



CENTER FOR
CYBERSIKKERHED

Vejledning

Logning – en del af et godt cyberforsvar

Slå loggen til og bevar muligheden for at se tilbage

Indhold

Indledning	3
Læsevejledning	3
Gode steder at logge.....	4
Rekursive Domain Name System (DNS) servere	4
Interne Dynamic Host Configuration Protocol (DHCP) servere	4
Datatrafik ind og ud af organisationen (firewalls)	4
Autentificeringsservere	4
Interne routere	5
Internetvendte webservere og webservices baseret på HTTPS	5
Øvrige internetvendte tjenester	6
Web proxy-servere	6
Antimalware-systemer.....	6
E-maisystemer, ind- og udgående gateways og spam/virus-filtreringstjenester	6
Andet end netværkskomponenter	7
Log management.....	7
Generering af logs	7
Opsamling af logs	8
Test af logs	9
Lagring af logs.....	9
Anvendelse af logs	9
Sletning af logs	10
Anbefalinger.....	10



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

Forsideillustration: Pasioka/Science Photo Library/Ritzau Scanpix

3. udgave januar 2023.

Indledning

Slå loggen til og bevar muligheden for at se tilbage. Center for Cybersikkerhed og it-sikkerhedsfirmaer oplever ofte at stå uden de logs, der er nødvendige for at kunne afdække, hvad der er sket. For at kunne gennemføre en god og forsvarlig analyse af en hændelse er der mange steder, man skal sikre sig, at loggen er slået til og gemt. Erfaring fra håndtering af konkrete it-sikkerhedshændelser i en række organisationer har vist, at det ikke altid er tilfældet.

Logning er en del af et godt cyberforsvar, fordi det er gennem logs, man kan undersøge de it-sikkerhedshændelser, der er sket, eller de mistanker om it-sikkerhedshændelser, man har. Denne vejledning skal læses som en hjælp til at sikre, at der er anvendelige logs bevaret, hvis der skal foretages hændelseshåndtering. Anvendelsen af logs er en væsentlig del af det tilbagevendende arbejde med at planlægge, implementere, monitorere og forbedre cybersikkerheden.

Læsevejledning

Denne vejledning er todelt. Den første del er en konkret liste over de steder i netværket, man med fordel kan generere logs fra. Den anden del beskriver kort de organisatoriske overvejelser, man skal gøre sig, for at sikre, at logningen bliver meningsfuld i forhold til cybersikkerheden.

Den konkrete liste sætter fokus på de steder, en tekniker typisk vil efterspørge logs fra i forbindelse med en hændelseshåndtering. Det er således i en situation, hvor en it-sikkerhedshændelse er erkendt, eller der er mistanke om en it-sikkerhedshændelse, at disse logs kommer i spil.

Vejledningen er henvendt til de personer, der har ansvaret for, at der foretages logning, typisk CISO'er og it-direktører. Den henvender sig også til dem, der skal sikre, at logningen er slået til, og sikre, at loggen indeholder de rette oplysninger.

Der kan logges på mange enheder i et netværk og på andre enheder end de, der specifikt er nævnt her. Nogle logs kan have interesse ud fra et driftsmæssigt perspektiv, såsom eksempelvis at finde fejl eller optimere hastighed. Denne vejledning beskæftiger sig med logs set ud fra et håndteringsperspektiv i forhold til it-sikkerhedshændelser, og de nævnte logs er dem, der har den største interesse i forhold til at analysere en hændelse.

Loganalyse og beskyttelse af logdata er ikke dækket af denne vejledning.

Gode steder at logge

Organisationen bør logge på alle rekursive Domain Name System (DNS) servere

Logs fra rekursive DNS-servere er vigtige for at afgøre, hvilket internt system (klienter, servere med videre) der har forespurgt på hvilke domænenavne samt tidspunktet for opslaget. En sådan logning af DNS-opslag vil eksempelvis kunne bruges til at identificere et stykke malware, når det kommunikerer med en Command & Control server (C2-server).

Organisationen skal logge:

- Tid (UTC¹)
- Forespørgerens IP-adresse
- DNS-forespørgslen med indhold og svar og retursvar.

