

Quick Guide

Optimering af efterforskningsmulighederne
ved datakriminalitet

Quick Guide

Til optimering af efterforskningsmulighederne
ved datakriminalitet

Quick Guide til optimering af efterforskningsmulighederne
ved datakriminalitet

1. udgave, 1. oplag 2004

Copyright: DANSK IT

Oplag: 500

Forfatter: Tom Engly Henriksen

Tryk og layout: Jannerup offset a/s

Denne publikation er udarbejdet af forfatteren,
der er ansat i Rigspolitiets Kriminaltekniske Afdeling - IT-sektionen,
under ledelse af en referencegruppe under DANSK IT's Task Force
for internet-sikkerhed.

DANSK IT er en it-brugerorganisation stiftet i 1958 med det formål
at udbrede kendskabet til informationsteknologien og dens anvendelse,
at fremme anvendelsen af it til gavn for samfundet og den enkelte bruger
samt at samle alle it-brugere og it-professionelle om denne opgave.

DANSK IT
St. Kongensgade 59A
1264 København K

Quick Guide

– optimér efterforskningsmulighederne

Visionen:

- At gøre virksomheder i stand til at handle på den mest optimale måde i relation til bevismateriale, der senere skal bruges i forbindelse med en evt. straffe eller civilretlig sag.

Målet:

- At optimere virksomheders kendskab til de efterforskningsskridt der er nødvendige for at muliggøre forfølgning af en sag - hvad enten den ender som en straffesag eller som en civilretlig sag.
- At virksomhederne handler efter denne guide.
- At kendskabet til guiden udbredes mest muligt.

Indledning:

Det har længe været et ønske, at der blev udarbejdet en guide til, hvordan virksomheder forholder sig i relation til bevissikring af materiale i forbindelse med uautoriseret adgang til IT-systemer eller forsøg på samme. Ønsket kommer bredt fra såvel den industrielle som den finansielle sektor.

Bevissikring i sådanne sager adskiller sig markant fra den fysiske verden, hvor politiet i forbindelse med f.eks. en drabssag eller andet selv står for bevissikringen på et traditionelt gerningssted.

Der har til tider været kritik af, at "virksomhederne jo selv skal forestå efterforskningen". En virksomhed med store, komplicerede IT-systemer har næppe noget større ønske om, at politiet indfinder sig, spærrer området af og begynder at fordybe sig i systemerne. Politiet har i dag særligt uddannede specialister til at efterforske denne form for kriminalitet, men det må dog stå helt klart, at efterforskning altid vil foregå i nært samarbejde med den virksomhed, hvis systemer er kompromitterede, idet administratoren det pågældende sted er den eneste, som kender systemet indgående. Anmelderen må derfor også være indstillet på dette samarbejde igennem sagsforløbet.

Politiet kan altid kontaktes for en uformel snak om, hvad der kan være sket, og om det passerede i givet fald kan anses for at være ulovligt – også uden at indgive en anmeldelse. Mange tvivlsspørgsmål kan afklares ved en sådan uformel henvendelse. Virksomheder bør ikke være tilbageholdende med en sådan henvendelse af frygt for at blive "eksponeret". Det vil altid stå klart, om en reel anmeldelse er indgivet og hvilke konsekvenser det måtte medføre.

Det skal bemærkes, at denne guide er praktisk orienteret. At overholde gældende lovgivning er til enhver tid op til den enkelte virksomhed, der ønsker at anvende denne guide.

Hvad er et bevis?

I den fysiske verden er beviser spor, der peger på en gerningsmand – det kan være fingeraftryk, blodspor, fotooptagelser, vidneforklaringer osv. I den digitale verden er der sjældent nogen af de nævnte beviser tilstede. Som oftest er der udelukkende tale om "digitale fingeraftryk".

Quick Guide

– optimér efterforskningsmulighederne

IP-adresser er en vægtig faktor, når vi taler efterforskning. Det er i mange tilfælde den eneste vej videre i en efterforskning, men gerningsmænd kan også efterlade sig en signatur på andre måder – f.eks. en adgang til en ftp-server, i ini-filer, kaldenavne eller lignende. Det må derfor understreges, at hver en "bit" på et system i den sidste ende kan være potentielt elektronisk bevis.

