DI og DI ITEKs vejledning om beskyttelse mod elektronisk industrispionage fra udlandet

Sammenfatning

Denne vejledning adresserer risikoen for industrispionage fra statssponserede aktører i udlandet mod danske virksomheders elektroniske data. Vejledningen gennemgår trusselsbilledet og gennemløber en overordnet risikovurdering med udgangspunkt i truslerne, følsomheden af de data, som virksomheden er i besiddelse af, samt virksomhedens sikkerhedstiltag. På den baggrund gives et sæt anbefalinger.

Risikoen for industrispionage

Der har gennem de seneste par år været en stigende opmærksomhed på at inkludere aktiviteter udført af fremmede landes efterretningstjenester i trusselsbilledet. I FEs "Efterretningsmæssig risikovurdering 2013" hedder det bl.a.: "De alvorligste cybertrusler mod Danmark kommer fra statslige aktører, der udnytter internettet til at spionere". Dette har betydet et tilsvarende behov hos danske virksomheder for at inkludere disse mulige trusler i deres risikovurderinger.

Mulighederne for at udøve industrispionage er tæt forbundet med de regler, som efterretningstjenesterne er underlagt tillige med deres tekniske kapacitet. I nogle lande er området ikke reguleret, og det er derfor kun den tekniske kapacitet, der sætter grænser. I andre lande findes der lovgivning, som regulerer området. I den vestlige verden findes der typisk lovgivning, som tillader efterretningsaktiviteter, når det sker af hensyn til national sikkerhed, alvorlige forbrydelser, beskyttelse af landets økonomiske interesser eller som følge af internationale aftaler.

Der er i de forskellige lande forskellige tilgange til at indhente efterretninger. I nogle lande foretages indhentningen af specialiserede dele af efterretningstjenesterne. I andre lande udføres indhentning af private aktører, som handler på efterretningstjenesternes vegne. Vi vil derfor i denne vejledning bruge termen statssponserede aktører, om de organisationer, der står bag efterretningsindhentningen.

Afhængig af deres tekniske kapacitet, baserer de statssponserede aktører typisk indhentningen på tre typer af aktiviteter. For det første kan de planlægge og gennemføre målrettede angreb for at nå specifikke mål. For det andet kan de foretage masseovervågning og analysere den trafik, de indsamler, for at søge efter mønstre eller specifik information. For det tredje kan de forberede kapacitet til fremtidig indhentning af informationer.

Målrettede angreb

De målrettede angreb er bl.a. beskrevet i "Trusselsvurdering: APT-angreb mod danske myndigheder, virksomheder og organisationer", udgivet af Forsvarets Efterretningstjeneste (FE). APT står for advanced persistent threats og er særligt avancerede, målrettede og vedholdende angreb. I FEs trusselsvurdering redegøres der for, at angrebene "oftest [sker] med sigte på at udøve spionage, særligt industrispionage, og det er derfor meget sandsynligt, at det ofte er statssponserede aktører, der står bag". Danmark har ved flere lejligheder været ramt af denne type målrettede angreb, bl.a. rettet mod Erhvervs- og Vækstministeriet og mod private virksomheder indenfor højteknologiske sektorer.

Danmark er ikke alene med at komme med denne trusselsvurdering. Den mest omfattende offentlige vurdering kommer fra virksomheden Mandiant, der har kortlagt målrettede angreb fra statssponserede aktører rettet mod 141 organisationer, fortrinsvis i engelsk talende lande. Målrettede angreb kan også

være rettet mod enkeltpersoner, og særlig præcisionsangreb (spearphishing) på virksomhedsledere eller it-administratorer, som har bred adgang til fortrolige informationer, udgør en trussel. Denne type angreb har til formål enten direkte at give adgang til informationer, eller at give adgang til rettigheder på virksomhedens it-systemer, som indirekte kan give adgang til informationer.

Masseovervågning

Masseovervågning foretages ligeledes af en række lande. Masseovervågning er karakteriseret ved, at man indsamler informationer og informationsmønstre (metadata) i stor skala fra en række forskellige kilder. Efterfølgende foretager man analyser af data for søge efter mønstre eller specifik information. Ofte lagres data også således, at man kan foretage søgninger på historiske data ud fra en konkret mistanke og/eller se mønstre over tid.

Konkret har bl.a. lækager af klassificerede dokumenter vist, at statssponserede aktører foretager masseovervågning i store dele af internettets infrastruktur, herunder teleselskabernes trafikdata og de fiberoptiske kabler, som forbinder verdensdelene. Virksomheders data indsamles også i sådan masseovervågning, og virksomhedernes fortrolighed bliver dermed truet. Der foreligger imidlertid kun få kendte eksempler på, at data misbruges til industrispionage, og disse eksempler vedrører ikke den vestlige verden.

Forberedende kapacitet

De statssponserede aktører kan også opbygge kapacitet til fremtidig overvågning og angreb. Der indsamles viden om ubeskyttede software sårbarheder (zero-days), indbygges bagdøre, opbygges kompetencer til at bryde kryptering og indgås aftaler om udveksling af data med andre aktører.

En opsummering af de statssponserede aktørers aktiviteter viser altså, at der er risiko for, at virksomhedernes data på forskellig vis opsamles af statssponserede aktører uden virksomhedernes viden og i modstrid med deres ønske, og at datas fortrolighed dermed er truet. Der er altså god grund for virksomhederne til at inkludere trusler fra statssponserede aktører i deres trusselsbillede.

Risikovurdering, dataklassifikation og sikkerhedstiltag

Virksomheden bør altid lave en risikovurdering. Risikovurderingen bør tage højde for de aktuelle trusler, følsomheden af virksomhedens data, og virksomhedens opbygning (teknisk, fysisk og personalemæssigt), herunder eksisterende sikkerhedstiltag.

