NATIONALT CYBER CRIME CENTER
VIRKSOMHEDSGUIDE

Forholdsregler

Ved brud på it-sikkerhedssystemer

NC3 POLITI

dansk·it

Indhold

01 Introduktion 2

1.01 Indledning 2
1.02 Opbygning 2
1.03 Hvad er et bevis inden for IT-efterforskning? 2
1.04 De elektroniske beviser er afgørende 3
1.05 Dataintegritet 4
1.06 Samarbejde mellem politiet og virksomhederne mod it-kriminalitet. 4

02 Forberedelse på sikkerhedsbruddet 5

2.01 Computer Incident Response Plan (CIRP) 6
2.02 Kend dit netværk 6
2.03 Brugeradministration 7
2.04 Netværkssegmentering 7
2.05 Network Time Protocol-Server (NTP-server) 7
2.06 Logning 7
2.07 Backup og kryptering 9
2.08 Konfiguration af digitale enheder og opsætning af sikkerhedspolitikker 9
2.09 Opdater systemerne 9
2.10 Uddannelse og awareness 9

03 Forholdsregler ved et muligt kompromitteret netværk 11

3.01 Udpeg en kompetent person til at håndtere hændelsen 12
3.02 Få et overblik 12
3.03 Er systemet aktuelt kompromitteret? 12
3.04 Beslut om politiet skal involveres 12
3.05 Begynd at indsamle data 13
3.06 Anden dokumentation til politiet 14

04 Afsluttende bemærkninger 14

01 Introduktion

1.01 Indledning

Denne guide er udarbejdet i samarbejde med DANSK IT og skal give virksomheder en vejledning i, hvad de bør gøre for at sikre sig, at politiet kan få de nødvendige spor hvis politiet skal efterforske en it-relateret hændelse.
Rigspolitiets Nationale Cyber Crime Center (NC3) har gennem længere tid erfaret, at når politiet bliver involveret, så er det ofte enten for sent, da de relevante spor ikke længere eksisterer, eller også har der ikke været indsamlet de rigtige spor til at begynde med. Dette skyldes både tiden, fra gerningen er sket og til anmeldelse, men det skyldes lige så meget, at den enkelte it-afdeling ikke har haft fokus på at indsamle spor og derfor ikke ved, hvilke beviser der bør sikres.
Målet med denne guide er derfor at:

- Oplyse virksomheder om, hvad de selv kan gøre for at sikre indsamling af de nødvendige oplysninger inden et eventuelt brud på it-sikkerheden.

- Hjælpe med at sikre, at eventuelle spor ikke bliver ødelagt/forvansket, hvis der skulle opstå et brud på it-sikkerheden.

- Give en kort anvisning i, hvordan virksomhedens netværk sikres, så politiet har de bedste arbejdsbetingelser.

- Gøre det nemmere at indsamle de nødvendige spor til politiet, hvis skaden sker.

1.02 Opbygning

Guiden er delt op i en introduktion efterfulgt af to dele. Introduktionen beskriver baggrunden for udarbejdelsen af denne guide, og hvorfor it-sikkerhed bør tages alvorligt.
Guidens del 1 giver bud på, hvilke tiltag man kan gøre for at forberede sig, så politiet har de bedste arbejdsbetingelser, hvis en sikkerhedshændelse skulle opstå.
Guidens del 2 giver bud på, hvordan man sikrer beviserne på en måde, så de kan bruges i retten, hvis der allerede er sket et sikkerhedsbrud.
Denne guide forudsætter, at virksomheden selv drifter netværket i virksomheden. Hvis jeres virksomhed har udliciteret driften af netværket til tredjepart, bør I sikre jer i kontrakten med denne, at de kan efterleve forholdsreglerne nedskrevet i denne guide.
Det skal bemærkes, at denne guide er praktisk orienteret. Det er til enhver tid op til den enkelte virksomhed, der ønsker at anvende denne guide, at overholde gældende lovgivning.

1.03 Hvad er et bevis inden for it-efterforskning?

I den fysiske verden er beviser spor, der peger på en gerningsmand. Det kan være fingeraftryk, blodspor, videooptagelser, vidneforklaringer osv.
I den digitale verden er der sjældent nogen af de nævnte beviser til stede. Som oftest er der udelukkende tale om ”digitale fingeraftryk”.
Digitale fingeraftryk kan være ip-adresser, men ip-adresser er ofte langt fra det eneste, man skal bruge for at identificere en eventuel gerningsmand. De fleste netværk er konfigureret med DHCP-servere, der tildeler ledige ip-adresser til computerne på netværket. Denne ip-adresse bliver tildelt til computeren i et foruddefineret tidsrum. Når dette tidsrum er gået, kan computeren blive tildelt en ny ip-adresse. Ip-adressen kan også skiftes manuelt for at besværliggøre en eventuel efterforskning.

