MORGENAVISEN Jyllands-Posten

ERHVERVSJURA

NEM KRYPTERING BLIVER ET ELDORADO FOR IT-KRIMINELLE

IT-SIKKERHED: Onsdag den 21. januar var Europæisk Databeskyttelsesdag, og med nye løsninger fra Google og Apple har det aldrig været lettere at beskytte sig selv og sine data. Men det bryder politi og efterretningstjenester sig nu ikke meget om.

LARS BO LANGSTED
professor, leder af IECC Crime Research Centre, Aalborg Universitet
finans@finans.dk

Det er farligt at færdes på internettet. Vi kan næsten dagligt læse om identitetstyverier, phishing-sider, hvor man bliver narret til at handle eller afgive personlige oplysninger til kriminelle, der så kan misbruge oplysningerne, hacking, hvor data hos virksomheder eller offentlige myndigheder bliver stjålet; DOS-angreb, hvor hjemmesider lægges død i kortere eller længere tid og meget andet skidt.

Vi læser ikke nær så meget om den fuldstændigt gnidningsfri kommunikation mellem venner, kolleger og forretningsforbindelser, om den ikke helt så gnidningsfri digitale kommunikation med det offentlige eller om de millioner af andre legale transaktioner, der finder sted hver eneste dag. Men det er naturligvis heller ikke så interessant at læse og skrive om. Det er blot vores nye digitale hverdag.

Vi har taget internettet til os – og det samme har naturligvis de kriminelle. Det er jo på nettet, der er handel, det er der, industri- og erhvervshemmelighederne kan findes, det er der, der er pengeoverførsler. Men hvordan kan den gode borger og den lovlydige offentlige myndighed så beskytte sin kommunikation og sine data mod kriminelle anslag?

Gennem kryptering. Kryptering af e-mails og andre digitale transmissioner og kryptering af lagrede data gør det ikke umuligt for de kriminelle at finde ud af, at der sendes mails, eller at der opbevares data. Men de kan ikke læse indholdet – og så bliver det uinteressant for dem.

I Datatilsynets sikkerhedsvejledning fra 2001 stilles der da også krav om kryptering ved transmission af personfølsomme oplysninger over "det åbne internet" – det vil sige helt almindelige e-mails. I vejledningen, der gælder for offentlige myndigheders behandling af personfølsomme oplysninger, hedder det således:

»Hvad angår fortrolighed kan denne sikres ved forsvarlig kryptering af de transmitterede oplysninger. Hvis der er tale om transmission af fortrolige oplysninger, herunder personnummer, skal der som minimum foretages en kryptering. Hvis de transmitterede oplysninger er af følsom karakter (omfattet af persondatalovens § 7, stk. 1 og § 8, stk. 1), skal der anvendes en stærk kryptering, baseret på en anerkendt algoritme.«

I november sidste år traf Datatilsynet f.eks. en afgørelse over Sønderborg Kommune:

»Idet Datatilsynet tidligere har udtalt kritik af, at Sønderborg Kommune har sendt ukrypterede e-mails indeholdende fortrolige og følsomme personoplysninger, finder Datatilsynet, at Sønderborg Kommunes manglende overholdelse af persondataloven er meget kritisabel.«

I en udtalelse fra 2012 til IT-Universitetet om indgåelse af en kontrakt med Microsoft om en cloud-løsning, bl.a. vedrørende personfølsomme oplysninger, skrev tilsynet bl.a.:

»Tilsynet skal endvidere anbefale, at IT-Universitetet undersøger mulighederne for – og så vidt muligt sørger for – at personoplysninger lagres i krypteret form hos Microsoft. Sikkerhedsforanstaltningerne ved transmission og login samt spørgsmålet om logning bør efter tilsynets vurdering også indgå i IT-Universitetets risikovurdering og videre overvejelse om anvendelse af Office 365.«

Jo stærkere kryptering, jo større sikkerhed mod at personoplysninger eller følsomme forretningshemmeligheder falder i forkerte hænder. Problemet for flertallet af almindelige net- og databrugere er, at det er ret bøvlet at arbejde med kryptering, og derfor er det da også de færreste, der bruger det.

