2025-01-14

Finansdepartementet
Försvarsdepartementet
Justitiedepartementet

Stärkt krishantering vid stora cyberangrepp

Svenska Bankföreningen hemställer om att regeringen *dels* vidtar åtgärder för att stärka krishanteringen vid stora cyberangrepp mot den finansiella sektorn, *dels* inför brottet datastörning i brottsbalken. Förslagen enligt denna hemställan är sammanfattningsvis följande.

1. Tillse att Riksbanken får i uppdrag att snarast etablera funktionen för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur.

2. Tillse att Riksbanken får i uppdrag att tillsammans med Nationellt cybersäkerhetscenter, NCSC, definiera tydliga roller och ansvar för funktionen gentemot NCSC, CERT-SE och Försvarets Radioanstalt, FRA, för krishanterande och stödjande åtgärder vid cyberangrepp mot samhällsviktig finansiell verksamhet.

3. Tillse att Riksbanken, med stöd av NCSC, CERT-SE och FRA, får i uppdrag att etablera konkreta stödjande åtgärder till verksamhetsutövare av samhällsviktig finansiell verksamhet vid omfattande cyberangrepp.

4. Inför brottet datastörning i brottsbalken.

Besök (Visit):
Blasieholmsgatan 4B
Stockholm
Sverige (Sweden)

Post:
Box 7603
SE-103 94 Stockholm
Sverige (Sweden)

t: +46 (0)8 453 44 00

e: info@swedishbankers.se
www.swedishbankers.se

AVSNITT 1

Bakgrund krishantering vid cyberangrepp

Sedan Rysslands olagliga annektering av ukrainska Krim 2014 har Sveriges säkerhetspolitiska läge successivt försämrats. I och med Rysslands invasion av Ukraina i februari 2022 har den europeiska säkerhetsordningen upphört som ett gemensamt system. Sverige befinner sig i ett besvärligt säkerhetspolitiskt läge vilket också påverkar hotbilden mot den finansiella sektorn och bankerna.

Risken för antagonistiska gråzonsaktiviteter med syfte att påverka banker och finansiell infrastruktur bedöms ha ökat. Svenska banker utgör idag en stor del av de baltiska ländernas finansiella infrastruktur vilket också påverkar hotbilden. Bankerna har det yttersta ansvaret för sin egen säkerhet. De är vana vid att skydda verksamheten mot olika hot och att planera och öva för att kunna hantera och återställa verksamheten vid cyberangrepp och incidenter. Utvecklingen kräver ett långsiktigt beredskapsarbete i Sverige och förmågan att kunna upptäcka och bekämpa storskaliga cyberangrepp mot privata verksamhetsutövare som bedriver samhällsviktig verksamhet såsom bankerna.

Under senare delen av 2024 har svenska banker blivit utsatta för avancerade överbelastningsattacker i syfte att påverka internettjänsters tillgänglighet. Överbelastningsattacker är i sig inget nytt för bankerna, de har förekommit från tid till annan under åtminstone de tio senaste åren. De senaste angreppen visar dock på en ökad styrka och omfattning enligt följande exempel.

- Varaktigheten: Varaktigheten har ökat tiofaldigt jämfört med tidigare förhållanden.
- Styrkan: Angreppen har varit cirka 15 gånger kraftigare än tidigare.
- Skadan: Den exakta kostnaden är svår att beräkna med prislappen för angreppen beräknas uppgå till tvåsiffriga miljoner. Angreppen drabbar framför allt förtroendet för verksamheten.
- Geografin: Angreppen har skett från nordiska IP-adresser, vilket försvårar avvärjning.
- Syftet: Hotaktören har inte publikt uttalat något syfte med angreppen.

Angreppen utgörs av koordinerade och synkroniserade handlingar som avsiktligen inriktas mot sårbarheter i finansiella system. Motiven till denna typ av angrepp kan vara flerfaldiga, men på ett övergripande plan handlar det om att destabilisera och skada förtroendet för de finansiella tjänsterna och de finansiella företag som utför dessa. Detta kan leda till oönskade följdeffekter för samhällsekonomin, förtroende för den svenska finansiella marknaden internationellt och den fria konkurrensen.

Vidare kan olika destabiliserade åtgärder samverka för att få människor att vidta åtgärder för att skydda sina medel. Åtgärder som objektivt sett är omotiverade, men som tack vare desinformation om störningarna via till exempel sociala medier kan

förefalla vara rationella för den enskilde. Att inte kunna logga in i internetbanken och kontrollera sina tillgångar skapar dessutom oro och frustration hos den enskilde.

