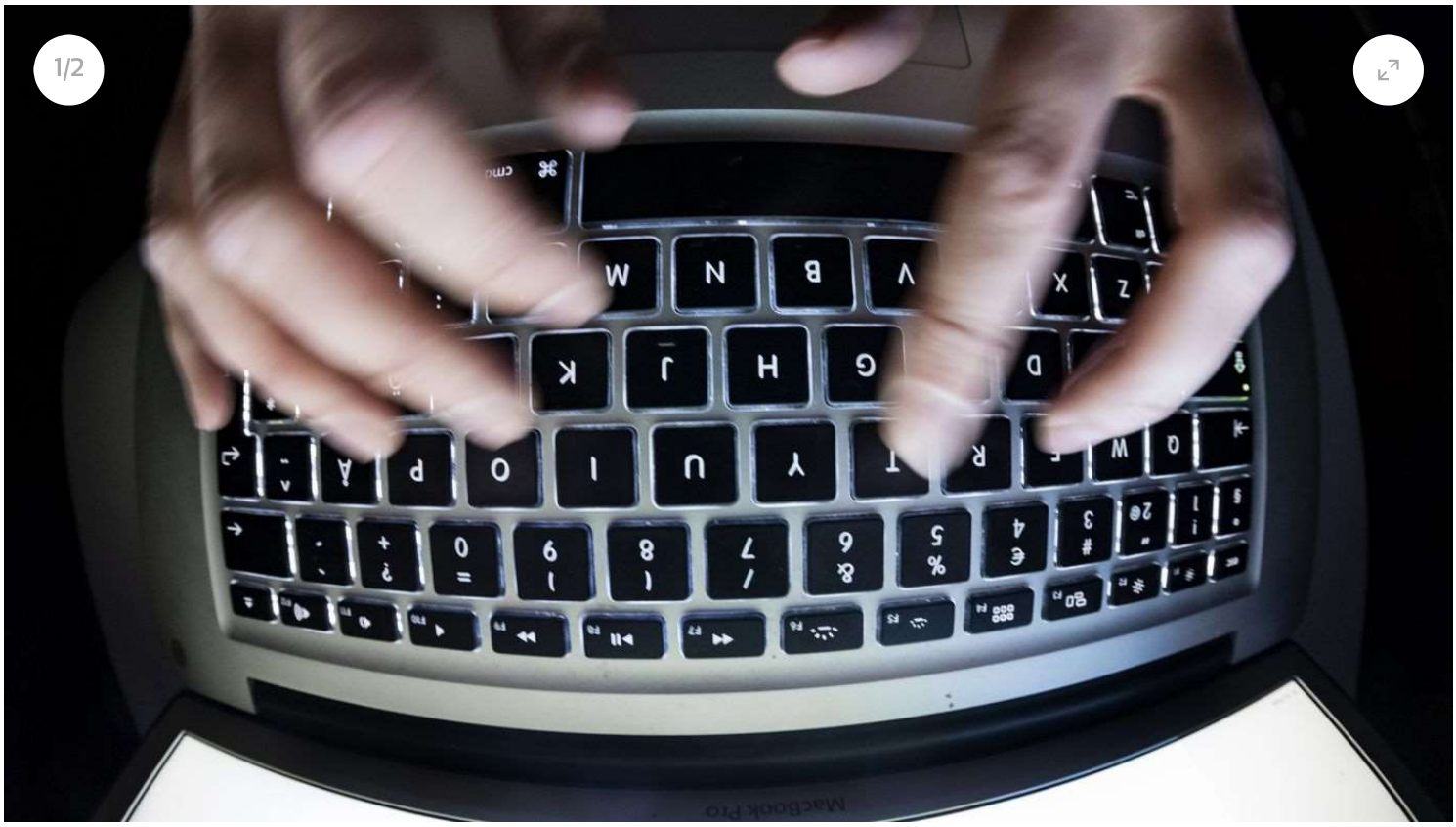
Riskfyllt hacka kriminellas mobiler

Med hemlig dataavläsning ska polisen få hacka kriminellas mobiler och ta del av information innan den krypteras.
Men intrång av den här typen kan innebära risker.
Trojaner kan hamna i orätta händer och vanliga användare kan drabbas när säkerhetshål i it-system förblir öppna.

Anja Haglund / TT
Publicerad 09:15



– Det är ingen lätt lag. Det går att göra rätt, men det går också att göra fel, säger it-säkerhetsexperten Jonas Lejon.

I veckan presenterade regeringen sitt lagförslag om hemlig dataavläsning, som ska ge polisen rätt att gå in i brottsmisstänktas datorer och mobiler för att läsa krypterad information. Bakgrunden

datorer och mobiler för att läsa krypterad information. Bakgrunden är att brottslingar i allt högre grad använder sig av kryptering när de kommunicerar, vilket gör att nuvarande tvångsmedel inte räcker till.

I praktiken sker hemlig dataavläsning genom att virusliknande program – trojaner – installeras i mobiler eller datorer. Där kan de göra allt från att granska dokument, registrera position och snappa upp lösenord till att kolla bilder, avlyssna chattar och samtal och se vilka hemsidor som besöks.

Intrånget i den kriminelles dator eller mobil kan ske på flera sätt. Men en förutsättning är att det finns en sårbarhet som kan utnyttjas för intrång. Det kan handla om allt från en bugg i ett it-system till brister i säkerhetstänk hos den kriminelle. Exempelvis kan användaren luras att installera trojanen genom att klicka på en länk i ett mejl.

