Frankfurter Allgemeine | 19.10.2020 - Aktualisiert: 20.10.2020, 09:00 Uhr
https://www.faz.net/-gzl-a4ki7

Gefährdete Infrastruktur

„Stillstand innerhalb weniger Stunden bei Stromausfall“

Hessische Uni-Forscher warnen vor dem Ausfall von digitalen Netzen nach Katastrophen oder Cyberangriffen. Informatikprofessor Matthias Hollick erklärt, wie sich IT-Systeme schützen lassen und warum Corona ein Umdenken fördern kann.

Von SASCHA ZOSKE

© dpa

Geknickte Infrastruktur: Im November 2005 zerstörte ein Schneesturm im Münsterland viele Leitungen. Tagelang gab es keinen Strom.

In der ersten Corona-Welle hat sich die IT-Infrastruktur in Deutschland weitgehend bewährt. Sind unsere Kommunikationsnetze also wenigstens in dieser Hinsicht virenfest?

Bisher sind wir mit unserer Informations- und Kommunikationstechnologie in der Corona-Krise tatsächlich relativ gut gefahren. Die Netze waren nicht dramatisch überlastet. Zwar haben sich die Datenmengen anders über den Tag verteilt, aber das hat nicht zu großen Problemen geführt.

Könnte es trotzdem zu Ausfällen der Infrastruktur kommen? Schließlich werden viele Computer von Menschen bedient, und die können sich infizieren.

Das kann in der Tat zu einem Problem werden. Bisher waren wir noch ein Stück weit davon entfernt, auch in anderen Ländern, die von Corona schlimmer getroffen wurden. Trotzdem ist die Gefahr real, dass Energieversorgung, Kommunikation oder Verkehr gestört werden – wenn der Krankenstand so hoch wird, dass der Betrieb nicht mehr

sichergestellt werden kann. Wir haben in der Vergangenheit Fälle gesehen, bei denen krankheitsbedingt Stellwerke der Bahn nicht mehr bedient wurden. Und auch ein Kraftwerk oder ein Kommunikationsnetz muss verwaltet werden, auch wenn sich vieles aus der Ferne steuern lässt.

Sie haben mit Kollegen der Unis Darmstadt, Marburg und Kassel ein Strategiepapier verfasst, in dem Sie vor Risiken für die IT-Netze warnen. Was sind in Deutschland die größten Gefahren? Wohl eher Hackerangriffe als Naturkatastrophen, oder?

Hackerangriffe sind das größere Risiko. In Mitteleuropa und Deutschland haben wir bisher keine so großflächigen, dramatischen Naturkatastrophen gesehen wie etwa in Japan.

Beim „Münsterländer Schneechaos“ 2005 gab es allerdings auch einen mehrtägigen Stromausfall, weil Überlandleitungen zerstört worden waren.

Das war letztlich ein relativ kleines Ereignis, betroffen waren etwa 250.000 Menschen. Das Technische Hilfswerk hat damals ein Notfallnetz aufgebaut; aus ganz Deutschland wurden Stromerzeugungskapazitäten dort hingekarrt. Damit ist man dann gerade so klargekommen. Wenn aber zum Beispiel das Frankfurter Stromnetz ausgeschaltet würde, etwa durch einen terroristischen Angriff, dann wäre das auf diese Art nicht zu bewältigen. Und selbst das wäre noch ein regional begrenztes Unglück. Cyber-Attacken könnten noch viel weiter reichende Folgen haben.

© Privat

Matthias Hollick ist Professor für Sichere Mobile Netze an der Technischen Universität Darmstadt.

Wie wahrscheinlich ist so ein Großangriff auf die Infrastruktur?

Das wissen wir nicht. Wir wissen ja auch nicht, wann die nächste Pandemie kommt. Schon vor Corona wusste aber jeder, dass es Pandemien gibt und dass sie dramatisch werden können. Und schon im Frühjahr ist vor der zweiten Corona-Welle gewarnt worden. Jetzt ist sie da, und man kann sich fragen: Hätten wir uns besser vorbereiten müssen? So ist es auch mit Cyberangriffen. Das Problem ist, dass unsere Systeme nicht resilient, also widerstandsfähig genug sind. Je nachdem, wo und wie ein Angriff geführt wird, kann er fatale Folgen haben.

Was wären die Konsequenzen einer solchen Attacke?

Wenn es zu einem großflächigen Stromausfall kommt, wird sehr schnell auch die übrige Infrastruktur zusammenbrechen. Die Wasserpumpen stehen still, die Kühlung im Supermarkt fällt aus, empfindliche Lebensmittel verderben in kürzester Zeit.

Wie lange dauert es, bis alles still steht?

Das kann sehr schnell gehen, innerhalb weniger Stunden. Tankstellen haben – anders als Krankenhäuser – meist keine Notstromaggregate, da ist sofort Schluss. Die Kommunikationsnetze haben keine einheitliche Notstromversorgung, aber nach einem Tag würden wahrscheinlich nur noch das Behördennetz und einige lokale Inseln funktionieren.

Wer kann solche Attacken ausführen? Erpresser, Terroristen, ausländische Staaten?

