Motion till riksdagen
2013/14:Ju269

av Eliza Roszkowska Öberg (M)

It-brottslighet

Förslag till riksdagsbeslut

Riksdagen tillkännager för regeringen som sin mening vad som anförs i motionen om en översyn av hur polisen bättre kan samordna verksamheten med expertis inom den privata sektorn.

Motivering

I ett samhälle som är beroende av it riskerar förekomsten av it-relaterad brottslighet att undergräva såväl allmänhetens förtroende för tekniken som staten. Det är således viktigt att lagstiftningen uppdateras i takt med utvecklingen och att myndigheterna eftersträvar att ligga ett steg före it-brottslingarna.

Under 2012 utsattes hela 65 000 svenskar för identitetsstölder. Omsatt i illegala inköp i andras namn motsvarade detta ungefär 3 miljarder kronor. Antalet identitetsstölder ökar stadigt och de brottstyper som ökade i flest antal anmälda brott 2011–2012 var bland annat bedrägeri med hjälp av internet och dataintrång.

Internationellt sett har it-brottsligheten ökat dramatiskt sedan år 2007. Tillvägagångssätten har blivit alltmer sofistikerade och svåra att utreda. Det ligger i it-brottslighetens natur att vara gränsöverskridande och att sopa igen spår. Det är en teknik som förfinats genom åren. I Sverige har dessvärre bristande resurser medfört att många anmälningar blivit liggande för att sedan skrivas av. I flera fall har det också blivit tydligt att kunskapen på it-området inte är tillfredsställande inom polisen och rättsväsendet.

Avancerade och storskaliga datorangrepp kan numera ske med hjälp av ändamålsenlig programvara. Kända exempel är Zeus och SpyEye, vars användarvänlighet och utbyggda funktionalitet möjliggjort för såväl experter som noviser att relativt enkelt fjärrstyra tusentals datorer, logga tangentnedslag, exploatera kund- och inloggningsuppgifter samt länsa bankkonton. Det

senare har drabbat många EU-medborgare i länder som Spanien och Tyskland.

Ingenting tyder på att utvecklingen avtar, utan tvärtom ökar tillgängligheten och kommersialiseringen av skadlig programvara. Ett exempel på hur långt utvecklingen gått är möjligheten att hyra så kallade botnets, med vilka beställaren via ombud kan angripa specifika mål genom så kallade distributed denial-of-service-attacker (DDoS). Denna typ av angrepp upplevde svenska myndigheter i stor skala hösten 2012. Vidare finns en rad företag som testar programvaror på sårbarheter för att sedan sälja dessa (så kallade exploits) på en internationell marknad till ibland hundratusentals kronor.

För att mota och utreda en alltmer avancerad och offensiv it-brottslighet måste polisen ligga i framkant och inhämta expertis från det civila. En snabbt expanderande informationssäkerhetsbransch skulle exempelvis kunna nyttjas till polisens och allmänhetens fördel och bespara myndigheterna både tid och resurser.

Stockholm den 27 september 2013

Eliza Roszkowska Öberg (M)