taz.die tageszeitung vom 01.03.2022, Seite 18 / Medien

"Das würde Panik erzeugen"

Russland führt seinen Krieg nicht nur analog, sondern auch digital. Experte Mischa Hansel erklärt, was hinter Cyberattacken steckt und wie Deutschland sich auf sie vorbereiten kann

Interview **Hanna Gersmanntaz: Herr Hansel, die hat vor wenigen Tagen bereits erklärt, dass sich die Sicherheitsbehörden auf mögliche Cyberangriffe vorbereiteten. Wie groß ist die Gefahr?**SPD-Bundesinnenministerin Nancy Faeser**Mischa Hansel:** Stromnetze ließen sich attackieren. Ebenso Krankenhäuser. Im Jahr 2020 konnte die Düsseldorfer Uniklinik ein lebensgefährlich verletztes Unfallopfer nicht versorgen, weil das IT-System gehackt worden war. Auch Banken könnte es treffen, sodass niemand mehr wüsste, ob das eigene Geld noch da ist. Das würde Panik erzeugen. Solche Angriffe brauchen immer eine lange Planung. Aber wir wissen, dass Russland die Fähigkeiten hat. Die Frage ist nur, ob Präsident Putin sie auch nutzen will. Ausschließen lässt sich das nicht. Er könnte sie möglicherweise als Vergeltung für Wirtschaftssanktionen starten.

Kann eine Cyberattacke das Land existenziell treffen?

Sollte sich Russland entscheiden, alles einzusetzen - dann ja. Russland gehört mit den USA und China zur ersten Liga der Cybermächte. Wir beobachten das in der Ukraine schon seit Längerem. Die Ukraine ist für Russland zum Testgelände geworden, seit diese sich 2014 mit der Maidan-Revolution dem Westen zugewandt hat.

Was beobachten Sie genau?

Bei der ersten Parlamentswahl nach der Revolution manipulierten Hacker die Website der Wahlkommission. 2015 übernahmen sie das Stromnetz, eine Viertelmillion Ukrainer waren im Winter ohne Strom. 2016 ähnlich. Natürlich kann oft nicht zweifelsfrei geklärt werden, von wo die Hacker genau angreifen, aber Fachleute vermuten dahinter die russischen Sicherheitsbehörden. Es wird manipuliert, auch spioniert.

?So wie Ende 2020, als Teile der US-Regierung betroffen waren

Es war einer der bisher spektakulärsten Fälle von Cyberspionage. Und ja, auch da kamen die Hacker vermutlich aus Russland. Diese kaperten ein Update einer Netzwerksoftware der texanischen Firma SolarWinds. Das luden Tausende Behörden, Unternehmen, Betreiber kritischer Infrastruktur weltweit runter. So fingen sie sich die Späher ein. Betroffen waren etwa das US-Energieministerium, Finanzministerium, Handelsministerium, Heimatschutzministerium, Außenministerium und Teile des Pentagons. Die Täter hatten monatelang Zeit, sich umzusehen und vertrauliche Informationen mitzulesen.

Wie sind die Hacker ausgebildet?

Zunächst einmal gibt es Cyberspionage schon seit Jahrzehnten. Cyberangriffe auf kritische Infrastrukturen sind auch nicht neu. Die Risiken sind spätestens vor zwölf Jahren praktisch demonstriert worden. Da wurde ein Computervirus, Stuxnet, entdeckt. Den hatten wahrscheinlich die USA und Israel entwickelt, um Irans Atomprogramm zu sabotieren. Attacken auf kritische Infrastrukturen sehen wir jetzt immer öfter. 2017 traf es jene, die in der Ukraine Steuern zahlen oder auch Geschäfte betreiben. Es ist nicht so, dass das nur ganz wenige könnten.

Sondern?

Es gibt vielerorts gut ausgebildete Menschen mit IT-Kenntnissen, die aber keinen Job finden. Zum Beispiel in Ländern wie Nigeria, die gerade in der Pandemie wirtschaftlich besonders zu leiden hatten. Andernorts können die Löhne in der offiziellen Wirtschaft nicht ansatzweise mit dem großen Geld, das Cyberkriminelle auch als Neueinsteiger machen, mithalten. Es gibt eine systematische Rekrutierung durch Cyberkriminelle.

Ist Deutschland gewappnet?

