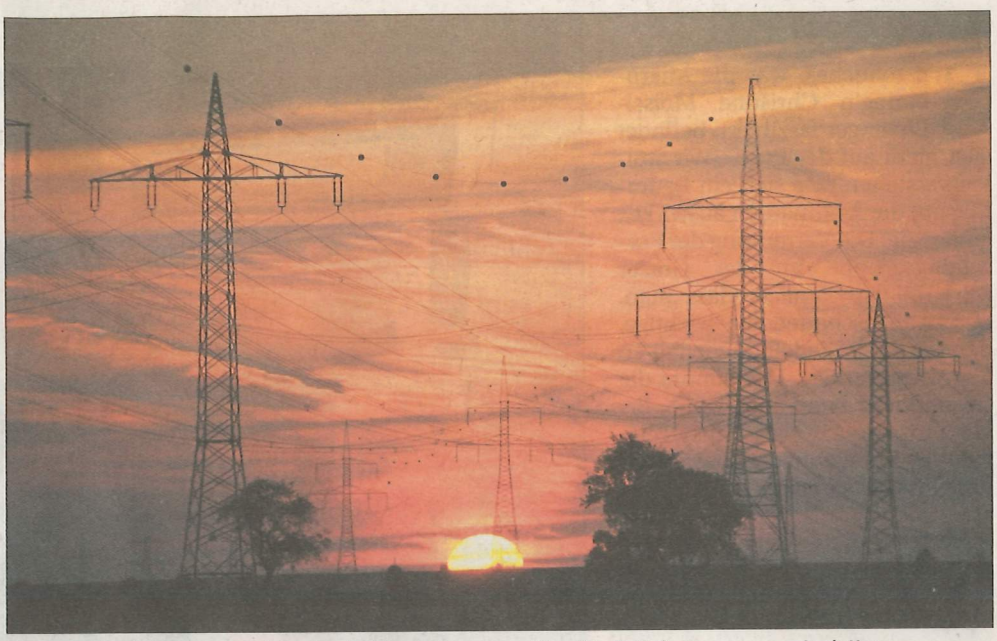
Den Hackern einen Schritt voraus

IT-Sicherheit. Der Informatiker Edgar Weippl rechnet Bedrohungsszenarien für kritische Infrastruktur und Industrieanlagen durch. Die Erkenntnisse daraus fließen in deren Schutz.

VON CORNELIA GROBNER

Bitcoin ist ein Stromfresser. Und kein kleiner. Die Kryptowährung generiert derzeit einen etwa so hohen Stromverbrauch wie ein mittelgroßes europäisches Land. Wegen ihres dezentralen Charakters gibt es aber keine offizielle Statistik, sondern lediglich Schätzungen. Bedeutet das eine neue Gefahr für unsere Stromnetze – zum Beispiel, wenn durch manipulierte Vorgänge während der Bitcoin-Prozesse in deren Frequenz eingegriffen wird? „Derzeit ist es noch nicht gefährlich", sagt Edgar Weippl, der sich mit Blockchain, der Technologie hinter der virtuellen Währung Bitcoin, beschäftigt und gestern, Freitag, bei einem Arbeitskreis des Forums Alpbach, der sich dem Schutz kritischer Infrastrukturen widmete, gesprochen hat. Er ist Forschungsleiter am SBA Research, an dem man als Kompetenzzentrum auch oben erwähnte Forschungsfragen der IT-Sicherheit bearbeitet.



Unsere optimierten Stromnetzwerke sind besonders angreifbar für digitale Frequenzmanipulation. [pixabay.com]

Bitcoin und Fabriken als Zielscheibe

Grundsätzlich müsste für ein Blackout, dem plötzlichen und lang anhaltenden Ausfall des Stromnetzes, der Stromverbrauch innerhalb weniger als einer halben Minute über ein großes Gebiet hinweg hochgefahren werden: „Das Netz in Österreich braucht etwa dreißig Sekunden, um so eine Veränderung auszugleichen. Davor gehen die Kraftwerke aus Sicherheitsgründen offline. Es kommt zum Blackout." Das Szenario sei nur dann plausibel, wenn eine große Anzahl an smarten Geräten wie Kühlschränken und Laserdruckern durch ein Schadprogramm dazu gebracht würden, synchronisiert innerhalb von wenigen Sekunden möglichst viel Strom zu verbrauchen. „Je mehr smarte Geräte, desto größer wird die Gefahr", so Weippl. Ein „bösartiger" oder gehackter Betreiber eines Mining-Pools – dabei handelt es sich um einen organisierten Verband von Kryptointeressierten, vergleichbar mit Spielgemeinschaften beim Lotto – könnte durch falsche synchronisierte Befehle an die Mitglieder ebenfalls den Stromverbrauch erhöhen. Diese Situation hat Weippl mit seinen Kollegen durchgerechnet und gibt Entwarnung: „Derzeit reicht die Last dazu nicht aus." Da die Weiterentwicklung in dem Bereich ungewiss ist, seien Prognosen, wann Bitcoin eine reelle Gefahr werden könnte, seiner Meinung nach aber unseriös.

Er verwehrt sich gegen dystopische Verschwörungstheorien, aber: „Es ist wichtig zu erkennen, wie wesentlich Stromversorgung ist und wie abhängig wir mittlerweile davon sind. Ohne Google-Maps findet man heute nirgends mehr hin, wer hat schon noch Landkarten?" Langfristig über die Schaffung von regionalen Inseln mit Energieautonomie nachzudenken sei in jedem Fall sinnvoll.

Im Lauf der Jahre sind IT-Sicherheitsprobleme und Hackerangriffe gewandert: von der Softwareentwicklung über die Mobiltelefonie zur Automobilindustrie. Als nächsten logischen Schritt könnten große Industrieanlagen ins Visier geraten. Weippl will darauf nicht warten, sondern sich schon vorab gegen mögliche Angriffe auf Schwachstellen wappnen. Seit Anfang des Jahres leitet er das dafür gegründete Christian-Doppler-Labor für die Verbesserung von Sicherheit und Qualität in Produktionssystemen der TU Wien.

> „Je effizienter und zentralisierter Systeme werden, desto stärker hängen wir davon ab."
>
> Edgar Weippl, Informatiker, Technische Universität Wien

Industrielle Produktionssysteme wie Stahlwerke kontrollieren leistungsstarke Prozesse und gewährleisten spezielle Standards in Hinsicht auf Sicherheit und Umweltschutz. Durch die zunehmende Digitalisierung werden diese Produktionssysteme nach und nach an das Internet angeschlossen. „Das hat große Auswirkungen auf die Sicherheit", erklärt Weippl. „Automationstechnik, mechanische Planung, Hydraulikplanung – alle verwenden unterschiedliche Softwaretools, deren Integration verbesserungswürdig ist."

Zudem ist in dieser Branche viel Wissen nicht festgeschrieben, sondern an einzelne Mitarbeiter gebunden. Da man auch zunehmend an verschiedenen Standorten produziert und lokale Subunternehmer einbezogen werden, ergeben sich deshalb Sicherheitslücken beim Austausch von Information. Weippl und sein Team wollen nun herausfinden, wie anomales und möglicherweise gefährliches Verhalten im Produktionsprozess erkannt werden kann. [Luiza Puiu]