Kendskabet, til hvornår en given handling er foregået, er altså en lige så stor faktor som kendskabet til port-numre, MAC-adresser, netværksnavne, brugernavne og andet. Logs er derfor ofte den vigtigste kilde til spor i en efterforskning. Det er meget vigtigt, at man indsamler logs fra forskellige kilder. I guidens del 1 vil der komme eksempler på kilder, man kan indsamle logs fra, og et bud på, hvordan man kan lette en del af indsamlingsarbejdet ved på forhånd at implementere diverse løsninger som eksempelvis 'SIEM'.

1.04 De elektroniske beviser er afgørende

Ikke blot i sager vedrørende indtrængen i virksomheders systemer udefra er de elektroniske beviser afgørende, men i stigende grad også i efterforskningen af en lang række andre forbrydelser, der kan være begået mod en virksomhed.
Her er det vigtigt at gøre op med den praksis, der har været dominerende indtil nu, hvor fokus har været på udefra kommende trusler og i stedet kigge bredt på trusler både indefra og udefra. Hvis man først kom ind i et netværk, var der frit spil og ingen eller få forhindringer. Tilliden til de ansatte har været høj – ofte for høj. Dette problem udstilles i høj grad, når virksomheder fx rammes af ransomware. Når en godkendt bruger på virksomhedens netværk trykker på et link, besøger en inficeret hjemmeside eller åbner en inficeret fil, har ransomwaren ofte frit spil til at kryptere hele netværket. Nogle gange også diverse backup-drev. Ransomwaren har adgang til alt det, som brugeren, der aktiverer den, har.
It-sikkerhed bør derfor i lige så høj grad dreje sig om at sikre netværket mod uautoriseret adgang fra brugere internt på netværket.
Man kan groft sagt inddele aktører i en sikkerhedshændelse i tre kategorier: Den utilsigtede aktør, den ondsindede insider og outsidere.

1. *Den utilsigtede aktør* dækker fx over ansatte, der uforvarende kommer til at klikke på et link i en e-mail, besøger en inficeret hjemmeside, åbner et dokument eller anden fil med indlejrede macroer eller sætter et ukendt usb-stik i sin computer og derved aktiverer ondsindet software såsom ransomware.
2. *Ondsindede insidere* kan eksempelvis være årsag til tilstedeværelse af børnepornografi på et af virksomhedens systemer (servere eller arbejdsstationer), misbrug af e-mails eller læk af fortroligt materiale til pressen eller konkurrerende virksomhed. Det kan være en tidligere ansat, der fortsat har adgang til systemer og bruger denne adgang til egen vinding. Det kan også være en nuværende eller tidligere ansat, der har set sig sur på virksomheden og ønsker at gøre skade ved at ødelægge dens it-systemer.
3. *Outsidere*, altså folk udefra, kalder man normalt hackere. De søger bevidst at udnytte en svaghed i netværket og skaffer sig derved uautoriseret adgang. Motivet er ofte økonomisk vinding, men kan også være politisk eller hævn. I denne kategori falder både de personer, der går specifikt efter at komme ind i én bestemt virksomhed, og de personer der skanner en stor mængde netværk og leder efter sårbarheder, så de kan få adgang til et hvilket som helst netværk.

Hvert af ovenstående eksempler kan ende med en retssag, og her er det vigtigt, at de elektroniske beviser er i orden. Jo mere og jo bedre man kan dokumentere sine beviser, jo større er chancen for, at en sag kan vindes.
Virksomheder har en stor interesse i hurtigt at få reetableret systemerne og få forretningen i gang igen, men hvis sikringen af beviserne grundlæggende ikke er i orden, inden systemerne gendannes, kan det være vanskeligt i den sidste ende at føre en retssag. Dette betyder ikke, at driften skal negligeres. Tværtimod handler det om at have nogle procedurer på plads på forhånd, så man hurtigst muligt får de rigtige beviser og hurtigt kan gendanne systemerne.
Hvis man alene fokuserer på trusler udefra, kan der godt gå lang tid, før en indtrængen bliver opdaget. Globalt set gik der i 2017 i gennemsnit 191 dage[1], fra et netværk blev kompromitteret, til det blev opdaget. Dette er en forbedring i forhold til 2016, der var på 201 dage, men det kan stadig blive bedre.
En meget stor del af de hændelser, som Rigspolitiets Nationale Cyber Crime Center (NC3) bliver involveret i, omhandler insidere. Den bedste måde at strukturere sin netværkssikkerhed på er derfor at gå ud fra, at netværket allerede er kompromitteret (Assume breach).

[1] 2017 Cost of Data Breach Study, Global Overview, Benchmark research sponsored by IBM Security, independently conducted by Ponemon Institute LLC, June 2017, © Ponemon Institute Research Report.

1.05 Dataintegritet

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 sikre data og logs så tidligt i forløbet som muligt og sikre sig, at de ikke er blevet ændret.
Jo mere der gøres ud af bevissikringen, jo større vægt kan denne form for beviser tillægges.
Guidens del 2 vil give eksempler på, hvad man kan gøre for at sikre sig, at dataintegriteten på de beviser, man sikrer sig, er i orden.

