STANDPUNKT

E-Government braucht Sicherheit

Digitale Angebote staatlicher Einrichtungen sollen unter dem Stichwort „E-Government" eine bessere Zusammenarbeit zwischen Staat und Bürger bzw. Staat und Unternehmen ermöglichen. Europäischer Vorreiter und „Betatester" für E-Government ist Estland. Esten können über das Internet ein Gewerbe anmelden und Parkgebühren bezahlen – während das Parlament papierlos arbeitet und Kabinettssitzungen online abgehalten werden.

Neue Chancen, neue Risiken

Das Beispiel Estland zeigt jedoch auch die Risiken der zunehmenden Digitalisierung und Vernetzung. Durch einen groß angelegten Angriff auf die digitale Infrastruktur wurden im Jahr 2007 die Internetseiten mehrerer estnischer Institutionen, unter anderem des Parlaments, lahmgelegt.

Wie auch in der Industrie (Stichwort „Kritische Infrastrukturen") hat eine zunehmende Digitalisierung insgesamt mehr Einfallstore für die Manipulation und Extraktion von Informationen zur Folge. Zudem nehmen Täter, die diese Schwachstellen ausnutzen, immer häufiger auch staatliche Einrichtungen ins Visier. Der bisher umfangreichste Vorfall war ein Angriff auf das Office of Personnel Management (OPM) in den USA im Juni 2015. Die persönlichen Daten (Adressen, Sozialversicherungsnummern, Hintergrundinformationen und auch über eine Million Fingerabdrücke) von mehr als 21 Millionen Bewerbern auf Stellen im öffentlichen Sektor waren davon betroffen.[1]

Hergang und Folgen eines Angriffs

Der genaue Hergang im Fall OPM ist nicht bekannt. Im Fall des im Juli dieses Jahres erfolgten Angriffs auf das Datennetz des Deutschen Bundestags wird angenommen, dass er durch Schadsoftware (Trojaner) ermöglicht wurde, die vermutlich per E-Mail an Nutzer verschickt wurde.[2] Grundsätzlich bieten jedoch auch über das Internet zugängliche Schnittstellen (zum Beispiel für den Austausch von Antragsdaten) ein potenzielles Einfallstor.

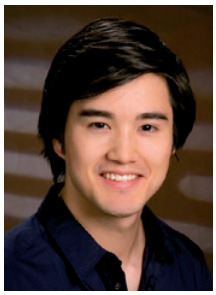
Die Erfahrung mit vergleichbaren Vorfällen zeigt, dass der weitere Ablauf nach dem initialen Eindringen der Angreifer oft ähnlich ist. Sofern die zuerst erbeuteten Benutzerkonten oder -rechte nicht ausreichen, um sich im Netzwerk frei bewegen zu können, werden die Hacker mit unterschiedlichen Hilfsmitteln versuchen, sich von Computer zu Computer sowie von Benutzer-Account zu Benutzer-Account weiterzuhangeln, bis sie hohe Administratorrechte und damit größtmögliche Bewegungsfreiheit erreicht haben. Im Zuge dessen werden die von den Angreifern „besuchten" Systeme meist vollständig kompromittiert.

Während und nach dieser Angriffsphase werden außerdem das Netzwerk und die daran angeschlossenen Systeme durch die Täter erkundet. Je nach Motiv und Auftraggeber suchen Angreifer nach Daten, deren Entwendung, Manipulation oder Zerstörung lohnenswert sind.

Landen sensible Daten im Netz oder werden digitale Dienstleistungen lahmgelegt, entsteht ein Schaden für die betroffenen Personen. Generell leidet aber auch die Akzeptanz für E-Government unter Datenklau oder Sabotage. Bereits jetzt stehen viele Bürger der digitalen Entwicklung skeptisch gegenüber. Häufen sich Vorfälle, kann dies zu einer übergreifenden Ablehnung der entsprechenden Dienste führen.

Was ist zu tun?

Um diesem Szenario vorzubeugen, braucht E-Government zwingend Sicherheit[3]:



Pascal Pillokeit
Senior Associate,
KPMG AG Wirtschaftsprüfungsgesellschaft,
Security Consulting

Jan Ludwig Tiedemann
Assistant Manager,
KPMG AG Wirtschaftsprüfungsgesellschaft,
Forensic Technology

Prävention kann sowohl technische (zum Beispiel Schutz von sensiblen Daten mittels Firewalls, Verschlüsselung oder physischer Abkoppelung) als auch organisatorische Maßnahmen (Aufbau eines Informationssicherheitsmanagements) umfassen.

Der **Detektion** (Aufdeckung) liegt die Einsicht zugrunde, dass sich Vorfälle nie ganz verhindern lassen. Neben einem aktuellen Schutz vor Schadsoftware kann auch eine (datenschutzgerechte) Analyse des Netzwerkverkehrs Hinweise auf unerwünschte Gäste geben.

Auf die Erkennung muss eine effektive **Reaktion** folgen. Neben dem „Herauswurf" der Angreifer stehen dabei auch die Wiederherstellung des Betriebs und vor allem das Lernen aus dem Vorfall im Fokus. Um die Strafverfolgung zu erleichtern, sollte auf eine korrekte forensische Herangehensweise geachtet werden.

Verlorenes Vertrauen ist nur schwer wiederherzustellen. E-Government kann deshalb nur erfolgreich sein, wenn Sicherheit bereits von Anfang an höchste Priorität hat.

1 Wired (2015): The Massive OPM Hack Actually Hit 21 Million People, 9.7.2015. Abrufbar unter: www.wired.com

2 Spiegel Online (2015): Cyberangriff auf den Bundestag: Hacker kopierten Abgeordneten-E-Mails, 18.6.2015. Unter: www.spiegel.de

3 Vgl. Dolle, W. et al. (2014): Das IT-Sicherheitsgesetz – lästig oder längst überfällig? In: PublicGovernance Winter 2014