POVZETEK HP-JEVIH VARNOSTNIH UKREPOV

Za zaščito podatkov uporabnikov HP upošteva zanesljiv nabor ukrepov za informacijsko varnost, vključno s pravilniki, praksami, postopki in organizacijskimi strukturami za zaščito zaupnosti, celovitosti in razpoložljivosti svojih podatkov in podatkov strank (vključno z osebnimi podatki, kot so opredeljeni v HP-jevem dodatku za obdelavo uporabnikov in podatkov). V nadaljevanju so opredeljeni HP-jevi tehnični/organizacijski varnostni ukrepi v celotnem podjetju.

1. Varnostni pravilnik

   HP ima pravilnike, standarde in postopke za zaščito HP-jevih podatkov in podatkov strank na globalni ravni. Podrobnosti HP-jevih varnostnih pravilnikov so zaupne zaradi zaščite celovitosti HP-jevih podatkov in sistemov. Povzetki naših ključnih pravilnikov pa so vključeni v nadaljevanju.

2. Organizacija za informacijsko varnost

   HP-jev program informacijske varnosti je oblikovan za usmerjanje in vzdrževanje varnostne strategije in nadzornih ukrepov organizacije. Ta sistem zagotavlja skladnost celotnega podjetja s HP-jevimi varnostnimi pravilniki in varnostnimi ukrepi ter izpolnjevanje varnostnih zahtev HP-jevih strank. Okvir je strukturirani v skladu z okvirji za kibernetsko varnost, ki predstavljajo panožni standard, zakoni in predpisi ter ga vsakoletno pregledamo in prilagodimo razvijajočim se nevarnostim, ki jim je izpostavljen HP.

3. Upravljanje tveganj kibernetske varnosti

   HP-jev program za obvladovanje tveganj kibernetske varnosti je zasnovan za zagotavljanje zaupnosti, celovitosti in razpoložljivosti njegovih informacijskih sredstev. Program zagotavlja dosleden pristop k prepoznavanju, ocenjevanju, prednostnem razvrščanju in obravnavi tveganj za kibernetsko varnost, odpravljanju njihovih posledic, sledenju in poročanju o njih. HP opredeljuje svoj prag tveganjem kot sprejemljivo raven izpostavljenosti izgubam in toleranco za tveganja kot stopnjo odstopanja od tega praga. Tveganja se ocenijo z uporabo vnaprej opredeljene metodologije, kar HP-ju omogoča zmanjšanje tveganj za informacijsko varnost na sprejemljivo raven. Ta program je usklajen s HP-jevim postopkom upravljanja tveganj v podjetjih.

Zadnja posodobitev: september 2024

4. Varnost človeških virov

   HP-jev pravilnik o varnosti človeških virov zagotavlja informacijsko varnost skozi celoten življenjski cikel zaposlenih z določitvijo procesov za dostop do objektov, informacijskih sistemov in drugih sredstev. To vključuje pridobitev pisnih potrditev s pogodbami o varstvu zaupnosti in nerazkritju ter izvedbo postopkov za preverjanje preteklosti. Vsi kandidati za zaposlitev pri HP-ju morajo opraviti preverjanje preteklosti v skladu z ustreznimi zakoni, predpisi in etičnimi načeli.

5. Upravljanje sredstev

   HP ima postopek za prepoznavanje tehničnih informacijskih sredstev, kategoriziranje najpomembnejših sredstev in vzdrževanje postopkov dokumentiranega ravnanja za vsako vrsto razvrstitve informacij, vključno s tistimi, ki vsebujejo osebne podatke. Ti postopki zajemajo shranjevanje, prenos, komunikacijo, dostop, beleženje, zadržanje, uničenje, odlaganje, upravljanje dogodkov in obveščanje o kršitvah. HP-jevi varnostni pravilniki in standardi prav tako določajo, da je varno odlaganje nosilcev podatkov obvezno.