1.06 Samarbejde mellem politiet og virksomhederne mod it-kriminalitet

NC3Skyt er et samarbejde mellem NC3 og især små og mellemstore virksomheder, hvor ambitionen er at opnå bedre vidensdeling med henblik på at højne den generelle it-sikkerhedsbevidsthed i virksomhederne. Samarbejdet blev søsat i begyndelsen af 2016 og sigter primært imod forebyggelse af it-kriminalitet og skadesbegrænsende aktiviteter. Aktiviteter som vil kunne føre til, at virksomhederne bliver bedre til at beskytte sig mod angreb og bedre rustet til at håndtere de negative effekter af eventuelle angreb på deres it-systemer.

Som deltager i NC3Skyt får din virksomhed adgang til følgende:

- Møder med andre medlemsvirksomheder og politiet, hvor der kan udveksles viden og erfaringer om it-angreb med henblik på at styrke virksomhedens modstandsdygtighed over for it-kriminalitet.

- Informationsmateriale fra NC3 om nationale og internationale tendenser mv., som kan indeholde oplysninger om forskellige typer af malware, ransomware mv. udarbejdet af NC3 og Europol.

- Mulighed for at kommunikere med politiets NC3Skyt-medarbejdere ved spørgsmål om it-relateret kriminalitet.

Det koster ikke noget at være medlem af NC3Skyt.

Du kan efter aftale med din lokale NC3Skyt-repræsentant lægge hus til møder eller arrangementer, hvis din virksomhed har mulighed for det.

Som medlem af NC3Skyt kan du som deltager få kendskab til dine meddeltageres interne it-sikkerhed og til konkrete forhold og hændelser. Derfor forventer vi, at du iagttager tavshedspligt. Hvis du udtræder af NC3Skyt, gælder tavshedspligten stadig.

Henvend dig til NC3Skyts sekretariat pol-nc3-skyt@politi.dk, hvis du på vegne af din virksomhed ønsker at blive medlem eller har yderligere spørgsmål.

02 Forberedelse på sikkerhedsbruddet

2.01 Computer Incident Response Plan
Hav en plan , der forklarer, hvad der skal gøres, hvis skaden skulle ske

2.02 Kend dit netværk
Udarbejd et diagram over dit computernetværk

2.03 Brugeradministration
Giv kun brugerne de rettigheder, som de har brug for

2.04 Netværkssegmentering
Opdel netværket i forskellige segmenter, og opsæt regler for, hvem der må tilgå hvilke segmenter

2.05 Network Time Protocol Server (NTP)
Sørg for, at tiden er den samme på hele netværket

2.06 Logning
Vær opmærksom på at logge det rigtige samt gemme og beskytte dine logs

2.07 Backup og kryptering
Hav en a backup-politik, der gør, at I både kan genoprette systemet og samtidig undgår at overskrive beviserne

2.08 Konfiguration af digitale enheder og opsætning af sikkerhedspolitikker
Konfigurer enhederne og indstil sikkerhedspolitikkerne

2.09 Opdater systemerne
Hold systemerne opdaterede, så I får lukket sikkerhedshullerne

2.10 Uddannelse og awareness
Uddan medarbejderne i it-sikkerhed

2.01 Computer Incident Response Plan (CIRP)

Det er vigtigt at have en formaliseret plan for, hvordan der skal handles, og hvem der er de ansvarlige, hvis der sker en større it-relateret hændelse. En sådan plan kaldes for en Computer Incident Responce Plan (CIRP).
En CIRP bør laves for sig og ikke indlejres i virksomhedens øvrige planer for fx nedbrud i systemerne, da en CIRP typisk bliver ret omfattende med mange specifikke oplysninger og udførlige step by step-guides.
Da virksomheder har forskellige computersystemer, er det umuligt at lave en generisk CIRP, men den er meget vigtig at have, og der bør afsættes tid til at udfærdige, vedligeholde og træne den.
En CIRP bør blandt andet indeholde:

- En definition af, hvad der er en større it-relateret hændelse.
- Kontaktoplysninger til de ansvarlige ved en it-relateret hændelse.
- Information om, hvornår der skal ringes til politiet.
- Kontaktoplysninger på dem, der må udtale sig til pressen, og hvornår de må det.
- Oplysninger om, hvor man kan finde netværksdiagrammet (se punkt 2.02 ”Kend dit netværk”), og hvem der skal kontaktes.

Der er mange andre ting i en CIRP, ovenstående er blot til inspiration.
Når dette er på plads, er det vigtigt at øve simulerede angreb/nedbrud. Øvelserne skal sikre, at planen huskes, når systemerne er nede, og at kun de relevante personer går i gang med at genoprette systemerne.
Dermed begrænses virksomhedens nedetid, tab af indtjening og lavere tillid hos aktionærer.
Beviserne sikres desuden bedre og får en høj bevismæssig værdi i en eventuel retssag.

