CENTER FOR CYBERSIKKERHED

UNDERSØGELSESRAPPORT

INGEN LOG – INTET INDBRUD

Betydningen af logs for at kunne undersøge og beskytte sig imod cybertrusler

1. udgave juni 2021.

Indhold

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave juni 2021.

Formål
Denne undersøgelsesrapport beskriver, hvordan logning i it-systemer har stor betydning for, at cyberangreb kan undersøges tilstrækkeligt. I mange tilfælde må CFCS opgive at undersøge sager til bunds på grund af manglende logs hos ofrene. Målgruppen for denne rapport er primært it-ledelse og it-teknikere.

Resumé

- Manglende logning i it-systemer er et stort problem, da det betyder, at cyberangreb ikke kan undersøges og imødegås tilstrækkeligt.
- Center for Cybersikkerhed (CFCS) arbejdede i 2020 med en sag, hvor en statsstøttet hackergruppe angreb en dansk myndighed. Sagen viser, at god logning er afgørende for at kunne undersøge og rydde op efter cyberangreb.
- I mindst 75 % af alle centrets operative sager begrænser manglende eller ufuldstændige logs undersøgelsen af cyberangreb.
- CFCS vurderer også, at manglende eller ufuldstændige logs begrænser mange private sikkerhedsfirmaers arbejde med cyberangreb fra kriminelle hackere.
- Logning er en forudsætning for at undersøge cyberangreb ordentligt, men der er flere andre gode grunde til, at logning bør prioriteres i enhver organisation.
- CFCS giver i vejledningen "Logning - en del af et godt cyberforsvar" anbefalinger til, hvordan man opsætter god logning.

Indledning

Når Center for Cybersikkerhed (CFCS) begynder at undersøge, om en dansk myndighed eller virksomhed er blevet kompromitteret af hackere, bliver organisationen som noget af det første spurgt om logs fra de ramte systemer. I mange tilfælde findes der enten ingen logs, eller også er de af meget dårlig kvalitet. I andre tilfælde dækker logs kun en meget kort tidsperiode.

Det begrænser mulighederne for at undersøge, om en organisation er kompromitteret, og hvad en hacker i givet fald har lavet i organisationens netværk. Det kan også skabe usikkerhed om, hvorvidt hackerne stadig er i systemerne.

I flere tilfælde har CFCS helt måttet opgive at undersøge potentielle it-sikkerhedshændelser, fordi der ikke har været logs eller data. I flere af sagerne har der været tale om potentielt alvorlig cyberspionage med betydning for dansk sikkerhedspolitik.

God logning er dog ikke kun vigtig, for de dele af samfundet, hvor truslen fra cyberspionage er **MEGET HØJ**. Truslen fra cyberkriminalitet er nemlig **MEGET HØJ** for alle dele af det danske samfund. Det betyder, at det er meget sandsynligt, at danske myndigheder eller virksomheder vil blive udsat for forsøg på cyberangreb fra kriminelle. Hvis disse angreb skal kunne undersøges og imødegås, er gode og retvisende logs essentielle. Det gælder for alle organisationer, lige fra offentlige myndigheder, over store koncerner, til små og mellemstore virksomheder.

Log
En log registrerer hændelser i en organisations netværk eller system. Logs består typisk af loglinjer, der hver især beskriver den specifikke hændelse som loglinjen refererer til.

Tidligere blev logs primært brugt til problemløsning, men i dag har logs flere anvendelsesmuligheder. For eksempel kan logs bruges til netværks- og systemoptimering, dokumentation af hændelser, og ikke mindst til undersøgelser af cyberangreb.

Denne rapport belyser problemet med manglende logs med udgangspunkt i en sag, som CFCS arbejdede med i 2020. I den konkrete sag undersøgte CFCS en mistanke om, at en statsstøttet hackergruppe havde forsøgt at kompromittere en dansk myndighed. Sagen viser, hvordan kvaliteten af logs var afgørende for, at CFCS kunne undersøge om organisationen blev angrebet, samt hvordan hackerne angreb. Logs gjorde det også muligt at vurdere, om angrebet var lykkedes.

