Hacker-Lexikon: Was gilt als kritischer Infrastrukturen der Nation?

Autor: Kim Zetter.Kim Zetter Sicherheit

WIRED | 2016.02.16

Wie die US-Regierung den jüngsten Hack der ukrainischen Stromnetz betrachtet, die seit dem Stuxnet-Angriff gegen das iranische Atomprogramm nur der zweite Hack dieser Art gegen kritische Infrastruktur wurde im Jahr 2010 entdeckt, sind die Auswirkungen auf die US-Stromnetz deutlich.

"[E] sehr wenig ist dies in den USA Gitter machbar", Robert M. Lee, ein ehemaliger Cyber Warfare Operations Officer für die US Air Force und Mitbegründer von Dragos Sicherheit, einer kritischen Infrastruktur-Sicherheitsfirma, sagte WIRED über die hacken.

Kritische Infrastrukturen ist im Rampenlicht mehr denn je im Gefolge von Stuxnet, da es klar geworden ist, dass viele wichtige Systeme verwendet die Gesellschaft den Betrieb und gesunde Wasseranlagen zu halten, Anlagen zur Energieerzeugung, Ölraffinerien-haben verwundbare Systeme, die in einigen Fällen , sind für Hacker über das Internet zugänglich.

Aber was ist in diesen Tagen kritische Infrastrukturen in Betracht gezogen?

TL; DR: Kritische Infrastrukturen ist ein System oder die eine hohe Bedeutung für die Sicherheit und den Betrieb des Landes hat. Die Regierung hat sechzehn Branchen identifiziert, die diese Kriterien erfüllen, eine Kategorisierung, die nicht nur Wasser und Kraftwerke, sondern auch zur Überraschung vieler, Hollywood Filmstudios wie Sony beinhaltet.

Im weitesten Sinne bezieht sich kritische Infrastrukturen auf ein beliebiges System von hoher Bedeutung für die Sicherheit und den Betrieb des Landes. Die meisten Menschen gehen davon aus das gilt für Kraftwerke, Wasseraufbereitungsanlagen und andere Dienstprogramme-wie, was in gehackt wurde sowohl der Stuxnet-Angriff die ukrainische Angriff. Aber in Wahrheit umfasst die Regierung Definition eine breite Schneise von Branchen und Einrichtungen.

Die US-Regierung hat tatsächlich sechzehn Sektoren kritischer Infrastrukturen definiert, die für das Funktionieren des Landes wichtig sind, und könnten daher Sabotagerisiko sein. Im Großen und Ganzen kategorisiert umfassen die Branchen: Chemie, Kommunikation, kommerzielle Einrichtungen, kritische Fertigung, Dämme, Verteidigung Industrie, Notdienste Reaktion und Erholung, Energie, Finanzdienstleistungen, Ernährung und Landwirtschaft, staatliche Einrichtungen, Gesundheitswesen und öffentliche Gesundheit, Informationstechnologie, Kern Reaktoren und Materialien, Transportsysteme, Wasser- und Abwasseranlagen.

Auf der Oberfläche, die meisten von ihnen nicht umstritten zu sein scheinen. Aber viele Leute waren überrascht zu erfahren, nachdem die Sony im Jahr 2014 zu hacken, dass die Regierung die Entertainment-Unternehmen als kritische Infrastrukturen zu sein, da Filmproduktionsstudios in den gleichen geschützten Kategorie fallen, wie kommerzielle Einrichtungen wie Hotels, Freizeitparks, Kongresszentren und Sportstadien . Nicht jeder stimmt mit der Einschätzung der Regierung.

"Das erscheint mir als schwach lächerlich", Paul Rosenzweig, ehemaliger stellvertretender Staatssekretär für die Politik im Ministerium für innere Sicherheit, schrieb nach dem Lernen, dass Sony kritische Infrastruktur betrachtet wurde. "Amerika wird nicht zusammenbrechen, wenn Hollywood dunkel ist. Wenn alles kritisch ist, dann ist nichts wirklich kritisch. "

Wenn alles kritisch ist, dann ist nichts wirklich kritisch. Paul Rosenzweig

Die Definition der kritischen Infrastruktur ist wichtig, denn obwohl viele der Einrichtungen, die unter diese Definition fallen, von privaten Parteien gehören, die Regierung zu schützen CI vor dem Angriff begangen hat. "Die gemeinsame Verteidigung in Privatbesitz kritischer Infrastrukturen von bewaffneten Angriff oder von physischen Eindringen oder Sabotage durch ausländische Streitkräfte oder internationale Terroristen ist eine zentrale Aufgabe der Bundesregierung", die im Jahr 2009 erklärte Cyber Bericht des Präsidenten, diese in die umfasst geführt Angriffe digitalen Bereich.