2.02 Kend dit netværk

Få udarbejdet et netværksdiagram. Brug tid på dette og sørg for at vedligeholde det, når nye systemer tilføjes eller fjernes fra netværket.
Hvis det er muligt, vil det være en stor sikkerhedsmæssig fordel, hvis man opsætter netværket, således at man får besked, når der tilføjes nye ikke-godkendte enheder til netværket. Dette kan gøres automatisk med et nmap-script, men der findes også mange kommercielle værktøjer, der kan hjælpe med at give et overblik over virksomhedens netværk og de enheder, der er på det.
På samme måde kan man opsætte netværket og de tilsluttede enheder til kun at eksekvere programmer, der er på en godkendt liste. Det vil hjælpe med til at modvirke ransomware og hackerværktøjer.
Et netværksdiagram er et meget følsomt dokument og vil ikke indgå som sagsmateriale. Det vil alene være et arbejdsdokument mellem virksomheden og politiet.
Når du kender dit netværk, så gælder det om at holde det løbende monitoreret. Dette kan gøres via forskellige sikkerhedsværktøjer såsom Intrusion Detection System (IDS), Intrusion Prevention System (IPS) eller andet afhængigt af jeres virksomhedsnetværk.
Det er vigtigt at uddanne medarbejderne i at bruge værktøjerne, konfigurere dem og holde dem opdaterede, så de virker, som de skal. Hvis ikke det sker, kan de i værste fald give så mange falske positiver, at de får den modsatte effekt, nemlig at medarbejderne ignorerer alle advarsler.

Hvad man skal monitorere efter, afhænger af virksomhedens type, størrelse og netværk. Det, der bør give en advarsel, kunne eksempelvis være benyttelsen af ”krypterede tunneller" til at sende data ud af netværket. Disse kan have en legitim årsag, men hackere og ransomware benytter ofte krypterede tunneller til at sende data ud af netværket eller kontakte en server for at få instrukser.
Desuden kan man se efter, hvilke lande der kontaktes. Hvis virksomheden ikke har aktiviteter i Kina eller Qatar, kan der blokeres for trafik dertil, eller omvendt kun tillade trafik til de områder som virksomheden har aktiviteter i. Dette skal selvfølgelig gøres med varsomhed og ikke bare implementeres uden at teste det først. Der kan være programmer, der kræver en aktiv forbindelse til et bestemt land.

2.03 Brugeradministration

Brugerne på jeres netværk bør kun gives de rettigheder, de har behov for. Det ses alt for ofte, at medarbejdere har administratorrettigheder uden at have behov for dem. Hvis en hacker overtager en profil, har det stor betydning, om profilen har administratorrettigheder eller ej. Selv den administrerende direktør behøver ikke at kunne tilgå alt.
Når ansatte forlader en virksomhed, og nye kommer til, bør de gamle brugere slettes og nye brugere oprettes. Gamle inaktive brugere bliver ofte ikke slettet, og de bliver dermed ideelle for hackere at overtage. En løsning på det problem kunne være, at den sikkerhedsansvarlige modtog en besked, når en bruger med administratorrettigheder blev oprettet, eventuelt hvis det sker uden for arbejdstid.
Derudover bør I opsætte to-faktor-godkendelse af adgang til informationer, der vurderes kritiske i jeres virksomhed.

2.04 Netværkssegmentering

Opdel netværket i forskellige segmenter og opsæt regler for, hvem der må tilgå hvad. Traditionelt set har netværk været fokuseret på trusler udefra. Hvis man først kom inden for netværkets forsvar mod ydre trusler, var der frit spil og ingen eller få forhindringer.
Det er et problem, som i høj grad udstilles, når virksomheder rammes af ransomware. Når en bruger på netværket trykker på et link, besøger en inficeret hjemmeside eller åbner en inficeret fil, har ransomwaren tit frit spil til at kryptere hele netværket. Nogle gange inklusive diverse backup-drev. Man kan undgå dette ved at segmentere netværket og kun give adgang til de enkelte segmenter, hvis det er nødvendigt. Husk på, at ransomwaren kun kan kryptere de områder, som den inficerede bruger har adgang til.
Adgang til meget følsomme oplysninger bør have to-faktor-godkendelse. Eksempler på følsomme områder kan være backuppen eller logningsserveren.
Den bedste fremgangsmåde til at gøre netværket sikkert er at gå ud fra, at ens netværk allerede er kompromitteret.

2.05 Network Time Protocol-Server (NTP-server)

En NTP-server er en central server på netværket, som andre enheder på netværket kan synkronisere tiden med, så alle enhederne har den nøjagtigt samme tid. Det er meget vigtigt, at enhederne synkroniseres og har nøjagtigt samme tid, da det ellers er yderst vanskeligt at efterforske. Bare 1/100 sekund har enorm betydning for efterforskningen.
Når en NTP-server er sat op, så implementér procedurer, der sikrer, at nye enheder bliver synkroniseret med serveren, og eksisterende bliver tjekket for, om tiden stadig passer.