Vigtigheden af det elektroniske bevis

Det elektroniske bevis er afgørende. Ikke blot i sager vedrørende indtrængen i virksomhedens systemer udefra, men i stigende grad også til en lang række af andre forbrydelser, der kan være begået mod en virksomhed. Det kan for eksempel være tilstedeværelse af børnepornografi på et af virksomhedens systemer (servere eller arbejdsstationer), misbrug af e-mails, fortroligt materiale, der videresendes til presse eller konkurrerende virksomhed, en tidligere ansat, der fortsat har adgang til systemerne. Listen er lang. Enhver af disse eksempler kan ende med en retssag, og det er her betydningen af det elektroniske bevis står sin prøve. Jo mere man kan dokumentere, jo større chance er der for, at en sag kan vindes. Det er svært at give en definition på det "endegyldige" bevis, der som nævnt kan findes mange steder på systemet.

Virksomheden har forståeligt en interesse i hurtigt at få reetableret systemerne set ud fra et forretningsmæssigt synspunkt, men hvis sikring af beviserne grundlæggende ikke er i orden, kan det være vanskeligt i den sidste ende at føre en retssag. Guidens 2. del giver et bud på, hvilke tiltag man kan gøre for at forberede sig.

Integritet

Nogle grundprincipper vedrørende beviser er, at de skal kunne præsenteres troværdigt i en eventuel retssag, og at der ikke må være tvivl om disse. Det gælder naturligvis også digitale beviser i form af logfiler etc. Det er derfor vigtigt, at integriteten i de elektroniske beviser sikres. Det kan gøres ved at tage en backup i så tidlig en fase som muligt. Jo mere der gøres ud af bevissikringen - jo større vægt kan denne form for beviser tillægges.

Hvad gør jeg så?

Guiden er udarbejdet i 2 dele. En 10 - punkts udgave, der giver bud på, hvordan virksomheden forholder sig, når det er gået galt, og endnu en 10 - punkts udgave med bud på hvad der kan gøres for at optimere de efterforskningsmæssige muligheder før det går galt.

Guiden er opsat i punkform og kan betegnes som en checkliste, men den fordrer - sikkert for de fleste - at de enkelte punkter uddybes nærmere, hvilket gøres i det følgende.

Forholdsregler ved et muligt kompromitteret system 1

1. Indsæt en kompetent person til at håndtere sagen

- Det er væsentligt, at der i virksomheden findes en person, der har den fornødne tekniske indsigt i systemerne. Derfor bør en sådan indsættes til at håndtere situationen. Denne bør i forvejen have et mandat til at handle på virksomhedens vegne.
- Det kan evt. være en systemadministrator i virksomheden, men også gerne en udefra kommende konsulent, hvis virksomheden ikke selv råder over fornøden kompetence. Det er ikke sjældent, at det er en direktør i virksomheden, der henvender sig i en anmeldelsessituation og dermed ønsker at være kontakttled til politiet. Det er helt i orden i starten, men kommunikation vedrørende det tekniske bør dirigeres hen til en tekniker.
- Den direkte kommunikation mellem den teknisk kompetente person og eventuelt politiet er af stor vigtighed.

2. Integritet – tag backup af systemet under mistanke

- Det er, som indledningsvis nævnt, vigtigt at sikre integriteten af de systemer der mistænkes. Det er fristende at begynde at arbejde på systemet for at søge sporene – og det ses ofte. Når mistanken er "stor" nok, bør man øjeblikkeligt tage en backup af systemet. Når først den er sikret, er der ikke noget i vejen for at undersøge systemet, og eventuelt lade det køre videre i det omfang, man finder det forsvarligt. Det er jo ikke sikkert, at man sådan uden videre kan tage systemet ud af produktion. Vær dog opmærksom på, hvilke skader systemet eventuelt forøver mod andre systemer – er det eksempelvis med i et Dos-angreb (Denail of Service)?
- Det er vigtigt at sikre en fuld backup – evt. disaster backup – af systemet. Ved tape backup er det blot vigtigt at informere om, hvilken båndtype, software, samt version der er anvendt – således at politiet eller andre kan indpasse dette i forbindelse med en efterfølgende dataundersøgelse. Det er samtidig vigtigt at skelne imellem en data-backup og en fuld diskdump (bitcopy). Ved den fulde diskdump er det også muligt at søge efter beviser i det uallokerede område, hvor der ved databackup kun kan søges i det aktive filsystem. Søgning i det uallokerede område er aktuelt i forbindelse med søgning efter materiale, som gerningsmanden har slettet.
- Evt. kan anvendes Linux DD, Symantec Ghost, eller andet format. Politiet anvender selv EnCase™ og Forensic Toolkit™ til selve dataundersøgelsen, og disse værktøjer kan også håndtere forskellige former for Backup – bl.a. Linux DD.
- Backup er det grundlæggende bevis i sagen. Uanset om der i senere faser foretages udtræk til dokumentation, så vil en sådan backup altid kunne tages frem i tvivlstilfælde.
- Data som er "gruppet" ud fra eksempelvis en logfil, er et godt og overskueligt arbejdsgrundlag, men af hensyn til integriteten er det stadig vigtigt at have råmateriale.
- Politiet er naturligvis opmærksom på, at en fuld backup kan indeholde forretningsmæssige følsomme oplysninger, men disse vil naturligvis ikke indgå i en eventuel sag. Kun materiale relevant for sagen vil blive udtrukket og dokumenteret.