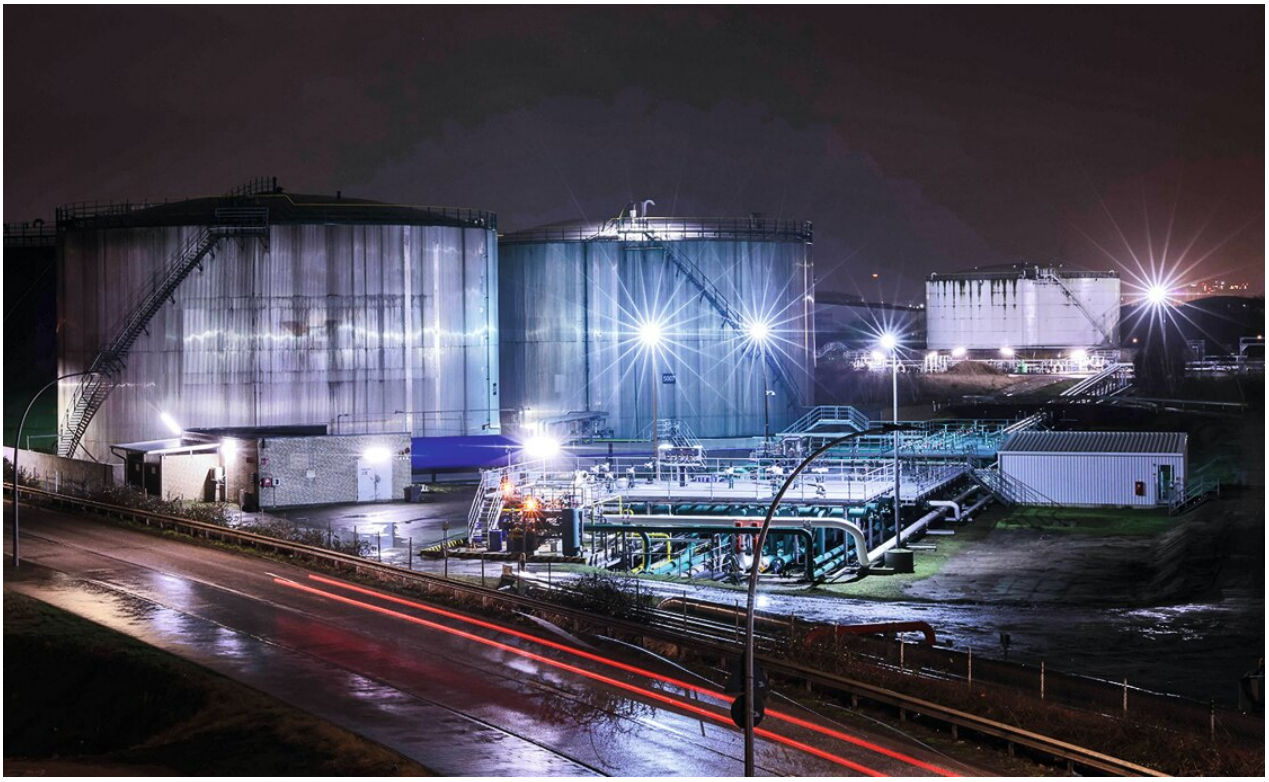
Im vergangenen Jahr gab es einen Hackerangriff auf die Server des Landkreises Anhalt-Bitterfeld. Die gesamte Verwaltung war blockiert, es konnten wochenlang keine Sozialleistungen ausgezahlt werden. Kommunen haben oft zu wenig Personal für IT. Da ist meist gespart worden. Das rächt sich jetzt. Behörden, Unternehmen, Krankenhäuser und so weiter müssen Notfallpläne erstellen und anpassen.

Wer macht es besser?

Estland. Das Land ist hochgradig digitalisiert, selbst Wahlen finden online statt. Und Staat und Gesellschaft haben viele Lehren aus einer massiven Blockade von Servern durch russischsprachige Hacker schon 2007 gezogen. Dort gibt es eine Art freiwillige IT-Feuerwehr, Ehrenamtliche, die den Notfall proben, im Ernstfall helfen. Die Ampelregierung verspricht im Koalitionsvertrag nun auch ein Cyber-Hilfswerk, ein CHW ähnlich dem Technischen Hilfswerk THW. Das ist gut. Allerdings entlässt das die Sicherheitsbehörden nicht aus ihrer Pflicht, eng miteinander zusammenzuarbeiten, um Angriffe schnell zu erkennen, Warnungen zu veröffentlichen, Nothilfen zu starten.

Mischa Hansel

42, ist Experte für sicherheitspolitische Risiken im Internet. Er leitet den Forschungsschwerpunkt Internationale Cybersicherheit am Institut für Friedensforschung und Sicherheitspolitik in Hamburg, das die Bundesregierung berät.



Das Tanklogistikunternehmen Oiltanking in Hamburg ist Ende Januar auch Ziel eines Hackerangriffs geworden Christian Charisius/dpa

Hanna Gersmann

Quelle:	taz.die tageszeitung vom 01.03.2022, Seite 18
Dokumentnummer:	T20220103.5837842

Dauerhafte Adresse des Dokuments:
https://www.wiso-net.de/document/TAZ__d85f28a9b9dde90e33d5ad04123238662eaafe82