CFCS har udgivet vejledningen: Logning – En del af et godt cyberforsvar. Ved at følge anbefalingerne i vejledningen kan man høste de forskellige fordele, som god logning giver, herunder særligt muligheden for at undersøge cyberangreb. Der findes mange kommercielle systemer, der kan hjælpe med at sikre god logning på store komplekse netværk. Mange mindre organisationer kan dog komme rigtig langt med flere gratis løsninger eller værktøjer, der allerede er integreret som standard i eksempelvis Windows.

Logning i sig selv forhindrer ikke nødvendigvis et cyberangreb, men den er uundværlig, når angreb skal opdages og undersøges. CFCS har bl.a. til opgave at undersøge mulige cyberangreb hos danske myndigheder eller virksomheder, som varetager en samfundsvigtig funktion. Men uden logs fra de ramte systemer er det meget svært at hjælpe med konkret vejledning.

Logs viste, at hackere rekognoscerede mod myndighed

I de følgende afsnit beskrives en konkret sag, hvor CFCS hjalp en dansk myndighed med at undersøge et cyberangreb. Det er meget sandsynligt, at angrebet kom fra en statsstøttet hackergruppe, og det er meget sandsynligt, at formålet med kompromitteringen var cyberspionage. CFCS modtog logfiler af flere omgange. Logfilernes omfang og kvalitet var afgørende for, at det fulde angreb kunne afdækkes.

Når CFCS undersøger et cyberangreb, følges der typisk en fast fremgangsmåde, som bl.a. omfatter en vurdering af hændelsens omfang, svagheder i netværket, mulige remedierende tiltag, attribuering og anvendelse af TTP (Tools, Tactics, and Procedures) til yderligere detektion hos andre kunder eller til generelle varsler.

For at afklare disse punkter har CFCS en række forskellige værktøjer og analysemetoder til rådighed. En af de vigtigste er loganalyse, da det forholdsvis hurtigt giver et indblik i, hvad der er sket på offerets systemer. Derfor er god og fyldestgørende logning på offerets systemer afgørende for, at metoden kan bruges.

CFCS kontaktede i april 2020 en statslig myndighed, fordi der var mistanke om, at en statsstøttet hackergruppe angreb myndigheden. CFCS havde modtaget oplysninger om, at hackergruppen gennem specifikke IP-adresser muligvis havde kommunikeret med den danske myndigheds netværk. Da myndigheden er tilkoblet CFCS' sensornetværk, kunne CFCS bekræfte, at der havde været kommunikation mellem de mistænkelige IP-adresser og myndigheden. For at kunne undersøge aktiviteten yderligere, bad CFCS om myndighedens interne logfiler, hvor de pågældende mistænkelige IP-adresser kunne figurere.

CFCS' sensornetværk
CFCS monitorerer løbende netværkstrafikken til og fra myndigheder og virksomheder, der er tilsluttet sensornetværket. Indsatsen er målrettet særligt avancerede statsstøttede aktører og andre aktører med betydelige ressourcer.

CFCS modtog logs fra myndighedens centrale logløsning. I disse kunne CFCS se, at en aktør af flere omgange sendte forespørgsler til flere af myndighedens IP-adresser fra de mistænkelige IP-adresser. Den type forespørgsler er typisk noget, hackere sender mod et potentielt offer for at undersøge forskellige dele af et netværk. Den viden kan hackere bruge forud for en eventuel kompromittering.

I det konkrete tilfælde var der tale om en såkaldt portskanning. Den trafik bliver ofte ikke flaget som værende skadelig af sikkerhedssystemer. Der findes enorme mængder af sådan trafik, som typisk ikke er skadelig i sig selv. Det er derfor oftest kun, hvis man ved, at bestemte IP-adresser bliver brugt af hackere, at man fanger det i sine systemer.

Rekognoscering
Rekognoscering dækker over en bevidst, ofte automatiseret, handling fra en ondsindet aktør, som har til formål at identificere, indhente viden om og profilere it-systemer via internettet for at udnytte denne viden til senere angreb. Det kan f.eks. ske ved sårbarheds- eller portscanninger.