1 Forholdsregler ved et muligt kompromitteret system

3. Noter serverens tidsstempeling i forhold til realtiden

- Tidspunkterne på de berørte systemer skal noteres og sammenholdes med realtiden – eventuelt frk. Klokken eller tekst-tv. Tidspunkter er af stor betydning i sager, idet det nøjagtige tidspunkt kan være afgørende for at identificere, hvem der har været tildelt en IP-adresse på et givent tidspunkt.

4. Tag et øjebliksbillede af aktivitet på aktuelt system (Netstat, Fport etc.)

- Selvom der er taget en fuld backup af systemet, og denne kan køres op igen, er det en stor hjælp at tage et "øjebliksbillede" af systemet. Det vil i praksis sige, hvilke processer kører, hvilke porte er åbne, og ikke mindst, hvilke fjernsystemer er tilsluttet systemet.
- Til brug for dette kan anvendes kommandoen netstat -an, udskrevet til en fil (netstat -an >filnavn.txt) husk at angive nøjagtig dato / tidspunkt for, hvornår det er foretaget. Vær opmærksom på, at et kompromitteret system kan have fået skiftet lige netop denne fil ud – anvend derfor helst en fil, hvor integriteten er sikret. Det er altid en god ide for en systemadministrator, at have de mest nødvendige (originale) filer på cd-rom eller andet medie.
- På Windows systemer kan Fport fra www.foundstone.com anvendes til at identificere ukendte porte og deres tilhørende applikationer. Denne udskrives også til en fil (Fport -p > filnavn.txt) Husk igen dato / tidspunkt. Fport er freeware.

5. Vær opmærksom på andre systemer som kan være interessante (firewall, proxy, routere etc.)

- Det er ikke nødvendigvis altid tilstrækkeligt med de logfiler, der findes på det aktuelle system / server. Står serveren f.eks. på et LAN kan informationer fra f.eks. firewall, proxy-server, router m.v. være yderst relevante. En god logfil, der blot henviser til virksomhedens firewall har ingen værdi, hvis det ikke er muligt at se næste spor i firewallens log. Der skal sikres informationer hele vejen fra virksomhedens gateway til Internet og ind til det aktuelle system.
- Overvej hvordan man i øvrigt er kommet ind til det berørte system – kan firewallen også være kompromitteret?

Forholdsregler ved et muligt kompromitteret system 1

6. Opsæt eventuelt en netværkssniffer med henblik på analyse af trafikken

- Det er i mange tilfælde uoverskueligt at pege på noget konkret, der foregår på systemet. I et WinNT system er det i værste fald ikke muligt at finde noget. Vær opmærksom på, at det er muligt at skjule filer og processer i et sådant system. Ved at dumpe netværkstrafikken er det muligt at identificere de skjulte processer, der eventuelt kører. Af hensyn til risikoen for at blive "opdaget" er det ideelle at sætte snifferen op på et selvstændigt system. Selv ved et kortvarigt dump af trafik kan det være værdifuldt. Der er eksempler på, at ftp-servere (bl.a. Serv-U) har været skjult helt i Windows systemet, men er identificeret via netværkssnifferen.
- Af mulige sniffer kan anvendes Ethereal, der findes både i en Windows og Linux version. Se eventuelt www.ethereal.com.
- Råtrafikken kan senere være til stor hjælp i efterforskningen, men det lades op til den enkelte virksomhed at vurdere, hvorvidt total dump af trafik kan foretages. Generelt er det dog sådan, at en virksomhed legalt kan "dumpe" egen trafik, med henblik på analyser. Virksomheden kan så overgive denne trafik til politiet som eventuelt bevis.
- At virksomheden forbeholder sig ret til at dumpe trafikken, kan være et punkt i IT-sikkerheds politikken.

