Bundeskriminalamt

HERBST-TAGUNG 2013
BKA AUTUMN CONFERENCE

Cybercrime –

Bedrohung, Intervention, Abwehr

BKA-Herbsttagung vom 12. - 13. November 2013

Cyberterrorismus, Cyberspionage und Cyberwar – eine aktuelle Bedrohungseinschätzung aus Sicht der Wissenschaft

Kurzfassung

Dr. Sandro Gaycken

Technik- und Sicherheitsforscher an der Freien Universität Berlin

Strategisch bedeutsame Cyberspionage und Cyberwar sind keine theoretischen Konzepte mehr.

Dafür gibt es inzwischen Belege. China etwa wurde 2012 mit einer militärischen Cyberwar-Truppe bei hochwertiger Industriespionage erwischt. Dieser „APT-1“ genannte Angreifer horchte systematisch Hochtechnologieunternehmen aus, mit dem inzwischen aus China bekannten Ziel, die eigenen Unternehmen zu Marktführern in globalen Hochtechnologiemärkten zu machen. Dieses Ziel scheint strategisch wichtig genug zu sein, um APT-1 selbst bei einer Entdeckung nicht gleich zurückzufahren. Die Kampagne ist immer noch aktiv, nur von Afrika aus und auf Europa gerichtet. Aber auch andere Staaten sind transparenter geworden. Über das US-Cybercommand etwa sind über den Enthüller Snowden interessante Fakten bekannt geworden. Eine besonders brisante Information ging erst vor kurzem durch die Fachmedien. Das Command hat 2011 231 offensive Operationen durchgeführt und 652 Millionen US-Dollar in hochwertige Hintertüren im IT-Ökosystem investiert. Diese Zahlen sind überaus bezeichnend. Die 231 offensiven Operationen wie Stuxnet und Flame im Jahr 2011 betrafen über 18.000 teilweise hochgesicherte Rechner und Netzwerke und nicht eine einzige der Operationen ist auch nur ansatzweise entdeckt und bekannt geworden – eine immens wichtige Beobachtung zu den systematischen Defiziten unserer Vorstellungen von IT-Sicherheit und über die eben nur scheinbare Effizienz unserer CERTs und SOCs, unserer Detection und Awareness. Und eine Investition von 652 Millionen US-Dollar in Hintertüren ist ebenfalls ein Game-Changer für sich. Bei einem strategischen Einbau der Hintertüren „Early On“ in der Produktion und „Bottom Up“ im Stack kann man bei dieser Zahl davon ausgehen, dass eine signifikanter Teil unseres IT-Environments bereits auf Hardwarebasis und über Betriebssysteme nachhaltig infiziert ist – erneut bis heute vollkommen unentdeckt.

Andere Länder sind noch schwieriger zu beobachten, werden aber kaum zurückhaltender sein. Indikatoren dafür sind etwa in den Aktivitäten und Budgets des britischen GCHQ zu sehen, im epidemischen Anwachsen von Cyber-Söldnerfirmen, die hochwertige Exploits im internationalen Markt anbieten oder in der Aufnahme von „Cyber“ im Curriculum der School of Economic Warfare in Paris.

Diese rapide voranschreitende Evolution und die Kommerzialisierung der Offensive machen eine Kontrolle der immer zahlreicher entstehenden Cyberwaffen immer schwieriger. Trotzdem haben wir keine tragfähigen Schutzkonzepte gegen diese Variante von Akteur. Wie soll also unsere Cybersicherheit in Zukunft aussehen? Eine Entwicklung von Hochsicherheits-IT wäre eine Option,

und sogar eine, die wir speziell in Deutschland gut ansiedeln könnten. Unsere industrielle Basis, unsere sicherheitspolitische Zurückhaltung in der Offensive und unser Fokus auf hohe Sicherheit unter gleichzeitiger Berücksichtigung bürgerlicher Freiheiten und Privatheiten machen uns zu einem ideal aufgestellten Akteur für diese neue Variante des Computers. Allerdings müssten wir dafür ein paar Geburtswehen über uns ergehen lassen. Hochsicherheits-IT macht eine Abkehr vom "IT-Business as Usual" erforderlich. Ohne diese Abkehr werden wir aber ohnehin nicht weitermachen können. Das Versagen des „IT-Security Business As Usual“ wird jeden Tag greifbarer und muss dringend öffentlich gemacht und politisch anerkannt und adressiert werden.