U.S. INTERNATIONAL CANADA ESPAÑOL 中文
The New York Times

von ZEYNEP TUFEKCI

Hier sind die digitalen Hinweise darauf, was Musk wirklich vorhat

Feb. 21, 2025, 5:03 a.m. ET

Viele Beobachter, die Elon Musk und seine Bande junger Gefolgsleute dabei beobachtet haben, wie sie sich ihren Weg durch die Bundesregierung gebahnt haben, haben sich schwer getan zu verstehen, wie eine so kleine Gruppe in so kurzer Zeit so viel Schaden anrichten konnte.

Der Fehler besteht darin, Musk ausschließlich in den politischen Kontext einzuordnen. Er geht an diese Herausforderung nicht wie ein haushaltsbewusster Beamter heran. Er geht an die Sache heran wie ein Ingenieur, der Schwachstellen ausnutzt, die in die technischen Systeme der Nation eingebaut sind, und der als das agiert, was Cybersicherheitsexperten eine Insider-Bedrohung nennen. Wir wurden vor diesen Schwachstellen gewarnt, aber niemand hat zugehört, und die Folgen - für die Vereinigten Staaten und die Welt - werden enorm sein.

Insider-Bedrohungen gibt es schon lange: der CIA-Maulwurf, der im Büro der sowjetischen Regierung im Stillen aber hart arbeitete, der Boeing-Ingenieur, der heimlich Informationen über das Space-Shuttle-Programm an die chinesische Regierung weiterleitete. Moderne digitale Systeme verstärken diese Bedrohung, indem sie mehr und mehr Informationen aus vielen verschiedenen Bereichen zusammenführen.

Dieser Ansatz hat offensichtliche Vorteile in Bezug auf Komfort, Zugang, Integration und Geschwindigkeit gebracht. Als die parteiübergreifende Kommission für den 11. September beschrieb, wie die Segmentierung von Informationen zwischen den Behörden die nachrichtendienstlichen Bemühungen behindert hatte, bestand die Lösung darin, integrierte Systeme für die Erfassung und gemeinsame Nutzung riesiger Datenmengen zu schaffen.

Der Betrieb integrierter digitaler Systeme erfordert jedoch, dass einige wenige Personen mit weitreichenden Privilegien ausgestattet werden. Das sind die Sysadmins, die Systemadministratoren, die das gesamte Netzwerk, einschließlich seiner Sicherheit, verwalten. Sie haben Root-Rechte, im Fachjargon die höchste Zugriffsstufe. Sie erhalten Zugang zum God View, wie Uber sein internes Tool nannte, das es einer außergewöhnlich großen Anzahl von Mitarbeitern ermöglichte, die Uber-Fahrten anderer zu sehen.

Als Edward Snowden bei der NSA war, konnte er deshalb so viele Informationen mitgehen lassen, darunter auch umfangreiche Datenbanken, die wenig mit den Vorgängen zu tun hatten, die er als Whistleblower aufdecken wollte. Er war ein Systemadministrator, der über Benutzer wacht, die ihre Zugriffsrechte missbrauchen, der aber einen großen Spielraum hat, seine eigenen Rechte auszuüben.

„Auf bestimmten Ebenen sind Sie der Prüfer“, erklärte ein Geheimdienstmitarbeiter gegenüber NBC News die Leichtigkeit, mit der eine einzelne Person mit Unmengen von geheimen Daten auf

einem USB-Stick abhauen kann. Es ist die moderne Version eines der ältesten Probleme der Staatsführung: „Quis custodiet ipsos custodes?“, fragte der römische Dichter Juvenal vor etwa 2.000 Jahren. Wer überwacht den Systemadministrator?

Man denke nur an die Empörung über das Rentensystem für Bundesbedienstete, ein plumpes Programm, auf das Musk kürzlich aufmerksam machte. Der gesamte Prozess läuft fast ausschließlich auf Papier, wobei jede Rentenakte von Hunderten von Beschäftigten *in einer Kalksteinmine 230 Fuß unter der Erde* von Hand bearbeitet wird, die Papierstücke zwischen den einzelnen Höhlen hin- und herschieben, um sie in den richtigen Aktenordner zu stecken. Da es in der „Mine“ keine offene Flamme geben durfte, wie die Washington Post 2014 berichtete, musste das gesamte Essen von außen kommen. Der Pizzabote hatte also eine Sicherheitsfreigabe. Mehrere Modernisierungsversuche scheiterten, was zu einem frustrierend schleppenden Prozess führte, bei dem einfache Suchvorgänge oft Monate dauern.

Nicht so beim Einstellungs- und Entlassungsprozess im *Office of Personnel Management (O.P.M.)*, wo alle Beschäftigungsunterlagen in einer Super-Personalabteilung für die gesamte Bundesregierung fein säuberlich digitalisiert wurden. Deshalb machte sich ein Team von Musks so genannter Abteilung für Regierungseffizienz (DOGE) direkt auf den Weg zum O.P.M. und schleppte Sofabetten zum Schlafen an, damit sie rund um die Uhr da sein konnten. O.P.M. ist der Root-Zugang zur gesamten Regierung der Vereinigten Staaten.

Mit dieser Art von Zugang kann selbst ein kleines Team die gesamte Regierung nach Mitarbeitern durchsuchen, deren Jobtitel Hinweise auf falsches Denken enthalten, oder die sich gegen Übernahmen wehren oder bürokratische Mittel einsetzen könnten, um das Tempo der Veränderungen zu verlangsamen.