7. Identificer mulige logfiler både på det kompromitterede system samt firewall / proxy / router

- Det er en stor hjælp i forbindelse med en eventuel efterforskning, at virksomheden selv er behjælpelig med at identificere de logfiler, der måtte være relevante i sagen. Som tidligere nævnt kender virksomheden selv sine systemer bedst.
- Husk igen, at logfiler fra flere systemer kan være nødvendige for at sammenkæde hændelsen og i sidste ende identificere en fjendtlig IP-adresse.
- Der er intet i vejen for at foretage udtræk fra de forskellige logfiler (evt. hvis kun en IP-adresse er interessant) husk blot, at den komplette logfil skal forefindes i uredigeret form (integritet).

8. Undlad selv at tage affære ved at kontakte eksterne parter

- Hvis virksomheden ønsker at foretage en anmeldelse til politiet eller anlægge en privat sag er det vigtigt, at der ikke selvstændigt indledes en efterforskning ud af huset. Der er adskillige eksempler på, at der er rettet henvendelse til abuse hos eksterne ISP'ere, hvorefter disse igen har rettet henvendelse til deres kunder, der så har mulighed for at slette spor efter sig. De endelige beviser ligger som oftest ikke på de kompromitterede systemer, men findes i forbindelse med ransagning og beslaglæggelse hos gerningsmanden og efterfølgende undersøgelse af dennes computere.
- Det kan naturligvis være nødvendigt at kontakte egen ISP, men det bør gøres klart for ISP'en, at denne ikke foretager sig yderligere end de aftalte undersøgelser (f.eks. ved at kontakte gerningsmandens ISP o.s.v.).

1 Forholdsregler ved et muligt kompromitteret system

9. Forsøg at klarlægge, om systemet er aktuelt kompromitteret

- Det er vigtigt at sondre imellem et aktuelt kompromitteret system altså hvor gerningsmanden kan være koblet til systemet her og nu og et system, der nok er kompromitteret, men hvor der ikke er aktuel aktivitet. Ved et aktuelt kompromitteret system er der naturligvis størst mulighed for at sikre de nødvendige beviser. Dette set ud fra, at hackere gør et stort arbejde ud af at skjule deres færden på systemer inden de forlader dem.
- Ved et aktuelt kompromitteret system bør politiet inddrages med det samme og gerne i form af en uformel henvendelse.

10. Tag kontakt til politiet lokalt for anmeldelse eller Rigspolitiets Kriminal Tekniske Afd. IT-sektionen for vejledning på 3314-8888

- Som udgangspunkt skal en anmeldelse indgives til det lokale politi. Det lokale politi har så mulighed for at trække på assistance via Rigspolitiets IT-sektion under Tekniske Afdeling.
- IT-sektionens formål er primært at bistå politikredsene med efterforskning i alle sager vedrørende IT-kriminalitet.
- IT-sektionen står gerne til rådighed for den uformelle samtale med virksomhederne, og kan i såfald kontaktes direkte.

10 hovedpunkter

- Indsæt en kompetent person til at håndtere sagen.
- Integritet - Tag backup af systemet under mistanke.
- Noter systemets / serverens tidsstempeling i forhold til realtiden.
- Tag et øjebliksbillede af aktivitet på aktuelt system (Netstat, Fport etc.)
- Vær opmærksom på andre systemer som kan være interessante (firewall, proxy, routere etc.)
- Opsæt eventuelt netværkssniffer med henblik på analyse af trafikken.
- Identificer mulige logfiler – både på det kompromitteret system, samt firewall / proxy / routere.
- Undlad selv at tage affære ved at kontakte eksterne parter.
- Forsøg at klarlægge, om systemet er aktuelt kompromitteret.
- Tag kontakt til politiet – lokalt for anmeldelse, eller Rigspolitiets Kriminaltekniske Afd. IT-sektionen for vejledning på tlf.: 3314 8888.

Kom på forkant med efterforskningen **2**

1. IT-sikkerhedspolitik, hvor efterforskning er tydeliggjort

- Megen usikkerhed om hvordan en virksomhed skal forholde sig ved mistanke om misbrug af systemer etc. kan helt eller delvist elimineres, hvis en virksomhed på forhånd tager højde for, at situationer af den art kan opstå. IT-sikkerhedspolitikken er et glimrende sted at implementere sådanne forholdsregler. Det er her muligt på forhånd at tage højde for størsteparten af de punkter, som tidligere er nævnt. En gennemarbejdet plan, hvor procedurer er fastlagt i rammer, vil skabe den nødvendige ro der skal til for at arbejde optimalt med "bevissikringen".
- Awareness overfor brugere i virksomheden er også et væsentligt punkt. Det er set, at en medarbejder – ikke nødvendigvis af ond vilje – ødelægger et bevis ved f.eks. at slette en e-mail helt. Det digitale spor i en e-mail findes i den oprindelige header, og en udprintet version har ingen værdi, hvis ikke headeren er sikret. Det nytter altså ikke meget blot at videresende en e-mail, da de oprindelige header oplysninger så går tabt.