2.06 Logning

Manglende logning og overvågning af systemerne er tit en kendsgerning, og det kan føre til, at det ikke er muligt at komme videre i en efterforskning. I bør derfor overveje at logge så meget som muligt og overvåge systemerne bedre. Dette vil give optimale muligheder for at finde de elektroniske spor, hvis skaden skulle ske.
Med hensyn til logningen er det endvidere en stor fordel, hvis den foretages særskilt – helst på en særskilt server. Hackere er ofte meget bevidste om at slette sporene efter sig, og hvis logningen er opsat med standardopsætningen, gør det arbejdet for hackerne meget nemmere. De færdige ”hacker tools”, der er lettilgængelige på internettet, vil i flere tilfælde være konstrueret således, at de også sletter spor i logfiler og event logs. 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 og 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 webserver-log – hvilke kommandoer, der er anvendt, styresystem, browser etc. Desuden bør man opsætte de individuelle computere til at logge kommandoer foretaget i kommando-prompten. Mange af ovennævnte funktioner findes i mange operativsystemer og skal bare aktiveres. Hvad der bør logges er forskelligt fra system til system. Det vigtigste er, at der i logningen er tilstrækkelig information til at bevise handlingen.
Der er en tendens til kun at monitorere og reagere på fejl i systemet, men det kan være lige så vigtigt at monitorere succesfulde handlinger. Mange logger kun de åbenlyse områder såsom firewalls, mens

eksempelvis DHCP-logs glemmes eller kun gemmes i så kort tid, at de er overskrevne, når politiet bliver involveret. Sørg derfor for at få styr på alle loggene og opsætte logningen, så de ikke overskrives for hurtigt. Husk på, at der kan være foretaget forberedende handlinger, længe før hændelsen opstår.
Præcis hvad I vælger at logge, er op til jer, men vær opmærksom på, at logning kan være lovpligtig efter dansk lovgivning eller bestemt i diverse lovtekster såsom EU's Persondataforordning (GDPR).

Politiet har udarbejdet en liste over logs, som erfaringerne har vist enten manglede eller var overskrevne, når politiet har været involveret. Loggene kunne have løst sagen, såfremt de var tilgængelige. Listen er ikke udtømmende, men er blot til inspiration.

- Firewall
- Router
- IDS-systemer
- IPS-systemer
- DMZ
- Proxy
- DHCP
- Gæstenetværk
- Active directory
- Fysisk accesslog (Nøglekort og lignende)
- Logs over lokalt udførte terminal kommandoer
- Overvågning (Både fysisk og netværksovervågning)
- Antivirus
- Event logs

Politiet er opmærksom på, at man ikke kan logge alt for evigt. Dog bør I tage aktivt stilling til, hvilke logs I vil gemme og i hvor lang tid.
Listen indeholder en stor mængde logs i mange forskellige formater, men heldigvis findes der forskellige programtyper såsom Security Information and Event Management (SIEM), der kan opsættes til at samle alle loggene i et fælles format, som I så kan overvåge. I kan endda opsætte regler for, hvornår noget skal defineres som unormalt og bør alarmere den sikkerhedsansvarlige. I bør udarbejde procedurer for, hvem der modtager alarmerne, og hvordan I reagerer. Det skal understreges, at det ikke er nok med et ugentligt tjek. Systemerne bør monitoreres konstant. Hackerne arbejder sjældent inden for normal kontortid, og det bør jeres vagtordning derfor tage højde for.

Hvis et program som SIEM implementeres, bør I udover anskaffelsen, og tiden I bruger på at implementere det, bruge tid på at uddanne medarbejdere i programmet samt opsætte og finjustere reglerne for, hvornår der skal adviseres om sikkerhedsbrud. Hvis I ikke bruger tid på at opsætte regler, kan I risikere, at der kommer så mange falske positiver, at hændelsen drukner i mængden eller slet ikke bliver opdaget.
Der bør implementeres to-faktor-godkendelse eller lignende for at kunne tilgå loggene og kun tillade udvalgte medarbejdere at tilgå den.

2.07 Backup og kryptering

Hav en backup-politik, der både gør jer i stand til at genoprette systemet og undgå at overskrive beviserne. Vær opmærksom på at isolere backup-systemet fra det normale netværk. Hvis man fx rammes af ransomware, hjælper en backup ikke meget, hvis den også er krypteret.
Følsomme data, der befinder sig stationært, bør krypteres. Dette gælder selvfølgelig eventuelle backups, men især også interne arbejdsprocedurer, oversigter over netværk samt eventuelle kodeord. Husk at overvåge tilgang til de krypterede data og rapportér samt log eventuelle uautoriserede forsøg på adgang.

2.08 Konfiguration af digitale enheder og opsætning af sikkerhedspolitikker

Der findes et utal af kommercielle samt indbyggede programmer til at konfigurere digitale enheder og opsætte sikkerhedspolitikker.

