Diebstahl von Politikerdaten: Vertrauen zerstört - was nun?

Dr. Axel Spies ist Rechtsanwalt bei Morgan, Lewis & Bockius LLP in Washington DC und Mitherausgeber der ZD.

ZD 2019, 49 Nach dem Leak privater Politiker- und Prominentendaten hagelt es Kritik am Vorgehen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die Fakten sind durch die Presse gegangen. Hunderte Personen sind betroffen. Die Bundesregierung erwägt nun strengere Sicherheitsvorgaben für Softwarehersteller und Betreiber von Internetplattformen. Das BSI verweist darauf, dass es in erster Linie für die Kritische Infrastruktur in Deutschland und den Schutz von Regierungsnetzen zuständig sei. Die vermutlich von einem Einzeltäter gestohlenen Daten stammen nach derzeitigem Kenntnisstand aber überwiegend aus "privaten oder persönlichen Accounts."

Das BKA warnte alle Bundestagsabgeordneten in einem Schreiben: "Es ist in Betracht zu ziehen, dass die betroffenen Personen nicht nur im direkten zeitlichen Zusammenhang Ziel beispielsweise von (anonymen) Beleidigungen und Bedrohungen oder vereinzelt Sachbeschädigungen werden können." Die Links zu den Daten seien zwar aktuell nicht mehr zugänglich. "Es ist jedoch davon auszugehen, dass bereits Kopien heruntergeladen wurden und beispielsweise über WhatsApp oder andere offen zugängliche Internetseiten weiterverbreitet worden sind."

Zu Hackerangriffen auf den Deutschen Bundestag kommt es leider immer wieder. Vor allem sind die Betroffenen selbst zur mehr Vorsicht anzuhalten. Es mag bequem sein, aber es zeugt von purem Leichtsinn, z.B. Fotos von Ausweiskopien und Kreditkarten ins Netz zu stellen. Die Besorgnis der Bürger geht allerdings weiter: Lebenswichtige Daten, wie Daten von Atomkraftwerken oder der Wasser- und Stromversorgung, könnten ebenfalls Hackern zugänglich sein. Die besorgte Öffentlichkeit fragt berechtigterweise: Wie bekommen wir die Datensicherheit in den Griff?

Im Unternehmen anfangen

Sicherlich, die Zusammenarbeit der Sicherheitsbehörden im Bereich der Cybersicherheit könnte besser sein. Erfolgversprechender ist aber ein Ansatz von unten nach oben. Die Gewährleistung der Datensicherheit fängt präventiv in jedem Unternehmen an. Art. 32 DS-GVO gibt den Verarbeitern und Verantwortlichen nur allgemeine Vorgaben zur Datensicherheit. Im neuen BDSG findet man Teile von Art. 32 DS-GVO in § 64 BDSG -- allerdings gelten diese Vorschriften nur für den Bereich der Polizei und Justiz. Nach Art. 33 DS-GVO ist für die Unternehmen eine interne Data Breach Policy nicht explizit vorgesehen. Eine solche detaillierte und intern erprobte Richtlinie, was bei einem tatsächlichen oder nur vermuteten Bruch der Datensicherheit zu tun ist, kann den Schaden minimieren. Es geht darum, intern frühzeitig Hackerangriffe zu erkennen und diese Erkenntnisse zügig weiterzuleiten. Das interne Data Breach Response-Team sollte der Dreh- und Angelpunkt für die weiteren Maßnahmen sein. Jeder muss wissen, was im Ernstfall zu tun ist. Interne Schulungen zur Datensicherheit sollten in allen Unternehmen eine Selbstverständlichkeit sein.