2. Udarbejd et regelsæt for, hvornår virksomheden ønsker at anmelde til politiet

- Det er vigtigt at virksomheden gør sig klart, hvornår og i hvilke situationer man ønsker at anmelde sager vedrørende IT-kriminalitet.
Sager som vedrører overtrædelse af Straffelovens § 263 er - som loven er i dag - betinget offentligt påtalt, hvilket betyder, at virksomheden skal gøre sig klart, om den vil forfølge en sådan sag hele vejen igennem. Det er før set, at sager, der har været efterforsket et stykke tid, må opgives hvis en anmelder ikke længere ønsker at forfølge sagen. En sag under efterforskning kan holdes fortrolig med respekt for de reaktioner efterforskningskridt medfører. Hvis sagen ender i retten, er sådanne sager som udgangspunkt offentligt tilgængelige.

3. Identificer en koordinator i virksomheden, som er kompetent til at styre en given situation

- Virksomheden bør identificere, hvilke nøglepersoner der ønskes anvendt i situationer, hvor en potentiel sag opstår. En kompetent koordinator behøver ikke nødvendigvis være den, der har det dybdegående tekniske kendskab til de implicerede systemer – han kan mere sammenlignes med en projektleder.

4. Identificer kompetente personer, der er eksperter på virksomhedens anvendte systemer – evt. eksterne sikkerhedskonsulenter hvis nødvendigt

- Personer med en kompetent teknisk viden om de enkelte systemer er vigtig. Såfremt virksomheden ikke selv råder over sådanne, kan en ekstern konsulent fra et sikkerhedsfirma anvendes. Dette gælder naturligvis også, hvis hosting og sikkerhed i forvejen er outsourcet til en ekstern virksomhed.

2 Kom på forkant med efterforskningen

5. Udarbejd et netværksdiagram, så systemernes sammenhæng let kan klarlægges

- Systemers opbygning og sammenhænge er ofte komplekse. Kendskab til selve netværksstrukturen er et vigtigt element for at kunne klarlægge og belyse en sag - og i sidste ende opklare, hvordan et system eventuelt er kompromitteret.
- Det er derfor en fordel, at der i selve beredskabet foreligger et netværksdiagram, som kan belyse disse punkter og hermed fremme kommunikationen og hindre misforståelser. Et netværksdiagram - der er et meget følsomt dokument - vil ikke indgå som sagsmateriale, men alene være et arbejdsdokument imellem virksomheden og efterforskeren.

6. Opsæt optimal logning / auditing. F.eks logning på særskilt logserver med begrænset adgang

- Manglende loginformation og auditing på systemerne er tit en kendsgerning, og det kan føre til, at det ikke er muligt at komme videre i en efterforskning. Det bør derfor overvejes at sætte så meget logning op som muligt, ligesom den tilgængelige auditing bør aktiveres. Dette vil give optimale muligheder for at finde de elektroniske spor, som er nødvendige. Med hensyn til logningen er det endvidere en stor fordel, hvis logningen foretages særskilt - og helst på en særskilt server. Hackere er ofte meget bevidste om at slette sporene efter sig, og hvis logningen er opsat default gør det arbejdet for hackerne meget nemmere. De færdige "hacker tools" som er let tilgængelige på Internettet, vil i flere tilfælde være konstrueret således, at de også sletter spor i logfiler / eventlogs. Det fordrer selvsagt, at logningen er default, hvilket er endnu et argument for at tænke alternativt. Husk, at det primært er i logningen, at de elektroniske beviser skal findes. Det er endvidere vigtigt at overveje, hvad der skal logges. Source IP, Dato/Tidspunkt, Source port, Target IP, Target port er nogle af de vigtige poster, men det er naturligvis også vigtigt, at det er muligt at se, hvad der reelt er foregået - f.eks. i en IIS log se hvilke kommandoer, der er anvendt, styresystem, browser etc. Dette vil naturligvis være forskelligt fra system til system, men essensen er, at der i logningen er tilstrækkelig information til at bevise handlingen. I audit er der en tendens til kun at sætte audit på failure, men det kan være lige så vigtigt at sætte audit på succes.

