Vom Atom- zum Cyberkrieg

Freitag, 02. Dezember 2011

Ahrweiler Computer-Chaostage: Hacker-Attacken und Datenbunker

Im Oktober 1966 wird Bad Neuenahr-Ahrweiler erstmals Schauplatz eines Atomkrieges. Im Regierungsbunker wird drei Wochen geplant, geprobt, organisiert, dann ist der Krieg vorbei, Europa zerstÃ¶rt â€“ auf dem Papier. Die NATO-Ãœbungen Fallex, Cimex und Wintex sind Bestandteil des Kalten Krieges bis 1989. Doch auch heute ist die Stadt an der Ahr regelmÃ¤ÃŸig Schauplatz groÃŸ angelegter KatastrophenÃ¼bungen, die an RealitÃ¤tssinn nichts verloren haben. Aktuelles Beispiel: LÃ¼kex 11. Der Inhalt: Cyber-Attacken legen wichtige Computernetzwerke lahm. In der Folge kollabieren weite Bereiche des zivilen Lebens, wird der Staat von Hackern bedroht und erpresst.

Am deutschen Himmel ist kein Flugzeug mehr unterwegs, denn die LuftraumÃ¼berwachung kÃ¤mpft mit Viren im System. Kraftwerke sind auÃŸer Kontrolle, Stromversorger mÃ¼ssen abschalten, FinanzkreislÃ¤ufe brechen zusammen. Und in Bundes-Netzwerken reiten Trojaner ein. Wie sensibel IT-Systeme sind und wie verzahnt, macht LÃ¼kex 11 deutlich. Die so genannte â€žstrategische KrisenmanagementÃ¼bungâ€œ des Bundes ist moderner Nachfolger der Ãœbungsserie aus Zeiten des Kalten Krieges. Sie kommt heute ohne den Regierungsbunker aus, hat aber bei den Teilnehmerzahlen zugelegt. Bundesweit sind an mehreren, ganz realen Standorten, 2.500 Ãœbende in den virtuellen Cyber-Krieg gezogen.

Schlachtfeld Internet

Dabei sind die Annahmen des â€žBundesamtes fÃ¼r BevÃ¶lkerungsschutz und Katastrophenhilfeâ€œ als Ãœbungskonstrukteur und Auswerter eher defensiv ausgerichtet: die SchÃ¤den durch IT-KriminalitÃ¤t wird bei 60.000 im vergangenen Jahr festgestellten FÃ¤llen mit 61,5 Mio. Euro beziffert. Was aber mit einem Staat und seinen elektronischen Lebensadern passiert, wird eine massive Netz-Attacke gefahren, musste beispielsweise Litauen 2008 erfahren: Im Anschluss an diplomatische StÃ¶rungen zu Russland wurde das litauische Internet ideologisch mit Symbolen des Nachbarstaates (Hammer, Sichel, Sowjetstern) unterwandert, wichtige Datenwege lahm gelegt.

Seither haben sich die MÃ¶glichkeiten, Ã¼ber die virtuelle Welt ganz reale SchÃ¤den zu verursachen, verfeinert. Konsequent sind also Ãœbungen â€“ wie aktuell LÃ¼kex 11, ein Wortkonstrukt aus â€žLÃ¤nder Ãœbergreifende Krisenmanagement-Ãœbung/Exerciseâ€œ â€“ auf maximale Schadensbegrenzung ausgerichtet. Und weil kaum bekannt ist, wer der Feind ist und welche

MÃ¶glichkeiten er hat, wird der Kollateralschaden als Ausgangslage angenommen. Das unterscheidet LÃ¼kex von Wintex, wo die Ãœbenden im AbwÃ¤rtsstrudelÂ miserabler Drehbuchvorgaben trotz FreischwimmerqualitÃ¤ten im GroÃŸen und Ganzen eines Weltkrieges untergingen. Die moderne KatastrophenÃ¼bung dauert nur zwei Tage und bezeichnet den Supergau als Ausgangssituation, die es nun zu meistern gilt. Nicht Kleckern sondern Klotzen hieÃŸ es denn auch an den abschlieÃŸenden Ãœbungstagen, die eineinhalb Jahre vorbereitet wurden.