Wir haben einen Hinweis darauf, wie wichtig die Regierung ihre Rolle hält kritische Infrastrukturen zu schützen, wenn Präsident Obama eine Executive Order im Jahr 2015 ermöglicht die Regierung wirtschaftliche Sanktionen gegen Einzelpersonen im Ausland zu erheben unterzeichnet, die in zerstörerischen Cyber-Attacken oder Wirtschaftsspionage engagieren.

Sanktionen kann nur für erhebliche Angriffe erhoben werden, die eine bestimmte Schwelle von Schaden treffen. Sie müssen zum Beispiel verletzt direkt die "nationale Sicherheit, die Außenpolitik, die wirtschaftliche Gesundheit oder die finanzielle Stabilität der Vereinigten Staaten", nach der Ankündigung des Präsidenten. Aber der Schaden Schwelle durch die Unterbrechung von Computernetzen durch eine weite Verbreitung von DDoS-Attacken, oder durch den Diebstahl von Finanzdaten, Geschäftsgeheimnisse oder geistiges Eigentum in einer Weise erfüllt werden könnten, die die Nation die wirtschaftliche Stabilität schadet. Die Sanktionen können natürlich nur dann angewandt werden, wenn die Regierung die Angriffe auf eine bestimmte Nation oder Organisation zuzuschreiben ist in der Lage, aber sie würden nur direkt in die Cyber-Attacken und Diebstahl Eingriff zu Parteien nicht anwendbar. Der Auftrag kann auch die Regierung Sanktionen gegen Personen und Einrichtungen anzuwenden, die wissentlich Daten in solche Angriffe gestohlen verwenden und zu empfangen. Dies könnte gelten, zum Beispiel für ein Unternehmen, dass Hacker mietet Daten zu stehlen von einem Wettbewerber einen Marktvorteil oder Einkäufe nach der Tat gestohlene Daten zu gewinnen.

Was all dies bedeutet im Hinblick auf präventiven Schutz für kritische Infrastruktureinrichtungen ist unklar. Da die meisten kritischen Infrastrukturen in den Händen des privaten Sektors ist, kann die Regierung verhängen sich nicht auf diesen Branchen oder Mandat, dass sie bestimmte Sicherheitsmaßnahmen zu ergreifen. Es gibt eine Ausnahme von dieser-die wenigen Branchen, die Regierung geregelt, wie die Finanz-, Gesundheits- und Nuklearindustrie sind. All die Regierung kann für andere Branchen zu tun, die nicht geregelt sind, wird Best Practices, zu teilen Bedrohung Intelligenz mit ihnen beraten und bieten Forensik und Wiederaufbauhilfe nach einem Angriff. Die Regierung kann auch seine Intelligenz Befugnisse nutzen, Angriffe zu erkennen, die in den Werken sind und abwehren sie ab, obwohl die Art und Grenzen, was die Regierung in dieser Hinsicht sind trübe noch tun können.

Dies bedeutet nicht, dass die Unternehmen keine Schritte auf eigene Faust nehmen kann die kritische Infrastruktur zu schützen wir alle vertrauen auf. Die Hacker, die in Energieverteilungszentren in der Ukraine im vergangenen Dezember bekam und schaltete das Licht auf mehr als 230.000 Kunden aus konnten dies zu tun, weil es nur wenige Hindernisse in Ort, um sie daran hindern, den Internet verbundenen Unternehmensnetzwerke der Distributionszentren aus Springen zu den kritischen Produktionsnetze in denen die Arbeitnehmer das Stromnetz gesteuert. Als Lee WIRED nach dem Angriff gesagt, sind die US-Systeme genauso anfällig für die gleiche Art von Angriff.

Zurück zum Anfang. Wechseln zu: Anfang des Artikels.

lesen: http: //www.wired.com/2016/02/hacker-lexicon-what-counts-as-a-nations-critical-infrastructure/