Imidlertid meddelte Google først på efteråret 2014, at man snart ville lancere en løsning for Gmail-brugere, hvor man meget enkelt og brugervenligt kunne kryptere sin mails med en såkaldt PGP-kryptering, og hurtigt fulgte Apple efter. Ikke blot mails, men også alle data, der opbevares på mobiltelefoner, vil med de nyeste opdateringer af Android- og Apple-styresystemerne som udgangspunkt være krypteret.

Kryptering er med andre ord et perfekt værn mod, at uvedkommende læser ens mail og ens data, hvad enten man er privat eller offentlig. De store teknologiudviklere bakker op om, at det ikke bare er vigtigt at sørge for at holde uvedkommende væk – det skal også være så let, at alle kan gøre det.

Umiddelbart burde alle juble. Især det politi, der gerne vil gøre rigtigt meget for at beskytte borgerne mod netkriminalitet.

Alligevel ser både politi og efterretningstjenester med stor bekymring på al denne sikkerhed. Chefen for FBI udtalte endda sidste år, at disse krypteringstiltag gav folk mulighed for at »stå uden for loven«.

Dermed mener han naturligvis ikke, at der er noget ulovligt i kryptering – eller at kryptering skaber lovløse tilstande. Det, han mener, og det, der bekymrer ham, er, at folk ved brug af PGP-kryptering også beskytter deres korrespondance mod indholdsovervågning af politi og efterretningstjenester. Og det vil sige, at den også beskytter kriminelle mod at blive "aflyttet", og at terrorister frit kan maile sammen uden frygt for, at nogen kan læse indholdet.

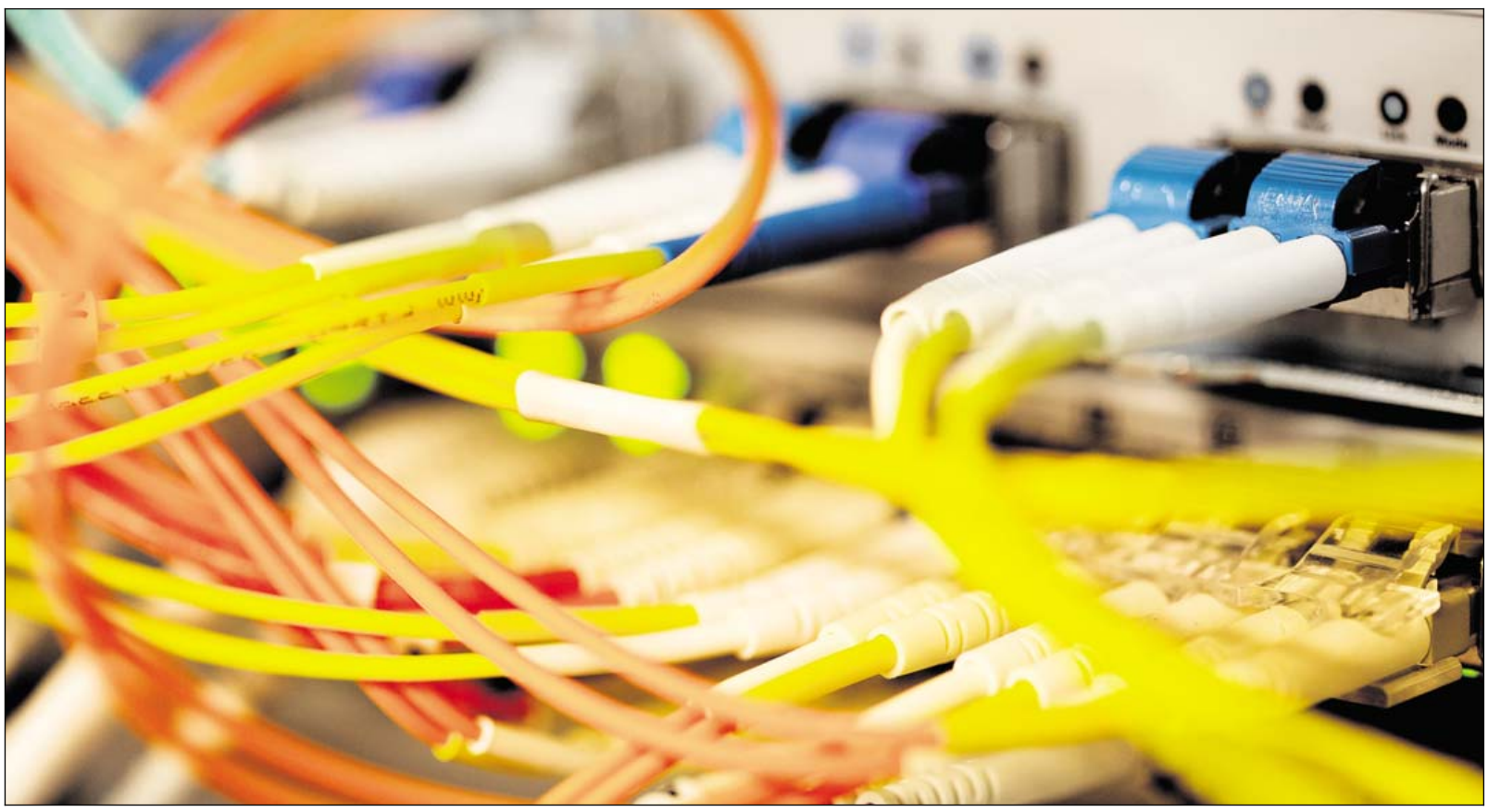
Så også her opstår dilemmaet: Skal man forbyde kryptering og derved forbyde myndigheder, virksomheder og personer i at beskytte deres data mod kriminelle? Eller skal man acceptere kryptering og dermed støtte de kriminelle i at undgå at blive overvåget af politi og efterretningstjenester?

