HP TURVAMEETMETE KOKKUVÕTE

Kliendiandmete kaitsmiseks järgib HP tugevaid infoturbe kontrolle, sealhulgas põhimõtteid, tavasid, protseduure ja organisatsiooni struktuure, et kaitsta enda ja oma klientide teabe konfidentsiaalsust, terviklikkust ja kättesaadavust (kaasa arvatud HP kliendi ja andmetöötluse lisades määratletud isikuandmed). Alljärgnevalt antakse ülevaade HP tehnilistest/organisatsioonilistest turvameetmetest kogu ettevõtte ulatuses.

1. Turbe põhimõtted

   HP säilitab globaalselt rakendatavad põhimõtted, standardid ja protseduurid, mis on mõeldud HP ja Kliendi andmete kaitsmiseks. HP turbe põhimõtete üksikasjad on konfidentsiaalsed HP andmete ja süsteemide tervikluse kaitsmiseks. Allpool on esitatud meie peamiste põhimõtete kokkuvõte.

2. Infoturbe organisatsioon

   HP infoturbe programm on mõeldud ettevõtte infoturbe strateegia ja juhtimise suunamiseks ja säilitamiseks. See süsteem tagab ettevõtteülese vastavuse HP turbe põhimõtetele ja juhtimisele ning klientide turvanõuete järgimise. Raamistik on struktureeritud kooskõlas tööstusstandardite küberturvalisuse raamistike, seaduste ja määrustega ning see vaadatakse igal aastal läbi, et kohandada seda HP areneva ohumaastikuga.

3. Küberturvalisuse riskihaldus

   HP küberturvalisuse riskihaldusprogrammi eesmärk on säilitada teabevarade konfidentsiaalsus, terviklikkus ja kättesaadavus. Programm pakub järjekindlat lähenemisviisi küberturvalisuse riskide tuvastamiseks, hindamiseks, prioriteetide seadmiseks, käsitlemiseks, parandamiseks, jälgimiseks ja aruandluseks. HP määratleb oma riskiisu aktsepteeritava kahjukontsentratsiooni ja riskitaluvuse tasemena. Riske hinnatakse kindla metoodika abil, mis võimaldab HP-l tagada teabeturbega seotud riskid vastuvõetavale tasemele. See programm ühildub HP ettevõtte riskihalduse protsessiga.

4. HP turvalisus

   HP inimressursside turbe põhimõtted tagavad infoturbe kogu töötaja tööea jooksul, luues juurdepääsuprotsessid rajatistele, infosüsteemidele ja muudele varadele. See hõlmab kirjalike kinnituste saamist konfidentsiaalsuse ja mitteavaldamise kokkulepete kaudu, samuti tausta sõeluuringute läbi viimist. Kõik HP töötajakandidaadid peavad läbima taustkontrolli vastavalt asjakohastele õigusnormidele ja eetikale.

5. Varahaldus

   HP-s on protsess tehnilise teabevara tuvastamiseks, kriitiliste varade liigitamiseks ning dokumenteeritud käsitsemisprotseduuride haldamiseks teabe iga klassifikatsioonitüübi, sealhulgas isikuandmetega seotud toimingute jaoks. Need toimingud hõlmavad säilitamist, edastamist, suhtlust, ligipääsu, logimist, säilitamist, hävitamist, kõrvaldamist, intsidentide haldust ja rikkumisest teavitamist. HP turbe põhimõtted ja standardid volitavad samuti andmekandjate turvalist käsutamist.

6. Andmete turvalisus

   HP andmeturbe programm annab ülevaate turbetavadest ja tehnilistest kontrollidest, mida tuleb rakendada andmete konfidentsiaalsuse, autentsuse ja terviklikkuse kaitsmiseks. Juriidilised nõuded, väärtus, kriitilisus ja tundlikkus autoriseerimata avalikustamise või muutmise suhtes on mõned tegurid, mis määravad ära, kuidas teave HP andmeturbe põhimõtete kohaselt liigitatakse. Lisaks andmete krüptimisprotseduuridele on põhimõtetes välja toodud andmete krüptimine, kustutamine, kogumine ja töötlemine, säilitamine, varundamine ja andmekao ennetamine.