6. Varnost podatkov

   HP-jev program za podatkovno varnosti določa postopke varnosti in tehnične varnostne ukrepe, ki jih je treba izvesti za varstvo zaupnosti, pristnosti in celovitosti podatkov. Pravne zahteve, vrednost, nujnost in občutljivost na nepooblaščeno razkritje ali spremembe so nekateri od dejavnikov, ki določajo, kako se podatki razvrščajo v HP-jevem pravilniku o varnosti podatkov. Pravilnik poleg postopkov ravnanja s podatki opisuje tudi šifriranje, izbris, zbiranje in obdelavo, hranjenje in varnostno kopiranje podatkov ter preprečevanje izgube podatkov.

7. Nadzor dostopa

   HP uporablja načelo najmanjše pravice za logični nadzor dostopa in uporabnikom omogoča dostop prek enoličnih ID-jev in gesel uporabnika. Pravilnik o geslih določa zapletenost, moč in veljavnost gesel ter kontrolnike za zgodovino gesel. Pravice do dostopa se redno preverjajo in prekličejo ob odhodu osebja. Dogovorjeni postopki za ustvarjanje in izbris uporabniških računov se izvajajo za dodeljevanje in preklic dostopa do odjemalskih sistemov med sodelovanji.

8. Kriptografija

   HP je določil nabor vzdržljivih postopkov za kriptografijo, s katerim se zagotavlja zaupnost, celovitost in razpoložljivost informacijskih sredstev. Odobreni protokoli zahtevajo šifriranje nekaterih sredstev, vključno s tistimi, ki vsebujejo osebne podatke. Naš program kriptografije vključuje uporabo matematičnih pristopov za zaščito podatkov in komunikacije, s čimer zagotovimo, da lahko do podatkov dostopajo samo pooblaščene osebe. Izjemno pomemben del HP-jevega programa za informacijsko varnost varuje podatke pred nepooblaščenim dostopom in spreminjanjem.

9. Fizična in okoljska varnost

   HP-jevi objekti so zaščiteni z uporabo različnih ukrepov za fizični in elektronski nadzor dostopa, vključno z varnostnimi varovali, elektronskim nadzorom dostopa in video nadzorom. Objekti so opremljeni tudi z ustrezno infrastrukturno podporo, vključno z nadzorom temperature in varnostnim kopiranjem, uporabo brezprekinitvenega napajanja in/ali dizelskih generatorjev za podporo nujnih storitev. Vse HP-jevo osebje je registrirano in mora imeti ustrezno identifikacijsko značko.

10. Upravljanje poslovanja

    HP je določil minimalne zahteve za utrditev tehnološke infrastrukture, vključno z delovnimi postajami, strežniki in omrežno opremo. Te naprave uporabljajo vnaprej utrjene posnetke operacijskega sistema z zahtevami, ki se razlikujejo glede na operacijski sistem in uvedene nadzorne ukrepe. Poleg tega HP uporablja sisteme za zaznavanje in preprečevanje omrežnih vdorov (NIDS/NIPS), ki ga vse dni v tednu spremljamo in upravljamo 24 ur dnevno.

11. Komunikacijska varnost

    Komunikacijska varnost zagotavlja varstvo podatkov v poslovnih omrežjih. To vključuje namestitev in upravljanje varnostnih komponent omrežja (npr. požarne zidove), ločevanje omrežij ter ukrepe za spletno filtriranje in ravnanje z e-pošto. Poleg tega vključuje nadzor in upravljanje komunikacijskih poti za odkrivanje in preprečevanje nepooblaščenega dostopa ali podatkovnih kršitev.

12. Sistemska varnost

    HP-jev pravilnik določa varno razvojno metodologijo za sisteme in programsko opremo skozi njihovo celotno življenjsko dobo. Življenjski cikel za razvoj programske opreme zajema sprožitev postopka, razvoj/pridobitev, izvedbo, delovanje in ukinitev. Ocenjuje se vpliv vseh komponent sistema na splošno varnost. HP je vzpostavil nadzorne ukrepe za transakcije aplikacijskih storitev, vključno s preverjanjem poverilnic uporabnikov, digitalnimi podpisi, šifriranjem, varnimi komunikacijskimi protokoli ter shranjevanjem podrobnosti o transakciji v ustreznem varnostnem območju omrežja. Izvajajo se tudi redni pregledi, ali obstajajo notranje ranljivosti.

