Promemoria
2018-06-29

Dnr/ref: 2018-57

Johan Bålman
Johan.balman@pensionsmyndigheten.se
0722102619

Åtgärder mot att användare vilseleds att logga in någon annan med sin e-legitimation

Allt fler rapporter har kommit om att företag erbjuder webbtjänster som uppmanar sina användare att legitimera sig mot myndigheters e-tjänster. Den som släpps in i e-tjänsten är emellertid inte användaren utan företaget som hämtar information. På detta sätt vilseleds användare att logga in någon annan med sin e-legitimation.

En myndighet behöver stoppa detta om det sker i myndighetens e-tjänster eftersom det är straffbelagt enligt 15 kap. 12 § brottsbalken som missbruk av urkund. Det kan också strida mot dataskyddsförordningen, offentlighets- och sekretesslagen, registerlagar eller författningar på informationssäkerhetsområdet.

eSams juridiska expertgrupp anser att det nu behövs en samordnad informationsinsats riktad mot i första hand privatpersoner kring detta.

Inledning

I ett rättsligt uttalande den 24 april 2017 har eSam redovisat bestämmelser i brottsbalken där straff föreskrivs för den som åberopar någon annans e-legitimation för att bli insläppt under sken av att vara den som anges i e-legitimationen.

I maj 2018 har regler införts i betaltjänstlagen enligt vilka en tjänsteleverantör måste identifiera sig vid varje transaktion. Pensionsmyndigheten har i sina föreskrifter infört regler om att e-legitimation inte får användas i myndighetens tjänster så att den åberopas såsom gällande för någon annan än den e-legitimationen avser. Missbruk med användning av bankers webbtjänster har därefter i praktiken förhindrats.

Allt fler rapporter har emellertid kommit om att företag i sina webbtjänster uppmanar sina användare att legitimera sig gentemot myndigheters tjänster för att företagets tjänst ska kunna hämta information under sken av att det är användaren som själv besöker myndighetens tjänst. Ofta införs detta med hjälp av tjänsteleverantörer som utvecklar och tillhandahåller särskilda tjänster för att genomföra missbruket.

För allmänhetens tillit till e-legitimationer är det av avgörande betydelse att de inte missbrukas. Åtgärder måste därför vidtas. Som ett första steg föreslås en samordnad informationsinsats riktad till användare (som indirekt även når företagen och deras tjänsteleverantörer) om att dessa missbruk är kriminaliserade.

Samordningen föreslås ske så att myndigheter inför en varningstext med samma ordalydelse, ”Du får inte släppa in någon annan”, på de webbsidor där användare väljer e-legitimation för att logga in. Texten länkar till den nya webbplatsen e-legitimation.se som riktar sig till privatpersoner och den text som finns där om hur man skyddar sin e-legitimation.

Utgångpunkter

Myndigheter och företag ser missbruk av e-legitimation genom s.k. overlayteknik som ett konkret hot. Dessa förfaranden kan förenklat beskrivas genom en jämförelse med fysisk miljö där någon missbrukar en annan persons legitimationshandling, t.ex. ett körkort eller ett pass, för att bli insläppt någonstans.

Sådana förfaranden kan i och för sig användas öppet (jfr när den som hämtar ett paket i egenskap av bud ska visa både sin och mottagarens legitimation – användningen av annans e-legitimation sker då inte ”sanningslöst”). Men i it-miljö används overlayteknik ofta på ett dolt, vilseledande och rent av brottsligt sätt. Det analysarbete som bedrivits av myndigheter har resulterat i bedömningen att förfaranden av det slaget är straffbara enligt 15 kap. 12 § BrB som missbruk av urkund.

Vad som nu tillkommit, är att

- försäkringsförmedlare erbjuder som allmänt spridd tjänst att hämta information från t.ex. www.minpension.se,
- privata företags webbplatser börjat erbjuda användare inloggning till t.ex. www.skatteverket.se, för att det företag som tillhandahåller tjänsten ska hämta information för att verifiera användarens personuppgifter (samtidigt blir all information om användaren och alla tjänster på skatteverket.se tillgängliga för företaget),
- från maj detta år gäller nya regler i betaltjänstlagen enligt vilka berörda tjänsteleverantörer måste identifiera sig vid varje transaktion, jfr att en mellanman i traditionell fysisk miljö vanligtvis ska presentera fullmakt eller andra behörighetshandlingar, allt ska enligt betaltjänstlagen ske öppet[1], och
- Pensionsmyndigheten i sina föreskrifter (PFS 2018:1) om ändring i Pensionsmyndighetens föreskrifter (2012:9) om självbetjäningstjänster via internet har infört en bestämmelse om att en e-legitimation inte får användas i Pensionsmyndighetens självbetjäningstjänster via internet så att den åberopas såsom gällande för någon annan än den som e-legitimationen avser (3 a §).

Det finns alltså både nya tjänster som bygger på missbruk och nya regler för att skydda mot missbruk.

[1] I regeringens proposition 2017/18:77 Nya regler om betaltjänster (som genomför Europaparlamentets och rådets direktiv 2015/2366 av den 25 november 2015 om betaltjänster på den inre marknaden, PSD2) föreskrivs i 5 kap. lagen (2010:751) om betaltjänster att leverantören av en (a) betalningsinitieringstjänst *ska identifiera sig* gentemot betaltjänstanvändarens kontoförvaltande betaltjänstleverantör *varje gång* en betalning initieras (10 §) och att leverantören av (b) en kontoinformationstjänst ska *för varje kommunikationssession identifiera sig* gentemot den kontoförvaltande betaltjänstleverantören (17 §). Bestämmelserna motsvaras av tydliga krav i EU-direktivet. I författningskommentaren till den nämnda lagändringen uttalas bl.a. följande (a.prop. s. 356): ”Detta innebär, till skillnad från vad som ofta är fallet i dag, att den kontoförvaltande betaltjänstleverantören ska *få kännedom om att initiering görs via en leverantör* av sådana tjänster.”

eSams juridiska bedömning

Redan i ett rättsligt uttalande den 24 april 2017 har eSam redovisat de regler i brottsbalken där *straffansvar föreskrivs för den som åberopar någon annans e-legitimation* och släpps in under sken av att vara den som anges i e-legitimationen.