7. Juurdepääsu juhtimine

   HP kasutab loogilise juurdepääsu juhtimise jaoks väikseima privileegi põhimõtet, mis tagab kasutajale juurdepääsu unikaalsete kasutaja ID-ide ja salasõnadega. Salasõna põhimõte määratleb keerukuse, jõu, kehtivuse ja salasõna ajaloo kontrolli. Pääsuõigusi vaadatakse perioodiliselt üle ja need tühistatakse töötaja lahkumisel. Kasutajakonto loomise ja kustutamise kokkulepitud korda rakendatakse selleks, et anda ja tühistada seotuse ajaks ligipääs kliendisüsteemidele.

8. Krüptograafia

   HP on määratlenud kindlad krüptograafiaprotsessid, et tagada teabevarade konfidentsiaalsus, terviklikkus ja kättesaadavus. Heakskiidetud protokollid nõuavad teatavate, sealhulgas isikuandmeid sisaldavate varade krüptimist. Meie krüptograafiaprogramm hõlmab matemaatiliste tehnikate kasutamist teabe ja kommunikatsiooni kaitsmiseks, tagades andmetele juurdepääsu ainult volitatud osapooltel. HP infoturbeprogrammi kriitiline komponent kaitseb andmeid loata juurdepääsu ja võltsimise eest.

9. Füüsiline turvalisus ja keskkonnaohutus

   HP rajatised on turvatud mitmesuguste füüsiliste ja elektrooniliste juurdepääsuelementidega, kaasa arvatud turvavalvurid, elektrooniline juurdepääsukontroll ja suletud ringtelevisioon (CCTV). Rajatised on varustatud ka vajaliku infrastruktuuritoega, sealhulgas temperatuuri reguleerimise ja toite varundusega, kasutades UPS-i ja/või diiselgeneraatoreid kriitiliste teenuste toetamiseks. Kõik HP töötajad on registreeritud ja nad peavad omama asjakohaseid identifitseerimismärke.

10. Ettevõtluse juhtimine

    HP on kehtestatud minimaalsed karastusnõuded tehnoloogiataristule, sh tööjaamadele, serveritele ja võrguseadmetele. Need seadmed kasutavad eelnevalt karastatud operatsioonisüsteemi kujutisi, kusjuures nõuded erinevad operatsioonisüsteemi ja rakendatavate kontrollide järgi. Lisaks on HP juurutanud võrgu sissetungimise tuvastamise/ennetamise süsteemid (NIDS/NIPS), mida jälgitakse ja hallatakse ööpäevaringselt.

11. Kommunikatsiooni turvalisus

    Kommunikatsiooni turvalisus tagab teabe kaitse korporatiivsetes võrkudes. See hõlmab võrgu turbekomponentide (nt tulemüüride) installimist ja haldamist, võrkude eraldamist ning veebifiltrit ja e-posti käsitsemise juhtelemente. Lisaks hõlmab see sidekanalite jälgimist ja haldamist, et avastada ja vältida loata juurdepääsu või andmetega seotud rikkumisi.

12. Süsteemi turvalisus

    HP põhimõtetes antakse süsteemidele ja tarkvarale turvaline arengumetoodika kogu kasutusaja jooksul. Tarkvara arendamise elutsükkel hõlmab algatamist, arendust/omandamist, rakendamist, toiminguid ja kõrvaldamist. Kõiki süsteemi komponente hinnatakse selle põhjal, kas need mõjutavad üldist turvalisust. HP on loonud rakendusteenuste tehingute kontrollifunktsioonid, sh kasutajamandaadi valideerimine, digitaalallkirjad, krüptimine, turvalised kommunikatsiooniprotokollid ja tehingute üksikasjade talletamine vastavas võrguturbetsoonis. Regulaarselt skannitakse ja otsitakse ka sisemisi haavatavusi.