Det primära syftet med angreppen är informationspåverkan mot samhället och medborgarna genom att angriparna försöker visa att samhällsviktiga finansiella tjänster är i fara och därmed underminera förtroendet för finansiell samhällsviktig verksamhet. Om desinformation om allvarliga IT-incidenter inom de finansiella företagen får spridning och skapar "flockbeteenden" hos befolkningen kan följderna för den finansiella stabiliteten bli allvarliga.

Oklara mandat och ansvar för att avhjälpa cyberangrepp

NCSC har sedan 2022 en etablerad samverkan med samhällsviktiga aktörer inom finansiell sektor, "Finansforum". Målet för forumet är att stärka cybersäkerheten inom finanssektorn och öka Sveriges motståndskraft mot cyberangrepp. En viktig effekt av samverkan är att säkerställa kundernas och allmänhetens förtroende för det finansiella systemet. Forumet är dock främst inriktat på förebyggande åtgärder som exempelvis informationsdelning och har ingen incidenthanterande eller stödjande funktion vid större cyberangrepp.

I anslutning till de överbelastningsattacker som drabbade bankerna under hösten 2024 har bankerna som en del av sin incidenthantering sökt stöd och samverkan med NCSC, de i centret ingående myndigheterna och CERT-SE. Styrning och ledning från myndigheterna har upplevts som otydlig. Det är också oklart vilket stöd bankerna kan förvänta sig i anslutning till incidenthanteringen. Ingen av de i NCSC ingående myndigheterna förefaller ha något tydligt ansvar eller mandat att ingripa eller för att stötta i avhjälpandet av cyberangreppen. Det är också oklart om och i så fall hur myndigheterna ska kommunicera externt om cyberangreppen till allmänheten.

Brister i styrning och ledning av krishanteringsarbetet

I ett framåtblickande perspektiv är det oklart hur statens krishanteringsarbete vid cyberangrepp ska styras och ledas i förhållande till den finansiella sektorn. Finansdepartementets utredning "En ny funktion för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur"[1] presenterades i januari 2024 och föreslår att en sådan funktion ska inrättas av Riksbanken. Bankföreningen har ställt sig positiva till förslagen i utredningen. Ett knappt år senare finns dock inga besked om förslagen kommer att realiseras. Samtidigt pågår omorganiseringen av NCSC där FRA ska ha huvudansvar för att leda samordning, utveckling och genomförande av centrets verksamhet. I förslaget till Förordning om Nationellt cybersäkerhetscenter framgår inget om centrets uppgifter eller ansvar för krishanteringsåtgärder eller stöd till privata verksamhetsutövare vid större

[1] En ny funktion för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur - Regeringen.se

cyberangrepp. Utredningens förslag om att flytta CERT-SE från MSB till FRA och NCSC är bra och bör ske skyndsamt.

Förslag för att stärka krishanteringsarbetet vid cyberangrepp mot samhällsviktig finansiell verksamhet

a) Ledning och styrning

1. Inför snarast förslagen i utredningen "En ny funktion för krishantering vid allvarliga driftstörningar i den finansiella sektorns digitala infrastruktur" där Riksbanken ges uppdrag att etablera funktionen.

2. Tillse att Riksbanken får i uppdrag att tillsammans med NCSC definiera tydliga roller och ansvar för funktionen gentemot NCSC, CERT-SE och FRA för de krishanterande och stödjande åtgärder vid cyberangrepp mot samhällsviktig finansiell verksamhet.

3. Bankföreningen välkomnar regeringens förslag i Totalförsvarspropositionen 2025 - 2030 där det framgår att cyberförsvarsförmågan ska utökas och att ytterligare cyberförsvarsförband etableras och organiseras. Bankföreningen delar också regeringens förslag att cyberförsvarsresurserna i fred kan bidra till cybersäkerhetsarbetet inom ramen för NCSC då delar av cyberförsvaret kan fokusera på att stötta samhällsviktig verksamhet[2].

b) Stöd till samhällsviktig finansiell verksamhet vid omfattande cyberangrepp

Funktionen med stöd av NCSC, CERT-SE och FRA ska:

1. Vägleda de privata aktörerna i den finansiella sektorn med att identifiera omfattningen och konsekvenserna av cyberangrepp mot samhällsviktig finansiell verksamhet och arbeta för att begränsa incidenter när de inträffar.