Verbindungen der Industrie untereinander stärken

Wichtig ist auf einer anderen Ebene, dass die betroffenen Unternehmen frühzeitig und offen miteinander reden, um Verwundbarkeiten frühzeitig zu erkennen und Lücken zu schließen. Der

Erfahrungsaustausch muss nicht notwendigerweise nur über das BSI erfolgen. In den USA gibt es seit Jahren die National Cyber Security Alliance (NCSA). Die NCSA ist eine gemeinnützige Organisation, die 2001 als Public-Private-Partnership gegründet wurde. Sie arbeitet mit dem Department of Homeland Security und privaten Sponsoren zusammen, um das Bewusstsein für Cybersicherheit in kleinen und mittleren Unternehmen und in den Schulen zu fördern. Die NCSA ist ein wichtiges Forum für den Erfahrungsaustausch.

Kampagne: Erst nachdenken, dann online gehen

Die Aktion "National Cyber Security Awareness Monat" ist z.B. ein Ziehkind der NCSA. Ein weiteres erfolgreiches Projekt wurde zusammen mit der US-Regierung umgesetzt und lässt sich mit "Erst nachdenken, dann online gehen" übersetzen. Das Projekt beinhaltet eine breit angelegte Kampagne für Cybersicherheit. Das STOP. THINK. CONNECT.™ Toolkit beinhaltet einen ganzen Werkzeugkasten (Broschüren, Videos, Poster) für Interessierte, Eltern und Institutionen. Hier eine Übersicht über die vorhandenen Broschüren:

- Social Media Guide
- Internet of Things Tip Card
- Cybersecurity While Traveling Tip Card
- Chatting with Kids about Being Online
- Parents and Educators Tip Card
- Mobile Security Tip Card
- Best Practices for Creating a Password
- Best Practices for Using Public WiFi
- Identity Theft and Internet Scams
- Mobile Banking and Payments
- Online Gaming
- Online Privacy
- Reporting a Cybercrime Complaint
- Insider Threat
- Malware
- Five Every Day Steps Towards Online Safety
- Five Ways to be Cyber Secure at Work
- How to Recognize and Prevent Cybercrime
- Five Steps to Protecting Your Digital Home
- Your Part in Protecting Critical Infrastructure
- Phishing

Informationskampagnen der Datenschutzbehörden

Der Appell der Bundesdatenschutzbeauftragten Voßhoff im Sender NDR Info geht in diese Richtung. Sie forderte, die Politik müsse besser über die Gefahren der Digitalisierung aufklären. Der Leak zeige, "dass mit der Digitalisierung zwingend ein hohes Maß an Sicherheit einhergehen muss". Jeder müsse aber selbst dafür sorgen, die eigenen Daten zu sichern. Eine solche Aufklärung sollte allerdings nicht nur von "der Politik", sondern auch (und gerade) von den Datenschutzbehörden ausgehen, wenn sie ihrem Namen gerecht werden wollen. Die US Federal Trade Commission (FTC) ist keine Datenschutzbehörde im europäischen Sinn, ist aber schon seit Jahren aufklärend und verbraucherschützend tätig (vgl. Spies, ZD-Aktuell 2015, 04122). Wichtig ist die Leitlinie der FTC zur Datensicherheit.

Erwähnenswert ist auch der FTC-Staff-Report "Engage, Connect, Protect: The FTC's Projects and Plans to Foster Small Business Cybersecurity". Dort werden die FTC-Materialien in einfacher Sprache für kleine Unternehmen und Non-Profit-Organisationen beschrieben, die in der Regel kein internes IT-Personal

haben. Die FTC verteilte im Jahr 2017 fast 400.000 gedruckte Broschüren zur Cybersicherheit für Unternehmen. Sie geben praktische Tipps zum Schutz persönlicher und sensibler Informationen und beschreiben, was Betroffene tun sollten, wenn ein Datenschutzverstoß vorliegt. Die FTC behandelt auch Datensicherheitsthemen in ihrem Business-Blog, der über 65.000 Abonnenten hat. Zu den Themen des Business-Blogs gehören u.a. Einzelthemen wie der Datenschutz der Verbraucher bei Mietwagenverträgen und das US-Datenschutzgesetz zum Schutz von Kindern (COPPA).