CFCS' analytikere vidste, hvilke IP-adresser de skulle lede efter, og i logfilerne kunne de se, at de mistænkelige IP-adresser havde lavet forespørgsler til forskellige dele af netværket på flere portnumre. I nedenstående eksempler kan man bl.a. se TCP-forbindelser blive startet og lukket ned igen.

Eksempel på første del af logfilen

Apr dd 2020 tt:mm:ss: %ASA-6-302013: Built inbound TCP connection 740586367 for PUBLIC-DMZ: XXX.XXX.XXX.XXX/59819 (XXX.XXX.XXX.XXX/59819) to MYNDIGHEDMAIL-DMZ: owa.myndighedmail.dk/443 (owa.myndighedmail.dk/443)

Log	Forklaring
Apr dd 2020 tt:mm:ss:	Tidsstempel
%ASA-6-302013:	Cisco firewall med Adaptive Security Appliance (ASA)
Built inbound TCP connection 740586367	Indgående første del af et TCP 3-way handshake med event ID
for PUBLIC-DMZ:	Trafik til netværkets DMZ
XXX.XXX.XXX.XXX/59819	Angribers IP-adresse og portnummer
owa.myndighedmail.dk/443	Myndighedens OWA mailserver på port 443

Eksempel på anden del af logfilen

2020-04-dd tt:mm:ss: Local0.Info YYY.YYY.YYY.YYY 04/dd/2020:tt:mm:ss GMT: SERVERNAVN 0-PPE-1 "IPSource=XXX.XXX.XXX.XXX Host=owa2016.myndighed.dk URL=/owa/"

Log	Forklaring
2020-04-dd tt:mm:ss:	Tidsstempel
Local0.Info YYY.YYY.YYY.YYY	Lokal IP-adresse
SERVERNAVN 0-PPE-1	Lokal server-adresse
"IPSource=XXX.XXX.XXX.XXX	Angribers IP-adresse
Host=owa2016.myndighed.dk	Url-adresse på OWA-serveren

Figur 1: Anonymiseret eksempel på, hvordan de første logs, som CFCS modtog, så ud.

Ovenstående tekstboks illustrerer, hvordan man i logfiler kan se, at hackere foretager en portskanning. Hele logfilen er skrevet i syslog-formatet, men de forskellige applikationer, der har genereret loggen, har benyttet forskellige formater. Det kan bl.a. ses på tidsstemplerne.

Den første loglinje viser, at myndighedens Cisco firewall, som har Adaptive Security Appliance (ASA), ser en udefrakommende TCP-pakke med SYN flaget sat. Herefter "bygger" den første del af en forbindelse, for at kunne dele forbindelser op i sessioner. Loglinjen viser altså, at der er foretaget første del af et TCP 3-way handshake. Nummeret, der står efter "connection", er et event-ID

for første del af et 3-way handshake. Event-ID gør det muligt at sortere eller fremsøge visse hændelser i sine logs.

I den anden loglinje ser vi, at forbindelsen lukkes igen, grundet SYN timeout. Forbindelsen lukkes, da der ikke er set et fuldt 3-way handshake indenfor de 30 sekunder, som firewallen er sat til at tillade. Der er derfor ikke oprettet en fuld session.

De TCP requests, der kunne ses i logfilerne, er et typisk eksempel på rekognoscering eller en såkaldt aktiv skanning ved at bruge en TCP-protokol. Hackeren sender en forespørgsel afsted mod offeret for at se, hvordan systemerne svarer tilbage. Afhængig af typen af skanning får angriberen på baggrund af svaret detaljer om offerets netværk, såsom hardware, styresystemer og åbne porte. Hackeren vil på det stadie typisk gemme informationen og bruge den i sin kortlægning af netværket.

I den tredje loglinje, som kommer fra en anden applikation end de to første, er der anvendt et andet logformat end i de to foregående linjer. Loglinjen beskriver, at der er oprettet en forbindelse fra en IP-adresse til en specifik server, som her er en Microsoft Office Web Application (OWA). Det er positivt, at man kan se hvad, der er tilgået, nemlig myndighedens OWA-server. Det mindre positive er, at man ikke kan se præcis, hvad der sket. Man kan blot se, at nogen har tilgået webserveren.

