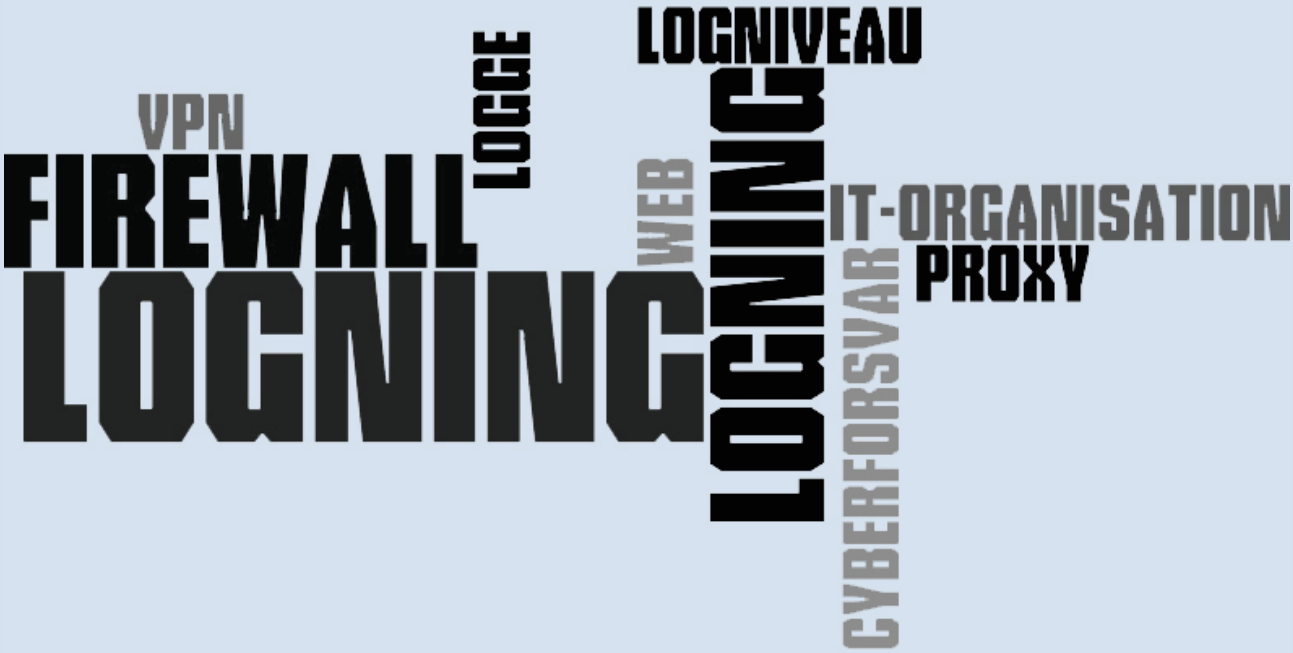
CENTER FOR CYBERSIKKERHED

Logning – en del af en godt cyberforsvar



Center for Cybersikkerhed

April 2016

Indledning

Center for Cybersikkerhed (CFCS) ser ofte, at organisationer bliver ramt af cyberangreb, hvor man efterfølgende kan konstatere, at vigtige logs fra de berørte it-systemer ikke er til rådighed til at analysere angrebet. Logning - og opsamling af disse - fra udstyr og systemer i organisationens infrastruktur er afgørende for myndigheder og virksomheders evne til at opdage et cyberangreb hurtigt og efterfølgende effektivt afdække konsekvensen.

Denne vejledning henvender sig til organisationer for at bidrage til, at logning kan indgå i et godt cyberforsvar. Det skal bemærkes, at vejledningen fokuserer på de logningsaspekter, der er relevante i forbindelse med et cyberforsvar. Aspekter ved logning i forbindelse med generel drift og som følge af revisionskrav ikke er dækket. Vejledningen henvender sig blandt andet til personer med teknisk viden på området.

Vejledningen berører nogle af de udfordringer, som CFCS ved, at mange organisationer står over for i forbindelse med logning. Vejledningen giver også en række anbefalinger og tiltag i relation til at inddrage logning i et godt cyberforsvar. Endelig peger vejledningen på en række specifikke komponenter i it-infrastrukturen, hvor logning med fordel kan indgå som del af et godt cyberforsvar.

