Kommittémotion

Motion till riksdagen 2017/18:3190

av Tomas Tobé m.fl. (M, C, L, KD)

Cyberbrott och internetbaserad brottslighet

Förslag till riksdagsbeslut

1. Riksdagen ställer sig bakom det som anförs i motionen om en skyndsam uppstramning av tillgången till id-handlingar för att minska id-stölder och bedrägerier och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om internationellt polisiärt samarbete rörande it-relaterad brottslighet och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om en samlad strategi för att höja kunskapen om den it-relaterade brottsligheten i hela rättsväsendet och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om ökad samordning av information kring bedrägerier, phishing och andra internetbaserade brott och tillkännager detta för regeringen.
5. Riksdagen ställer sig bakom det som anförs i motionen om branschsamverkan för att motverka internetbaserade bedrägerier och tillkännager detta för regeringen.

Motivering

De positiva effekter internetanvändandet i samhället har lett till har också en mörk baksida. En arena har öppnat upp sig för kriminalitet där den teknologiska utvecklingen i kombination med anonymiteten i användandet gör att kontroll och kartläggning av de brott som sker online är svåra att hantera. Brottslingar lockas av att risken att åka fast är liten och inkomsterna stora samtidigt som de slipper möta den utsatte öga mot öga. Krafttag måste tas mot brottslighet där internet och annan teknik används som verktyg.

Bland de brott som begås med internet som verktyg är till exempel bedrägerier och utpressning. Bedrägeribrotten inbegriper ofta till exempel id-kapningar, kontokorts-bedrägerier och annonsbedrägerier och tillhör en av de brottstyper som ökade mest i antal under 2016. Datorbedrägerierna, som ökade med 39 procent, var det brott som ökade allra mest. I de flesta fall handlar det om stulna kortuppgifter som används för köp på internet. Brottslingen kan till exempel ha hackat sig in i ett företags databas och

på så sätt kommit över tiotusentals kortuppgifter, eller ha skickat ut falska mejl där man utger sig för att vara från ett välkänt företag eller myndighet.

Många bedrägerier blir möjliga med hjälp av en kapad identitet, där gärningsmännen utnyttjar någon annans identitet för att ta lån och/eller göra inköp på kredit från flera olika ställen. Brottsoffret får ägna mycket tid och möda åt att ringa runt till flera olika banker och näringsidkare för att sätta stopp för brottslighet där brottsoffrets identitet används. Riksdagen har beslutat om ett tillkännagivande till regeringen om en brottsofferportal för personer som utsätts för id-kapningar eller bedrägerier.

Regeringen har sedan dess tagit vissa steg på området, bland annat genom att i maj 2016 ge Brottsoffermyndigheten i uppdrag att komma med förslag till ett bättre digitalt bemötande av den som blivit utsatt för brott. Förslagen presenterades i maj 2017 och föreslår bland annat att varje myndighet bör utveckla e-tjänster som möjliggör för brottsutsatta att kommunicera digitalt med myndigheterna, att Brottsoffermyndigheten bör få i uppdrag att verka för att information till brottsutsatta som presenteras på rättsväsendets webbplatser blir mer likformig och omfattar en beskrivning av hela rättsprocessen och att den drabbade bör kunna spärra sina identitetsuppgifter på ett och samma ställe.

Polisen har ägnat ökade resurser åt utredning av bedrägeribrotten sedan 2008, men enligt Brå finns fortfarande en obalans mellan brottsvolymen och de tillgängliga utredningsresurserna. Polisens förmåga står inte i paritet med antalet brott som begås, med långa handläggningstider och press att snabbt lägga ned ärenden som följd. Brottsförebyggande rådet har pekat på att det finns en uppfattning om att vissa viktiga kompetenser saknas inom polisens bedrägeriutredningsverksamhet, till exempel specialkompetens avseende välfärdsbedrägerier eller kompetenser som behövs vid analyser av olika typer av bevisningsunderlag, bland annat revisorer. Polisen måste ha de resurser som behövs för en effektiv brottsbekämpning. Riksdagen har beslutat om ett tillkännagivande till regeringen om att prioritera en stärkt förmåga inom polisorganisationen att utreda bedrägeribrott.

Brottsförebyggande rådet har betonat att det är av vikt för myndigheterna att tänka utifrån ett helhetsperspektiv när det gäller missbruk av identiteter och att de vid misstanke om att en identitet missbrukas ska sträva efter ett effektivare sätt att utbyta information. Allianspartierna anser att det behövs en utredning om ökad samordning och information mellan myndigheter i arbetet mot id-intrång för att underlätta det förebyggande arbetet, något som riksdagen har riktat ett tillkännagivande till regeringen om.

