POLITIKA INFORMACIJSKE VARNOSTI TEHNOLOGIJE

Kazalo

1. NAMEN

Namen te politike je zagotoviti organiziran sistem varovanja informacij, skladen s strategijo in cilji TBP. S politiko zagotavljamo zahtevano celovitost, razpoložljivost in zaupnost informacij ter izvajamo ukrepe in kontrole za obvladovanje informacijskih varnostnih tveganj. Ti ukrepi in kontrole vključujejo politike, pravila, procese, postopke, organizacijsko strukturo in druge, za informacijsko varnost pomembne, elemente.

2. POLITIKA

2.1. POLITIKA NA PODROČJU KONČNIH NAPRAV UPORABNIKOV

Vse naprave, ki se vključujejo v IKT okolje TBP, morajo biti registrirane. Nameščanje programske opreme na te naprave je dovoljeno le skrbnikom.
Naprave morajo biti redno posodabljane s popravki, ki jih objavi proizvajalec operativne ali aplikacijske programske opreme.
Vse naprave morajo imeti nameščeno zaščito proti zlonamerni programski opremi (anti-virus, anti-malware). Kjer to ni mogoče, je potrebno posebej paziti pri uporabi.
Uporaba mobilnih končnih naprav kot so prenosni računalniki, tablice ali pametni telefoni, predvsem zaradi povečane možnosti kraje ali izgube predstavlja za TBP povečano varnostno tveganje. Na te naprave je treba še posebej paziti predvsem v okolju z veliko koncentracijo ljudi. V takih okoljih je treba biti še posebej pozoren na ljudi za svojim hrbtom, predvsem pri vpisovanju gesel.
Naprave morajo biti fizično zaščitena pred krajo. Opremo, ki vsebuje občutljive in/ali pomembne poslovne informacije se ne sme puščati nenadzorovane; kjer je mogoče, jo je potrebno zakleniti v varen prostor. Ob vsaki zapustitvi prenosne naprave, je to potrebno zakleniti oziroma nastaviti avtomatično zaklepanje po njeni 5 minutni ne uporabi. Izjemo predstavljajo pametni telefoni in tablice, kjer je avtomatično zaklepanje nastavljeno na 1 minuto.
Kadar se naprave zaradi različnih razlogov pušča v osebnem avtomobilu, mora biti le-ta pospravljena v pokrit prtljažni prostor avtomobila tako, da je skrita očem. Če je le mogoče, se takih naprav v avtomobilu ne pušča nenadzorovanih.
Kadar se naprave izven lokacije TBP priključuje v javna omrežja, je potrebno posebej paziti na varnost.
TBP ne dovoljuje lastnih naprav (BYOD-Bring your own device). Za vsako izjemo je potrebno pridobiti potrditev skrbnika omrežja. Pri uporabi naprav BYOD se mora uporabnik strinjati, da TBP lahko nadzoruje napravo. Naprava BYOD mora omogočati ločevanje poslovno in zasebno uporabo. Če to ni mogoče, TBP nadzoruje tudi zasebni del naprave.

Pri uporabi naprav:
- je potrebno izvajati postopke za odkrivanje zlonamerne programske opreme, ki jih je potrebno redno posodabljati.
- je potrebno izvajati postopke za redno posodabljanje popravkov (PATCH) za operacijske sisteme,
- je potrebno izvajati namestitev in postopke za redno posodabljanje servisnih popravkov (service pack) za operacijske sisteme,
- je potrebno nastaviti zaščito naprave: naprava naj se v primeru 60 minut neaktivnosti samodejno zaklene (ohranjevalnik zaslona saver z geslom); izjema so pametni telefoni in tablice z nastavitvijo zaklepanja po 1 minuti neuporabe,
- *ob vsaki zapustitvi svojega delovnega mesta mora zaposleni zakleniti računalnik. To stori, npr., z uporabo tipke Windows + L,*
- prenosna naprava, s katero se dostopa do omrežja TBP, mora imeti aktivna pravila za povezovanje v in iz omrežja (osebne požarne pregrade) in programsko opremo za zaščito pred programsko opremo za vohunjenje,
- prenosna naprava, s katero se dostopa do omrežja TBP, ne sme biti hkrati priključena na javno omrežje in na omrežje TBP (ang.: dual homing),
- se mora obvezno uporabljati gesla, ki morajo biti v skladu s politiko gesel za kakršenkoli dostop do podatkov iz teh naprav
- je potrebno zagotoviti ustrezno šifriranje informacij, ki se nahajajo na napravi.