På Windows-arbejdsstationer kan man implementere The Enhanced Mitigation Experience Toolkit (EMET). EMET er indbygget i Windows 10, men skal stadig konfigureres specielt til jeres system for at virke optimalt, og hvis I bruger Windows 7 kan programmet hentes gratis hos Microsoft. Der er lignende programmer til Linux og Mac. Dette er ikke det eneste, I bør gøre med hensyn til konfiguration af enheder, men det er en stor hjælp.

Hav eventuelt et "sikkert billede" af en computer, der så køres på alle nye maskiner, og sørg for at holde dette "sikre billede" adskilt fra resten af netværket.
Tænk over, hvilke programmer, der skal kunne eksekveres hos de forskellige medarbejdere. Der er ingen grund til, at en medarbejder, der kun skal læse mails, have adgang til internettet og læse eventuelle vedhæftninger, eksempelvis skal kunne eksekvere PowerShell.

Hvis virksomheden har anskaffet sig SIEM, så opsæt den til at indsamle event logs og andre logs fra de lokale computere.

2.09 Opdater systemerne

Sørg for at alle systemer altid er opdaterede. Selv en netværksprinter kan bruges til at komme ind på følsomme områder, hvis den ikke er opdateret korrekt. Oftest går der ikke lang tid fra en sårbarhed bliver identificeret og publiceret, før der er udviklet hacker-værktøjer til at udnytte den. Man kan derfor gardere sig ved at holde systemerne opdaterede.
Nogle gange kan en opdatering ødelægge noget i jeres opsætning, så test den eventuelt på et test-netværk først. Såfremt den ødelægger noget, bør I lave andre sikkerhedsforanstaltninger, så sårbarheden ikke kan udnyttes.
Opdateringspolitikken bør I udforme således, at den tager højde for et pludseligt opstået behov for opdatering af et system, der ikke følger den normale opdateringscyklus.

2.10 Uddannelse og awareness

Udover løbende at uddanne sine it-sikkerhedsfolk, så er det også vigtigt at uddanne alle medarbejdere i korrekt it-sikkerhedsmæssig adfærd.
Når det kommer til jeres it-sikkerhedsfolk, bør de løbende modtage træning i, hvordan man sikrer data på den bedst mulige måde, så politiet har de bedste arbejdsbetingelser. For ofte ses det, at de beviser, som politiet får, er korrupte eller forurenede på grund af forkert håndtering. En hændelse kan ende med en retssag, og så skal beviserne være uangribelige.
Når det kommer til alle andre ansatte, kan jeres netværk være fuldstændig sikret imod indtrængning udefra og stadig være usikkert over for medarbejdernes uhensigtsmæssige adfærd. En medarbejder kan fx stadig blive udsat for spearphishing og lokkes til at eksekvere en ondsindet fil, der omgår jeres interne netværkssikkerhed. Der er eksempler på, at hackere bruger månedsvis på at opbygge tillid til en ansat (”social engineering”) for til sidst at få vedkommende til at eksekvere en fil på firmaets netværk.
Uddannelsen af medarbejderne bør altså være meget bred og ikke kun omhandle sværttilgængelige it-tekniske emner.

Når en medarbejder narres til at overføre store beløb til ofte udenlandske konti kaldes det BEC (Business Email Compromise) eller CEO fraud. Denne form for svindel kan imødegås ved løbende at uddanne jeres medarbejdere og dermed højne deres it-sikkerhed awareness. Som et led i uddannelsen kunne I fx hyre et firma til løbende at lave kampagner, hvor medarbejderne udsættes for falske forsøg på svindel. Selv velrenommerede it-sikkerhedsfirmaer laver den slags kampagner mod deres egne ansatte. For selv de bedste medarbejdere kan falde i, hvis de modtager en e-mail fra chefens egen e-mail-konto, hvori de bliver bedt om at lave en handling, overføre penge til en konto eller andet. Brug tid på at få udarbejdet nogle regelsæt i virksomheden, der klart beskriver, hvordan medarbejdere skal forholde sig i de forskellige situationer. Retningslinjerne kan fx indeholde forholdsregler for, at en overførsel over et vist beløb skal foretages via både e-mail og med et kontrolopkald. Husk løbende at træne disse regelsæt. It-sikkerhed skal ikke kun skal være noget for it-sikkerhedsfolk. Selv hvis jeres virksomhed udliciterer it-driften, er uddannelse i awareness et vigtigt punkt og skal omfatte alle i hele virksomheden, der har adgang til jeres systemer, fra direktøren til studentermedhjælperen.
Dette betyder ikke, at alle skal kende sikkerhedspolitikken for alt i virksomheden. Det betyder alene, at der i sikkerhedspolitikken bør tages højde for alle personalegrupper.
Der kan med fordel udarbejdes foldere eller lignende, der præciserer, hvordan de enkelte personalegrupper skal forholde sig i bestemte situationer. Denne folder bør være klar og præcis og holdes så kort som muligt.