All diese Akteure haben die Möglichkeiten dazu. Staaten haben die technischen Möglichkeiten für großflächige Cyberangriffe. Kriminelle können eher Nadelstiche setzen, indem sie etwa einen Erpressungstrojaner ins Computersystem einer Stadt oder einer Klinik einschleusen. Angriffe dieser Art werden immer häufiger, die Täter haben sich inzwischen arbeitsteilig professionalisiert: Als Erpressungsopfer bekommen Sie in einem Callcenter einen persönlichen Ansprechpartner, der Ihnen erklärt, wie Sie die Bitcoins überweisen müssen.

Apropos staatliche Akteure: Wie viel Sorge macht es Ihnen, dass beim Aufbau des 5G-Mobilfunknetzes Komponenten des chinesischen Herstellers Huawei zum Einsatz kommen könnten?

Nicht nur mit Blick auf Huawei, sondern für alle kritischen Infrastrukturen würde ich mir wünschen, dass der jeweilige Betreiber das System verstehen und im Krisenfall reparieren kann. Wenn man ein Huawei-System hätte, von dem man die Quellcodes kennt und das man bei Bedarf modifizieren könnte, dann würde mir das nicht mehr Kopfzerbrechen bereiten, als wenn die Technik von einem amerikanischen Anbieter käme.

In Ihrem Papier schreiben Sie mit Blick auf kritische Infrastruktur, Resilienz müsse genauso wichtig werden wie Effizienz. Was heißt das konkret?

Im Moment optimieren wir die IT auf Effizienz. Sie soll schnell und kostengünstig sein und so ausgelegt, dass der Anbieter damit möglichst hohe Gewinne erzielen kann. Wir bräuchten aber zuerst Resilienzvorgaben, und auf Grundlage dieser Vorgaben könnten die Entwickler dann die Effizienz optimieren. So könnte sich niemand einen Marktvorteil verschaffen, indem er die Systeme sehr billig, aber zu fragil baut.

Sie fordern, dass IT-Systeme redundant, divers und für den Krisenfall angemessen dimensioniert sein sollen. Können Sie an einem Beispiel erklären, was das bedeutet?

Redundanz bedeutet, dass ein System bestimmte Komponenten mehrfach enthält. Man kann zum Beispiel Mobilfunk-Vermittlungsstellen mit mehreren Servern bestücken. Wenn einer ausfällt, übernimmt ein anderer. Das reicht aber nicht. Wenn alle Server das gleiche Betriebssystem haben und es tritt dort ein Problem auf, dann sind alle Rechner betroffen. Deswegen ist auch Diversität wichtig. Idealerweise hat man unterschiedliche Hardware, verschiedene Betriebssysteme und unterschiedliche Anwendungssoftware. Die

Dimensionierung hängt davon ab, welche Ausfallszenarien man zugrunde legt. Man sollte ein gesundes Maß an Überkapazitäten bereithalten.

IT-Systeme sollen aber nicht nur mit erwarteten Unglücksfällen klarkommen, sondern auch mit bisher unbekannten Szenarien. Wie schafft man das?

Dazu wäre es wichtig, dass die IT-Systeme wandlungsfähig werden. So wie Anbieter von Elektrofahrzeugen die Reichweite bereits ausgelieferter Fahrzeuge durch neue Software steigern können, müssen auch die IT-Systeme der kritischen Infrastrukturen nachträglich anpassbar werden. Ein Beispiel, zu dem wir in Darmstadt forschen, sind mobile Endgeräte: Die meisten kommunizieren mit einer Basisstation. Wenn die ausfällt, könnten die Geräte auch direkt miteinander in Verbindung treten und ein Notfallnetz aufbauen. Wir haben gezeigt, dass das prinzipiell geht und in der Krise sinnvoll wäre. Auch hier helfen offene Quellcodes.

Wie wollen Sie das erreichen? Geht das nur mit staatlichem Zwang?

Ein gewisses Maß an Regulierung ist unvermeidlich. Das sieht man am Beispiel Huawei: Angesichts des wachsenden Drucks und staatlicher Vorgaben hat der Konzern erkennen lassen, dass er bereit sein könnte, Quellcodes offen zu legen. Man sieht: Wenn Kunden sagen, dass sie das wollen, dann bewegen sich Anbieter auch.

Aber hat der Kunde die Freiheit, sich einen anderen Anbieter zu suchen, wenn seine Wünsche nicht erfüllt werden?

Auf vielen Gebieten haben große Konzerne wie Microsoft, Google und Amazon eine monopolartige Stellung. Eine echte Wahl existiert hier nicht. Solche Strukturen aufzubrechen, ist extrem schwierig.

Wo müsste man den Hebel ansetzen?

Man sollte eine Strategie anwenden, die in der Politikwissenschaft „Positive Koordination“ genannt wird. Wenn man ein System aufbauen will, muss man sich am Anfang mit allen Akteuren zusammensetzen. Dann kann man im Dialog mit verschiedenen Anbietern zu einer Lösung kommen, die den Wünschen des Kunden und den Erwartungen an die Sicherheit entspricht. Hierauf aufbauend sollte man dann noch regulieren, zum Beispiel verbindliche Resilienzvorgaben für alle setzen.

Haben Sie den Eindruck, dass Sie mit Ihren Mahnungen Gehör finden?

Ich habe das Gefühl, dass die Appelle derzeit eher gehört werden – auch weil die Corona-Pandemie noch einmal zeigt, wie wichtig eine funktionierende Informations- und Kommunikationstechnik ist. Wäre sie nicht verfügbar gewesen, hätten unglaublich viele Dinge nicht funktioniert.

Link zum Strategiepapier: www.emergencity.de/s/pp1

Quelle: F.A.Z.