13. Tretje osebe in podizvajalci

    HP ima postopke za izbiro podizvajalcev, ki ustrezajo celovitim pogodbenim varnostnim zahtevam. Za ustrezne dobavitelje, ki obdelujejo podatke HP-ja ali strank ali imajo dostop do HP-jevega omrežja HP-jev oddelek za kibernetsko varnost izvede oceno tveganja za potrditev programa informacijske varnosti s fizičnimi, tehničnimi in upravnimi zaščitnimi ukrepi. Preden lahko dobavitelj dostopa do HP-jevih podatkov, mora opraviti to ocenjevanje.

14. Upravljanje dogodkov, povezanih z informacijsko varnostjo

    HP ima obsežen proces upravljanja kibernetskih dogodkov, ki opisuje namen, obseg, vloge, odgovornosti, vodstvene zaveze, organizacijsko usklajevanje, postopke izvajanja in preverjanje skladnosti. Ta proces vsakoletno pregledamo in posodabljamo. Ekipa za odziv na kibernetske dogodke, vključno s HP-jevim osebjem za kibernetsko varnost, usposobljenim za odzivanje in krizno upravljanje, izvaja redne temeljite preglede procesov in morebitnih incidentov ali dogodkov.

15. Upravljanje kontinuitete poslovanja

    HP-jev globalni program za kontinuiteto poslovanja zagotavlja celovito kontinuiteto skozi sodelovalne, standardizirane in dokumentirane postopke načrtovanja. Podjetje redno izvaja svoje načrte za kontinuiteto poslovanja za zagotovitev učinkovitosti ter vse načrte preskuša in posodablja vsaj enkrat letno. Poleg tega se vse osebje, vključeno v načrt za kontinuiteto poslovanja, ustrezno usposablja.

16. Skladnost z zakonodajo

    Skladnost z zakonodajo oblikuje HP-jev pristop k izpolnjevanju zakonskih, pogodbenih in internih pričakovanj za učinkovit program informacijske varnosti. Redna preverjanja informacijske varnosti zagotavljajo, da so protokoli vgrajeni v poslovanje posameznih poslovnih skupin. S postopki preverjanja se posodabljajo tudi dokumenti, da odražajo trenutne pravne obveznosti glede na spreminjajoče se zahteve.

17. Payment Card Industry

    Ogrodje Payment Card Industry (PCI) je vodilo za HP-jev pristop k doseganju skladnosti s PCI, saj podaja oris poslovnih odgovornosti in varnostnih nadzornih ukrepov, usklajenih s PCI DSS. Z namestitvijo in vzdrževanjem ukrepov omrežne varnosti, kot so požarni zidovi, HP zagotavlja, da ustreza zahteve za skladnost PCI.

18. Varnost izdelkov HP

    Varnost izdelkov HP vključuje nujne prakse za zaščito izdelkov HP, kot so podpisovanje kode, upravljanje varnostnih ranljivosti izdelkov, izdajanje varnostnih biltenov in poročanje o varnostnih težavah. Ti ukrepi zagotavljajo, da so HP-jevi izdelki še naprej varni in zanesljivi za uporabnike. Varnost izdelkov je v HP-ju izjemnega pomena, saj pomaga ohraniti zaupanje strank in ščiti pred morebitnimi grožnjami.

19. Varnost storitev HP

    Varnost storitev HP zajema prakse, nujne za zaščito storitev, ki jih HP zagotavlja strankam. Ta pravilnik obravnava različna področja varnosti storitev, vključno s tistimi, ki gostujejo v HP-jevi infrastrukturi ali pri drugih ponudnikih ter v okoljih, ki jih gostijo stranke. Ti ukrepi zagotavljajo, da so HP-jeve storitve še naprej varne in zanesljive za uporabnike. HP z uvajanjem zanesljivih varnostnih postopkov zagotavlja varnost in celovitost svojih izdelkov in storitev ter spodbuja varno in zaupanja vredno okolje za vse uporabnike.