Der var altså forskellige formater i de forskellige logfiler. Derudover var der heller ikke et gennemgående sessions-ID, som gjorde det muligt, at finde den samme hændelse frem på tværs af forskellige applikationer. Det gjorde det vanskeligere at sammenligne logs fra forskellige systemer, hvilket var nødvendigt for at afdække omfanget af rekognosceringen. På trods af de forskellige formater gjorde logfilerne det dog muligt, at CFCS kunne nå en konklusion. Det var meget sandsynligt, at den mistænkelige trafik, der havde startet undersøgelsen, var rekognoscering. Det indikerede, at hackerne havde intentioner om at angribe myndigheden. Men der var ikke tegn på, at hackerne havde angrebet endnu.

Brute force-angreb
Et (simpelt) brute force-angreb er et angreb, hvor hackeren forsøger at gætte alle mulige kombinationer af bogstaver, tal og tegn i et password. Et computerprogram kan gøre det meget hurtigt. Desto længere et password er, desto længere tid vil det tage at gætte den rigtige kombination. Foruden simple brute force-angreb findes der også nedenstående, som kan kombineres.

Ordbogsangreb
Forsøger alle ord i forskellige ordbøger, herunder kombinationer

Password spraying
Hackeren forsøger sig med generelt almindelige passwords.

Credential stuffing
Hvis hackeren har fundet en kombination af offerets brugernavn og password, som virker til andre sider.

Glemte logs viste, at myndigheden blev angrebet

Efter den første del af analysen var afsluttet, fandt myndigheden og CFCS frem til andre logs, som ikke var blevet gemt på den centrale logløsning. De nye logs var fra en mailserver, som sandsynligvis var det mål, hackerne hele tiden havde været interesseret i.

Disse logs var omfattende og detaljerede ift. hændelser i det specifikke system. Der var igen tale om en Microsoft OWA server, som er en webbaseret adgang til mails gennem en browser.

I de nye logs kunne CFCS se, at nogen forsøgte at logge ind på et meget stort antal mailkonti. Loginforsøgene kom fra de samme IP-adresser, som CFCS tidligere havde ledt efter, og som CFCS forbandt med en statsstøttet hackergruppe. Det er sandsynligt, at aktøren forud for angrebet havde samlet en liste over brugernavne knyttet til myndigheden. Aktøren brugte nu listen med brugernavne til at forsøge at logge ind via OWA-serveren. De forsøgte at logge ind ved at bruge et computerprogram til at gætte passwords til hver enkelt bruger. Den metode kaldes brute force. Nedenstående figur viser, hvordan brute force-angrebet ser ud i logfilerne. Eksemplet er forsimplet, og viser et enkelt loginforsøg på en enkelt konto.

Eksempel på nye logs

Apr dd tt:mm:ss: SERVERNAVN.myndighed.dk,
"Hostname":servernavn.myndighed.dk" "EventType":"AUDIT FAILURE",
"SeverityValue":4, "Severity":"Error", "AccountType":"User","Message":"The
Federation Service failed to validate a new credential. See XML for failure details.
<AuditResult>Failure</AuditResult> <FailureType>CredentialValidationError</
FailureType <UserId>user@myndighed.dk>/UserId>/
<Server>http//xx.myndighed.dk/adfs/services/trust</Server> <IpAdress>
XXX.XXX.XXX.XXX,YYY.YYY.YYY.YYY>/<IpAdress>
<ForwardedIpAddress>XXX.XXX.XXX.XXX,YYY.YYY.YYY.YYY<ForwardedIpAddress>

Log	Forklaring
Apr dd 2020 tt:mm:ss:	Tidsstempel
SERVERNAVN.myndighed.dk	Myndighedens server
"EventType":"AUDIT FAILURE"	Eventtype som her er fejl i login
"SeverityValue":4, "Severity":"Error"	Værdi og beskrivelse af fejltypen
"AccountType":"User"	Type af bruger
Message":"The Federation Service failed to validate a new credential. See XML for failure details. <AuditResult>Failure</AuditResult> <FailureType>CredentialValidationError </FailureType	Beskrivelse af fejl. Login kunne ikke verificeres
<UserId>user@myndighed.dk>/ UserId>	Bruger
<Server>http//xx.myndighed.dk/adfs/ services/trust</Server> <IpAdress>	Service på serveren
XXX.XXX.XXX.XXX	Angribers IP-adresse
YYY.YYY.YYY.YYY	Lokal IP-adresse
<ForwardedIpAddress>XXX.XXX.XXX.XXX,YYY.YYY.YYY.YYY<ForwardedIpAddress>	IP-adresser sendt videre fra load-balanceren forrest i netværket.

