web.de

Im Visier der Hacker: So sicher ist Deutschland vor Cyber-Angriffen

Von Marie Illner
8-10 Minuten

Aktualisiert am 13. Januar 2020, 06:57 Uhr

2020 ist digital, vernetzt, online. Neben wirtschaftlichen Chancen bietet das aber auch Einfallstore für Hacker, Cyberspione und Netz-Terroristen. Zwei IT-Experten erklären, wie gut Deutschland vor Cyber-Angriffen geschützt ist und was im Notfall passiert.
Es kann jederzeit passieren, zunächst unbemerkt und ohne Vorwarnung: ein Hackerangriff auf deutsche Unternehmen und Infrastrukturen. Vom einen auf den anderen Moment könnte das bedeuten: Diebstahl von vertraulichen Informationen, Stromausfall für Tausende Haushalte, Produktionsstopp in Firmen, Verkehrschaos auf Deutschlands Straßen, Flughäfen oder Schienennetzen.
Dass solche Szenarien längst kein reiner Filmstoff mehr sind, bewiesen Attacken wie „WannaCry" im Mai 2017. Die Schadsoftware verschlüsselte Computerdateien mehrerer global tätiger Konzerne und forderte einen Lösebetrag in der Kryptowährung Bitcoin. Betroffen waren beispielsweise der spanische Telekommunikationskonzern Telefónica, der britische National Health Service mit mehreren Krankenhäusern und das US-Logistikunternehmen FedEx. Auch Rechner der Deutschen Bahn wurden infiziert – der Ausfall von Anzeigetafeln und Videoüberwachungssystemen war die Folge.
Ein Jahr zuvor wurden durch einen britischen Hacker, der im Auftrag eines liberianischen Mitbewerbers handelte, zeitweise mehr als eine Million Router der Telekom lahmgelegt.

Täglich Millionen Angriffe

Neben wirtschaftlichem Schaden ist auch der Einfluss auf politische Wahlen ein Motiv: Im Jahr 2015 verschaffte sich mutmaßlich das Hackerkollektiv „APT28", eine Einheit des russischen Militärgeheimdienstes GRU, weitreichenden Zugang zur IT-Infrastruktur des Bundestages und saugte sensible Daten ab. Eine Attacke auf das deutsche Außen- und Verteidigungsministerium im Jahr 2018 geht vermutlich ebenfalls auf das Konto der russischen Cyberspione.
Deutschland ist also längst Zielscheibe. Allein die Telekom registriert laut Unternehmenschef Dirk Backofen täglich bis zu 46 Millionen Angriffe auf ihre Infrastruktur. Wie sicher sind wir in Deutschlands Städten vor Cyberattacken? Und: Was passiert im Notfall?

Digitalisierung schafft neue Einfallstore

Die IT-Experten Andreas Mauthe (Universität Koblenz-Landau) und Thorsten Holz (Ruhr-Universität Bochum) sind sich sicher: Die Angriffe werden zunehmen.
„Mit Entwicklungen hin zu 'Smart Cities' und 'Internet of Things' bieten sich immer mehr Einfallstore für Angreifer", sagt Wirtschaftsinformatiker Mauthe. Experte Holz ergänzt: „Im Rahmen der fortschreitenden Digitalisierung werden auch kritische Systeme mit dem Internet verbunden."
„Kritische Infrastrukturen" sind laut Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI) Organisationen oder Einrichtungen, die eine wichtige Bedeutung

für das staatliche Gemeinwesen haben. Heißt: „Ihr Ausfall hätte massive und nachhaltige Folgen, etwa in der Versorgung oder öffentlichen Sicherheit“, erklärt IT-Wissenschaftler Holz. Das BSI unterteilt kritische Infrastrukturen in neun Sektoren: Energie, Ernährung, Finanz- und Versicherungswesen, Gesundheit, Telekommunikation, Medien, Wasser, Transport und Staatsverwaltung. „Darunter fallen dann zum Beispiel Krankenhäuser, Elektrizitätswerke, der Schienenverkehr oder Banken“, erläutert Experte Mauthe.

Erhöhte Alarmbereitschaft

Angriffsszenarien auf solche Strukturen zeichnen dramatische Bilder, mit wirtschaftlichem, politischem und gesundheitlichem Schaden: Angreifer könnten Überwachungskameras zum Verstecken von Sprengstoff deaktivieren, durch Ransomware oder Stromausfall die medizinische Versorgung beeinträchtigen oder im Verkehr die Schaltzentralen manipulieren – genügend Gründe für erhöhte Alarmbereitschaft.
„Einen hundertprozentigen Schutz gibt es nicht, dessen müssen wir uns bewusst sein“, mahnt Mauthe. Regelmäßige Updates seitens der Administratoren, eine kritische und regelmäßige Analyse von Sicherheitslücken und redundante Systeme mit doppelter Absicherung würden aber das Risiko von erfolgreichen Angriffen senken. „Auch eine autarke Stromversorgung kann Schutz bieten, ebenso das Verwenden von unterschiedlichen Technologien – also verschiedene Provider, Software und Hardware“, so Mauthe.