Börjar dessa missbruk bre ut sig kan det emellertid också ifrågasättas om myndigheter ska anses röja sekretessbelagda uppgifter. Anses *ett otillåtet röjande ske av sekretessbelagda uppgifter* när myndigheten vet att beskrivna missbruk förekommer av myndighetens e-tjänster och tjänsterna inte stängs? Om ett utlämnande grundas på samtycke måste myndigheten rimligen pröva att ett giltigt samtycke föreligger. En sådan prövning kan knappast ske när myndigheten inte vet att den lämnar ut uppgifter till en tjänsteleverantör (med eller utan fullmakt) i stället för till den registrerade.

Expertgruppens rättsliga uttalande den 17 december 2015 om röjandebegreppet enligt offentlighets- och sekretesslagen kan knappast heller åberopas eftersom utlämnande myndighet inte har underlag för att bedöma om det är osannolikt att ett röjande kommer att ske. Den utlämnande myndigheten vet inte om att den förmås att lämna uppgifter till en annan tjänst än den myndigheten tillhandahåller åt e-legitimationsinnehavaren.

Lämnar en myndighet ut uppgifter genom behandlingar som omfattas av regler i en registerlag har myndigheten inte heller kunnat ta ställning till om ett *utlämnande på medium eller genom direktåtkomst* till någon annan än den som legitimerat sig är förenligt med berörd registerförfattning och om en sådan författning i övrigt kan förenas med utlämnande till någon annan än den registrerade själv. Exempelvis kan de ändamål för vilka personuppgifterna får behandlas enligt dataskyddsförordningen eller en registerlag visa sig oförenliga med de ändamål för vilka de ska behandlas när en robot hämtat dem till en privat tjänsteleverantör.

Till detta kommer *säkerhetskrav* enligt olika författningar. Någon analys och bedömning av hot- och risker har knappast kunnat göras, enligt dataskyddsförordningen, en registerlag, offentlighets- och sekretesslagen eller MSB:s föreskrifter eftersom mottagarmiljön är okänd.

Berörda myndigheter behöver också överväga om en hantering av detta slag kan förenas med förvaltningslagens krav på legalitet.

För vissa uppgifter som är särskilt attraktiva, nämligen pensionsinformation, kräver berörda tjänster dessutom ett insamlande och tillgängliggörande som grundas på att individen ingår avtal med Min Pension Aktiebolag och samtycker till viss hantering. Om användaren lockas att legitimera sig *på en annan webbplats* än www.minpension.se, för att den webbplatsens robot ska bereda sig tillträde till www.minpension.se och där klicka i erforderliga rutor för att komma åt informationen om användaren, har Min Pension Aktiebolag inte fått någon accept eller något samtycke från användaren. Användaren varken ser eller tar ställning till avtal och krav på samtycken när det är tjänsteleverantörens robot som besöker webbtjänsten och ”klickar” etc. för att komma åt information där.

Det finns alltså inte bara straffrättsliga hinder mot den overlayteknik som börjat sprida sig. Flera andra regelverk berörs och står i vägen för denna dolda hantering.

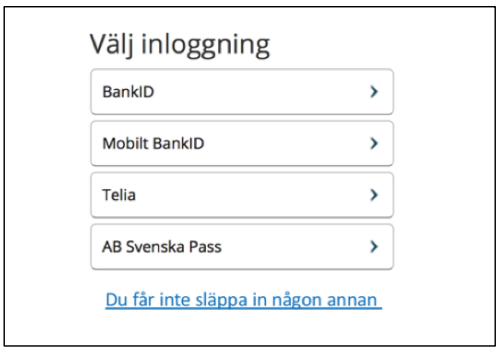
Åtgärder

På lång sikt behöver gärningsmännen lagföras och ett stärkt skydd införas, t.ex. genom högre krav på de system som används för identitetskontroll i anknytning till e-tjänster.

Gemensam informationsinsats

Det finns emellertid ett akut behov av att informera de som legitimerar sig (i syfte att ge annan tillträde) och de företag som ansvarar för webbtjänster (där en robot ger sig ut för att vara användaren) så att det inte kan råda någon tvekan för dem om att sådana förfaranden är förbjudna.

För att alla myndigheter ska lämna information och kunna göra det med en enkel arbetsinsats, utan kostsam förvaltning över tid, rekommenderar eSam att myndigheter för in en kort text på platsen för inloggning, som bör utformas lika på alla webbplatser (jfr det genomslag uttrycket ”Jag legitimerar mig” fått). En länk föreslås därför med texten ”Du får inte släppa in någon annan”. Länken bör placeras i anknytning till användarens aktivering av en inloggning – i enlighet med följande exempel:



Länken bör peka på den nya webbplatsen e-legitimations.se, som riktar sig till privatpersoner, och den text som finns där om hur man skyddar sin e-legitimation (Start / Skydda din e-legitimation / Låt inte andra personer eller webbplatser använda ditt e-leg):

https://e-legitimation.se/4.14dfc9b0163796ee3e73ee.html

Webbplatsen drivs av E-legitimationsnämnden och efter den 1 september av Myndigheten för digital förvaltning, DIGG.

Med en sådan utformning kan uppdateringar utarbetas av en aktör, i samråd med övriga, utan att varje aktör själv måste utforma en sådan text.