Procesi, ki niso nujno potrebni za delovanje prenosne naprave v smislu delovanja za službene namene, so onemogočeni do najvišje možne mere. Kontrola prometa odjemalcev v omrežju se preverja na notranjih in zunanjih požarnih pregradah, kjer se nepotrebni promet oziroma vsebine tudi filtrira in blokira.
Zaposleni morajo biti informirani o pravilni uporabi mobilnih naprav in brezžičnega omrežja. Odgovorni so za varovanje podatkov, ki se nahajajo na teh napravah ali za podatke do katerih se preko teh naprav lahko dostopa. Prav tako odgovarjajo tudi za naprave same, v smislu varovanja pred krajo oziroma nepooblaščeno uporabo.
Za izvajanje varnostnega nadzora TBP uporablja primerna orodja za izvajanje informacijskih varnostnih politik.

2.2. UPRAVLJANJE POSEBNIH PRAVIC DOSTOPA

Posebni dostopi so po svoji funkcionalnosti privilegirana vrsta dostopa in s tem predstavljajo večja tveganja. Posebne dostope dobijo uporabniki, ki prevzamejo naloge upravljanja posameznega sistema (administratorji). Vsi posebni dostopi morajo biti jasno vezani na posameznega uporabnika. Določitev nivoja posebnega dostopa je v pristojnosti neposrednega vodje zaposlenega ali skrbnika vira.
Vsi uporabniki morajo imeti omogočen dostop do IKT sistema TBP brez privilegiranega načina. Privilegirani uporabniški računi so ločeni od standardnih uporabniških računov. Zanje velja posebna politika gesel. Privilegirani dostopi se redno spremljajo.
Za začasne privilegirane dostope je potrebno določiti čas veljave in samodejno deaktivacijo.
TBP ima za potrebe upravljanja sistemov super-uporabniške račune. Identiteta in geslo za tak račun se hrani v zapečateni kuverti na varnem mestu. Super-uporabniški računi se uporabijo le v izjemnih primerih (nedosegljivost administratorjev, zaklenjeni privilegirani računi…). Za vsako uporabo super.uporabniškega računa je potrebno pripraviti ustrezen zapis. Po vsakokratni uporabi super-uporabniškega računa je obvezna menjava gesla.

2.3. OMEJITEV DOSTOPA DO INFORMACIJ

V TBP je dostop do informacij omejen s potrebo po vedenju po načelu najmanjših potrebnih pravic. Dostop do informacijskega sistema in pomembnih virov je omogočen z dodeljevanjem dostopnih pravic uporabnikom. Dostop do informacij v IKT sistemu brez avtentikacije je onemogočen.
Pravice se opredeli tako za dostop do informacij kakor tudi za obdelave le-teh.

2.4. NADZOR DOSTOPA DO PROGRAMSKE IZVORNE KODE

Vsa izvorna koda TBP se mora hraniti v namenskem sistemu za hranjenje izvorne kode. Potrebno je ustrezno upravljanje različic. Dostop do repozitorija izvorne kode mora biti ustrezno omejen. Onemogočeno mora biti nepooblaščeno spreminjanje izvorne kode. Vse spremembe morajo biti skladne z zahtevami, opisanimi v postopku upravljanja sprememb.

Pri izvorni kodi, ki jo razvija zunanji izvajalec, je potrebno opredeliti lastništvo, hranjenje in zaščito izvorne kode - ESCROW agreement (hranjenje kode pri nevtralni tretji stranki).

2.5. VARNI POSTOPKI PRIJAVE

Uporabnik dostopa do informacijskega sistema in pomembnih virov s pomočjo enega ali kombinacije naslednjih načinov:
- Uveljavljanje pravice dostopa na osnovi tega, kaj uporabnik ve (npr. uporabniško ime in pripadajoče geslo).
- Uveljavljanje uporabniške pravice na osnovi tega, kaj uporabnik ima (npr. identifikacijska kartica, ključ, žeton).
- Uveljavljanje pravice dostopa na podlagi tega, kar uporabnik je (npr. biometrija).

