DENNIS DRENNER (O.); MANDEL NGAN / AFP (L.); AFP (R.)

Pentagon, Präsident Obama, Internet-Spionageziel F-35: *Spektakuläre Cyber-Angriffe*

USA

Chefsache www

Nach den jüngsten Hackerangriffen erklärt Präsident Obama Internet-Sicherheit zum Topthema und macht das Weiße Haus zur Zentrale für den virtuellen Heimatschutz.

Als die neue Chefin des US-Heimatschutzministeriums (DHS) zum Antrittsbesuch in Berlin vorsprach, wollte sie deutlich machen, dass nun eine neue Ära des Aufbruchs und des Wandels begonnen habe. Janet Napolitano referierte über globale Naturkatastrophen, unkontrollierte Einwanderung und den Drogenhandel, und irgendwann, ziemlich zum Schluss, kam sie auch auf die Gefahren des Terrorismus zu sprechen.

Ein besonderes Anliegen ihres Chefs Barack Obama erwähnte sie sogar erst auf Nachfrage: die Cyber-Sicherheit. Sofort nach Amtsantritt habe der neue Präsident eine 60-tägige Überprüfung des virtuellen Heimatschutzes angeordnet. Danach, so kündigte Napolitano in Berlin an, werde wohl einiges neu organisiert.

Die Prognose der Ministerin scheint nun einzutreffen, allerdings wohl anders, als von ihr erhofft, denn bislang trägt ihre Mammutbehörde für die Internet-Sicherheit der USA einen Großteil der Verantwortung. „Die Regierung ist nicht angemessen auf das wachsende Problem vorbereitet“, urteilte die Leiterin der Prüfkommission Melissa Hathaway, Obamas „Direktorin für den Cyberspace“, auf einer Konferenz in San Francisco und nahm eine der Konsequenzen gleich vorweg: Ihr Report empfehle dem Präsidenten eine „neue organisatorische Einheit“ direkt im Weißen Haus einzurichten. Damit würde Obama, der schon in seinem Wahlkampf das Amt eines „Cyber-Beauftragten“ in Aussicht gestellt hatte, das Thema Internet-Sicherheit zur Chefsache machen und das DHS faktisch entmachten. Mit einer entsprechenden Ankündigung des Präsidenten wird diese Woche gerechnet.

Schon im Dezember hatte das einflussreiche Washingtoner Zentrum für strategische und internationale Studien (CSIS) die virtuellen Verwundbarkeiten der USA beklagt und die Rolle des DHS scharf kritisiert. CSIS-Technologie-Direktor James Lewis begrüßt die Obama-Pläne für einen „koordinierenden Dirigenten“, möglichst mit Budgetgewalt, als überfällig. Bislang herrsche unorganisierter Wildwuchs.

In den USA vergeht kaum ein Monat ohne Meldungen über spektakuläre Cyber-Angriffe der internationalen Hackerszene auf eines der vielen amerikanischen Prestigeziele, vom Pentagon bis zur Nasa. Ziel war auch das Heimatschutzministerium selbst, bei dem 2006 insgesamt 150 Rechner mit einer Schadsoftware infiziert wurden und monatelang unbemerkt größere Datenmengen abflossen – vermutlich in Richtung Fernost. Computerexperten aus China und Russland gelten weltweit als Vorreiter im digitalen Ausspähen und Abschöpfen fremder Computernetzwerke.

So wurde jetzt ein Spionagefall rund um das bisher umfangreichste US-Rüstungsprojekt publik, das insgesamt 300 Milliarden Dollar teure Programm zur Entwicklung und zum Bau eines Kampfjets vom Typ F-35. Seit 2007 habe es wiederholt Einbrüche in die Rechner mehrerer an der Entwicklung des Jägers beteiligter Unternehmen gegeben, berichtete das „Wall Street Journal“.

US-Behörden stehen derweil unter intensivem digitalen Dauerbeschuss. Nach aktuellen Zahlen des DHS stieg allein die Zahl der Cyber-Angriffe auf Rechner der US-Regierung im vorigen Jahr um 5000 auf rund 18000, das entspricht knapp 50 Zwischenfällen am Tag. Obama war auch selbst schon Opfer – seine vielgerühmte Wahlkampfseite wurde ebenso „gehackt“ wie die seines Konkurrenten John McCain. Noch während dieses Wahlkampfs wurde Obama im traditionellen Geheimdienst-Briefing für die Kandidaten darauf hingewiesen, dass die schlimmsten Szenarien Cyber-Angriffe auf Steuerungsrechner von Stromversorgern, Schienennetzen oder der Luftraumüberwachung beinhalten.

Derlei ist keineswegs Science-Fiction: Obamas oberster Geheimdienstkoordinator, Dennis Blair, räumte vor dem US-Kongress gerade ein, dass „Staaten wie Russland und China Teile der US-Informationsinfrastruktur stören können“. Sein Cyber-Experte erklärte im April an der Universität von Texas, man habe „chinesische Netzwerkoperationen in unseren Elektrizitätsnetzwerken entdeckt“. Ob ihn das beunruhige? „Darauf können Sie wetten!“

Die Obama-Regierung will es deshalb offenbar auch nicht bei einem zentralen zivilen Verteidigungskoordinator im Weißen Haus und dickeren Budgets belassen. Auch im US-Militär, wo bislang Marine, Heer und Luftwaffe um Cyber-Kompetenzen und -Etats rangeln, soll ein eigenständiges Cyber Command für das Internet entstehen. Es wäre ein Einschnitt in der Militärgeschichte, denn damit wären Amerikas Cyber Warriors auch ganz offiziell ihren Kameraden zu Lande, zu Wasser und in der Luft gleichgestellt.

Es geht dabei keineswegs nur um defensive Kapazitäten. Die USA spielen im internationalen digitalen Rüstungswettlauf eine führende Rolle und haben sogenannte Computernetzwerkoperationen seit dem Kosovo-Konflikt bereits verschiedentlich offensiv eingesetzt, auch in Afghanistan und im Irak. Das Verteidigungsministerium baut gerade an einer „National Cyber Range“, einer Art Schießplatz, auf dem die amerikanischen Cyber-Krieger Internet-Angriffe und deren Abwehr trainieren können, wobei vor allem Letzteres vonnöten scheint. „Unsere Verteidigung ist schwach, aber unsere offensiven Kapazitäten sind so gut wie die der Russen oder Chinesen“, sagt CSIS-Direktor Lewis.

JOHN GOETZ, MARCEL ROSENBACH