> Chefen for FBI udtalte endda sidste år, at disse krypteringstiltag gav folk mulighed for at »stå uden for loven«.
>
> Lars Bo Langsted

Mellemløsningen giver ikke mening: at forlange at alle krypteringssystemer skal have en "bagdør" (eller en "fordør", som FBI-chefen foretrak at kalde det), som politiet kan bruge, er det samme som at lave en dør, som også de kriminelle kan bruge til at trænge ind i kommunikation og data – ganske ligesom politi og efterretningstjenester fra lande, som vi bestemt ikke ønsker skal have adgang til vores data og forretningshemmeligheder.

EU-Domstolen traf sidste år afgørelse om, at logningsdirektivet var i strid med bl.a. retten til et privatliv, og den danske regering ændrede umiddelbart herefter sin egen logningsbekendtgørelse. Ifølge et notat fra ministeriet bl.a. fordi »erfaringerne (har) vist, at oplysningerne kun i meget begrænset omfang er brugbare i praksis i forbindelse med efterforskning og retsforfølgning af strafbare forhold.«

Der er således tale om en uhyre vanskelig balancegang mellem to helt legitime og beskyttelsesværdige hensyn, hvor det er nødvendigt at bevare hovedet koldt og tænke kreativt, så begge hensyn – hvis og så vidt det er muligt – kan varetages. Herunder må man også forholde sig til, om de ulemper og risici som et generelt forbud mod, at borgerne beskytter sig selv gennem kryptering, er proportionalt med den reelle gevinst for efterforskning og strafforfølgning, som et forbud vil kunne give.



Kryptering af personfølsomme e-mails giver private en fordel over for it-kriminelle, men de kriminelle og terrorister får samtidig lettere ved at skjule informationer over for politi og efterretningsvæsen. Foto: Thomas Borberg/Polfoto