Foto: ©solarseven/Shutterstock.com

# Pandemie des Verbrechens

**Cyberkriminalität** Erpressung im Internet erreicht einen neuen Höchststand. Selbst Kliniken sind vor Hackerangriffen nicht sicher. Experten machen auch die Regierung verantwortlich. *Von Igor Steinle*

Dass er mal Lösegeld-Verhandlungen führen würde, hätte Sebastian Schreiber früher nicht gedacht. „Hätten Sie mich das vor zehn Jahren gefragt, hätte ich gesagt, Sie spinnen“, so der IT-Sicherheitsunternehmer. Inzwischen aber erreicht ihn jeden zweiten Tag eine Anfrage von Unternehmen, deren Computersystem von Hackern übernommen wurde und die nun erpresst werden.

In vier Fällen hat Schreiber bisher aktiv verhandelt, in über 30 war er involviert. Das übliche Prozedere: Daten auf angegriffenen Rechnern werden verschlüsselt, bis die Opfer Bitcoin für die Entschlüsselung überweisen. Oft werden auch sensible Daten erbeutet, Geschäftsgeheimnisse etwa, verbunden mit der Drohung, diese zu veröffentlichen. Sicher scheint vor der Kriminalitätswelle niemand zu sein: „Kleine Firmen sind genauso betroffen wie Mittelständler und große Unternehmen“, so Schreiber.

Das zeigen auch die jüngsten Zahlen des Bundeskriminalamts (BKA). Egal ob Daten-Diebstahl, betrügerische Fake-Webseiten oder Schadsoftware: 2020 registrierte das BKA für das Vorjahr mit gut 100 000 Taten einen Anstieg von 15 Prozent – ein neuer Höchststand. Die Schäden stiegen mit 88 Millionen Euro sogar um 43 Prozent. Eine Zahl, die angesichts einer großen Dunkelziffer wahrscheinlich noch zu niedrig ist. Wegen Sorgen vor Reputationsverlust und Datenschutzstrafen melden viele Unternehmen Hackerangriffe nicht. Der Branchenverband Bitkom schätzt den Schaden durch Cyberangriffe deswegen um ein Vielfaches höher.

Die wenigen prominenten Fälle, die öffentlich wurden, betrafen in Deutschland bisher unter anderem Fresenius, Rheinmetall oder die Zeitungen der Funke Mediengruppe. Die in dem Verlag erscheinenden Tageszeitungen konnten lange nicht in vollem Umfang erscheinen. Wie hoch die Lösegeldforderungen oder -zahlungen waren ist nicht bekannt.

> „Eine Anhörung von Experten geriet zur Ohrfeige für die große Koalition.

IT-Unternehmer Schreiber berichtet von 3000 Euro im privaten Bereich bis zu acht Millionen bei Großunternehmen.

Noch gravierendere Schäden als finanzielle Verluste hätte dabei ein Hackerangriff im Februar auf die Trinkwasserversorgung im US-Bundesstaat Florida haben können. Unbekannte sind in das Computersystem eines Wasserwerks eingedrungen und haben das Wasser chemisch manipuliert. Mitarbeiter hatten die Änderung laut Betreiber aber sofort bemerkt und rückgängig gemacht.

Der Vorfall zeigt, wie ernst die Lage ist. Mit einer Beruhigung der Situation ist dabei vorerst nicht zu rechnen. Denn während die Corona-Pandemie die Welt nach wie vor im Griff hat, beobachtet die internationale Polizei-Organisation Interpol eine „Parallel-Pandemie des Verbrechens“. So würden Cyberkriminelle über schlecht abgesicherte private Computer der im Homeoffice Arbeitenden vermehrt in Firmennetze eindringen. Der Sicherheitssoftware-Hersteller Kaspersky etwa rechnet mit einen Anstieg digitaler Verbrechen um 25 Prozent. Besonders perfide seien dabei, so Gründer Eugene Kaspersky, Cyber-Angriffe auf Gesundheitseinrichtungen wie etwa auf die Düsseldorfer Uni-Klinik im vergangenen September, bei dem ein Mensch gestorben ist, weil er nicht eingeliefert werden konnte. „Solche Attacken auf Krankenhäuser, dazu noch in Corona-Zeiten, sind für mich Terrorismus, und genauso entschlossen müssten sie bekämpft werden“, so der IT-Experte

Innenminister Horst Seehofer (CSU) hat den Ball bereits aufgenommen und arbeitet seit Jahren an einem „IT-Sicherheitsgesetz 2.0“. Kritische Infrastrukturen wie Strom- und Wasserversorgung, das 5G- Netz und die Sicherheitsbehörden sollen damit gestärkt werden. Soweit die Theorie. Was die Praxis angeht, hagelt es an dem Gesetzesentwurf Kritik von allen Seiten. So durften am Montag von allen Fraktionen berufene Experten im Bundestag ihre Einschätzung abgeben. Die Anhörung geriet zur Ohrfeige für die IT-Sicherheitspolitik der Bundesregierung. Selbst von den Regierungsfraktionen berufenen Experten schimpften das geplante Gesetz ein „Anti-Sicherheitsgesetz“.