Figur 2: Forsimplet og anonymiseret eksempel på, hvordan brute force-angrebet så ud i den nye logfil

I ovenstående boks fremgår det, at der er en "audit failure" ved et forsøg på login fra den ondsindede IP-adresse, XXX.XXX.XXX.XXX, mod en af myndighedens IP-adresser, YYY.YYY.YYY.YYY. Der står også, at der er en "credential validation error". Det vil sige, at nogen har forsøgt at logge ind på kontoen user[@]myndighed.dk, men det er ikke lykkedes. I logfilerne kunne man ikke se, hvorfor login ikke lykkedes. Login fejlede enten, fordi der var tastet en forkert adgangskode, eller fordi det ikke lykkedes hackerne at omgå to-faktor-godkendelsen. Der er tale om en stærkt reduceret log i ovenstående eksempel. I virkeligheden fyldte log for denne specifikke hændelse knapt to siders tætskrevet tekst.

På baggrund af logfilerne kunne CFCS' analytikere konkludere, at det meget sandsynligt ikke var lykkedes aktøren at logge ind på nogen af myndighedens konti. Myndigheden havde flere forskellige sikkerhedsforanstaltninger på plads som f.eks. begrænsninger på, hvor mange mislykkede login-forsøg man kunne lave, samt to-faktor-godkendelse.

Ud fra de nye logs kunne CFCS derfor nå til en ny konklusion. Den statsstøttede aktør havde ikke kun rekognosceret mod myndighedens systemer, men havde også angrebet myndigheden. Det var også meget sandsynligt, at angrebet var blevet stoppet af myndighedens sikkerhedssystemer.

Angrebet afdækket – lige akkurat

CFCS kunne kun nå til ovenstående konklusion, fordi der var adgang til de nødvendige logfiler. Havde der ikke været adgang til alle de relevante logfiler, ville konklusionen have været ufuldstændig.

I dette tilfælde lykkedes angrebet ikke, men det gør det desværre i andre sager. Det havde selvfølgelig været mere kritisk, hvis angrebet var lykkedes. Så ville aktøren have haft adgang til myndighedens netværk, og ville have kunnet bevæge sig videre på netværket fra den kompromitterede konto - og det kan være særdeles vanskeligt at opdage, særligt uden tilstedeværelse af logfiler.

Myndigheden havde sikkerhedstiltag på plads, der var afgørende for, at angrebet ikke lykkedes. Dog kunne man have tilføjet et ekstra lag af sikkerhed, der ville gøre det nemmere, at opdage denne type angreb. Det kunne myndigheden have gjort ved at opsætte alarmer, der kunne give administratorerne besked om eksterne IP-adresser, der forsøgte at logge ind på flere konti uden held.

Analysen af de nye logfiler viste desuden, at flere IP-adresser end dem, CFCS i første omgang havde mistænkt, havde forsøgt at logge ind på mange konti. Analysen af de komplette logs gav derfor myndigheden et indblik i flere angrebsforsøg mod dem. Dermed gav analysen anledning til en overvejelse om, hvorvidt myndigheden burde revidere sin politik omkring, hvor mange fejlede loginforsøg en bruger må have, før denne blokeres.

Analysen af logfiler giver altså muligheder for at undersøge trafikken i et netværk, og dermed løbende tilpasse sit sikkerhedsniveau. Det kræver dog kvalitet i selve logfilerne, og at der er overblik over, hvor de er samlet. Derudover er det vigtigt, at der er ressourcer til, at medarbejdere har tid til løbende at analysere logfilerne. På den måde kan man bruge logs til løbende at tilpasse organisations sikkerhed til trusselsbilledet.

Manglende logning er et generelt problem

I den beskrevne case var det muligt at nå en konklusion, selvom det var tæt på, at de relevante logfiler ikke blev fundet. I mange sager er det dog desværre ikke muligt at finde frem til de rigtige logfiler.

