

Monokulturen sind leichter angreifbar – was tun gegen den Dominoeffekt?

Compass Security AG: Angreifbarkeit der BRD-Infrastruktur ebnet den Weg für Cyberterrorismus

Rapperswil, 23. September 2009 – „Stirb langsam 4.0“ – eine neue Art des Terrorismus bedroht Washington. Alle Computernetzwerke im Film werden unter Kontrolle und die Infrastruktur zum Erliegen gebracht. Dies könnte auch der Bundesrepublik Deutschland blühen, meinen Sicherheitsexperten. Marco Di Filippo, Regional Director Germany bei der Compass Security AG, zeigt auf, wie einfach es ist, Strom-, Internet- und Telefonnetze zu kompromittieren.

Der bundesweite Totalausfall des T-Mobile-Netzes im April hat bewiesen, welche Folgen ein solcher Vorfall nach sich ziehen kann: 40 Millionen Deutsche ohne Handyempfang – selbst die Bundesregierung und die Polizei sollen betroffen gewesen sein. Während laut Provider ein Softwarefehler im so genannten Home Location Register (HLR) das Problem war, könnte beim nächsten Mal ein Terroranschlag die Ursache sein.

„Es ist nur eine Frage der Zeit, bis Kriminelle die Schwachstellen der BRD-Infrastruktur ausnutzen“, sagt Marco Di Filippo. „Mit entsprechendem Know-how, das sich Terroristen beispielsweise einfach aus dem Internet ziehen könnten, ist es bereits ohne allzu große finanzielle Mittel möglich, unsere Netze zu manipulieren bzw. lahm zu legen. Alles würde zusammenbrechen.“

Wie gefährdet ist Deutschland?

Die Fakten (diese basieren auf Studien der KoSiB eG):

- 79% des deutschen Telefonfestnetzes sind in fester Hand eines Anbieters
- 81% der Virenangriffe haben mit der Monokultur unserer Desktops zu tun
- 99% der Anwender unterschätzen Trojaner und Spyware
- Fast 100% Abhängigkeit von USA und Monopolisten wie Intel, IBM, Cisco, HP, Microsoft
- Selbst der Staat fördert die Ausweitung von Monokulturen

Schon eine Vielfalt an Betriebssystemen würde die Gefahr eines Dominoeffektes erheblich mindern.

Netzkrieg – die totale Kontrolle

Die Beweggründe für Angriffe auf Monokulturen sind oft der Drang danach, Können unter Beweis zu stellen, Grenzen auszutesten und Aufmerksamkeit zu erregen. Aber auch eine neue Form des Terrorismus. Wie gezielt Hacktivistinnen vorgehen, beweist die aktuelle Denial-of-Service-Attacke auf die Website des australischen Premierministers Kevin Rudd. So wollten sie ihren Protest gegen die eingeführten Internetsperren deutlich machen.

Ein mögliches Angriffsszenario in Deutschland wäre folgendes: Das Ziel ist ELSTER (Finanzamt). Die technische Umsetzung erfolgt mit Hilfe eines einzigen Computers im weltweiten Netz. Es wird ein Programm entwickelt, das Steuernummern und Namen sammelt und innerhalb weniger Stunden oder gezielt zeitversetzt über einen Monat Tausende gefälschte Steuererklärungen abgibt. Konfusion im Finanzamt, keine Einkünfte für den Staat und Verunsicherung bei den Bürgern wären die Folgen.

Ein zweites Beispiel: Deutschland ohne Internet. Frankfurt ist de facto einer der Hauptknotenpunkte für das DFN (Deutsches Forschungsnetz), .de-Domains und Providernetzwerke. Wenn Frankfurt zum Ziel wird, kann folgende Vorgehensweise das gesamte Netz zusammenbrechen lassen: Zuerst werden die Knotenpunkte vor Ort aufgespürt und Personal bei einem großen Netzbetreiber eingeschleust. Die „neuen Mitarbeiter“ eruieren die entsprechenden Leitungen und zerstören sie. Der Bedarf an Bandbreite wird nicht mehr gedeckt und Server sind dadurch nicht mehr in vollem Umfang erreichbar. Die Folgen: kein Bargeld, keine Tankmöglichkeit, keine Tickets für Verkehrsmittel, Verkehrschaos, keine Zahlungen, wirtschaftlicher Schaden etc.

Wie kann sich die BRD schützen?

IT-Sicherheitsexperte Marco Di Filippo empfiehlt: „Im ersten Schritt ist es wichtig, Prävention zu betreiben. Dazu zählt, die bundesweiten Schwachstellen auszumachen, um die Angriffspunkte zu finden. Dann gilt es, Bedrohungsszenarien zu eruieren und zu analysieren. Verantwortliche sollten sich beraten lassen, welche neuen Sicherheitslösungen sie nutzen können. Hierzu gehört auch, deutsche Entwicklungen zu fördern, sich untereinander zu vernetzen und dezentral zusammenzuarbeiten. Nur so kann den Monokulturen und somit der Angriffsfläche, die die BRD bietet, entgegengewirkt werden.“

Zeichenzahl: 4.205

Kurzporträt Compass Security AG:

Die 1999 gegründete Compass Security AG mit Sitz in Rapperswil (CH) hat sich als europäisches Dienstleistungsunternehmen auf Security-Assessments zur Vertraulichkeit, Verfügbarkeit und Integrität von Unternehmensdaten spezialisiert. Mittels Penetrationstests, Ethical Hackings und Reviews beurteilt Compass ICT-Lösungen hinsichtlich Sicherheitsrisiken präventiv, spürt vorhandene Schwachstellen auf und unterstützt bei deren Beseitigung. IT-forensische Experten ermöglichen durch Erfassung, Prüfung und Auswertung digitaler Spuren die Rekonstruktion und beweisdienliche Dokumentation von Missbrauchsfällen im Zusammenhang mit digitalen Systemen. Praxisnahe Workshops und Schulungen zum Thema IT-Security sowie Live-Hacking-Vorträge zur Usersensibilisierung runden das Portfolio ab. Neutralität und Produktunabhängigkeit sind dabei wesentliche Bestandteile der Unternehmensphilosophie. Der Kundenstamm setzt sich aus nationalen und internationalen Kunden jeglicher Größenordnung und unterschiedlicher Branchen zusammen. Weitere Informationen unter: www.csnc.ch

Weitere Informationen:

Compass Security AG
Postfach 1628
Glärnischstrasse 7
CH-8640 Rapperswil

Tel.: +41 55 214 41 60
Fax: +41 55 214 41 61
www.csnc.ch

PR-Agentur:

Sprengel & Partner GmbH
Nisterstraße 3
D-56472 Nisterau

Ulrike Peter
Tel.: +49 (0)26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: up@sprengel-pr.com
www.sprengel-pr.com