DI og DI ITEK's vejledning om bevissikring

Udgivet af: DI ITEK
Redaktion: Henning Mortensen
ISBN 978-87-7353-974-3
0.05.12

Indledning

Denne vejledning er lavet med det formål at ruste danske virksomheder til at vurdere, hvad de skal foretage sig, hvis der - på virksomhedens it-systemer eller it-systemer virksomheden er forbundet til - opstår en sikkerhedshændelse, der eventuelt kunne kræve politiets involvering.

Når der er behov for en sådan vejledning skyldes det, at politiets mulige involvering kræver at dokumentation for hændelsen indsamles på en måde, der gør, at det kan anvendes som bevis i en retssag. Denne disciplin kaldes bevissikring[1]. I den fysiske verden indsamles f.eks. fingeraftryk ved et indbrud. Her er det vigtigt, at der kan indsamles fingeraftryk fra de mistænkte - og personalet skal så vidt muligt undgå at ødelægge disse beviser og sikre de optimale rammer for, at politiet kan gøre sit arbejde. På tilsvarende måde findes der også på it-systemerne ofte bevis på, at kriminelle har været på spil: de efterlader sig elektroniske fingeraftryk.

Denne vejledning er imidlertid ikke skrevet for politiets skyld. Når vi anbefaler danske virksomheder at være opmærksom på problemstillingen, skyldes det, at de ofte meget professionelle bagmænd skal stilles skakmat, så de ikke kan gennemføre deres kriminelle handlinger mod virksomhederne systematisk over tid. Det er i den enkelte og alle virksomheders interesse. Det er dette hensyn til forretningen, der motiverer efterforskning og korrekt bevissikring. Bevissikring er en særlig avanceret disciplin. Med mindre virksomheden har særlige kompetencer på området, anbefales det at inddrage eksterne tekniske eksperter eller politiet, såfremt der er tale om et strafbart forhold.

Vejledningen indeholder en første del, som er henvendt til virksomhedens ledelse, og en anden del, som er henvendt mod virksomhedens tekniske personale - uanset om disse er ansat i virksomheden eller hos en outsourcingpartner.

Kend loven

Der er to love som er særligt interessante i forbindelse med it-kriminalitet og bevissikring.

For det første har vi straffeloven[2], der kriminaliserer de hændelser, som vi oftest forbinder med it-kriminalitet - f.eks. hacking (§193 og §263), børnepornografi[3] (§235), databedrageri (§ 279a) og hærværk (§291). Denne lov bruges til at vurdere om en given hændelse kan være en kriminel handling og er dermed grundlaget for, om der kan rejses en straffesag.

For det andet har vi retsplejeloven[4], som blandt mange andre ting regulerer politiets efterforskning af forbrydelser (andet afsnit, kapitlerne 67-75b). I denne lov beskrives det, hvordan politiet må agere og hvad der kræves af deres ageren for at et bevis kan bringes for retten. Der kan på den ene side ikke kræves af

[1] Emnet går også i en dansk sammenhæng ofte under det engelske ord: Forensics.
[2] Se https://www.retsinformation.dk/Forms/R0710.aspx?id=138671.
[3] For en særskilt vejledning, om hvordan virksomhederne bør håndtere fund af børnepornografi, henvises der til "Vejledning til håndtering af fund af børnepornografisk materiale på arbejdspladsen", http://di.dk/Virksomhed/Produktion/IT/Informations-sikkerhed%20og%20Privacy/Trusler%20og%20loesninger/Pages/DIogRedBarnetudgivervejledningomboerneporno.aspx, udgivet af DI ITEK og Red Barnet.
[4] Se https://www.retsinformation.dk/Forms/R0710.aspx?id=138875.

virksomhederne, at de overholder denne lovgivning, når der indsamles beviser. På den anden side vil bevisernes værdi, når de ikke er indsamlet af politiet efter ovenstående regler, være svagere i en eventuel retssag.