I mindst 75 % af alle operative sager, som CFCS arbejder med, er der ufuldstændige logs. Det begrænser i meget høj grad muligheden for at analysere it-sikkerhedshændelser. Samtidig kan det gøre analyserne af cyberangreb langt mere tidskrævende, end de behøver at være. Dyrebar tid går tabt – tid, som hackerne uforstyrret kan bruge i offerets systemer.

I yderste konsekvens kan fraværet af logs betyde, at CFCS eller et sikkerhedsfirma må opgive at undersøge en sag, fordi der er for få data til rådighed. Hvis hackerne er inde i systemerne, og man ikke kan foretage en tilstrækkelig analyse, kan det få alvorlige konsekvenser. Hvis følsom viden bliver stjålet, eller systemer bliver krypteret, kan det blive dyrt for den berørte organisation. I nogle tilfælde kan det også skade Danmarks konkurrenceevne, sikkerhed og velfærd.

CFCS har foruden de sager, som centret selv er involveret i, også kendskab til andre sager, hvor manglende logning har skabt problemer. Det har bl.a. været sager, hvor danske virksomheder har været ramt af ransomware-angreb. It-sikkerhedsfirmaerne, der var hyret til at få virksomhederne tilbage på benene igen, har beskrevet, hvordan manglende logning hos de ramte virksomheder betød at:

- undersøgelserne af angrebene var unødigt tidskrævende.
- undersøgelserne kunne ikke nå til entydige konklusioner omkring, hvordan hackerne i første omgang kom ind.
- oprydningen var meget omfattende, og muligvis større end den havde behøvet at være, fordi undersøgelserne ikke med tilstrækkelig sikkerhed kunne afgrænse angrebets omfang.

God og struktureret logning er typisk ikke noget, der bliver prioriteret særlig højt i de fleste organisationer. Medmindre man er forpligtet af f.eks. lovkrav om logning, kan det virke fristende at nedprioritere en aktivitet, der primært er nødvendig, hvis man bliver ramt af et større cyberangreb. CFCS ser i den forbindelse ofte:

- Manglende politikker og processer omkring logning.
- Utilstrækkelig lagerkapacitet til de logs, der opsamles.
- Systemerne og løsningerne til god og struktureret logning er til stede, men er ikke konfigureret korrekt.
- Der er ikke afsat ressourcer til at opsætte, vedligeholde og analysere de logs, der er hensigtsmæssige at opsamle.
- Der er ikke sat alarmer op, der kan advare om mistænkelige hændelser i de logs, der genereres i systemerne.

Nedenfor er fem grunde til, at logning bør prioriteres i enhver organisation.

Fem grunde til at prioritere logning

Tilstrækkelig logning er helt essentielt for at kunne reagere hurtigt, når man er blevet ramt af et cyberangreb. Uanset om det er egne it-medarbejdere eller et eksternt sikkerhedsfirma, der skal finde ud af, hvad der er sket, så er logs typisk det første sted man kigger. Derfor vil ressourcer brugt på at sikre en god logning i mange tilfælde vise sig at være en god investering.

1 Basis for at undersøge et cyberangreb

Myndigheder og virksomheder bliver ofte udsat for mere eller mindre avancerede cyberangreb. Mange af disse angreb kan være forholdsvis simple at beskytte sig imod, men det gælder desværre ikke dem alle. Derfor bør alle organisationer forvente, at de på et tidspunkt vil have brug for at undersøge og udbedre et cyberangreb. Hvis der ikke er retvisende og tilstrækkelige logs, vil disse undersøgelser være meget vanskelige og i nogle tilfælde umulige.

Det kan i nogle tilfælde være muligt for et sikkerhedsfirma eller en organisations egne it-folk at undersøge netværksudstyr og computere individuelt og dermed komme frem til nogle overordnede konklusioner om angrebet. Det kan dog forlænge undersøgelsen, og forringer ofte kvaliteten betydeligt.

