Politiker- und Promi-Hack 2019

Timeline

- Juni 2015: „Bundestag-Hack“, es werden interne E-Mails veröffentlicht
- 20. Dezember 2018: gesammelte persönliche Daten und parteiinterne Dokumente deutscher Politiker und Personen des öffentlichen Lebens werden in einem Twitter-Adventskalender von einem gekaperten Twitter-Account (@_0rbit) eines Youtubers aus veröffentlicht.Private Chats und Dokumente sind offenbar auch darunter, eine bunte Mischung aus unterschiedlichen Quellen, allerdings vorwiegend ältere Daten, auch auch aus dem Bundestag-Hack (s.v.).
- Ende Dezember 2018: Das BSI informiert zunächst in seiner Funktion die betroffenen Personenkreise über die die Tatsache.
- 4.1.2019: Die Presse wird des Themas gewahr, RBB berichtet über eine große Hackerattacke ("Deutsche Politiker gehackt").
- 5.1.2019 Das BSI hat offenbar einen Informationsvorsprung vor dem BKA
- 8.1.2019: Verhaftung eines tatverdächtigen Schülers in Hessen
- 8.1.2019: Politik will ein „Früherkennungssystem für unbefugten Datenabfluss“ installieren und ein IT-Sicherheitsgesetz 2.0 (?!)
- 9.1.2019: Motivation: Der Tatverdächtige habe aus „Ärger über bestimmte Politiker und Prominente“ Daten, die er selbst und andere aus noch verschiedenen Quelle erhalten habe(n), veröffentlicht. → Doxing
- 10.1.2019: Es wird gemutmaßt, der „Hacker“ habe Daten und Passwörter teilweise im Internet gekauft.
- 10.1.2019: „Hacker“ war schon 2016 bekannt
- 10.1.2019: Bundesdatenschutzbeauftragter fordert Verpflichtung für bessere Passwörter und mehr Aufklärung über sicheren Umgang mit Internet-Diensten ♥

Wie kommen private Daten ins Netz? Diskussion

Böse Hacker dringen auf private Computer ein und stehlen private Dokumente und Bilder… ???

„Rechner Hacken“ - Stufen

1. Remote Exploit
   Über eine Sicherheitslücke, einen „zu offenen Dienst“, Schwachstelle, Backdoor (Hintertür, unzureichend geschützter Wartungs-Zugang) kommt der Angreifer i.d.R. als „unprivilegierter Benutzer“ auf den Rechner und kann sich umschauen. Wenn dort Dateien für alle lesbar „herumliegen“, kann er diese übers Netz abgreifen.

Hier könnte der Angreifer auch nach dem Exploit einen Dienst installieren, der es später erlaubt, „leichter“ wieder Zugriff zu bekommen, oder einfach alle Daten abgreifen, die für ihn lesbar sind.

2. Local Exploit
   Bedingt, dass der Angreifer bereits einen unprivilegierten („Normalbenutzer“) Zugang auf den Rechner hat, und verschafft ihm über einen Programmierfehler im Betriebssystem höhere Rechte (z.B. Admin-Status). → Rechte-Eskalation, jetzt kann der Angreifer ALLE Daten lesen und das System manipulieren, Malware installieren, weitere Backdoors installieren, die NICHT von Virenscannern gefunden werden können usw..
3. Ist der Angreifer zum Administrator des angegriffenen Systems geworden, kann er das System nach belieben manipulieren, neue Dienste installieren, die Webcam kontrollieren, Daten abgreifen, weitere Backdoors installieren, Systemkomponenten austauschen … → Das System so manipulieren, dass es Teil eines „Bot-Netzes“ wird, und mit Fernsteuerungssoftware jederzeit auch in Massen-Angriffen mitverwendet werden kann. „Ich habe nichts zu verbergen“, „auf meinem Rechner ist sowieso nichts wichtiges installiert“ → Aber Teil eines kriminellen Netzwerkes!

Was bereits im Internet liegt, kann abgegriffen werden vom Betreiber der Infrastruktur (Techniker, Angestellte, …), auch wenn diese nicht zu den „Freunden“ des Datenproduzenten gehören.

Dem Anwender des Smartphones/Notebooks/Tablets ist oft nicht bewusst, dass die Daten in der Cloud (Dropbox, icloud, Amazon, Google etc.) nicht nur von ihm selbst, sondern auch von anderen verwaltet bzw. gelesen werden können.

Lösung des Problems „meine privaten Daten liegen in der Cloud“?

1. Die „unangenehme“ Lösung: Keine Daten in die Cloud hochladen, die man auf keinen Fall öffentlich haben möchte! (Verlass dich nicht auf die Rechte, die in der App angezeigt werden).→ Änderung des Verhaltens gefordert, nicht immer konsequent durchsetzbar.
2. Eine eigene Cloud betreiben, z.B. Home Cloud (Server steht zuhause, ist evtl. per Router auch für authentifizierte Geräte von außen erreichbar), mit VPN zwischen Standorten, wenn gewünscht. → Kontrolle vollständig beim Anwender, aber auch die Verantwortung für Backups usw..
3. Verschlüsseln von Daten, BEVOR sie in die Cloud gestellt werden. Vorteil: Datenmenge des Anbieters kann voll genutzt werden. Nachteil: Empfänger müssen einen entweder symmetrischen oder asymmetrischen Schlüssel zur Entschlüsselung verwenden, bevor die Daten angeschaut werden können.