Organisationen bør logge på alle interne Dynamic Host Configuration Protocol (DHCP) servere

Logs fra DHCP-servere er nødvendige for at kunne afdække, hvilke interne enheder (eksempelvis klienter) der har anvendt en given IP-adresse på et bestemt tidspunkt.

Organisationen skal logge:

- Tid (UTC)
- Tildelt IP-adresse
- Forespørgerens MAC-adresse.

Organisationen bør logge alle steder, hvor der går datatrafik ind og ud af organisationen (firewalls)

Når man analyserer et cyberangreb, er det interessant at undersøge godkendt trafik for at få det fulde billede af organisationens trafik. Derfor er det vigtigt, at der i relation til organisationens firewall og andre steder, hvor der passerer trafik ud og ind af netværket, foretages logning af både godkendt og blokeret trafik.

Organisationen skal logge:

- Tid (UTC)
- Afsender/modtager-IP-adresse og port
- Beslutning (eksempelvis forbindelsen blev blokeret, godkendt eller lukket)
- Datastørrelser på sessionens trafik både sendt og modtaget.

Organisationen bør logge på alle autentificeringsservere

I forhold til autentificeringsservere² er der navnlig to typer events, der bør logges for senere at have et godt udgangspunkt for en analyse:

1. Events der, selvom de kun forekommer én gang, er mistænkelige. Eksempelvis at en normal brugerkonto tildeles adgang til en sikkerhedsmæssig følsom gruppe, når medlemskabet til gruppen bliver opdateret.
2. En akkumulering af engangsevents, der overstiger et forventet antal. Eksempelvis kan et usædvanligt stort antal mislykkede login-forsøg efterfulgt af et succesfuldt login tyde på et succesfuldt "brute force"-angreb. Omvendt kan et stort antal mislykkede login-forsøg være et tegn på et mislykket "brute force"-angreb.

¹ UTC, Universal Time Coordinated. (Tidsstempel)

² I et Microsoft-miljø kan man med fordel orientere sig her: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

Organisationen skal logge:

- Tid (UTC)
- Eventtype
- Kontonavn
- Forespørgerens IP-adresse
- Forespørgerens hostnavn
- Beslutning - resultat af autentifikationsforsøg.

Organisationen bør logge på alle interne routere

Routere kan konfigureres til at tillade eller blokere forskellige typer af netværkstrafik baseret på en politik. Routere, der kan blokere trafik, skal konfigureres til at logge, hvordan trafikken håndteres.

Organisationen skal logge:

- Tid (UTC)
- Afsender/modtager IP-adresse
- Port
- Beslutning (såsom forbindelsen blev blokeret, godkendt eller lukket).

Organisationen bør logge på alle klient Virtual Private Network (VPN) gateways

Ved fjernadgang for brugere til organisationens systemer (eksempelvis ved hjemmearbejde eller rejse) vil logningen indeholde informationer, der kan være med til at afdække, hvor forbindelsen kommer fra, og hvorvidt en bruger får adgang eller afvises. Det kan afsløre forsøg på kompromittering af fjernadgang og anvendes til sammenstilling med andre logdata.

Organisationen skal logge:

- Tid (UTC)
- Klientens ekstern IP-adresse
- Brugernavn
- Tildelt IP-adresse
- Fejlede og godkendte logins.

Organisationen bør logge på deres internetvendte webservere og webservices baseret på HTTPS (eksempelvis hjemmesider, API'er og MQ)

Nogle angribere bruger webservere til at opnå eller opretholde adgang til et netværk. Det kan eksempelvis være hjemmesider, webmail-adgange og web-API'er. Webserverloggen kan bistå i undersøgelsen af, hvad angriberen har foretaget sig. Hvis webservere står bag ved en proxy/load-balancer er det vigtigt at logge den oprindelige klient IP-adresse.

Organisationen skal logge:

- Tid (UTC)
- Afsenderens eksterne IP-adresse
- Metode (GET, POST og så videre)
- URIs
- Returkode
- Referer
- User-agent
- Antal afsendte og modtagne bytes.

