Appendiks 6. Logning og overvågning

Logs og logningspolitik

Et vigtigt element i virksomhedens cybersikkerhedsstrategi er at kunne opdage, når et cyber angreb sker. Til dette har virksomheden bl.a. brug for sine logs. Ved angreb – eller mistanke om angreb - er logs også forudsætningen for at kunne gå tilbage i tid og undersøge, hvad der rent faktisk er sket. Virksomheden skal derfor beslutte en logningspolitik. En logningspolitik:

- Fastlægges ud fra virksomhedens risikovurdering
- Skal omfatte de kritiske systemer og processer
- Skal omfatte eksterne krav til virksomheden
- Beslutter, hvorvidt der sker en centraliseret opsamling af logs eller ej (anbefales)
- Fastlægger serviceniveauer f.eks. Reaktionstider, og om loggen overvåges i døgndrift
- Fastlægger krav til virksomhedens egne kompetencer
- Beslutter brugen af en Managed Security Service Provider (MSSP) til at overvåge loggen
- Fastlægger, hvilke logs fra hvilke systemer, der skal opsamles
- Fastlægger, hvordan loggen skal behandles og analyseres
- Fastlægger, hvor længe loggen efterfølgende skal opbevares
- Fastlægger, hvordan det sikres at loggen er komplet og fyldestgørende

Overvågning

For aktivt at kunne opdage angreb kræves en pro-aktiv analyse af alarmer, dvs. virksomheden skal have et SIEM system og et Security Operation Center (SOC) med mennesker, processer og teknologi til at kunne analysere og reagere på mistænkelige hændelser. Etablering af et Security Operation Center (SOC), der arbejder i døgndrift, kan være dyrt og besværligt, ligesom det kan være svært at finde medarbejdere med de rigtige kompetencer. Derfor vælger mange virksomheder at købe det som en service fra en Managed Security Service Provider (MSSP).

Generelle anbefalinger/overvejelser til bestyrelsen omkring logning og overvågning:

- **Logningspolitik**: At virksomheden har en logningspolitik, som er afstemt med virksomhedens risikovurdering, samt hvilke overvågningsløsninger (eller services), virksomheden har købt.
- **Eksterne krav**: At krav til logning fra lovgivning, kunder, myndigheder eller standarder, om nogen, er afspejlet i logningspolitikken.
- **Ressourcer og kompetencer**: At virksomheden har de rette medarbejdere og kompetencer i forhold til den fastlagte logningspolitik. Dette kan enten være internt i virksomheden eller via aftale med sikkerhedsleverandør.
- **Reaktion**: At virksomheden kan reagere tilstrækkeligt hurtigt på indikationer på sikkerhedshændelser – både i forhold til analyse og reaktion på alarmer.
- **Opbevaring af logs**: At virksomhedens logdata er beskyttet mod uautoriseret adgang samt sletning og manipulation ved cyberangreb og at loggen opbevares i tilstrækkelig lang tid (hvilket typisk er minimum i 13 måneder).
- **Tilgængelighed**: At loggen er tilgængelig for interne medarbejdere, myndigheder og eksterne sikkerhedsfirmaer der evt. skal have adgang til loggen i forbindelse med håndtering og efterforskning af sikkerhedshændelser.