2. Tydliggöra vilket stöd och vilken hjälp de privata aktörer kan förvänta sig. Införa rutiner för eskalering och slå fast vilka åtgärder som ska sättas in givet cyberangreppets omfattning.

3. Analysera, berika och dela indicators of compromise (IOCs)[3] med de privata aktörerna samt annan relevant teknisk information.[4]

[2] Totalförsvaret 2025-2030
[3] Digitala bevis om att ett angrepp har inträffat.
[4] Idag sker detta endast i det förebyggande arbetet, inte i anslutning till att cyberangrepp sker.

4. Vägleda drabbade organisationer och deras incidenthanteringsfunktioner under cyberangreppet.

5. Bistå brottsbekämpande och nationella säkerhetsmyndigheter med information om cyberangreppet.

6. Säkerställa att sakligt korrekt, sammanhängande och enhetlig kommunikation ges till allmänheten, drabbade organisationer och andra intressenter.

Avslutningsvis vill Bankföreningen i denna del anföra att CERT-SE bör stärkas och ges ett tydligare incidentkoordinerande ansvar för de drabbade organisationerna under ett cyberangrepp och de myndigheter som är delaktiga i incidenthanteringen. Slutligen bör Polismyndigheten tillföras resurser så att myndigheten aktivt kan delta i NCSC Finansforum.

AVSNITT 2

Bakgrund straffrättsligt perspektiv och problembild

När ett finansiellt företag utsätts för ett angrepp som stör eller hindrar allmänhetens tillgång till dess tjänster blir detta uppenbart för såväl bankkunder som andra finansiella aktörer. Ofta går det inte att till exempel logga in, nyttja identifieringstjänster eller genomföra betalningar.

Aktörerna på den finansiella marknaden arbetar samtidigt intensivt för att stoppa angreppet och återställa tillgängligheten, vilket i vissa fall kan ta en inte obetydlig tid. Under tiden erhåller kunden om möjligt information om status och prognos för störningen.

Någon närmare extern information om den bakomliggande orsaken till störningen kan ofta vara svår att lämna, vilket i sin tur kan bero på till exempel att dessa omständigheter är okända för det finansiella företaget eller att brottsbekämpande myndigheter utreder eller kan behöva utreda saken och att kommunikation till kunderna kan försvåra en sådan utredning.

Sammantaget kan detta skapa en oro och frustration hos kunderna. Tjänster som finansiella företag erbjuder, innefattande till exempel förvaltning av någons ekonomiska tillgångar, är så pass viktiga att information som lämnar minsta utrymme för misstolkning kan få oönskade följder.

Ingen är betjänt av att angriparna lyckas uppnå sina syften, det vill säga att skapa oro, undergräva förtroendet och destabilisera.

Dataintrång är ett missvisande begrepp

Inom den svenska strafflagstiftningen infördes år 1973 brottet dataintrång.[5] Dataintrång, som sedan uppkomsten har varit en teknikneutral bestämmelse, har med tiden kommit att omfatta olikartade situationer av otillåtna intrång, påverkan, m.m. Värt att notera är att det inte ställs krav på att dataintrånget sker i ett visst syfte eller att det medför någon särskild effekt, såsom skada. Inte heller förutsätts att någon säkerhetsåtgärd kringgås.

Den tekniska utvecklingen, inte minst i förhållandet till uppkomsten av internet, har sedan år 1973 varit omfattande – informationstekniken nu och då är inte jämförbar. Utvecklingen har inneburit att dataintrång har kommit att omfatta skeenden som inte existerade när lagen stiftades.[6]

Den vida och – utifrån den informationstekniska utvecklingen – utökade tolkningen medför dock bristande precision i förhållande till alltmer komplicerade brottsmodus. Det är naturligtvis inte önskvärt med brottsbeskrivningar som i detalj preciserar ett specifikt modus med en viss teknik. Det skapar inlåsningseffekter och en alltför snabbt obsolet lagstiftning.

Istället är det fråga om att hitta en lämplig balans mellan precision, effektivitet och förutsägbarhet inför lagen. Begreppet dataintrång torde för de flesta skapa en föreställning om att ett data- eller informationssystem har utsatts för just ett intrång. Att någon obehörigen har berett sig tillgång till ett innehåll genom att tränga in bakom ett skydd av något slag, ofta ett så kallat skalskydd.