Organisationen bør logge øvrige internetvendte tjenester (f.eks. FTP og SSH)

Andre internetvendte tjenester kan være interessante mål for angribere, og derfor bør aktiviteter herpå også logges. Hvilke aktiviteter, der er relevante at logge for de forskellige tjenester, afhænger af typen af tjeneste. Logningsdata fra internetvendte tjenester kan afsløre kompromittering af brugerkonti, anvendt software, tilgængeligt indhold, konfigurationsindstillinger med videre.

Organisationen skal logge:

- Tid (UTC)
- Afsenderens eksterne IP-adresse
- Relevant aktivitet for den pågældende tjeneste.

Organisationen bør logge alle web proxy-servere

Hvis man anvender en web proxy til udgående internettrafik, kan loggen fra denne hjælpe til at finde potentielt ondsindede domænenavne og forespørgsler fra kompromitterede maskiner.

Organisationen skal logge:

- Tid (UTC)
- Klientens IP-adresse
- Metode (GET, POST og så videre)
- URIs
- Returkode
- Hostnavn og bruger (hvis muligt).

Organisationen bør logge hændelser på alle antimalware-systemer

Logs fra Antimalware-sandbox-systemer, Anti-virus (AV), Endpoint Detection and Response (EDR) og logs fra Intrusion Detection System (IDS) kan bidrage til et samlet overblik over angrebsforsøg og eksempelvis forsøg på afvikling af malware. Gem kopier af de filer, der er sat i karantæne, til senere analyse.

Organisationen skal logge:

- Tid (UTC)
- Handling (eksempelvis karantæne eller blokering)
- Proces/filnavn/aktivitet der forårsager begivenheden.

Organisationen bør logge alle email-systemer, inklusive ind- og udgående gateways og spam/virus-filtreringstjenester

Logs fra email-systemer, inklusive ind- og udgående gateways og spam/virus-filtreringstjenester, kan hjælpe til opdage og efterforske phishingforsøg, levering af malware og nogle eksfiltreringsmetoder.

Organisationen skal logge:

- Tid (UTC)
- Afsender/modtager emailadresser
- Navn og IP-adresse på afsender-/modtagergateways
- Emne
- Størrelse på besked
- Navne på vedhæftede filer.

Organisationen bør logge på andet end netværkskomponenter

Ud over hvad der er nævnt ovenfor, findes der også andre logs, der kan være relevante i forbindelse med undersøgelse af en it-sikkerhedshændelse. Man kan eksempelvis overveje følgende:

- Logs på klienter
- Logs på kritiske filservere
- Logs af "success" og "failure" audits på tværs af platforme
- Logs fra software til at håndtere privilegerede konti og passwordmanagement-suites
- Logs af administrative loginforsøg og handlinger
- Logs fra application whitelisting-løsninger og af blokerede Powershell scripts
- Logs fra industrielle kontrolsystemer.

Der findes forskellige værktøjer til logopsamling og konfigurationsstyring, der bør vælges ud fra det gældende trusselsbillede og organisationens analysebehov i forbindelse med en it-sikkerhedshændelse. Valg af værktøjer og detaljeringsgrad af logs bør foretages i tæt dialog med dem, der skal foretage analysen i tilfælde af en sikkerhedshændelse.

Forud for indsamling af logs ligger en række organisatoriske beslutninger af styringsmæssig karakter, der kort beskrives i det følgende afsnit.

Log management

For at en organisation får det optimale ud af de logs, der genereres, og kan bruge dem i – særligt – en analysesituation, bør man etablere en logningspolitik, der fastsætter formålet med logning og fastsætter de procedurer, der sikrer, at det er det rigtige, der logges, og at der logges på en hensigtsmæssig måde.

Politik og procedurer skal beskrive generering, indhentning, lagring, retentionsperioder, proaktiv og reaktiv analyse af logs samt sletning af logs. Og de skal, som tidligere nævnt, afstemmes med dem, der skal bruge de indhentede logs i tilfælde af en hændelse. Det kan være personer internt i organisationen, offentlige myndigheder eller det kan være et sikkerhedsfirma, man har indgået aftale med om hjælp i tilfælde af, at der opstår en it-sikkerhedshændelse. Politikken skal sikre, at gode og anvendelige logs er tilgængelige, at de er læsbare og rækker tilstrækkeligt langt tilbage i tid.