– Det kan också vara en uppdatering av en drivrutin eller liknande, något som personen förväntar sig att få, säger Jonas Lejon, som jobbat med kryptering och kvalificerad it-säkerhet i många år.

Lite mer avancerat kan det handla om att styra om ett anrop från den brottsmisstänktes dator till en webbsida så att datorn i stället dirigeras till en webbsida som kontrolleras av polisen. Personen förmås sedan att ladda ner skadlig programkod.

Ytterligare en metod kan vara att helt enkelt förse den kriminelle med en mobiltelefon där polisen redan planterat programvara.

– Den misstänkte har kanske beställt en ny mobil med posten eller deltagit i någon tävling och vunnit en mobil, och så får personen en annan telefon som är modifierad, säger Jonas Lejon.

Frågan är hur myndigheterna ska få tillgång till den typ av hackerverktyg som krävs. Polisen är mycket förtegen om vilken teknik och programvara man skaffat sig, och om man planerar att utveckla egna trojaner eller inte. Men enligt Jonas Lejon är en kombination trolig.

– Ser man på andra länder som tillämpar hemlig dataavläsning så har de både köpt in trojaner av kommersiella aktörer och skapat egna, säger han.

Trojanerna som säljs kan ha uppemot 20 olika funktioner.

– Du kan välja att aktivera vissa av de här funktionerna beroende på vad ditt mål är, säger Jonas Lejon.

För att kunna installera trojaner kan polisen ha ett behov av att införskaffa så kallade zero-days, det vill säga sårbarheter i it-system som inte är kända av tillverkarna och som därför kan utnyttjas. Tidigare köptes och såldes de enbart på svarta marknaden men nu

finns de öppet tillgängliga.

– Man kan mycket väl tänka att svensk polis kommer att använda sig av det, säger Jonas Lejon.

Zero-days är dock mycket dyra och kan kosta åtskilliga miljoner kronor.

Men det kan också vara riskfyllt att hacka telefoner på det här sättet. För myndigheterna handlar det om att den avlyssnade kan bli misstänksam och ändra sitt beteende, exempelvis om en trojan gör så att mobilen plötsligt börjar dra mycket mer batteri. Antivirusprogram kan också upptäcka trojanen och flagga den som skadlig kod. Har man då använt den mot flera misstänkta kommer alla att få meddelandet. I värsta fall kan trojanen förstöra eventuella bevis.

– Det kan vara något som går fel vid installationen, datorn kanske kraschar och blir obrukbar, säger Jonas Lejon.

Men säkerheten kan också äventyras för vanliga användare, enligt Anne-Marie Eklund Löwinder, säkerhetschef på Internetstiftelsen.

– Det normala beteendet när man hittar en sårbarhet i programvara skulle ju vara att rapportera det till leverantören så att den får möjlighet att skicka ut en lagning till alla användare. Men här kan man föreställa sig att man vill spara sårbarheter till den gången man ska plantera in trojaner, säger Anne-Marie Eklund Löwinder.

På det sättet riskerar myndigheterna att skapa bakdörrar som kan undergräva it-säkerheten för många, anser hon.

– Man kan också fråga sig om myndigheterna efter det att de utnyttjat en sårbarhet kommer att rapportera den till leverantören, så att företaget får en möjlighet att åtgärda. Kommer de bara att utnyttja sårbarheten en gång, eller flera? Det är många frågetecken.

En risk är också att trojaner som används eller utvecklats av polisen läcker och hamnar i orätta händer.

– I USA för några år sedan hade NSA (den amerikanska underrättelsetjänsten) samlat på sig en verktygslåda med sårbarheter som de råkade läcka av misstag, vilket utnyttjades av kriminella och drabbade en massa stora företag över hela världen, säger Anne-Marie Eklund Löwinder.

Trots svårigheterna anser ändå båda att det är rimligt att svensk polis får uppdaterade verktyg.

– Det är komplicerad lagstiftning. Men med rätt metoder, processer, rutiner och teknik kommer man att kunna nå framgång, säger Jonas Lejon.

Lejon.

Fakta: Så fungerar hemlig dataavläsning

Hemlig dataavläsning kan ske genom att hård- eller mjukvara placeras, antingen fysiskt eller elektroniskt, i en användares tekniska utrustning.

Om avläsningen sker via mjukvara betyder det att polisen hackar en misstänkt persons telefon eller dator och planterar en programvara, en så kallad trojan, för att kunna fjärrstyra enheten eller i smyg läsa av data.

Sker den via hårdvara kan det till exempel handla om att installera en så kallad ”key logger” på datorn, en liten maskin som registrerar tangentbordstryckningar. På det viset kan polisen till exempel lista ut vilka lösenord en misstänkt använder.

Källa: Ny Teknik

Fakta:

Lagen om hemlig dataavläsning ska träda i kraft den 1 mars 2020.

Den ska bara få användas vid allvarlig brottslighet, exempelvis mord och grova narkotikabrott.

Den ska gälla i fem år. Därefter måste den förnyas av riksdagen.

Polisen, tullen, Säpo och Ekobrottsmyndigheter får använda metoden.

Tillstånd för hemlig dataavläsning ska ges av domstol.

Metoden får användas vid brott med minimistraff två år

Vid ljud- och bildupptagning via till exempel datorns mikrofon eller kamera krävs minimistraff fyra år.

Lagförslaget har skickats till Lagrådet för yttrande. Därefter läggs en proposition i riksdagen

Liknande lagstiftning finns redan i en rad andra länder, bland annat Danmark, Norge, Nederländerna, Storbritannien och Tyskland.

Källa: Regeringen

Anja Haglund / TT