Ledelsesbeslutning

Ledelsen i virksomheden bør inden en hændelse indtræffer have skabt rammerne for en fornuftig håndtering. Dette indebærer blandt andet nedenstående punkter, som DI og DI ITEK har behandlet i andre vejledninger:

- at der er lavet en proces, som sikrer, at virksomheden ledelse løbende tager stilling til sikkerheden[5]
- at der er foretaget en risikovurdering
- at der er skrevet en sikkerhedspolitik med uddybende retningslinjer, som tager udgangspunkt i forretningens behov[6]
- at personalet er orienteret om disse politikker og er i stand til at efterleve dem
- at de iværksætter de fornødne korrigerende tiltag - f.eks. antivirus, firewalls og andre tekniske tiltag[7]

For at sikre mulighederne for en fornuftig bevissikring når en hændelse optræder, bør virksomhedens ledelse have forhold til sig følgende:

1. Der bør udpeges en person, som er ansvarlig for sikkerheden. Hele virksomhedens personale bør kunne kontakte denne person, hvis de er i tvivl om der er tale om en hændelse. Den sikkerhedsansvarlige bør altid kunne få fat i ledelsen, således at der hurtigt kan træffes beslutninger, hvis en hændelse opstår.
2. Det bør være muligt forholdsvis hurtigt at kunne skabe sig et overblik over netværket i virksomheden således at man bedre bliver i stand til at gribe ind hurtigt i tilfælde af en hændelse.
3. Der skal være iværksat tekniske foranstaltninger, som understøtter en fornuftig og effektiv bevissikring. Som minimum bør ledelsen sikre sig, at der foretages relevant logning, at der kan tages backup af relevante beviser, og at der er korrekt synkron tidsstempling.
4. Det skal være afklaret om de tekniske foranstaltninger er lovlige - herunder især at de ikke krænker personalets rettigheder og implementeres med personalets vidende[8].
5. Hvis en hændelse opstår skal det hurtigt kunne afgøres om der er tale om en sikkerhedshændelse eller ej.
6. Det skal hurtigt kunne besluttes om hændelsen har en sådan karakter for forretningen, at der skal gribes ind øjeblikkeligt (f.eks. penge der er ved at blive fjernet fra en konto eller et produktionsapparat der er ved at blive lukket ned) eller om man kan iagttage forbryderens

[5] Se "Ledelse af IT-sikkerhed - for forretningens skyld", http://di.dk/Virksomhed/Produktion/IT/Informations-sikkerhed%20og%20Privacy/Sikkerhedformindrevirksomheder/Pages/Ledelse%20af%20sikkerhed.aspx.
[6] Se "IT-sikkerhedsskabelon", http://di.dk/Virksomhed/Produktion/IT/Informations-sikkerhed%20og%20Privacy/Trusler%20og%20loesninger/Pages/It-sikkerhedspolitik.aspx.
[7] Se en holistisk tilgang til at arbejde med virksomhedens informationssikkerhed: "Forøg virksomhedens informationssikkerhed", http://di.dk/Virksomhed/Produktion/IT/Informations-sikkerhed%20og%20Privacy/Sikkerhedformindrevirksomheder/Pages/DS-484.aspx.
[8] Se afsnittet "Information til personalet" i nærværende vejledning.

handlinger over tid (f.eks. at han arbejder på at få adgang til uskadelige informationer) for at sikre de bedste beviser.

7. Uanset om man griber ind med det samme eller ej skal det besluttes, om der skal inddrages eksterne parter til at vurdere hændelsen - herunder i særdeleshed tekniske eksperter med kendskab til hændelsens IT-faglige område og med kendskab til bevissikring. I denne forbindelse skal det også vurderes, om politiet skal inddrages. Sørg for altid at have kontaktpersoner hos tekniske eksperter og hos politiet, så man hurtigt kan komme i gang hvis hændelsen skulle opstå. Se relevante kontakt-informationer til hhv. Politiet og potentielle samarbejdspartnere senere i nærværende dokument.
8. Det skal vurderes, om hændelsen kan karakteriseres som en oplagt kriminel handling. I tvivlstilfælde – herunder om en handling er ulovlig i et givent land, hvorfra den kriminelle agerer – kan en advokat eller politiet kontaktes.
9. Virksomheden bør sikre sig at ingen personer fra personalet handler alene. Der bør altid være minimum to personer, der vurderer beviserne, således at en person fra personalet ikke pludselig kan pådrage sig mistanke for at have tilknytning til kriminaliteten. Desuden bør disse to personer dokumentere, hvad de foretager sig.
10. Der skal fastlægges personalemæssige konsekvenser. Herunder skal der tages stilling til hvornår en medarbejder skal bortvises med øjeblikkeligt varsel. I den forbindelse er det vigtigt også at huske at inddrage fjernadgang. Det skal meget nøje overvejes at inddrage politiet på forhånd, således at medarbejderen ikke evt. kan nå at fjerne beviser fra f.eks. en privat PC.