En måde at udarbejde dækkende politikker og procedurer på er at udarbejde scenarier over den slags it-sikkerhedshændelser, man gerne vil kunne undersøge i tilfælde af en hændelse.³

Generering af logs

Start med en risikovurdering. Enhver organisation skal løbende vurdere hvilke logs, der er relevante, hvis der skal prioriteres ud fra et ressourcemæssigt perspektiv.

³Se eventuelt: DS/ISO/IEC 27033-3. Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues

For at kunne træffe beslutning om logning bør der gennemføres en risikovurdering, der tager organisationens opgaver/forretning, sårbarheder og trusselsbilledet i betragtning. Det er ikke alle logs, der er lige væsentlige i forhold til cybersikkerhed. Ud over overvejelser vedrørende de risici, organisationen påfører sig ved udnyttelsen af digitaliseringsmuligheder, skal der tages stilling til eventuelle regler, love, branchestandarder og lignende, som organisationen kan være underlagt. Noget regulering kan pålægge organisationen særlige krav til logning, herunder hvad der ikke må logges, hvor lang tid logs må opbevares og så videre.

Når organisationen har risikovurderingen på plads, skal man, for at organisationen får det optimale ud af sin logning, have følgende på plads:

- Hav et overblik over hvilke regler om logning, der gælder for organisationen.
- Hav et godt overblik over it-arkitekturen (topologi). Gerne suppleret med et oversigtsdiagram.
- Hav beskrivelser af alle internetforbindelsespunkter og de regelsæt, de følger (eksempelvis firewallregler).
- Hav en oversigt over alle DNS- og DHCP-servere samt VPN-koncentratorer.
- Dokumentér alle implementerede logningsløsninger inklusive eventuelle Group Policy Objects, der definerer logningspolitikker.
- Kontrollér, at log-niveauet er tilstrækkeligt detaljeret og viser de informationer, der er nødvendige for at belyse en hændelse. Jævnfør det man har beskrevet i sin politik.
- Kontrollér, at klienters rigtige IP-adresser logges, og at de ikke er erstattet af IP-adressen på eksempelvis en proxy eller load-balancer.
- Hav et samlet overblik over alle de logs, der genereres. Mange logs bliver genereret på enkeltsystemer og anvendes i den daglige drift, men de kan med fordel indgå i en samlet plan for logning i forhold til cybersikkerhed. Det kræver, at der er den rette forståelse for de enkelte log-typer.
- Sørg for at stille krav til leverandører om hvilke logs, der skal genereres hos partnere, og hvordan de logs kan tilgås.
- Hav tilstrækkelig lagerkapacitet til rådighed til opbevaring af logs i den tidsperiode, der er besluttet i organisationen. Dette bør automatiseres.

Opsamling af logs

Målet med denne vejledning er at hjælpe organisationer til at have de bedste muligheder for at kunne analysere en it-sikkerhedshændelse. Derfor anbefaler Center for Cybersikkerhed, at organisationen etablerer et system, der samler alle logs ét centralt sted.

Nedenfor beskrives nogle af de elementer, der bør indgå i logpolitik og procedurer:

- Tidsstempling er afgørende. For at logs i centrale log-systemer og på decentrale enheder senere skal kunne anvendes og korreleres, er det altafgørende, at logoptegnelsen sker med en tidsstempling (UTC), der er synkroniseret fra en central tidsserver.
- Dataintegritet er et must. Både ved generering af logs på de enkelte enheder, ved overførsel af logs til centrale systemer eksempelvis via syslog og ved opbevaring af logs på centrale opsamlingsenheder, skal det sikres, at der ikke kan blive manipuleret med logdata. Det gælder beskyttelse imod, at medarbejdere med privilegerede rettigheder, eksterne samarbejdspartnere og udefrakommende angribere kan slette, ændre eller tilføje data i loggen.⁴

⁴ Se eventuelt: DS/ISO/IEC 27002. Information technology – Security techniques – Code of practice for information security controls, afsnit 8.2

- Dokumentér. Organisationen bør udarbejde dokumentation for, hvorfra der logges, og hvad der logges. Det letter tredjeparters mulighed for at få et overblik over hvilke data, der er til rådighed i tilfælde af en hændelse.