7. Overvej eventuelt et IDS-system

- Såfremt virksomheden har mulighed for det, er det en fordel at indføre IDS-systemer. Dette vil i mange tilfælde muliggøre identifikation af mulige angreb i en tidlig fase.

8. Synkroniser servere/systemer med tidsserver

- Det er vigtigt at alle berørte enheder, (firewall, routere, servere m.v.) synkroniseres med en tidsserver, således at der altid er tale om realtid på samtlige enheder i routingen. Såfremt beviserne skal findes på flere enheder er det en stor hjælp, at der er tale om korrekte realtider. Det er væsentligt nemmere at dokumentere ved en eventuel senere retssag. Forskellige tidsstempler på forskellige involverede enheder vil altid være genstand til forvirring. Det korrekte tidspunkt er vigtigt, hvis en bruger af en IP-adresse senere skal identificeres.

9. Identificer procedure for indsættelse af netværkssniffere

- At opsætte en netværkssniffer er ikke nødvendigvis en nem sag, og det kan derfor være en fordel at "øve" sig på dette i en testsituation, således at man i den skarpe situation har en helt fastlagt procedure for, hvordan der skal reageres, hvilke sniffere og hardware der skal bruges etc. I en "øjeblikssituation" skal tingene som regel gå hurtigt, og ved at forberede sig effektivt, forøges chancerne samtidig for at tingene gøres rigtigt. Som tidligere nævnt er formatet trafikken dumpes i, ikke det vigtigste, men Ethereal og TCP-dump er værktøjer, der kommer med et output, som kan konverteres om til de værktøjer, som f.eks. politiet anvender. (Proceduren bør være beskrevet i IT-sikkerhedspolitikken).

10. Identificer procedure for hurtig databackup

- En databackup er heller ikke noget der foretages på et øjeblik, hvis ikke en vis forberedelse har fundet sted. Det fleste virksomheder råder over backup-systemer, men alligevel er det en god idé at forberede proceduren - igen i lyset af, at der kan blive brug for at handle hurtigt.
- Er det i øvrigt nødvendigt at geninstallere eget system ud fra en i forvejen sikret backup - så vær opmærksom på, om denne backup er "ren". Det er før set, at et system er geninstalleret fra en backup, der i forvejen har været hacket med deraf følgende installerede trojanere.

2 Kom på forkant med efterforskningen

10 hovedpunkter

- IT- Sikkerhedspolitik, hvor efterforskning er tydeliggjort.
- Udarbejd et regelsæt for, hvornår virksomheden ønsker at anmelde til politiet.
- Identificer en koordinator i virksomheden, som er kompetent til at styre en given situation.
- Identificer kompetencepersoner, der er eksperter på virksomhedens anvendte systemer – evt. eksterne sikkerhedskonsulenter hvis nødvendigt.
- Udarbejd et netværksdiagram, så systemernes sammenhæng let kan klarlægges.
- Opsæt optimal logging / audit – hvis muligt på særskilt log server med begrænset adgang.
- Overvej eventuelt et IDS-system.
- Synkroniser servere/systemer med tidsserver.
- Identificer procedure for indsættelse af netværkssniffere.
- Identificer procedure for hurtig databackup.



Afslutning:

Formålet med denne guide er at højne awareness omkring efterforskningsproblematikken. Ingen forventer, at denne guide fører til uddannede efterforskere, men det er håbet, at den har givet anledning til at sætte tanker i gang om, hvad der egentlig skal til for at føre en god sag. Listen er ikke udtømmende, men de mest vitale punkter skulle gerne være dækket.

Denne guide kan frit distribueres og anvendes såfremt indholdet i guiden ikke ændres.

Denne publikation skal gøre virksomheden i stand til at handle på den mest optimale måde i relation til at indsamle elektroniske spor i forbindelse med datakriminalitet til brug i en eventuel retssag.

Publikationen er primært rettet mod de teknisk ansvarlige for virksomhedens it-sikkerhed, men kan med fordel også læses af alle med interesse for it-sikkerhed.

Forfatteren Tom Engly Henriksen arbejder til daglig i Rigspolitiets Kriminaltekniske afdeling - it-sektionen med efterforskning af datakriminalitet.

ISBN: 87-88972-36-4

DANSK IT

St. Kongensgade 59A
1264 København K
Tel. 33 11 15 60
Fax. 33 93 15 80
www.dansk-it.dk