Punkterne 5-8 udgør et proces flow der iværksættes når en hændelse opstår. Vi har skitseret disse i Bilag A.

Det anbefales, at virksomheden ved en konkret hændelse tager en uformel snak med politiet og får en uformel vurdering af, om der skal foretages en formel anmeldelse. Dette vil bl.a. bero på hændelsens karakter (f.eks. kriminel eller ej), politiets muligheder for at gribe ind (f.eks. i Danmark eller i udlandet) og bevisernes karakter (f.eks. har man solide tekniske spor at gå efter).

Information til personalet

For at virksomhedens politikker og retningslinjer kan være effektive, skal de være let tilgængelige, og hver medarbejder skal kende og forstå indholdet. Nogle virksomheder forvalter dette ved, at den enkelte medarbejder får tilsendt en kopi af politikker og retningslinjer og kvitterer for modtagelsen. Andre virksomheder sikrer, at politikker og retningslinjer altid er tilgængelige - f.eks. via intranet. Ved nye tiltag er det vigtigt, at der afholdes informationsmøder eller på anden måde tydeligt gøres opmærksom på tiltagene.

Virksomhedens Samarbejdsudvalg eller tillidsrepræsentanter bør forelægges retningslinjerne forud for information til medarbejderne. Man kan med fordel give en tidsfrist til ikrafttrædelse af retningslinjerne.

Virksomheden skal desuden være opmærksom på, at når der behandles personfølsomme oplysninger i personaleadministrationen skal der være foretaget en anmeldelse til Datatilsynet. Dette gælder helt generelt og er ikke betinget af tiltag rettet mod bevissikring.

Yderligere information og yderligere tiltag

Som nævnt ovenfor er den første og vigtigste opgave, at ledelsen forholder sig til bevissikring. Der er hertil en række mulige ekstra tiltag, samt en række steder, hvor man kan få ekstra hjælp, hvis der skulle opstå en hændelse:

Tekniske foranstaltninger:

- Som minimum bør virksomheden sikre sig, at relevante aktiviteter logges, at man kan tage backup af relevante beviser - f.eks. logs - og at tidsstemplingen i virksomheden er synkron.

Hjælp fra eksterne eksperter:

- En række virksomheder i Danmark beskæftiger sig med informationssikkerhed og nogle af disse er eksperter i bevissikring. Du kan få et overblik over sikkerhedsvirksomheder her: http://itek.di.dk/Medlemsservices/Oversigt/Pages/Oversigt%20over%20udvalg%20og%20erfa-grupper.aspx?cid=176923. Desuden kan du også kontakte DI ITEK, som kan hjælpe dig videre, tlf. 3377 3377, e-mail: itek@di.dk
- Forespørgsel om eller anmeldelse af en hændelse kan ske til dit lokale politi eller til Rigspolitiets Nationale IT-efterforskningscenter, NITEC, www.politi.dk/da/hjaelppolitiet/itkriminalitet/. Ved forhold af hastende karakter kan der rettes henvendelse på tlf. 4515 0605.

Tiltag for mindre og mellemstore virksomheder

Alle virksomheder bør have etableret et minimum af tekniske foranstaltninger i infrastrukturen, som kan detektere hændelser og bruges til bevissikring, men som i mange tilfælde også kan bruges til andre ting - f.eks. at optimere driftsstabiliteten.