Udfordringer

I mange organisationer ligger ansvaret for logning hos en eller få systemadministratorer. Logning i disse organisationer er ofte baseret på den enkelte medarbejders erfaring og arbejdsrelaterede behov. Hele organisationens ønske om/behov for et samlet overblik over aktiviteter og hændelser i it-infrastrukturen vil derfor ikke nødvendigvis blive imødekommet.

Man vil for ofte opleve, at en given it-medarbejder i driftsafdelingen fokuserer på de driftsrelaterede logs, relateret til de komponenter han har ansvaret for f.eks. til brug ved en eventuel fejldiagnosticering. Men i sammenhæng med et godt cyberforsvar vil disse logs ikke nødvendigvis være de bedst egnede.

Der kan også være andre årsager til, at en organisation i forbindelse med en given situation ikke har adgang til de fornødne logs. Disse årsager kan være:

- Organisationen kan have fravalgt at opsamle logs på givent udstyr som følge af kapacitetsmæssige overvejelser, idet opsamling af logs vil kræve såvel processorkraft som lagerkapacitet. Denne kapacitet har det anvendte udstyr ikke nødvendigvis til rådighed.
- Manglende forståelse i organisationen for betydningen af logs fra det konkrete udstyr. Mange organisationer har meget svært ved at forstå hvilke specifikke logs, de som minimum bør opsamle og gemme.
- Manglende krav til outsourcing-partner om behovet for logning. Mange outsourcingpartnere vil som udgangspunkt kun foretage logning, hvis der er indgået specifikke aftaler herom, da opsamling og håndtering af logs som udgangspunkt kræver ressourcer ud over traditionel drift.
- Mangelfuld konfiguration af udstyr, der nok sikrer opsamling af logs, men ikke at disse opbevares i tilstrækkelig lang tid. På grund af manglende indsigt i hvilke krav til lagringskapacitet et givent system har, vil man ofte opleve, at disse bliver overskrevet, når den afsatte lagerplads til logs er opbrugt.

Anbefalinger om indledende tiltag

Forankring i topledelsen
Grundlaget for et godt cyberforsvar er, at topledelsen er involveret. Topledelsen skal blandt andet sikre, at der er fokus på logning i organisationen, og at formålet med logning er fastlagt. Topledelsen skal også sikre, at der er tilstrækkelige ressourcer i organisationen eller tilknyttet denne, så krav til logning og opfølgning kan honoreres.

Et andet aspekt som ledelsen også bør være opmærksom på er, at anvendelsen af en struktureret logning også vil give organisationen mulighed for at opnå en forståelse af, hvor og hvorfor de eksisterende sikringstiltag svigtede i forbindelse med et eventuelt cyberangreb.

Viden om it-infrastrukturen
Det er ligeledes en forudsætning, at man i organisationen har et godt overblik over og viden om den it-infrastruktur, som man anvender. Dette overblik og denne viden kan f.eks. fås via:

- Et overordnet diagram over netværksinfrastrukturen (topologi)
- Beskrivelse af alle internetforbindelsespunkter samt deres regelsæt (f.eks. firewall regler)
- Oversigt over alle DNS, DHCP servere og VPN koncentratorer
- Liste over alle Windows domæner samt GPO'er, der definerer logniveauet på Windows maskiner samt alle etablerede lognings-løsninger

Risikobaseret tilgang
På baggrund af topledelsens krav skal it-organisationen i samarbejde med forretningen identificere hvilke logs, der skal opsamles. Da det ikke nødvendigvis er alle dele af it-infrastrukturen, der har

stor betydning for organisationens daglige virke, bør organisationen derfor overveje hvilke logs, der bidrager bedst i det samlede cyberforsvar. For at kunne vurdere dette anbefaler CFCS, at der udarbejdes en risikovurdering på baggrund af relevante cybertrusler. På baggrund af en risikovurdering afgøres det hvilke typer af logs, der bidrager mest i forebyggelsen af disse trusler eller bedst reducerer konsekvenserne.

CFCS Trusselsvurdering
På CFCS' hjemmeside publiceres jævnligt trusselvurderinger på flere specifikke områder.

Juridiske forhold
Inden organisationen iværksætter en omfattende logning, skal man være opmærksom på, at der i forbindelse med logning er en række juridiske aspekter, som organisationen skal forholde sig til. Det ligger ikke inden for rammerne af denne vejledning at dække dette område.