I förhållande till bankverksamhet ligger det – utifrån bankkundens synvinkel – nära till hands att kunden drar den felaktiga slutsatsen att ett brottsligt angrepp riktats mot dennes tillgångar, som därmed är i fara. Eller i vart fall att någon obehörig kan ta del av uppgifter om kundens konton m.m. och dra nytta av denna information. Att detta ska bli bankkundens upplevelse av situationen är i linje med de syften som angriparen har. På så sätt undergrävs förtroendet för bankväsendet och förmågan till finansiell stabilitet.

Dataintrång är därmed en missvisande och vilseledande brottsrubricering i exempelvis de vanligt förekommande situationer som utgörs av överbelastningsattacker.[7] Följderna av denna vilseledande rubricering är i praktiken vidsträckta eftersom de har direkt bäring på brottets syften.

Vidare minskar den missvisande rubriceringen i vissa fall benägenheten från privata aktörer såsom finansiella företag att anmäla brottsligheten till brottsbekämpande

[5] Se vidare appendix.
[6] Det är svårt att skatta om, och vilken omfattning det i praktiken numera uppkommer situationer där svårigheter föreligger att applicera brottsrubriceringen dataintrång. Eftersom tolkningen av brottet är vid och förarbeten samt praxis vid olika tidpunkter har utökat tillämpningen, om än på ett relativt svåröverskådligt vis, är det rimligt att föreställa sig att det är sällsynt.
[7] Motsvarande resonemang är relevant även för andra samhällsviktiga informationssystem som mer eller mindre frekvent utsätts för överbelastningsattacker, tillhörande till exempel sjukvården, Försäkringskassan, Skatteverket eller andra statliga myndigheter.

myndigheter. Finansiell verksamhet bygger i mångt och mycket på allmänhetens förtroende och spridandet av desinformation om dataintrång hos en bank, när något intrång per definition överhuvudtaget inte ägt rum, kan vara förödande för verksamheten. Detta i synnerhet vid upprepade fall och hos mindre aktörer. Det är nämligen inte ovanligt att samma finansiella företag utsätts för upprepade överbelastningsattacker.

Det är även av vikt för de finansiella företagen att i möjligaste mån ha kontroll över vilken information om angrepp mot företagen som sprids till allmänheten samt vid vilken tidpunkt och på vilket sätt detta sker. Det är inte fråga om att undanhålla allmänhet, media eller myndigheter information, utan att begränsa risker och skadeverkningar såväl i ekonomiskt som förtroendemässigt hänseende. Att de finansiella företagen drabbas av förluster till följd av brott och nedsatt förtroende är knappast önskvärt. I förlängningen drabbar detta såväl kunder som samhället i stort.

På grund av den nuvarande strafflagstiftningens bristande precision måste missvisande beskrivningar och kommunikation avseende incidenter med brottslig bakgrund i så stor utsträckning som möjligt undvikas. Detta oavsett om kommunikationen härrör från de finansiella företagen, de brottsbekämpande myndigheterna eller funktioner som NCSC.

Behov av en mer utvecklad och preciserad lagstiftning

Det är rimligt att påstå att svensk lagstiftning ofta har värnat enkelhet, enhetlighet och teknikneutralitet. Dessa är i allmänhet eftersträvansvärda intressen och förenklar tillämpningen inom inte minst teknikdrivna rättsområden, även om det i vissa fall kan ske på bekostnad av förutsebarhet och rättssäkerhet.

Det ifrågasätts inte att dataintrångsbestämmelsen, utifrån dess vidsträckta motiv, ska tolkas på ett sådant sätt att överbestaningsattacker faller in under tillämpningsområdet. Inte heller ifrågasätts i allmänhet de slutsatser som *Utredningen om it-brottskonventionen*[8] kom till i dessa delar, utifrån de förhållanden som förelåg vid tidpunkten.

Värt att notera är dock att till exempel Finland valt en annan väg. Utan att i detta sammanhang närmare gå in på konventionens[9] krav, införde den finska lagstigaren en brottskatalog innefattande bl.a. brotten *störande av post- och teletrafik* och *systemstörning*.[10] Bestämmelser som, i enlighet med parlamentets och rådets syften, på ett mer adekvat sätt beskriver den it-relaterade brottsligheten.