2 Mulighed for at kende omfanget af cyberangreb

Det kan blive en meget dyr affære, hvis man ikke kan afdække omfanget af en kompromittering. CFCS kender til flere eksempler på, at organisationer har været nødt til at genetablere en meget stor del af eller hele deres netværk, fordi man ikke med sikkerhed kunne afklare, hvor stor en del af netværket, der var kompromitteret. Det er både sket i sager, som CFCS har været direkte involveret i, og i sager, som har været håndteret af private it-sikkerhedsfirmaer.

Hvis man har god logning, har man langt bedre forudsætninger for at kunne fastslå angrebets omfang og dermed inddæmme det. I stedet for at skulle bygge en organisations netværk op fra bunden, behøver man kun at geninstallere eller udskifte det ramte software og hardware.

3 Mindre nedetid i forbindelse med cyberangreb

Hvis der ikke er logs på et system, er det oftest langt mere tidskrævende at undersøge kompromitteringer. Hvis man i stedet for at analysere logs f.eks. er nødt til at analysere images af servere og klienter, medfører det ofte lang nedetid for den enkelte server eller klient, mens man undersøger, om den har været kompromitteret eller ej.

Nedetid er ofte et stort problem og kan koste dyrt. Langt de fleste organisationer i dag er meget afhængige af, at it-systemer fungerer tæt på 100 % af tiden. Manglende salg eller produktion i perioden kan betyde røde tal på bundlinjen for den enkelte organisation. For samfundsvigtige myndigheder og virksomheder kan det også påvirke de ydelser, borgere og kunder er afhængige af. Derudover forøger det regningen fra sikkerhedsfirmaet, der støtter med undersøgelse af angrebet.

4 Lagerplads er billigt

Opbevaring af flere og mere omfattende logs vil typisk betyde, at man har brug for mere lagerplads. Prisen på lagerplads er de seneste år faldet meget, og harddiske med flere terabytes eller store mængder lagerplads i skyen er efterhånden forholdsvis billigt. Mere plads er derfor ofte en mindre investering relativt til mange andre sikkerhedsløsninger. En investering, der kan vise sig at give godt igen.

5 Viden om normalbilledet i netværket

God og kontinuerlig logning og efterfølgende analyse heraf, kan bidrage til at opbygge et normalbillede af sin netværkstrafik. Først når man kender normalbilledet, kan man reagere, når noget uventet ses i logfilerne. Man kan gøre det løbende tæt på realtid eller i faste intervaller i batches, alt efter hvordan systemerne genererer og transmitterer logs til den centrale logløsning.

Ved at analysere sine logs løbende og opsætte alarmer ved afvigelser fra normalbilledet i sit netværk, opnår man lidt af den samme effekt som de såkaldte intrusion detection systemer (IDS). IDS er den samlede betegnelse for to forskellige løsninger, der overvåger aktivitet på enten netværks- (NIDS) eller host-niveau (HIDS). IDS'er giver alarmer, hvis systemet opdager en mulig ondsindet aktivitet på baggrund af forskellige regler. Hvis man som organisation ikke har ressourcer til at investere i et IDS, kan logning kombineret med opsætning af alarmer ved visse hændelser hjælpe et godt stykke ad vejen.

Sådan forbedrer du dine logs

En af CFCS' opgaver er at undersøge mulige cyberangreb mod danske myndigheder og virksomheder, der varetager en samfundsvigtig funktion. Men uden logs er det stort set umuligt at afdække, hvad der er sket, og dermed give situationsbestemt rådgivning.

CFCS har udgivet vejledningen: Logning – en del af et godt cyberforsvar, som kan findes på CFCS' hjemmeside. Her er konkrete anbefalinger til, i hvilke systemer logning bør prioriteres. Vejledningen indeholder også anbefalinger til, hvilke data der bør opsamles i de enkelte systemers logs. Vi anbefaler, at man læser vejledningen i sin helhed, og bruger den som udgangspunkt for at etablere god logning i sin organisation.

Der findes mange kommercielle løsninger, der kan hjælpe organisationer med at opsætte og strukturere sin logning. Det kan for mange give god mening at benytte nogle af disse løsninger. Men uanset hvilken løsning man vælger, har organisationen taget et skridt i retning af bedre cybersikkerhed, hvis man følger rådene i CFCS' vejledning.

FE bruger denne skala for sandsynligheder i analyser