Beslutning om brug af de enkelte logs
Når det er besluttet hvilke logs, der skal indsamles, skal organisationen tage stilling til, hvordan de enkelte logs skal bruges. Det er CFCS' opfattelse, at logs primært indgår i det reaktive cyberforsvar af organisationen. Visse typer af logs kan med fordel anvendes i det præventive forsvar f.eks. i forbindelse med en periodisk gennemgang af hvilke generelle aktiviteter, der har været på og i mod en specifik komponent i it-infrastrukturen.

Afhængig af den konkrete anvendelse af en specifik log skal det derfor på forhånd besluttes, om loggen skal gennemgås regelmæssigt, eller om man kan nøjes med at bruge den, når en hændelse er indtruffet. I den forbindelse skal det besluttes, hvordan en sådan gennemgang skal foretages. Skal gennemgangen være værktøjsunderstøttet eller om den skal ske helt manuelt.

Tidssynkronisering
Af hensyn til et eventuelt udredningsarbejde i forbindelse med et cyberangreb, er det af afgørende betydning, at alle logs er tidssynkroniseret op imod samme tidsserver. På den måde bliver det nemmere at spore eventuelle hændelsesmønstre igennem it-infrastrukturen.

Centralisér og beskyt dine logs
I en konkret situation, hvor der er behov for adgangen til specifikke logs, kan organisationen samle sine logs fra it-infrastrukturen – f.eks. i en Security Information and Event Management (SIEM) platform. Hvis man ikke har en SIEM-løsning, bør man på anden vis lagre logs centralt. I den forbindelse bør det sikres, at de enkelte logs er sikret imod uautoriseret ændringer – også (om muligt) imod personer/processer med administrative rettigheder. I den forbindelse skal det fastlægges, hvem der skal gives adgang til organisationens logs.

Arkivering af logs

Et sidste væsentligt aspekt, der skal tages stilling til, er hvor lang tid de enkelte logs skal opbevares. Her er det væsentligt at bemærke, at man ikke nødvendigvis opdager et cyberangreb med det samme. Der kan let gå mange uger eller måneder fra, at et angreb har fundet sted til, at man bliver opmærksom på de uønskede aktiviteter. I en sådan situation er det vigtigt, at de relevante logs ikke er blevet slettet eller overskrevet.

Som udgangspunkt bør man opbevare de enkelte logs så lang tid, som det giver mening. Dette bør man tage stilling til i risikovurderingen.

I National Institute of Standards and Technology (NIST's) "Guide to Computer Security Log Management" giver de følgende forslag til opbevaringsperioder for forskellige kategorier af logs:

Kategori	Lav betydning	Medium betydning	Høj betydning
Opbevaringsperiode	1 til 2 uger	1 til 3 måneder	3 til 12 måneder

Hensynet til omkostninger kan ligeledes indgå i de risikomæssige overvejelser. Endelig skal man også være opmærksom på, at visse typer af logs skal opbevares i et på forhånd givet tidsrum af hensyn til efterlevelse af regulatoriske/lovgivningsmæssige krav.

Fokuspunkter for logning

I dette afsnit gennemgås en række infrastrukturkomponenter, hvor en logning med fordel kan bruges i forbindelse med et godt cyberforsvar.

Domain Name System (DNS)

Logs fra interne DNS-servere er vigtige for at afgøre, hvilket internt system (pc'er, servere mv.), der har - eller har forsøgt - at kontakte et kendt ondsindet domænenavn, og hvornår. Dette kan f.eks. ske, når malware kommunikerer med en Command & Control server (C2-server). I Microsoft-miljøer betyder DNS-serveren typisk domain controlleren. Desværre indeholder Microsoft DNS-log som standard ikke tilstrækkelig information uden aktivering af den ordrige "debug logging". Man bør logge dato/tid, forespurgt domænenavn og oplyst IP-adresse samt afsender IP-adresse/maskine.

Dynamic Host Configuration Protocol (DHCP)

For at kunne afgøre hvilke interne systemer (pc'er, servere mv.), der har tilgået en intern eller ekstern ressource, er det afgørende, at man kan fastlægge hvilket system, der har anvendt en given IP-adresse på et specifikt tidspunkt. En af de primære årsager til spildt tid og ukorrekte konklusioner i undersøgelser af cyberangreb er undersøgelser af det forkerte system på grund af manglende DHCP-logning. Man bør logge dato/tid, IP-adresse, MAC-adresse og maskinnavn.

