Cyber-Spionage - Hackerangriff erschüttert USA

Erst langsam wird das ganze Ausmaß des verheerenden Hackerangriffs auf die USA sichtbar. Betroffen sind auch andere Länder, auch Deutschland. Die wichtigsten Fragen und Antworten.

Der mittlerweile "Sunburst" genannte Cyber-Großangriff hat über Monate hinweg Teile der US-Regierung, Forschungseinrichtungen und Privatfirmen infiltriert. Am Donnerstag bestätigte auch die Nationale Verwaltung für Nukleare Sicherheit, NNSA innerhalb des US-Energieministeriums, Opfer eines großangelegten Hackerangriffs geworden zu sein. Sie ist verantwortlich für die US-Atomwaffen.

Zuvor haben bereits mehrere weitere US-Regierungsbehörden entdeckt, dass Hacker in ihre Systeme eingedrungen sind, darunter die Ministerien für Heimatschutz, für Handel, für Finanzen und das Außenministerium.

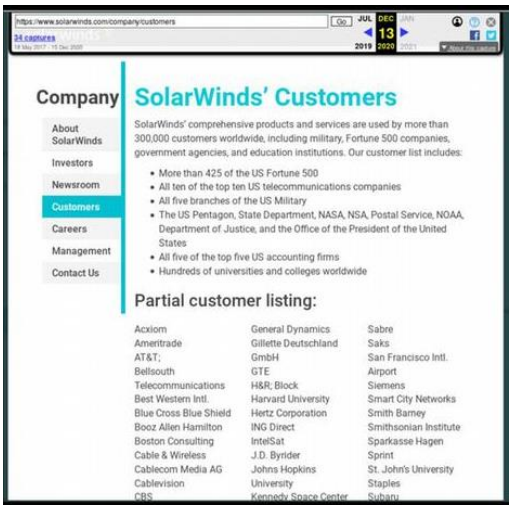
Die dem US-Heimatschutzministerium unterstellte Behörde für Cyber- und Infrastruktur–sicherheit (Cisa) stuft den jüngsten Hackerangriff als "ernste Gefahr" ein. Die amerikanische Nachrichtenagentur AP zitiert anonym bleibende US-Beamte mit der Einschätzung, es handele sich um den "schwersten Hacker-Angriff in der Geschichte Amerikas".

Der Tech-Riese Microsoft enthüllte am Donnerstag, mehr als 40 Regierungsbehörden, Denkfabriken, Nichtregierungsorganisationen und IT-Unternehmen seien von den Hackern infiltriert worden. 80 Prozent von ihnen befanden sich in den Vereinigten Staaten - fast die Hälfte von ihnen Tech-Unternehmen. Opfer gebe es aber auch in Kanada, Mexiko, Belgien, Spanien sowie Großbritannien, Israel und den Vereinigten Arabischen Emiraten. In einem Firmenblog betonte Microsoft Präsident Brad Smith, dass der Angriff fortdauert. Die Zahl der Opfer und auch die Zahl der betroffenen Länder werde mit Sicherheit steigen, erwartet der Microsoft Chef. Sein Fazit: Selbst für das digitale Zeitalter sei das keine "gewöhnliche Spionage".

Wie gingen die Angreifer vor?

Die Hacker hatten bereits im Frühjahr die US-Softwarefirma SolarWinds im texanischen Austin digital unterwandert. Das war der erste Schritt in ihrer sogenannten "Lieferkettenattacke". SolarWinds bietet Technik für das Management und die Sicherung von Computernetzwerken und war nicht das eigentliche Ziel des Angriffs, sondern der Angriffskanal. Die Angreifer konnten ihre Schadsoftware in einem Update für die Software Orion verstecken, das von rund 18.000 SolarWinds-Kunden heruntergeladen wurde. Die Opfer installierten ihre Malware über diesen Weg quasi selbst.

SolarWinds hat eine lange Liste illustrer Kunden: Neben einer Fülle von Regierungsbehörden nutzen in den USA 425 der Fortune-500-Unternehmen die betroffene Software, inklusive großer Rüstungskonzerne wie Lockheed Martin, ebenso alle großen Mobilfunkbetreiber und Universitäten.



Inzwischen nicht mehr im Netz: Die SolarWinds Kunden-Seite

Gehüllt in den Mantel des vertrauenswürdigen IT-Dienstleisters hatten die Eindringlinge in den Zielsystemen mehr als acht Monate Zeit, die E-Mail-Kommunikation mitzuverfolgen, Daten zu stehlen und Kontrolle über Systeme zu erlangen.

Am Ende entdeckten nicht staatliche Cyberabwehrorganisationen die Hacker, sondern die ebenfalls angegriffene Cyber-Security-Firma FireEye. In einem Blogeintrag erklärte CEO Kevin Mandia, "dass wir Zeugen eines Angriffs durch eine Nation mit erstklassigen Offensivfähigkeiten sind. Dieser Angriff unterscheidet sich von den Zehntausenden von Vorfällen, auf die wir im Laufe der Jahre reagiert haben." Mandia fährt fort: "Sie verwendeten eine neuartige Kombination von Techniken, die weder wir noch unsere Partner in der Vergangenheit gesehen haben."