03 Forholdsregler ved et muligt kompromitteret netværk

3.01 Udpeg en kompetent person til at håndtere hændelsen

3.02 Få et overblik
Find ud af, hvad der er sket, og hvornår. Iværksæt foruddefinerede procedurer.

3.03 Er systemet aktuelt kompromitteret?
Find ud af, om hændelserne stadig er i gang, og iværksæt de korrekte procedurer

3.04 Beslut om politiet skal involveres

3.05 Begynd at indsamle data
Indsaml hurtigst muligt data, så man undgår forurening samt tab af data

3.01 Anden dokumentation til politiet
Giv den rigtige dokumentation til politiet for at speede processen op

3.01 Udpeg en kompetent person til at håndtere hændelsen

Indsæt en kompetent kontaktperson til at håndtere sagen og være bindeleddet mellem firmaet og NC3, såfremt politiet skal involveres og gerne en alternativ kontaktperson, såfremt den udpegede person ikke er tilgængelig. Begge kontaktpersoner bør have den nødvendige træning/erfaring i at håndtere it-sikkerhedskriser.

3.02 Få et overblik

Følg jeres CIRP, som beskrevet i denne guides del 1, pkt. 1.
I bør som minimum få et overblik over følgende:

- Er hændelsen isoleret?
- Netværket. Find netværksdiagrammet, men foretag også en vurdering af, om det stadig er aktuelt.
- Kan systemerne genoprettes, og ødelægges beviser, der skal sikres på forhånd, hvis dette gøres?
- Er det nødvendigt at udelukke eventuelle indtrængere fra systemet, eller kan det vente, indtil man har overblik over deres hensigter og eventuelle identitet?
- Hvilke tiltag har virksomheden foretaget indtil nu for at genoprette systemerne eller smide indtrængere ud?
- Hvilke dele af systemet er påvirket, og hvilke er ikke?
- Hvad betyder hændelsen for jeres system?
- Gerningstidsrum? Husk på, at der kan være foretaget forberedende handlinger lang tid i forvejen.
- Har I mistanke til en bestemt person eller personalegruppe?

Derudover bør kontaktpersonen så hurtigt som muligt begynde på en detaljeret log over, hvad der foretages i sagen inklusive nøjagtig tid for, hvornår det er foregået. Dette er en stor hjælp for politiet, men selv hvis politiet ikke bliver involveret, er det en stor hjælp til jeres virksomhed for at få et efterfølgende overblik.
Såfremt der er tale om en decideret indtrængning i jeres netværk, så forsøg så vidt muligt at undgå at bruge e-mail, da hackerne kan overvåge disse og dermed finde ud af, at de er opdaget.

3.03 Er systemet aktuelt kompromitteret?

Det er vigtigt at sondre mellem et aktuelt kompromitteret system, altså hvor gerningsmanden kan være koblet til systemet her og nu, og et system, der sandsynligvis er kompromitteret, men hvor der ikke er aktuel aktivitet. Ved et aktuelt kompromitteret system er der størst mulighed for at sikre de nødvendige beviser. Hackere gør nemlig 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.

3.04 Beslut om politiet skal involveres

Det skal hurtigst muligt besluttes, om politiet skal involveres.
Som udgangspunkt skal en anmeldelse indgives til det lokale politi. Det lokale politi har så mulighed for at få assistance af NC3. Selv hvis I ikke er sikre på, om politiet skal involveres, står NC3 gerne til rådighed for en uformel samtale og vejledning. Vær venligst opmærksom på, at der alene bør rettes henvendelse direkte til NC3, såfremt der er et aktuelt sikkerhedsbrud eller i tæt tilknytning hertil. Et opkald til NC3 er ikke en anmeldelse til politiet. Dette gøres enten ved at kontakte det lokale politi eller ved online på https://www.politi.dk/da/borgerservice/anmeldelser/hacking. Inden for normal arbejdstid kan NC3 kontaktes på +45 2283 4439 eller i mindre hastende tilfælde på it-kriminalitet@politi.dk. Uden for normal arbejdstid skal

der ske henvendelse til det lokale politi, der så vurderer, om henvendelsen er af en sådan karakter, at NC3 bør kontaktes.
Det understreges, at der kun kan foretages en anmeldelse via det lokale politi. Ovenstående telefonnummer er alene ment som en hjælp i forbindelse med et aktuelt sikkerhedsbrud, hvor tingene kan være meget kaotiske.

3.05 Begynd at indsamle data

Uanset om I vurderer, at politiet skal involveres lige nu eller ej, så bør I altid indsamle logs så tidligt som muligt i processen for at undgå at miste data eller undgå, at de data, der er til rådighed, bliver forurenede. I bør ligeledes begynde at nedskrive præcist hvilke skridt, der tages, så dataintegriteten opretholdes. Hver gang, der bliver foretaget en handling, skal præcis tid for handlingen, hvem der har foretaget handlingen og hvordan handlingen blev udført, skrives ned.
I bør indsamle logs fra alle tilgængelige kilder. Selv om de ikke virker relevante nu, så kan de sagtens blive aktuelle i fremtiden, hvis nærmere undersøgelser viser, at politiet skal inddrages. Vær opmærksom på, at alle logs ikke bliver gemt lige længe, og at de kan blive overskrevet, hvis I venter for lang tid. Se pkt. 2.06 i denne guide for inspiration til log-kilder. Denne proces bør være nedfældet i jeres CIRP.