Dass man mit den Ãœbungsinhalten in eine sensible Flanke des Staatswesens stÃ¶ÃŸt, wissen auch die beteiligten BundesÃ¤mter: Schwachstellen in der IT-Sicherheit sind â€žanzunehmenâ€œ und laut Drehbuch als Korridor durch Eindringlinge lokalisiert. Doch wie im Kalten Krieg gilt auch noch heute: Offensive und Defensive entwickeln sich stÃ¤ndig weiter. Wird also ein empfindlicher Bereich nachtrÃ¤glich geschÃ¼tzt, lÃ¤uft der nÃ¤chste Versuch, das System zu knacken, lÃ¤ngst an anderer Stelle.

IT-Hightech im 70er-Jahre-Bunker

BundeslÃ¤nder wie Baden-WÃ¼rttemberg sind in diesem Hase- und Igelspiel mit der Einrichtung hochgesicherter Datentresore bereits vor Jahren neue Wege gegangen. Ausgerechnet den ehemaligen Atomschutzbunker der Landesregierung in Oberreichenbach hat man fÃ¼r die Sicherung der Landesdaten umgebaut. Wo frÃ¼her ArbeitsrÃ¤ume fÃ¼r BevÃ¶lkerungsbewegung eingerichtet waren, stehen heute sÃ¼ndhaft teure Rechner und sollen auch dann noch funktionieren, wenn der Feind Ã¼ber das Internet angreift oder den Bunker mit StromstÃ¶ÃŸen bearbeitet. Auch der gegenteiligen Idee, die Energieversorgung zu kappen, setzt die IT-Trutzburg ihr 70er-Jahre-Innenleben entgegen: Eigenstromversorgung kann fÃ¼r mehrere Wochen alles am Laufen halten.

Eine Idee, die Schule macht: Auch die ausrangierten NATO-Bunker in Ruppertsweiler und BÃ¶rfink sollen als IT-Hochsicherheitsbereiche wieder erÃ¶ffnen. Unternehmen aus Luxemburg und Leonberg wollen so ein StÃ¼ck vom Kuchen der Datensicherung abschneiden. Ãœbungen wie aktuell LÃ¼kex, bei der im ehemaligen Ausweichsitz Baden-WÃ¼rttemberg die Lichter mangels Ãœbungsteilnahme ausblieben, sind eher ein Beleg fÃ¼r die Zukunft dieses GeschÃ¤ftsmodells. Abschreckend wirkt dagegen der immens hohe Unterhalt solcher Systeme hinter mehreren Metern Stahlbeton. Allein die monatliche Stromrechnung liegt im fÃ¼nfstelligen Bereich - und die erste Ziffer hat einen respektablen Sicherheitsabstand zur Zahl eins. Auch die permanente IT-AufrÃ¼stung und der aufwÃ¤ndige Umbau in Datenbunkern schlagen zu Buche. So geht man in BÃ¶rfink zunÃ¤chst kleine Schritte und rÃ¼stet einen Ã¼berschaubaren Bereich der Anlage auf. Sollte das GeschÃ¤ft allerdings gut laufen, kann man auf fast unendliche Bunkerressourcen

zurÃ¼ck greifen. Denn wenn es etwas gibt im groÃŸen BÃ¶rfinker Keller, dann ist es Platz.

So gilt fÃ¼r das LÃ¼kex-Krisenszenario in Ahrweiler: Raus aus dem Bunker und wieder rein. Denn nach der Aufgabe des Regierungsbunkers als geschÃ¼tztem Krisenzentrum Ã¼bt man nun zwar oberirdisch, allerdings mit Inhalten, die lÃ¤ngst wieder bunkatibel sind. So sorgt die IT-Sicherheitslage fÃ¼r eine Wiederentdeckung der Schutzbauten, die zwar wegen der Sicherheitsauflagen kaum zu betreten sind, aber dank wirtschaftlicher Nachnutzung immerhin erhalten bleiben.