Dataklassifikation

Virksomhederne anbefales at gennemføre en dataklassifikation, hvor man som minimum klassificerer de data, der er af størst forretningsmæssig betydning for virksomheden, og dermed sikrer den bedst mulige beskyttelse af dem. En guideline til at gennemføre en dataklassifikation er Statsministeriets Sikkerhedscirkulære, hvor der skelnes mellem om kompromittering af data kan medføre ”skade”, ”alvorlig skade” eller ”overordentlig alvorlig skade”. Det afhænger meget af, hvilken virksomhed der er tale om, men ofte vil det kun være mellem 0,5 % og 2 % af virksomhedens data, som skal klassificeres i den højeste kategori, hvor deres kompromittering kan medføre alvorlig skade, og som dermed kan retfærdiggøre omfattende sikkerhedstiltag.

Sikkerhedstiltag

Virksomhedens organisering er afgørende for, hvordan virksomheden skal beskytte sig. Hvis virksomheden har outsourcet IT systemer med forretningskritiske data til en professionel leverandør eller en cloud service provider, vil virksomheden opnå den fordel, at der foreligger en service level kontrakt, som fastslår, hvilket sikkerhedsniveau leverandøren skal levere. I mange tilfælde vil dette sikkerhedsniveau være bedre, end hvad virksomheden selv kan tilvejebringe. Det skyldes, at den professionelle leverandør har flere kompetencer og et mere dedikeret fokus på sikkerhedsområdet end den typiske virksomhed. Dermed vil der være veluddannede dedikerede medarbejdere til at håndtere f.eks. teknisk opdatering og konfiguration af tekniske sikkerhedsforanstaltninger. Den professionelle leverandør vil også ofte have sikkerhedspolitikker, retningslinjer og andre procedurer for arbejdet på plads. Yderligere vil der ofte være kontroller, som sikrer, at det lovede serviceniveau faktisk efterleves. Ved at bruge en outsourcing leverandør eller en cloud service provider kan virksomheden udnytte de nye teknologiske trends som cloud computing, social, mobile og big data og dermed opnå produktivitetsgevinster. Når der anvendes outsourcing eller cloud computing bør man sikre sig, at der foretages kontrol af en tredjepart og indhentes revisionserklæringer som f.eks. ISAE3402. I fald der anvendes kryptering, er det vigtigt, at virksomheden selv har kontrollen med krypteringsnøglerne.

Hvis virksomheden drifter sine egne it-systemer, har virksomheden selv ansvar for sit tekniske sikkerhedsniveau. Ofte kan det anbefales at gå frem efter en sikkerhedsstandard som f.eks. ISO27000, som sikrer, at virksomheden kommer hele vejen rundt om sikkerheden. Særlig opmærksomhed bør der være på opdatering af applikationer og operativsystemer, minimering af antallet af privilegerede brugere, deaktivering af lokale administratorer, generel adgangskontrol, rettighedsstyring, logning, sikkerhed på mobile devices, begrænsning (whitelisting) af tilladte applikationer, beskyttelse af databaser og applikationer samt afskærmning af data, så databaser kan services af administratorer, uden at der gives adgang til data. Forsvarets Efterretningstjeneste og Digitaliseringsstyrelsens anbefalinger i "Cyberforsvar der virker" kan bruges som inspiration.

Afhængig af den enkelte virksomheds trusselsvurdering kan en række yderligere tekniske sikkerhedstiltag være relevante (evt. kun for virksomhedens højt klassificerede data):

1. Kryptering af relevante tjenester, data og kommunikationsveje.
2. Opsplitning af data på nationalt eller regionalt afgrænsede datacentre.
3. Krav til leverandørers gennemsigtighed af arbejde med privacy og datasikkerhed.

I praksis har mange virksomheder en kombination, hvor nogle services driftes inde i virksomheden, mens andre driftes hos en professionel leverandør. I nogle tilfælde kan de samme applikationer køres både inde i virksomheden eller ude på internettet. I sådanne tilfælde taler man om hybrid cloud service. Dermed vil en del af sikkerheden blive håndteret af en professionel leverandør, mens virksomheden selv skal håndtere resten af sikkerheden.

Udover den tekniske sikkerhed bør virksomheden også forholde sig til behovet for fysiske og personalemæssige sikkerhedstiltag (f.eks. adgangskontrol og uddannelse), idet målrettede angreb fra statssponserede aktører også kan omfatte f.eks. falske opringninger eller forsøg på at få fysisk adgang.

Anbefalinger

Målrettede angreb fra statssponserede aktører kan rettes mod en virksomhed, uanset hvor dens forretningskritiske data er opbevaret. De fleste mindre og mellemstore virksomheder, som ikke har lige så stærke sikkerhedsmæssige kompetencer som en professionel udbyder, vil derfor i forhold til denne type angreb være bedst stillet ved at have sine data hos en professionel leverandør.

Når data transmitteres via internettet ud af virksomheden, kan datas fortrolighed blive kompromitteret. Hvis virksomheden har højt klassificerede data af interesse for statssponserede aktører, bør der anvendes stærk kryptering ved såvel lagring som transmission for data på udstyr, der (direkte eller indirekte) er koblet til internettet.

Det er ledelsens ansvar i samarbejde med de teknisk ansvarlige og HR at sikre, at virksomhederne laver en risikovurdering og en dataklassifikation og implementerer de rette sikkerhedstiltag, således at den forretningsmæssige risiko er under kontrol og acceptabel for virksomheden.