De implicerede arbejdsstationer/enheder bør sikres så hurtigt som muligt. Afhængig af hændelsens karakter bør I også overveje at sikre RAM. Sikring af arbejdsstationer og RAM kan være en kompliceret proces, så tag enten NC3 med på råd, eller vær sikker på, at personen, der foretager sikringen, har den fornødne træning og kender processen.
Indsamlingen bør foregå på en måde, så der er mulighed for løbende at kontrollere dataintegritet. Sikringen skal som hovedregel ske i følgende rækkefølge:

1. Sikring af volatile data (Primary storage, fx RAM)
Dette skal naturligvis afvejes med vigtigheden af det pågældende system, idet der kan ske nedbrud i enheden som følge af sikringen. Om computeren er krypteret eller ej har også betydning for, om der skal sikres RAM. Tal evt. med NC3 om behovet.

2. Sikring af offline data (Secondary storage, fx harddisk)
Når enhederne, der skal sikres, er identificerede, er det vigtigt at anføre måden, datasikringen bliver foretaget på, hvem der gjorde det samt dato/tid for indsamlingen. Tiden skal være så præcis som muligt. Der kan være situationer, hvor systemet kan lukkes ned, og efterfølgende sikring kan foretages. Der kan være situationer, hvor systemet er nødt til at blive sikret kørende. Og der kan være situationer, hvor det ikke er muligt at sikre data som i de to ovennævnte eksempler, og man må så sikre den data, man kan, på andre måder.
Tag eventuelt kontakt til NC3 for vejledning.

3. Sikring af yderligere oplysninger
Et fuldstændigt spejl af en maskine giver ikke altid alle oplysninger. Man kan være heldig at finde nogle ting i RAM, men det er ikke helt sikkert, at man kan finde alt. Man bør derfor altid eksekvere nogle kommandoer i terminalen eller i kommandoprompten for at få alt med. Tag kontakt til NC3, der har scripts til formålet, og som kan gennemses inden eksekvering. Eftersom der også her er en risiko for nedbrud, kan der på forhånd tages kontakt til NC3 for at få disse scripts udleveret og efterprøvet, inden de anvendes i en skarp situation.

Der bør laves en fælles standard for navngivningen af de sikrede effekter. "Lars Larsens bærbare arbejds-PC" giver forvirring, når der er flere involverede parter. Kald dem eventuelt ”Enhed 1”, ”Enhed 2” og så videre og lav et sideløbende dokument, hvori de enkelte enheder og deres sikring bliver beskrevet i detaljer. Såfremt NC3 allerede er involveret, bør navngivningen aftales med dem.

Hvis enheden er krypteret, skal der IKKE dekrypteres inden sikring. Tag eventuelt kontakt til NC3 for retningslinjer i disse tilfælde, idet en dekryptering potentielt kan ødelægge beviser.

For hver enhed, der sikres, bør der tages en hashværdi af al sikret data inklusive logs umiddelbart efter sikring. På denne måde undgår man at begynde at arbejde på korrupte/ændrede beviser.

Dette kan lyde for omstændeligt, men NC3 har set eksempler på, at man er begyndt at arbejde på sikret data, der var så skadet, at man ikke kunne bruge det.

3.06 Anden dokumentation til politiet

Anden dokumentation, der kan hjælpe politiet med opklaringen af hændelsen, kunne eksempelvis være:

- De procedurer, der blev fulgt ved sikkerhedsbruddet (fx Incident Responce Plan).
- Et netværksdiagram.
- En oversigt over, hvilke systemer der er påvirket inklusive operativsystemer og installerede 3.-partsprogrammer.
- Information om patch-niveauet.
- Retningslinjer for brug af systemet.
- Liste over brugere/administratorer i systemet.
- Liste over systemejere.
- Liste over ip-ranges i systemet.
- Liste over nyligt afskedigede medarbejdere (hvis relevant).

04 Afsluttende bemærkninger

It-sikkerhed er en nødvendighed, og noget der bør stå meget højt på jeres virksomheds dagsorden. Det forventes ikke, at I fra dag ét implementerer alle punkterne, og mange punkter vil sikkert indeholde områder, der ikke er relevante for jeres virksomhed, men det forventes, at der som minimum tages stilling til hvert punkt.
Det er meget nemmere og billigere i længden, hvis I på forhånd har tænkt grundigt over it-sikkerheden. Når først netværket er kompromitteret, og driften bliver forstyrret, vil det være for sent, og der kan være sket uoprettelig skade på jeres virksomhed.