ID-handlingar

De runt 15 godkända identitetshandlingar som finns i Sverige idag kan utfärdas av tre myndigheter – Polisen, Skatteverket och Transportstyrelsen. Utöver detta kan större banker utfärda SIS-godkända id-kort (SIS = Swedish Standards Institute) åt sina kunder, och anställda vid vissa företag och myndigheter kan få SIS-godkända id-kort utfärdade av sina arbetsgivare. Det stora antalet godkända identitetshandlingar i Sverige benämns i Brottsförebyggande rådets kartläggning av bedrägeribrottsligheten i Sverige som ett problem. Det underlättar missbruk och gör det svårare att kontrollera identiteter. Två åtgärder efterfrågas från flera berörda myndigheter och delar av näringslivet: ett nationellt id-kort samt en central aktör som garanterar säkra identitetshandlingar. Kvaliteten på och antalet godkända id-handlingar i Sverige bör snarast ses över, för att

på så vis minska möjligheterna till utnyttjande av annans identitet. En utredning tillsattes i augusti 2017 i mening att förbättra hanteringen och säkerheten kring svenska identitetshandlingar. Med anledning av det stora antalet bedrägerier måste en skyndsam förändring till för att skydda enskilda från identitetsstölder och bedrägerier.

Internationellt samarbete

I maj 2017 infekterade en massiv krypteringsattack hundratusentals datorer i runt 150 länder. Attacken spred ett krypteringsvirus (ransomware) som låste filer på infekterade datorer. Krav på tusentals kronor i ersättning krävdes för att upplåsning av datorerna skulle ske. Detta exempel är bara ett av många där internetrelaterad brottslighet har en internationell prägel.

Eftersom många internetbaserade brott kan spåras utomlands minskar möjligheterna att klara upp brotten. I de fall då andra stater ligger bakom dataintrång eller annan brottslighet ökar svårigheterna att utreda brottet och väcka åtal ytterligare. Internationellt polisiärt samarbete är därför viktigt för att kunna lagföra många av de som står bakom olika typer av internetbaserad brottslighet. Svensk polis deltar redan nu i internationell verksamhet inom ramen för operativa och strategiska avtal med länder och organisationer. EU-samarbetet liksom det nordiska polissamarbetet, Schengensamarbetet, de internationella missionerna samt det arbete som sker via Polisens sambandskontor utomlands har hög prioritet. Samarbetet med organisationer som till exempel Europol, Cepol och Interpol är också centralt för den internationella verksamheten. En ökad internationalisering av brottsligheten, framför allt när det gäller brott som begås med internet som redskap, ställer krav på ökat internationellt samarbete på mellanstatlig och polisiär nivå och en översyn av detta bör därför göras.

Samlad strategi för att höja utbildningsnivån för att utreda IT-relaterad brottslighet

Internet har också blivit en ny arena för brott. Hat, hot och kränkningar sprids på bloggar och andra forum, ett snabbt klick på en länk kan leda till ett länsat bankkonto, att öppna en fil kan leda till att samtliga filer på datorn krypteras och genom utpressning kan vi tvingas att betala för att få tillbaka kontrollen över våra datorer. För att möta hoten inom IT-området är det viktigt att höja kunskapen om den IT-relaterade brottsligheten i hela rättsväsendet. Fler brott måste utredas och bestraffas, men kunskapen inom rättsväsendet är ofta bristfällig och anmälningar blir liggande eller läggs ner i samma ögonblick som de kommer in. Det behövs en samlad strategi för att se över hur man kan höja utbildningsnivån för att utreda IT-relaterad brottslighet inom hela rättsväsendet.

Ökad information

Den krypteringsattack som nämnts ovan och som i maj 2017 påverkade hundratusentals personer världen över är bara en av de attacker som har skapat stora svårigheter för såväl privatpersoner som företag. Risken för att falla offer för den här såväl som andra typer av IT-relaterade brott, såsom till exempel phishingmejl, där brottslingen försöker få tillgång till exempelvis lösenordsinformation eller kontokortsnummer, är stor, men kan till stor del undvikas om man har rätt kunskaper. Många brott kan undvikas genom

att konsumenter och företag ges ökad information kring hur man undviker att utsättas för såväl bedrägerier och annan typ av internetrelaterad brottslighet. Om man utsätts är det också viktigt att man i enlighet med Brottsoffermyndighetens förslag, och även allianspartiernas tidigare förslag om en brottsofferportal, kan spärra sina identitets-uppgifter på ett och samma ställe.

Samverkan för att motverka bedrägerier

Flera branscher som berörs av bedrägerier har forum eller branschorganisationer där säkerhetsansvariga träffas för att utbyta erfarenheter och viss samverkan och utbyte av information sker redan inom näringslivet. Enligt Brottsförebyggande rådet är samordningen viktig för att snabbt identifiera nya brottstrender och genom att konkurrenter enas om en standard i säkerhetsfrågor blir det lättare att öka intresset för säkerhet hos företagen. Branscher som inte har några samverkansforum och företag som inte ingår i en branschorganisation har å sin sida mycket att vinna på att inleda samarbeten eller kopiera säkerhetslösningar. I annat fall finns en risk att de drabbas hårdare av brottsligheten, eftersom de annars lättare kan uppfattas som måltavlor. Intervjuerna med gärningspersonerna talar enligt Brottsförebyggande rådet också för att det snabbt sprider sig vilka företag som ligger efter med säkerhetsarbetet. Näringslivet har ansvaret för ökad samordning av information såväl när det gäller bedrägerier som när det gäller annan typ av IT-relaterad brottslighet. Regeringen bör se över möjligheten att underlätta ökad samordning av information för att motverka denna typ av brottslighet.

Tomas Tobé (M)

Johan Hedin (C)

Roger Haddad (L)

Andreas Carlson (KD)