Aktörerna i Finland, såväl de brottsbekämpande myndigheterna som de finansiella företagen, har därmed en annan spelplan som skapar ett större mått av förutsebarhet och stabilitet när det gäller bl.a. extern kommunikation och premisser för brottsanmälningar.

[8] Se vidare appendix.
[9] Europarådets konvention om it-relaterad brottslighet och dess tilläggsprotokoll.
[10] Jfr. Finska strafflagen (19.12.1889/39), 38 kap. ”Om informations- och kommunikationsbrott”.

Även om anpassningen av den finska strafflagstiftningen möjligen inte fullt ut passar svenska förhållanden torde det finnas alternativ som utgör åtminstone ett närmade i förhållande till konventionsbestämmelserna och som skapar tillräcklig förutsebarhet, tydlighet och överskådlighet.

Det nya brottet datastörning ska införas i brottsbalken

Utgångspunkten enligt vad som framförts ovan är att brottsrubriceringen dataintrång inte på ett ändamålsenligt vis beskriver eller återspeglar bland annat de överbelastningsattacker som drabbar inte bara finansiella företag, utan även andra aktörer såsom myndigheter och organisationer.

Ingen av dessa aktörer är betjänta av en felaktig beskrivning av ett skeende, som innebär att de ska ha utsatts för ett obehörigt intrång. Den enda aktör som är betjänt av en sådan beskrivning är den antagonist som ligger bakom eller utfört överbelastningsattacken. En attack framstår antagligen för antagonisten som mer lyckad om den även innebär ett intrång i ett skalskydd och därmed utgör ett hot mot information som finns förvarad där.

Vad det i själva verket är fråga om är en störning av ett informationssystem som kan vara mer eller mindre varaktig. Denna störning drabbar tillgången till -, eller driften av ett visst system eller viss tjänst, dvs. inte uppgifterna eller innehållet bakom. Bara detta förhållande i sig talar för behovet av en ny straffbestämmelse.[11]

Bestämmelsens skyddsintresse tar alltså sikte på kontinuiteten av en viss tillgång och straffbelägger uppsåtliga störningar av denna kontinuitet.

Den som ska dömas för *datastörning*[12] är den som obehörigen överbelastar, hindrar, avbryter eller annars stör ett informationssystems funktion.

Själva störningen kan utgöras av ett aktivt handlande i form av upprepade anrop eller organisation av sådana anrop, eller andra liknande åtgärder i angivet syfte.

Handlandet bör kräva resultat i form av att åtminstone en olägenhet inträder för någon, men inte nödvändigtvis en påvisad skada för denne.

För att datastörningen ska kvalificeras som *grovt brott* kan ledning hämtas från de rekvisit som kvalificerar dataintrång som grovt, dvs. om gärningen har *"orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art".*[13]

Värt att notera i detta sammanhang är att överbelastningsattacker ofta torde vara svåra att skatta i termer av ekonomisk skada och antalet uppgifter som attacken

[11] Jfr. brytande av post- eller telehemlighet jämlikt 4 kap. 8 § brottsbalken, som skyddar själva meddelandet och inte dess innehåll i sak.
[12] Andra brottsrubriceringar, såsom till exempel ”systemstörning” eller ”cyberstörning” är tänkbara. Av grundläggande intresse är dock konventionen och direktivet gör åtskillnad på intrång i informationssystem, systemstörning respektive datastörning.
[13] Jfr. 4 kap 9 c § andra stycket brottsbalken.

avsett. Avgörande för att en datastörning ska vara för handen bör istället vara om angreppet skett mot en samhällsviktig funktion, dvs. störningens faktiska eller potentiella farlighet för samhället. Den nya kvalificerande bestämmelsen bör återspegla detta.

Den som på ett eller annat vis *tränger in* i informationssystemet under sådana förutsättningar som anges i 4 kap 9 c § brottsbalken, eller utför andra åtgärder som enligt tidigare förarbeten och praxis hittills ansetts omfattas av dataintrång, ska alltså även fortsättningsvis dömas för detta brott.

Även om det primära syftet med föreslagen lagstiftning om datastörning är tydlighet och förutsebarhet inom svensk jurisdiktion, innebär förslaget att svensk strafflag på området på ett tydligare sätt, än vad som är fallet för närvarande, närmar sig vad som föreskrivs enligt konventionen. Vidare skapar en harmonisering inom EU förutsebarhet för finansiella företag som driver gränsöverskridande verksamhet inom EU. Det torde för övrigt inte vara ovanligt att en störning hos en bank med gränsöverskridande verksamhet drabbar tillgängligheten i bankens verksamhet olika länder.

