# Rüsten gegen den Riesen-Blackout

## Kritische Infrastruktur ist vor Cyberangriffen unzureichend geschützt / Karlsruher Forum erörtert Sicherheit im Netz

*Von unserem Redaktionsmitglied Alexei Makartsev*

**Karlsruhe.** Er hat mit diesem Anruf gerechnet. Trotzdem zuckt Eberhard Oehler zusammen, als er die bekannte Stimme in der Leitung hört: „Bist du am Computer? Dann lese ich dir deine E-Mails vor". Ein Hacker ist in das Netz der Stadtwerke Ettlingen (SWE) eingedrungen. „Ein Klick auf die Enter-Taste hätte genügt, um die gesamte Stadt auszuschalten", erinnert sich der SWE-Geschäftsführer an die Extremsituation. Dieser eine finale „Klick" kam nicht, weil die Cyberattacke auf das Versorgungsnetz nur ein Test war und der „Bösewicht" keine bösen Absichten hegte.

„Nach nur 26 Minuten hatte er das Passwort unseres Softwarelieferanten geknackt. Nach vier Stunden dann auch das Passwort des IT-Administrators",

### Plünderungen nach drei Tagen ohne Strom

erinnert sich Oehler vier Jahre später an den simulierten Angriff auf die Strom-, Wasser- und Gasversorgung, dem seine Zentrale schutzlos ausgeliefert war. Und der Gastredner bei der Tagung des Karlsruher Forums für Kultur, Recht und Technik sorgt beim Publikum mit einer beunruhigenden Erkenntnis für Stirnrunzeln: Das kleine Ettlingen wäre damals nach einer Stunde wieder am Netz gewesen. „In Karlsruhe hätte man aber keine Chance, im Angriffsfall die großen Netze händisch zu bedienen".

Die Tagung des Forums im Zentrum für Kunst und Medien (ZKM) am Donnerstag trägt den abstrakt anmutenden Titel „Zwischen Selbstbestimmung und Fremdnutzung" und dreht sich um die Probleme der Sicherheit in digitalen Infrastrukturen. Da wäre zunächst die Gefahr des sogenannten „Blackouts" der wichtigen Versorgungsnetze nach einem Internet-Angriff. Laut SWE-Chef Oehler ist sie derzeit sehr präsent: „Wir bekommen permanent Phishing-Mails, und wenn wir einmal nicht aufpassen, kann das System durch Trojaner infiziert werden, ohne dass man es merkt". Und dann? Der Fachmann zitiert aus einer Prognose, wonach es nach drei Tagen ohne Wasser und Strom zu Plünderungen kommen könnte. Erschwerend käme hinzu, dass heute rund 270 weitere Stadtwerke in Deutschland mit derselben Software arbeiten würden. „Wenn ein Hacker bei uns eindringt", führt Oehler weiter aus, „könnte er auch die Nachbarnetze erfolgreich angreifen. Und wenn dann zehn Netze auf einmal ausfallen, entsteht ein Dominoeffekt, den die Kraftwerke nicht mehr ausgleichen können."


*DIE COMPUTER WERDEN IN UNSERE KÖRPER HINEINWACHSEN, prophezeit Constanze Kurz bei der Tagung des Karlsruher Forums im ZKM. Umso wichtiger sei es, den Schutz vor den Hackerattacken zu verbessern, sagt die Berliner Informatikerin.* *Foto: Hora*

Die Cyber-Sicherheitslage in der deutschen Energieversorgung sei „katastrophal", warnt der Fachmann und beruft sich auf eine Umfrage des Zentrums für Europäische Wirtschaftsforschung (ZEW) bei den Unternehmen in diesem Bereich: Lediglich 28 bis 40 Prozent hätten angegeben, gegen die Netz-Angriffe auf ihre Steuerungssoftware gut geschützt zu sein. Zumindest in Ettlingen scheint man aus dem „Test-Hack" die nötigen Lehren gezogen zu haben. So bezieht Oehler alle Mitarbeiter, „auch die Reinmachefrau", ins Sicherheitsmanagement mit hinein und betrachtet jeden Tablet-Computer bei der SWE als eine potenzielle Gefahrenquelle. Seine Bilanz: „Auf Störungen im Netz können wir heute viel schneller reagieren."