Wer steckt hinter dem Angriff?

Ein derart ausgefeilter und langandauernder Angriff ist das Werk eines staatlichen Akteurs. Die "Washington Post" und auch die "New York Times" zitieren ungenannt bleibende US-Beamte, die auf Russland als Urheber des Angriffs weisen. Der Demokratische Senator Richard Blumenthal nannte in einem Tweet am Dienstag ebenfalls Russland als Angreifer, nach einem geheimen Briefing, dass "ihn zutiefst beunruhigt, ja gerade erschreckt" habe.

Auch Außenminister Mike Pompeo macht Russland für den Angriff verantwortlich. Die Täter hätten mit großem Aufwand versucht, über die Software eines Drittanbieters auf die IT-System der Regierung zuzugreifen, sagte Pompeo in einer Radiosendung. Es sei "ziemlich eindeutig", dass Russland hinter diesen Attacken stecke. Zuvor hatte er noch Nordkorea und China im Sinn.

Russland streitet die Vorwürfe ab. "Bösartige Aktivitäten im Datenraum widersprechen den Prinzipien der russischen Außenpolitik, den nationalen Interessen und unserem Verständnis von

zwischenstaatlichen Beziehungen", schrieb die russische Botschaft in Washington auf Facebook. "Russland führt keine offensiven Operationen in der Cyber-Domäne durch."

Ist Deutschland betroffen?

Auch in Deutschland wird die kompromittierte Software Orion von SolarWinds von Behörden und Unternehmen eingesetzt. Auf DW-Nachfrage erklärt eine Sprecherin des zuständigen Bundesamtes für Sicherheit in der Informationstechnik, BSI, die Zahl der Betroffenen sei nach derzeitigem Kenntnisstand gering. Das BSI empfiehlt den Unternehmen und Behörden sich nicht auf das Einspielen von Patches zu beschränken, sondern zu analysieren, ob die Schwachstelle ausgenutzt und weitere Angriffsaktivitäten in den IT-Systemen festgestellt werden können.

Insgesamt warnt das BSI davor, sich in einer vernetzten Welt auf digitale Lieferketten zu verlassen: "Angreifer suchen hier mit zunehmend professionellen Methoden nach dem schwächsten Glied in der Kette, so dass es selbst bei einem sehr hohen Sicherungsstandard zu Angriffsversuchen kommen kann", so die Sprecherin.

Was passiert als Nächstes?

Präsident Trumps früherer Berater für Inlandsicherheit Thomas Bossert, warnt, die Tragweite des Angriffs sei kaum zu übertreiben. In einem Meinungsbeitrag in der New York Times warnte Bossert, es könne Jahre dauern, um festzustellen, über welche Netzwerke die Hacker die Kontrolle erlangt haben.

In einem ersten Schritt hat die Cybersicherheitsbehörde CISA eine Notverordnung herausgegeben. Die verpflichtet alle Bundesbehörden, sofort zu handeln: Computer mit alten Versionen der betroffenen Software müssen sofort abgeschaltet werden. Die CISA teilte weiter mit, das Entfernen des Angreifers aus betroffenen Systemen werde sich voraussichtlich "hochkomplex" gestalten. Der oder die Täter hätten "Geduld, operative Sicherheit und komplexe Handwerkskunst" bewiesen.

Joe Biden will Angreifer zur Verantwortung ziehen

Derweil beginnt die Diskussion über mögliche Vergeltungsmaßnahmen. Der künftige US-Präsident Joe Biden erklärte, Cyberangriffe würden unter seiner Regierung nicht unbeantwortet bleiben. Verantwortliche würden in Abstimmung mit Verbündeten zur Rechenschaft gezogen werden.

Zur Verfügung steht ein ganzes Arsenal von Möglichkeiten - offen wie etwa Sanktionen, oder auch verdeckt, durch eigene Cyberoperationen. Schon 2018 erklärte der damalige Sicherheitsberater John Bolton gegenüber Journalisten, dass künftig auch offensive Cyber-Operationen gegen ausländische Rivalen nun Teil des US-Arsenals seien.

AP zitiert den Cyber-Konflikt Experten Jason Healey von der Columbia Universität mit der Aussage, "wir können ihre Systeme komplett zum Schmelzen bringen". Denkbar wären auch peinliche Enthüllungen über die Vermögensverhältnisse von Wladimir Putin und Mitgliedern seines Kreises.

Auch wenn es möglicherweise eine Weile dauern kann: Eine Antwort aus Washington dürfte kommen.

Quelle: https://www.dw.com/de/hackerangriff-ersch%C3%BCttert-usa/a-55990457 (20.9.2021)