Gesetzliche Vorgaben

Das BSI arbeitet dabei mit den Betreibern von kritischen Strukturen zusammen, tauscht sich aus, erarbeitet Krisenmanagementstrukturen und führt Notfallübungen durch. „Für Betreiber mit einer gewissen Größe gibt es gesetzliche Vorgaben, die Sicherheitsstandards beschreiben. Diese betreffen etwa Firewall und Virenschutz. Betreiber müssen Vorfälle außerdem melden, damit die Bedrohungslage transparent wird“, sagt Holz.
Rahmen dafür ist die Cyber-Sicherheitsstrategie der Bundesregierung aus dem Jahr 2016. In ihr enthalten sind beispielsweise Maßnahmen wie die Einführung eines IT-Sicherheitsgütesiegels, um Cyber-Sicherheit für Anwender fassbar zu machen, die Ausweitung der Kooperation zwischen Staat und Wirtschaft sowie die Schaffung von „Mobilen Einsatzteams“ für die Unterstützung vor Ort.

Koordination durch das BSI

Beim BSI ist seit 2011 außerdem das „Nationale Cyber-Abwehrzentrum“ angesiedelt. Dort tauschen die für Cyber-Sicherheitsfragen zuständigen Bundesbehörden Informationen zu Cyber-Vorfällen aus und teilen ihre Bewertungen und Analysen.
„Die Zuständigkeiten sind zwar auf viele verschiedene Behörden und Ämter wie das Innenministerium, die Länder und Kommunen sowie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe verteilt, aber das BSI koordiniert gut“, meint Experte Holz. „Außerdem bietet eine verteilte Zuständigkeit auch Vorteile, weil man dadurch zentrale Schwachstellen vermeidet“, ergänzt Mauthe.

Sensibilisierung der Bevölkerung

Entscheidend ist aus Sicht der Experten auch die Sensibilisierung in der Bevölkerung: „Mitarbeiter von Unternehmen werden oft von Hackern als Zugang ausgenutzt, um so von innen heraus anzugreifen“, erklärt Mauthe. Sie müssten deshalb in Sachen Phishing-Mails und anderen Social-Engineering-Praktiken besonders aufmerksam sein. Ebenso dürfe die Bevölkerung in Notfallsituationen nicht in Panikhandlungen verfallen.

Was passiert beim „worst case scenario“?

Was aber würde im Extremfall passieren - angenommen eine Attacke auf die Stromversorgung ließe die Trinkwasserversorgung zusammenbrechen, Internet und Telefone fielen aus und Kassensysteme in Einkaufsmärkten würden nicht mehr funktionieren?
Mit einem solchen „worst case scenario“ setzt sich das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) auseinander.
Es hat Pläne für Treibstoffverteilung bei Stromausfall oder Notbrunnen bei einem Ausfall der Wasserversorgung, vereinbart Meldeketten, Lautsprecherdurchsagen und koordiniert Ersatzinfrastrukturen. In Sachen Katastrophenschutz kann die Digitalisierung dann auch wiederum von Vorteil sein: IT-Einsatz in Form von digitalen Lagekarten, Drohnen oder Notfall-Apps steigern Effektivität und Schnelligkeit.
Mauthe resümiert: „Wir dürfen nicht blauäugig sein und einfach hoffen, dass nichts passiert. Um konkurrenzfähig zu bleiben, muss Deutschland in Sachen Digitalisierung mitgehen.“
Prof. Dr. Thorsten Holz ist Informatiker und Professor an der Fakultät für Elektrotechnik und Informationstechnik an der Ruhr-Universität Bochum. Er forscht im Bereich der angewandten Aspekte von sicheren IT-Systemen mit dem Schwerpunkt auf systemnaher IT-Sicherheit.
Prof. Dr. Andreas Mauthe ist Professor für IT- und Datensicherheit am Institut für Wirtschafts- und Verwaltungsinformatik der Universität Koblenz-Landau. Er forscht im Bereich Netzwerk- und System-Resilienz und Cyber-Security.

Quellen:

- Kritische Infrastrukturen (BSI)
- Cyber-Sicherheitsstrategie (BMI)
- Bevölkerungsschutz Cybersicherheit (BBK)