Der „digitale Krieg" im Internet fügt jedoch nicht nur der globalen Wirtschaft einen Milliardenschaden zu. Die immer raffinierteren Angriffe von kriminellen und staatlich bezahlten Hackern gelten auch den Regierungen und Normalverbrauchern. Das macht bei der Tagung des Karlsruher Forums im ZKM die Berliner Datenschutz-Expertin und Sprecherin des Chaos Computer Clubs (CCC), Constanze Kurz, klar. Sie spricht von den transatlantischen Datenleitungen, durch die heute der deutsche Internetverkehr fließt und die permanent vom britischen Geheimdienst GCHQ auf verwertbare Informationen gefiltert werden: „Auch der Brexit wird daran nichts ändern". Neben der gegenseitigen Spionage würden immer mehr Staaten ihre offensiven Cyberkapazitäten für Vergeltungsschläge ausbauen, erklärt die IT-Expertin. Sie hält es für eine gefährliche, eine sinnlose Entwicklung angesichts der digitalen Übermacht der mit gigantischen Etats ausgestatteten US-Geheimdienste: „In Mitteleuropa sollte man daher besser in die digitale Defensive investieren und nicht glauben, dass man in der Kreisliga noch irgendwie mithacken könnte."

Kurz sieht die schlecht programmierte und von den Herstellern nicht aktualisierte Software als eine Gefahr für die Verbraucher. Sie will daher die Firmen stärker in Haftung nehmen, fordert aber auch ein Umdenken bei der IT-Ausbildung mit einem deutlichen Schwerpunkt auf der digitalen Sicherheit. Anderenfalls sei die Zukunft der Menschheit bedroht, warnt die CCC-Sprecherin. Denn die Computer werden bald „nicht nur auf unseren Tischen stehen, sondern auch in unsere Körper hineinwachsen". Die zunehmenden Cyberangriffe seien nicht schicksalhaft, sagt Kurz: „Wir können und wir müssen diese Entwicklung ändern".

Gerade auf der Bundesebene werde in Sachen Cybersicherheit derzeit viel unternommen, berichtet bei der Tagung im ZKM der Vizepräsident des Bundes-

### Täglich 400 000 neue Schadprogramme im Netz

amtes für Sicherheit in der Informationstechnik (BSI), Gerhard Schabhüser. Als „Kern der deutschen Cyberabwehr" sei seine Behörde 2017 um 180 Experten aufgestockt worden, 100 offene Stellen sollen noch besetzt werden. Der Kryptofachmann aus Bonn räumt offen ein, dass auch ein deutlich gestärktes Bundesamt keine 100-prozentige Sicherheit vor Cyberattacken und den täglich knapp 400 000 neuen Schadprogrammen im Internet bieten werde. Er verspricht jedoch mehr Transparenz bei den Sicherheitseigenschaften von digitalen Produkten durch die Einführung eines „IT-Gütesiegels", das den Verbrauchern die Auswahl von besser geschützter Technik erleichtern soll. Eine neue technische Richtlinie des BSI werde außerdem die Sicherheit von Routern verbessern.

„Ich habe keine Angst vor der Digitalisierung. Wir werden davon profitieren, wenn wir sie richtig anpacken", beantwortet Schabhüser einige besorgt klingende Fragen des ZKM-Publikums. Und schiebt einen Aufruf für mehr Sensibilität und Zurückhaltung im Netz hinterher: „Die Daten sind das Geld der Zukunft. Seien Sie sich also stets bewusst, was Ihre Daten im Netz wert sind."