Logimise ja seire kord

1. Eesmärk Käesoleva logimise ja seire korra eesmärk on kehtestada suunised turvalogide salvestamiseks, säilitamiseks ja analüüsimiseks, et tõhusalt tuvastada turvaintsidente ja neile reageerida. Käesolev kord tagab vastavuse regulatiivsetele nõuetele ja suurendab Ettevõtte turvalisust ennetava seire kaudu.

2. Skoop Käesolev kord kehtib kõigile töötajatele, töövõtjatele ja süsteemidele, mis on seotud turvasündmuste logimise, seire ja analüüsiga kogu Ettevõtte taristus, sealhulgas kohapealsetes ja pilvekeskkondades.

3. Logimise nõuded

- Kõik kriitilised süsteemid, rakendused ja võrguseadmed peavad genereerima logisid turbega seotud sündmuste kohta.
- Logid peavad sisaldama ajatemplied, allikat, kasutaja tegevust ja asjakohaseid sündmuse üksikasju.
- Süsteemi- ja turvalogisid tuleb säilitada tsentraalses logimisplatvormis koos asjakohaste juurdepääsukontrollidega.
- Logisid tuleb säilitada vastavalt Ettevõtte andmete säilitamise poliitikale ja regulatiivsetele nõuetele.

4. Seire ja teavitamine

- Turvalogisid tuleb pidevalt jälgida, kasutades automaatseid tööriistu, nagu turvaintsidentide ja sündmuste halduse (SIEM) süsteemid.
- Teavitused peavad olema genereeritud kahtlase tegevuse puhul, sealhulgas volitamata juurdepääsukatsed, privileegide laiendamine ja anomaalne käitumine.
- IT-turbe meeskond peab teavitusi üle vaatama ja võimalikke turvaintsidente õigeaegselt uurima.

5. Logide terviklus ja kaitse

- Logid peavad olema kaitstud võltsimise või volitamata muutmise eest.
- Juurdepääs logidele peab olema piiratud ainult volitatud personaliga.
- Logide tervikluse tagamiseks tuleb kasutada krüptograafilisi meetmeid, näiteks räsimist (hashing).

6. Integratsioon intsidendireageerimisega

- Logitud sündmused peavad olema seostatud Ettevõtte intsidendihalduse plaaniga, et hõlbustada turvaintsidentide kiiret tuvastamist ja neile reageerimist.
- Kõrge tõsidusastmega leiud peavad käivitama viivitamatu eskaleerimise intsidendireageerimise meeskonnale.

- Intsidendijärgsed raportid peaksid sisaldama logianalüüsi, et teha kindlaks algpõhjus ja maandada tulevasi riske.

7. Vastavus ja auditid

- Regulaarselt tuleb läbi viia auditeid, et tagada vastavus logimise ja seire nõuetele.
- Logid peavad olema vajaduse korral kättesaadavad kohtuekspertiisi uurimisteks ja regulatiivseteks audititeks.
- Logihaldusega seotud töötajad peavad läbima regulaarset koolitust parimate praktikate ja vastavuskohustuste osas.

8. Korra ülevaatamine ja uuendamine Käesolev kord tuleb üle vaadata igal aastal või vastavalt vajadusele, et arvestada muudatustega turvaohtudes, vastavusnõuetes ja tehnoloogilistes arengutes.