Det finns anledning att understryka att brottslighet i form av storskaliga angrepp mot till exempel samhällsviktig bankinfrastruktur är särskilt allvarlig. En ny brottsrubricering skulle även kunna bidra till en större diversifiering inom domstolarnas straffmätning och även ge möjlighet att under förundersökning använda vissa hemliga tvångsmedel.

SVENSKA BANKFÖRENINGEN

Hans Lindberg

Erik Wendeby

Magnus Jacobson

Appendix

Bestämmelsen om dataintrång infördes i brottsbalken 1998 i samband med att den tidigare datalagen (1973:289) ersattes med personuppgiftslagen (1998:204). Datalagens bestämmelse om dataintrång (21 §) överfördes då till brottsbalken utan ändring i sak. Bestämmelsen om dataintrång fick sin nuvarande sakliga utformning genom en lagändring 2007 som i huvudsak syftade till att genomföra EU:s rambeslut 2005/222/RIF om angrepp mot informationssystem. Då skedde även ett förtydligande och en språklig modernisering av dataintrångsbestämmelsen. Avsikten med det valda begreppet är att fånga in alla uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för en dator anpassad och läsbar form och att även program av olika slag ska omfattas av begreppet (prop. 2006/07:66 s. 40 och 49).

I augusti 2013 beslutades Europaparlamentets och rådets direktiv 2013/40/EU om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF (fortsättningsvis direktivet). Direktivet trädde i kraft den 3 september 2013 och skulle vara genomfört av medlemsstaterna senast den 4 september 2015.

Regeringen gav i oktober 2011 en särskild utredare i uppdrag att, efter en behovsanalys, lämna förslag på de författningsändringar som krävdes för att Sverige ska skulle kunna tillträda Europarådets konvention om it-relaterad brottslighet och dess tilläggsprotokoll (fortsättningsvis konventionen). Utredningen, som tog namnet Utredningen om it-brottskonventionen, fick genom tilläggsdirektiv den 11 oktober 2012 i uppdrag att även analysera behovet av och lämna förslag till de författningsändringar som behövdes för att genomföra direktivet.

Utredningen om it-brottskonventionen överlämnade i maj 2013 betänkandet Europarådets konvention om it-relaterad brottslighet (SOU 2013:39), vilken i sin tur utmynnade i propositionen Skärpt straff för dataintrång (Prop. 2013/14:92) och efterföljande riksdagsbeslut om straffskärpning.

I betänkandet gjordes en rad överväganden om behovet av lagändringar i förhållande till dels konventionen, dels direktivet. Sammanfattningsvis blev bedömning att svensk rätt genom främst dataintrångsbestämmelsen, uppfyller konventionens krav på vad som ska vara straffbelagt som systemstörning. Vidare behandlades frågan om överbelastningsattacker mot banker, varvid slutsats drogs att det är mycket tveksamt om andra straffbestämmelser än dataintrångsbestämmelsen skulle bli tillämpliga, trots att angreppet fått vittgående konsekvenser (SOU 2013:39, s 303).

Av intresse i förhållande till denna framställning är vidare att den som olovligen allvarligt stör eller hindrar användningen av en uppgift som är avsedd för automatiserad behandling omfattas av brottsrubriceringen dataintrång. Det straffbara förfarandet tar sikte på åtgärder som verkar på ett sådant sätt att de stör eller hindrar att uppgifter som är avsedda för automatiserad behandling kan användas på avsett sätt, dvs. åtgärder som påverkar driften av ett system och därmed också användningen av de uppgifter som finns i systemet utan att uppgifterna helt blockeras (prop. 2006/07:66 s. 43–44 och 50). Som exempel på sådana åtgärder nämns i propositionen tillgänglighetsattacker eller överbelastningsattacker. Vidare

anges att det t.ex. kan handla om program som skapar och sänder så stora mängder e-post att mottagarens system kollapsar eller får kraftigt nedsatt funktion och därmed hindrar eller stör användningen av de uppgifter som finns i systemet (prop. 2006/07:66 s. 50). Som ytterligare exempel på åtgärder som kan verka på ett sådant sätt nämns i propositionen bl.a. upprepade anrop eller försök till anrop.