1. Logfiler
Man kan logge stort set hvad som helst. Det er vigtigt at logningen er i overensstemmelse med virksomhedens forretningsmæssige behov og at personalet er bekendt med at logning finder sted. Loggen registrerer hvilken aktivitet der foregår fra hvilke personer på et bestemt tidspunkt. Der bør som minimum være logning af hvem der tilgår systemerne udefra og hvilke systemer udenfor virksomheden, som personalet tilgår. Denne type logs vil vise en IP-adresse, på hvor trafikken stammer fra og er helt central for at man kan finde ud af hvor (i verden) den kriminelle kommer fra. Man kan få særlige programmer til at hjælpe med at fortolke oplysninger i logfiler, som ellers kan være ganske uoverskuelige og uforståelige. Man kan også vælge en outsourcing partner til at håndtere ens logs.

2. Backup
Når en hændelse optræder, kan det være relevant at tage en ekstra backup, så man kan dokumentere hvordan et system præcist ser ud på et givent tidspunkt. På en måde kan man undgå at en forbryder sletter sine spor efter sig fra f.eks. en log når han er færdig.

3. Tidsstempling
Det er vigtigt at kunne dokumentere tidspunktet for en kriminel handling. Man bør derfor lade sit udstyr trække tiden via services udefra, således at de altid er synkroniserede med hinanden og med en ekstern kilde.

4. Ekstern hjælp
Man bør have kontaktinformation klar til eksterne kompetencer - f.eks. tekniske konsulenter og politiet.

5. Fotos
Hvis der sker en hændelse der efterlader fysiske spor er noget så simpelt som at tage et fotografi en god dokumentation.

Avancerede tekniske tiltag

Som allerede nævnt anbefales det at kontakte en ekstern ekspert i bevissikring, hvis man ikke har de fornødne kompetencer i virksomheden. Men har virksomheden tekniske eksperter inhouse, som har fået uddannelse i at beskæftige sig med bevissikring, kan der også iværksættes en række mere avancerede tiltag:

1. Avancerede logfiler
Som nævnt kan stort set alle aktiviteter logges. Foruden logning af IP-adresser for ind- og udgående trafik kan det også være relevant at logge trafikken på de enkelte delkomponenter i infrastrukturen (f.eks. firewalls, proxy-servere og routere), så man kan se hvor den kriminelle har været i virksomheden. Man kan også logge alt muligt andet end IP-adresser - f.eks. trafikkens omfang, mængde af ledig plads på lagermedier, type af trafik og trafikkens mønster.

Det er vigtigt at have overblik over, hvilke logfiler man har og har viden om, hvordan de forskellige informationer kan kædes sammen. Når man tilgår sine logs, er det vigtigt, at man ikke i processen ændrer dem, fordi beviset selv dermed bliver kompromitteret.

2. Backup
Ud over at tage backup af forskellige beviser som f.eks. logfiler kan man også vælge at tage backup af hele disken (bitcopy). Ved at lave sådant et diskdump kan eksperten også søge på de "tomme" dele af disken, hvor den kriminelle bagmand evt. måtte have slettet data.

3. Øjebliksbillede (Netstat, Fport)
Man kan via forskellige programmer tage et øjebliksbillede af et system og dermed dokumentere hvilke processer der kører, hvilke porte der er åbne og hvilke fjernsystemer, der er tilsluttet virksomhedens system. På denne måde kan man bevise hvilke metoder der er brugt for at kompromittere virksomheden.

4. IDS, IPS og netværkssniffere
Når der sendes trafik (f.eks. i form af en e-mail) på et netværk, opdeles denne i små pakker. Der findes forskellige programmer, som kan opsamle og kigge på (hele eller dele af) indholdet i disse pakker. I enkle termer opsamler netværkssnifferne trafikken, Intrusion Detection Systems (IDS) opsamler og analyserer ud- og indgående trafik for at genkende bestemte skadelige typer og mønstre, mens Intrusion Prevension Systems (IPS) gør alle disse dele tillige med at lukke for forbindelser den finder potentielt skadelige.

Bilag A

Procesmodel for beslutninger, når en hændelse opstår.