Test af logs

Husk at teste loggene løbende. Når logning er opsat, er det vigtigt at teste, om logningen er korrekt, om det er de rigtige data, der gemmes, og om de bliver gemt så længe, som det er defineret i organisationens politik. Det skal også testes, om der kan uddrages de ønskede informationer i forbindelse med en eventuelt sikkerhedshændelse. Kan man eksempelvis identificere hvem, der har gjort hvad hvornår? Inddrag dem, der skal efterforske eventuelle sikkerhedshændelser.

Lagring af logs

Et cyberangreb opdages ikke altid, mens det står på. Derfor skal logs gemmes.

Der kan ofte gå uger og måneder fra et angreb sker, til det bliver opdaget. Derfor skal organisationen tage stilling til, hvor længe de enkelte logs skal opbevares. Beslutningen om, hvor længe logs skal opbevares, må tages på baggrund af den enkelte organisations risikovurdering og hensyntagen til regulering på området, der i nogle tilfælde også regulerer, hvor længe logs må opbevares, inden de slettes. Dette bør beskrives i logpolitikken. Logs bør opbevares minimum 13 måneder, medmindre der er lovgivning, der kræver noget andet.

Under lagring skal organisationen sikre sig, at der er etableret de rette sikkerhedsforanstaltninger til at beskytte loggenes integritet, fortrolighed og tilgængelighed. Det betyder for det meste, at de skal beskyttes som organisationens øvrige sensitive informationer, og at der ikke må være adgang for uvedkommende. Det bør sikres, at ingen medarbejdere har mulighed for at manipulere med loggen, uden at det kan opdaget.

I forhold til lagring af logs skal organisationen også tage stilling til, hvordan de skal sikkerhedskopieres. Det anbefales, at der sikkerhedskopieres efter samme procedure som for andre sensitive informationer efter organisationens politik på området.

Anvendelse af logs

Ud over at logs er et værdifuldt værktøj, når man skal analysere en itsikkerhedshændelse, er det vigtigt kort at nævne, at monitorering også kan bruges proaktivt til driftsoptimering og til løbende at opdage uregelmæssigheder og uhensigtsmæssigheder i organisationens systemer.

Organisationens politik og procedure for logning bør indeholde retningslinjer for, hvordan de forskellige logs konkret kan anvendes. Skal en bestemt log eksempelvis gennemgås regelmæssigt, eller skal den kun anvendes i tilfælde af en sikkerhedshændelse? Det skal besluttes, hvordan en gennemgang af bestemte logs skal foretages, og hvad der skal søges efter. Samtidig skal det besluttes, om loggennemgang skal være værktøjs-understøttet, eksempelvis ved brug af et SIEM-system, om den skal ske manuelt eller noget helt andet. Center for Cybersikkerhed anbefaler, at gennemgangen er værktøjs-understøttet. Der er også mulighed for at aftale med en ekstern leverandør, at de periodisk eller i realtid gennemgår logs⁵.

⁵ Proaktiv anvendelse af logs ligger uden for rammerne af denne vejledning.

Sletning af logs

Når logs slettes, skal organisationen sikre sig, at de slettes helt fra alle de lagermedier de ligger på. Det gælder decentrale enheder (firewalls med mere), sikkerhedskopier, analyseplatforme og så videre. Sletning bør følge en fast beskrevet procedure, og organisationen bør jævnligt sikre sig at denne følges.

Anbefalinger

- Organisationen bør logge på alle internetvendte tjenester og centrale interne it-systemer.
- Organisationen bør centralisere logning og opbevarings af logs.
- Organisationen bør anvende en fælles tidskilde og samme tidszone (UTC).
- Logs bør opbevares minimum 13 måneder, medmindre der er lovgivning, der kræver noget andet.