Nichts bewegt sich ohne mehr Geld

Bei allem guten Willen: Ohne weitere Ausgaben zur Verbesserung der Cybersicherheit auf allen Ebenen wird es weitere Hiobsbotschaften geben. Während die USA 2017 für die Cybersicherheit rund 20 Mrd. ausgegeben haben, muss das deutsche BSI mit einem Etat von rund 110 Mio. auskommen, merkte der CDU-Politiker Frei an. Die Zahl für die USA ist eher zu niedrig gegriffen. Das Budget des US-Präsidenten des Haushaltsjahrs 2019 umfasst US-$ 15 Mrd. für Aktivitäten im Zusammenhang mit Cybersicherheit - eine Steigerung um US-$ 583,4 Mio. (4,1%) gegenüber dem Haushaltsjahr 2018. US-$ 1,7 Mrd. sind allein für das Department of Homeland Security angesetzt. Hinzu kommen u.a. die erheblichen Ausgaben der einzelnen Bundesstaaten für Cybersicherheit.

Es ist zwar schwer einzuschätzen, wie viel der US-amerikanische Privatsektor für Cybersicherheit ausgibt, doch das Forschungsunternehmen Gartner Group veröffentlicht regelmäßig Schätzungen der Ausgaben für Cybersicherheit. Danach sind die Ausgaben für Cybersicherheit 2018 um 8% auf US-$ 96,3 Mrd. gestiegen. Eine Studie der Gartner Group aus dem Jahr 2017 stellt fest, dass sich private Unternehmen von einem Fokus auf die reine Prävention abwenden und einen weiter gefassten Ansatz verfolgen, indem sie ihre Fähigkeiten zur Erkennung und Reaktion auf Sicherheitsvorfälle im Internet verbessern. Die International Data Corporation prognostiziert, dass die Ausgaben weiter auf US-$ 101,6 Mrd. im Jahr 2020 steigen werden.

Sanktionen bei Bruch der Datensicherheit

Zwar gibt es in den USA kein allgemeines, allumfassendes Datenschutzgesetz wie die DS-GVO, jedoch gibt es in allen Bundesstaaten strenge Gesetze, die bei einem Bruch der Datensicherheit Mitteilungen und Maßnahmen zur Schadensbegrenzung vorschreiben. Diese Vorschriften werden von den Behörden (meist vom bundesstaatlichen Generalstaatsanwalt) durchgesetzt und können empfindliche Sanktionen nach sich ziehen (vgl. Spies, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 2. Aufl. 2018, Teil V, Kap. 2, Rdnr. 36). Seit 2009 schreibt z.B. das wegweisende Gesetz von Massachusetts (201 CMR 17.00) denjenigen, die auf persönliche Daten von Einwohnern von Massachusetts Zugriff haben, solche Mitteilungen vor. Sie müssen auch eine Mitteilung machen, wenn sie wissen oder Grund zu der Annahme haben, dass personenbezogene Daten einer in Massachusetts ansässigen Person von Dritten unautorisiert erworben oder für einen nicht-autorisierten Zweck verwendet wurden. Das mehrfach ergänzte Gesetz schreibt u.a. die Verschlüsselung portabler Geräte vor, soweit dies technisch machbar ist. Die Definition der Verschlüsselung wurde kürzlich geändert, um sie technologieneutral zu machen. Solche Vorschriften haben zu erheblichen Sicherheitsfortschritten beigetragen.

Die hier aufgezeigten Maßnahmen können dazu dienen, den Zielen des Art. 32 DS-GVO, nämlich der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der IT-Systeme und -Dienste, näher zu kommen. Datensicherheit hat viel mit Vertrauen der Nutzer in die IT-Systeme zu tun. Das Vertrauen dauerhaft zurückzugewinnen ist für die Unternehmen und die Politik ein Marathon, kein Sprint.