



EMBASSY OF SWEDEN

Tokyo

Office of Science and Innovation

Niklas Kviselius 03-556 250 41
niklas.kviselius@growthanalysis.se



Date
11/01/2011

Löpande omvärldsbevakning

Niklas Z Kviselius, Tillväxtanalys Tokyo

1 Cyber Security – flera händelser i Japan visar på behov av stärkt IT-säkerhet

Under slutet av 2011 har så kallade ”cyberattacker” blossat upp som en het fråga bland politiker på den internationella arenan, och många ögon har riktats mot just Japan.

Inget land är numera förskonat från avancerade attacker på dess statsförvaltnings och företags IT-system. Cyberattackerna ökar i frekvens och i komplexitet och får allt större effekter på informationsutbyte begränsat till Internet, men även på den reella ekonomin - nationers, företags och individers verklighet.

1.1 Dataintrång/cyberattacker i Japan under 2011

- I april genomfördes en attack mot Sony Corp. med resultatet att personlig information för 100 miljoner kunder tillhörande PlayStation Network, inklusive en stor mängd kreditkortsnummer, senare publicerades på Internet. Ingen har tagit på sig ansvaret för denna aktion.
- I juni attackerades Nintendo i ett försök att dra ut information från dess nätverk, men där verkar attacken vara riktad mot känslig information rörande en ny större produkt lansering.
- I augusti skedde ett avancerat dataintrång i system tillhörande Mitsubishi Heavy Industries med oklar skada skedd. Företaget är Japans största försvarskontraktör. Attacken var inriktad mot företags huvudkontor, och dess fabriker tillverkande ubåtar, kärnkraftsanläggningar, och kryssningsmissiler.

Swedish Agency for Growth Policy Analysis

Tokyo
Office of Science and Innovation
Embassy of Sweden
1-10-3-400, Roppongi
Minato-ku
TOKYO 106-0032
Japan
Telephone +81 3 5562 5030
Telefax +81 3 5562 9090
info@growthanalysis.se
www.growthanalysis.se

Östersund (head office)
Studentplan 3, SE-831 40 Östersund, Sweden
Office address Studentplan 3
Telephone +46 (0)10 447 44 00
Telefax +46 (0)10 447 44 01
info@growthanalysis.se
www.growthanalysis.se
VAT Reg. no. SE 202100-6164
Bank: Nordea Bank AB
Account number: 9960-2605053327
Swift: NDEASESS
IBAN: SE9395000099602605053327

All offices
Östersund
Stockholm
Beijing
Brasilia
Brussels
New Delhi
Tokyo
Washington DC

- I oktober uppdagades även en attack med hjälp av ett virus mot Japanska Utrikesdepartementet och diplomatkåren genom en svag länk vid Japans ambassad i Seoul. Denna svaga länk öppnade informationskanaler till Japans beskickningar i Kanada, Kina, Frankrike, Myanmar, Holland, och USA. Viruset möjliggjorde att datorer på kontoren kunde nås via fjärraccess från okänd extern dator. Japanska UD kommunicerade senare att attacken inte verkar ha lett till att konfidentiell information har läckt ut. I samband med denna affär offentliggjorde även Japanska Näringsdepartement (METI) att de under 2010 haft dataintrång där ett 20-tal datorer öppnats med hjälp av virusmittade email nedladdade via email med välformulerade text och intern avsändare.

1.2 Politisk relevans, internationellt samarbete och åtgärder – IT-säkerhet högt på agendan

Händelserna har skakat om det politiska etablissemangen i Japan och skapat tydlig opinion för att landet behöver ett bättre försvar mot attacker, och att staten måste ta detta på allvar. Japans Chief Cabinet Secretary, Chair Information Security Policy Council, kände sig tvungen att efter de senaste attackerna gå ut med ett uttalande om hur Japan ska kunna besvara elden. Kärnan i framtida satsningar ska enligt detta ligga i utökade 'public-private partnerships' inom IT-säkerhet. Diskussionsgrupper med representanter från departementen och större företag som arrangerats nu i oktober/november, ska presentera sina initiala rekommendationer innan årsskiftet.

Problemet vad gäller försvar mot cyberattacker är att det naturligtvis inte räcker att sätta upp en nationell policy med lokala åtgärder som försvar mot flexibla och internationella "virtuella" fiender. U.S. Defense Secretary Leon Panetta på besök i Japan förmedlade 25 oktober att Japan och USA planerar sätta upp gemensamma projekt i syfte att hålla varandra informerade om dataintrång, och diskutera gemensamma preventiva åtgärder. Detta ska ses i ljuset av att USA, Australien och Nya Zeeland i september gjorde ett gemensamt uttalande under de tre ländernas militärpakt ANZUS (The Australia, New Zealand, United States Security Treaty), med samma innebörd. Och att President Obama valt att nyligen sätta ner foten genom att kortsluta resonemanget vad gäller kopplingen mellan Internet och den reella ekonomin, och likställa cyberattacker till direkta fysiska krigsaktioner vars bakomliggande personer kan bekämpas med konventionella vapen.

1.3 Relevans för Sverige och intressanta frågeställningar

Svenska statsförvaltningen må ha varit hittills relativt förskonade mot framgångsrika större cyberattacker – men är vi redo?

Sverige har redan kommit långt inom eFörvaltning inklusive en rad populära och resurseffektiva digitala tjänster t.ex. inom skatteadministration och bolagsbildning för att nämna några. I linje med att Sverige bygger vidare på en väl fungerande digital infrastruktur för dess medborgare – t.ex. med eJournaler - kommer

känsligheten för och åverkan vid en attack att öka. ”Cyber security” eller IT-säkerhet prioriteras nu upp ordentligt på den politiska dagordningen för många nationer.

Från statens sida handlar det om att:

- Informera anställda och bygga in senaste säkerhetstekniken i egna administrativa system
- Bygga in senaste säkerhetstekniken i system för eFörvaltning
- informera privatpersoner och företag för att skapa medvetande
- Upprätta kanaler till andra nationella initiativ för informationsutbyte och gemensamma åtgärder

Tillväxtanalys kontor fortsätter att hålla oss à jour med dessa frågor som en del av vår löpande bevakning.