In der Tat ist diese kleine DOGE-Crew zu Systemadministratoren für die gesamte Regierung geworden. Kurz nach dem O.P.M. drangen sie in das Finanzministerium ein, wo alle Zahlungen der Regierung gespeichert sind: Root-Zugriff auf die Wirtschaft (einschließlich vieler Unternehmen, die direkte Konkurrenten der Unternehmen von Musk sind). Vor kurzem haben sie ihre Bemühungen auf das Finanzamt und die Sozialversicherungsanstalt ausgeweitet, die beide über äußerst personenbezogene und sensible Daten verfügen: Root-Zugriff auf praktisch die gesamte amerikanische Bevölkerung.

The Atlantic berichtet, dass ein ehemaliger Tesla-Ingenieur, der zum Direktor der Technology Transformation Services ernannt wurde - einer wenig bekannten Einrichtung, die digitale Dienste für viele Teile der Regierung betreibt -, „privilegierten Zugang“ zu 19 verschiedenen IT-Systemen beantragt hat, angeblich ohne auch nur einen Background-Check zu absolvieren, wodurch er weniger überprüft wurde als die Person, die die Pizza an die „Mine“ liefert.

Alles dies hat sich mit einer anderen Art von Insider-Bedrohung vermischt und verstärkt, die sich seit Jahrzehnten auf der politischen Seite zusammenbraut: die Ausweitung der unkontrollierten Exekutivgewalt.

„Mit Geld werden wir Männer bekommen, sagte Cäsar, und mit Männern werden wir Geld bekommen“, schrieb Thomas Jefferson einmal, um davor zu warnen, dass das, was er Wahldespotismus nannte, zu einem sich selbst nährenden Kreislauf werden kann. Er befürchtete, dass ein gewählter autoritär handelnder Mensch die Institutionen, die seine Macht begrenzen

sollten, nicht nur pulverisieren, sondern sie auch als Waffen einsetzen würde, um sich selbst weiter einzugraben.

Nicht einmal Jefferson hätte sich eine Zukunft vorstellen können, in der das Arsenal zentralisierte Datenbanken mit umfassenden Aufzeichnungen über die Beschäftigung, die Finanzen, die Steuern und für einige sogar über den Gesundheitszustand jedes Bürgers umfasst.

Nachdem ein Richter eine Durchführungsverordnung von Trump blockiert hatte, teilte Elon Musk mit seinen mehr als 200 Millionen Anhängern auf X einen Beitrag, der den Namen, das Foto und den Job der Tochter des Richters enthielt, die angeblich im Bildungsministerium arbeitet. Es gibt keinen Hinweis darauf, dass er über sie Zugang zu Regierungsdatenbanken über hatte, aber woher sollen wir wissen, ob er einen solchen Zugang hatte oder ob er ihn in Zukunft haben wird?

Wie viele Menschen machen sich nun Gedanken über private Informationen über sich selbst oder ihre Angehörigen? Wie viele Unternehmen fragen sich, ob ihre sensiblen Finanzdaten jetzt in den Händen eines Konkurrenten sind? Wie viele Richter fragen sich, ob ihre Familie die nächste ist?

So hätte es nicht sein müssen. Im Laufe der Jahre hat ein Experte nach dem anderen und eine Organisation nach der anderen vor den Gefahren gewarnt, die mit der Zusammenführung so vieler Daten in den Händen von Regierungen (und Unternehmen) verbunden sind. Bereits 1975 warnte Jerome Wiesner, der damalige Präsident des M.I.T., dass die Informationstechnologie „der Regierung und privaten Interessen weitaus mehr Macht verleiht“ und dass „die weit verbreitete Sammlung persönlicher Daten eine Bedrohung für die Verfassung selbst darstellen würde“ und das Risiko einer „Informationstyrannei im unschuldigen Streben nach einer effizienteren Gesellschaft“ mit sich brächte.

Es geht hier nicht um die Wahl zwischen Effizienz und Aktenordnern in unterirdischen Minen. Es gibt viele vielversprechende Bemühungen um die Entwicklung digitaler Technologien, die unsere Privatsphäre schützen und gleichzeitig ihre Annehmlichkeiten bieten. Sie haben Namen wie *zero-knowledge proofs*, *federated learning*, *differential privacy*, *secure e*nclaves, *homomorphic encryption*, aber wahrscheinlich hat man noch nie etwas davon gehört. In der Eile, neuere, schnellere und gewinnbringendere Technologien zu entwickeln - und die Art von Unternehmensimperien zu ermöglichen, deren Chefs bei der Amtseinführung von Donald Trump neben ihm standen - schienen Datenschutz- und Sicherheitsvorschriften langweilig zu sein.

Jetzt haben wir es mit einem System zu tun, das denjenigen, die die legitimen Funktionen der Regierung ausüben wollen, die gleiche Effizienz bietet wie denjenigen, die sie abbauen oder für ihre eigenen Zwecke missbrauchen wollen. Es scheint nicht einmal einen Mechanismus zu geben, mit dem man herausfinden kann, wer mit welchen Privilegien Zugang zu welcher Datenbank erhalten hat. Die Richter fragen nach und erhalten nicht immer klare Antworten. Die einzigen, die es wissen, sind die Systemadministratoren, und die schweigen.

Übersetzt von Gerhard Kongehl unter Mitwirkung von DeepL.
21. Februar 2025