13. Kolmandad osapooled ja alltöövõtjad

    HP valib alltöövõtjad, kes järgivad ulatuslikke lepingulisi turvanõudeid. Kohaldatavate tarnijate puhul, kes käsitsevad HP või kliendi andmeid või kes sisenevad HP võrku, viib HP küberturvalisus läbi riskihindamise, et kontrollida infoturbeprogrammi füüsiliste, tehniliste ja haldusalaste kaitsemeetmetega. See hindamine on vajalik enne, kui tarnijale antakse juurdepääs HP teabele.

14. Infoturbeintsidentide haldus

    HP-s on ulatuslik küberintsidentide haldamise protsess, mis näitab eesmärki, ulatust, rolle, kohustusi, juhtimiskohustust, organisatsiooni kooskõlastamist, rakendamisprotseduure ja nõuetele vastavuse kontrolli. Seda protsessi vaadatakse läbi ja uuendatakse igal aastal. Küberintsidentide lahendamise meeskond, sealhulgas HP küberturvalisuse personal, kes on välja koolitatud intsidentidele reageerimise ja kriisiohjamise valdkonnas, teeb protsessi ja iga juhtumi või sündmuse kohta regulaarseid ülevaateid.

15. Talitluspidevuse haldamine

    HP globaalne talitluspidevuse programm tagab otsast lõpuni järjepidevuse koostöö-, standard- ja dokumenteeritud planeerimisprotsesside kaudu. Ettevõte teostab perioodiliselt oma talitluspidevuse kavasid, et tagada tõhusus, testimine ja ajakohastamine vähemalt igal aastal. Lisaks sellele saavad kõik talitluspidevuse kavaga seotud töötajad nõuetekohast koolitust.

16. Nõuetele vastavus

    Nõuetele vastavus kujundab HP lähenemisviisi juriidiliste, lepinguliste ja sisemiste ootuste täitmisele tõhusa infoturbeprogrammi puhul. Regulaarsed infoturbe ülevaated tagavad protokollide integreerimise igasse ärikontserni tegevusse. Läbivaatamise käigus uuendatakse dokumente ka nii, et need kajastavad kehtivaid juriidilisi kohustusi nõuete arenguna.

17. Maksekaarditööstus

    Maksekaarditööstuse (Payment Card Industry ehk PCI) raamistikus juhindutakse HP lähenemisviisist PCI nõuetele vastavuse saavutamisel, milles on kirjas PCI DSS-iga kooskõlas olev ärivastutus ja turbekontroll. Võrgu turbekontrollide, nagu tulemüürid, installimise ja haldamisega tagab HP selle vastavuse PCI nõuetele.

18. HP seadme turve

    HP seadme turve hõlmab HP toodete turvamise põhivõtteid, nagu koodi allkirjastamine, toote turvaaukude haldamine, turvabülletäänide väljaandmine ja toote turvaprobleemidest teavitamine. Nende meetmetega tagatakse, et HP tooted on kasutajatele turvalised ja usaldusväärsed. Toote turvalisus on HP-s ülimalt tähtis, kuna see aitab säilitada kliendi usaldust ja kaitsta võimalike ohtude eest.

19. HP teenuse turvalisus

    HP teenuse turvalisus hõlmab olulisi tavasid HP klientidele osutatud teenuste turvamiseks. See poliitika on suunatud erinevatele teenindusturbe valdkondadele, sh HP infrastruktuuri hostitud, kolmanda osapoole hostitud, partneri hostitud ja kliendi hostitud keskkonnad. Nende meetmetega tagatakse, et HP teenused on kasutajatele turvalised ja usaldusväärsed. Tugevate turvameetmete rakendamisega tagab HP oma toodete ja teenuste ohutuse ja terviklikkuse, pakkudes kõigile kasutajatele turvalist ja usaldusväärset keskkonda.