Firewall
Firewalls er ofte sat op til kun at logge blokeret trafik. I undersøgelser af cyberangreb er det dog oftest interessant at analysere godkendt trafik. I den forbindelse er det vigtig at påpege, at i relation til organisationens firewall bør logning foretages på såvel indersiden som ydersiden af denne for at fastholde det fulde billede af den trafik, der blokeres alternativt passerer igennem firewallen.

Man bør logge dato/tid, afsender/modtager IP-adresse og port, protokol og beslutning (såsom forbindelsen blev blokeret, godkendt, etc.).

Domain controller
På Domain controlleren bør man logge alle type 3 (netværkssessioner) og type 10 (Remote Desktop Protocol (RDP) sessioner) autentifikationer. Man bør logge dato/tid, type 3/10, brugernavn, afsender/modtager IP-adresse / maskinnavn. Man skal være opmærksom på, at Security event loggen på de fleste domain controllere bliver overskrevet i løbet af få timer, fordi der ikke er afsat tilstrækkelig plads til denne log. Dette skal der tages højde for.

Netflow
Routere og switches kan opsummere den trafik, de ser ved brug af Netflow-protokollen, information, der kan bruges som et supplement til firewall logning og/eller, hvis det er upraktisk at logge al godkendt firewall trafik. Man bør logge ingress interface, afsender/modtager IP- adresse og port.

Fuldt pakkeindhold
Hverken firewall eller Netflow loggene indeholder selve pakkeindholdet. Hvis man har mulighed for det, bør man også logge pakkeindhold og gemme det så længe som praktisk muligt. Husk at være opmærksom på eventuelle juridiske aspekter i denne sammenhæng.

Virtual private network (VPN)
I nogle tilfælde, efter succesfuld kompromittering, benytter angriberen sig efterfølgende delvist eller udelukkende af at få adgang til netværket via VPN. Man bør logge dato/tid, afsender IP-adresse/maskinnavn/brugernavn, midlertidig tildelt IP-adresse og VPN-koncentrator placering.

Web-servere
Nogle angribere placerer bagdøre på web-servere i den demilitariserede zone (DMZ), som en yderligere mekanisme for at bevare adgangen til et kompromitteret netværk. Hvis en bagdør på en web-server bliver opdaget, kan en webserverlog være behjælpelig med at undersøge, hvad angriberen har foretaget sig. Man bør logge dato/tid, afsender IP-adresse, handling (GET, POST, etc.) og URL.

Web proxy
Hvis man anvender en web proxy, kan dens logs hjælpe med at finde og blokere potentielt ondsindede domænenavne samt forespørgsler fra kompromitterede maskiner, som man ikke allerede kender til. Man bør logge dato/tid, URL, downloadede filer, IP-adresse/maskinnavn og bruger (hvis muligt) og så mange http header-felter som muligt, herunder f.eks. browserversion.

Andre logs
Selv om Intrusion Detection System (IDS) og Antivirus (AV) logs ofte er mindre brugbare i undersøgelser af cyberangreb af en vis kaliber, kan disse logs med fordel centraliseres (medtag kopi af filer sat i karantæne). Lokalt på Windows klienter bør man logge "success" og "failure" audits, hvis den enkelte maskine skal undersøges nærmere. Det samme bør overvejes for kritiske filservere. Logs fra privilegerede konti og password management suiter samt application whitelisting-løsninger bør også opsamles, ligesom der kan opstå behov for at analysere e-mail-logs, specielt i forhold til afsender/modtager IP-adresse, emne, intern modtager, evt. størrelse af body samt attachments.

Afsluttende bemærkninger

Som tidligere nævnt vil CFCS gøre opmærksom på, at logs i sig selv ofte primært anses for at indgå i det reaktive cyberforsvar af organisationen, og at man selvfølgelig også bør afsætte ressourcer på det proaktive forsvar. CFCS' vejledning "Cyber forsvar der virker" giver i den henseende en række gode bud på, hvor denne indsats bør iværksættes, men også andre informationskilder kan give inspiration til forbedring af sikkerheden, herunder Escal Institute of Advanced Technologies' (SANS) "Critical Security Controls"

Cyberforsvar der virker
På CFCS' hjemmeside kan du få gode bud på, hvordan I i din organisation skaber et godt cyberforsvar i publikationen "Cyberforsvar der virker".

Denne vejledning om logning er baseret på de erfaringer CFCS har gjort i forbindelse med håndtering af konkrete cyberangreb hos en række organisationer. Vejledningen er ikke tænkt som en "best-practise-guide", men som et bidrag til organisationers generelle vidensindsamling på området.