Der Branchenverband Bitkom etwa kritisiert unklare Formulierungen und sieht Unternehmen künftig größerer Bürokratie ausgesetzt. Der Entwurf sei überarbeitungswürdig und „nur bedingt geglückt“, so Bitkom-Experte Sebastian Artz. Noch deutlicher wurde Manuel Atug von der AG Kritis, einem Zusammenschluss von 40 Experten, die sich mit kritischen Infrastrukturen auseinandersetzen. Er spricht von einem von „fachfremden Personen mit der heißen Nadel gestrickten Entwurf“. Behörden würden die IT-Sicherheit bewusst schwächen, indem sie ihnen bekannte Sicherheitslücken für Überwachungszwecke offen lassen. Solche Lücken würden aber auch Hacker früher oder später aufspüren, weswegen sie umgehend geschlossen werden müssten.

Linus Neumann vom Chaos Computer Club zeichnete zusammenfassend ein verheerendes Bild der IT-Sicherheit in Deutschland, die „ein einziges Desaster“ sei: Private Kundendaten würden laufend im Internet landen, Erpressungssoftware grassiert seit Jahren, unsichere Produkte ohne Updates seien frei verkäuflich und niemand tue etwas dagegen. Stattdessen würde bekanntes Wissen für mehr IT-Sicherheit nicht umgesetzt. Behalten die Kritiker Recht, haben Sicherheitsunternehmer wie Sebastian Schreiber also auch in Zukunft jede Menge zu tun.

### Einfallstor Mensch

**Als größte Schwachstelle** in Sachen Cybersicherheit gilt der Mensch, der infizierte E-Mail-Anhänge öffnet oder manipulierte Links anklickt. Zudem setzen viele Behörden, Unternehmen und private Nutzer nach wie vor das eingestellte Betriebssystem Windows 7 ein, obwohl die Software inzwischen große Sicherheitslücken aufweist. In Deutschland laufen noch mehr als fünf Millionen unsichere Windows-Rechner. *dpa*

**Hintergrund**

## Netz der Spione

**Weltweit hat es** in den vergangenen Monaten aufsehenerregende Cyberaktionen gegeben. So sind Unbekannte im Dezember vergangenen Jahres in das Computersystem der Europäischen Arzneimittelbehörde EMA in Amsterdam eingedrungen und erbeuteten Dokumente der Impfstoffhersteller Pfizer und Biontech. Die niederländischen Behörden gehen von einem staatlichen Urheber aus. Laut EMA haben die Hacker die Dokumente zum Covid-Impfstoff manipuliert und dann im Internet veröffentlicht, darunter vertrauliche E-Mails über die Bewertung der Impfstoffe.

Bekannt ist jedoch, dass Nordkorea „bislang auf den Rüstungsbereich ausgerichtete Cyberaktivitäten nunmehr auf den Bereich Biotechnologie und hier besonders auf die Impfstoffentwicklung und -herstellung fokussiert“, wie es in einem Bericht des Verfassungsschutzes vom Januar heißt. So meldete der südkoreanische Geheimdienst schon im November, nordkoreanische Hacker hätten versucht, Daten von Impfstoffentwicklern in Südkorea zu stehlen. Zuvor hatte Microsoft mitgeteilt, russische und nordkoreanische Hacker hätten versucht, Impfstoffhersteller, unter anderem in Frankreich, Südkorea und den USA, auszuspähen.

Die als versiert bekannten nordkoreanischen Hacker haben dabei bisher vor allem mit digitalen Raubzügen zum Zwecke der Finanzierung des Atomwaffenprogramms ihres Landes auf sich aufmerksam gemacht. Laut einem UN-Bericht haben sie allein zwischen 2019 und November 2020 316 Millionen Dollar von Finanzinstituten gestohlen. Das US-Justizministerium geht sogar von mehr als 1,3 Milliarden US-Dollar aus und hat inzwischen gegen drei der laut zuständigem Staatsanwalt „besten Bankräuber der Welt“ Anklage erhoben.

Am bedrohlichsten für die USA ist jedoch eine Hackeratta-

> „Hinter der jüngsten Attacke soll Russland stecken.

cke, die ebenfalls Dezember 2020 bekannt wurde. Spione waren über die vielerorts genutzte Wartungssoftware der Firma Solarwinds in die Systeme verschiedener Ministerien, Bundesbehörden und auch Unternehmen eingedrungen und monatelang unentdeckt geblieben. Die US-Regierung vermutet hinter der Aktion Russland und hat bereits Gegenmaßnahmen angekündigt. „Wir werden sicherstellen, dass Russland versteht, wo die Vereinigten Staaten die Grenze für diese Art von Aktivitäten ziehen“, sagte der Nationale Sicherheitsberater von US-Präsident Joe Biden, Jake Sullivan, kürzlich. Experten bezweifeln jedoch, dass die Reaktion allzu heftig ausfallen wird. Denn kein Land ist wahrscheinlich so aktiv und versiert in diesem Bereich wie es die Vereinigten Staaten selbst sind *Igor Steinle*