Uporabnik, ki pridobi pristopno pravico na podlagi enolično razpoznavnega uporabniškega imena ali na podlagi drugega ustreznega načina nedvoumnega razpoznavanja uporabnika, je odgovoren za vse dejavnosti, ki so registrirane (revizijska sled) z njegovim uporabniškim imenom. Svoje metode razpoznavanja uporabnik ne sme posredovati drugi osebi. V primeru upravičenega razkritja gesla uporabnik poskrbi za takojšnjo menjavo gesla.

Za vzdrževanje učinkovitega nadzora dostopa do informacijskega sistema, lastnik posameznega sistema redno kontrolira uporabniške pravice.
Vsi sistemi za prijavo morajo onemogočati vpogled v vnosno polje. Pri dostopih do pomembnih informacij je potrebno dodati posebno opozorilo uporabnikom, da dostopajo do takih informacij.
Sporočila o napačni prijavi ne smejo razkrivati informacij.
Avtentikacijske informacije se po omrežjih ne smejo prenašati v čistopisu.

2.6. UPRAVLJANJE ZMOGLJIVOSTI

Za vse dejavnosti so definirane zahteve glede zmogljivosti sistemov, človeških virov in infrastrukture. Sisteme se redno spremlja, tako da se lahko pravočasno identificira potencialne težave v zvezi z njihovo zmogljivostjo. Osnova za preverjanje primernosti zmogljivosti opreme je popis sredstev.
Sisteme se tudi prilagaja, tako da se na ta način zagotovi njihovo razpoložljivost in če se le da, poveča njihovo učinkovitost. Na ta način se izogne možnim ozkim grlom, kar lahko ogrozi sistemsko varnost ali samo izvajanje storitev.

Navedeno velja tudi za vse na novo uvedene dejavnosti TBP, ko se načrtuje potrebne zmogljivosti sistemov.

V načrtih glede bodočih zahtev na področju zmogljivosti, se upošteva nove poslovne in sistemske zahteve, kot tudi trende glede zmogljivosti v svetu.

Posebno pozornost se namenja vsem sredstvom, katerih nabava poteka relativno dolgo časa in je povezana z visokimi stroški.

Vsi popravki in nadgradnje se morajo najprej opraviti v testnem/potrjevalnem okolju. Pregledati se mora delovanje in pravilnost nadgrajenega testnega sistema. Če niso ugotovljene napake in če sistem ustreza vsem varnostnim kriterijem, se lahko opravi nadgradnja na produkcijskem sistemu oziroma prevzem v produkcijo.

Lastniki procesov in kadrovska služba je odgovorna za spremljanje zmogljivosti človeških virov in pravočasno opozoriti na potrebo po novih zaposlitvah in/ali izobraževanjih.

2.7. KONTROLE PROTI ZLONAMERNI PROGRAMSKI OPREMI

V lokalnem računalniškem omrežju in na ostalih računalniško komunikacijskih napravah TBP se mora zagotavljati trajna zaščita pred zlonamerno programsko opremo, kar zajema odkrivanje in onemogočanje:
- računalniških virusov,
- trojanskih konjev,
- programov za motenje,
- programskih bomb,
- razširjanja lažnih preplahov in
- nezaželene pošte (SPAM).

Pri tem se mora zaščititi:
- vse komponente mrežnega operacijskega sistema in operacijskih sistemov delovnih postaj,
- aplikativno programsko opremo na strežnikih in delovnih postajah,
- podatke,
- programsko kodo in nastavitve strojne opreme, ki niso fizično zaščitene pred pisanjem.

Zaščita lokalnega omrežja in ostalih računalniško komunikacijskih naprav TBP mora biti popolna, kar pomeni, da so zaščiteni vsi strežniki, vse delovne postaje, vsi prenosni računalniki, ki se v omrežje priključijo občasno, in vse samostojne delovne postaje, ki v omrežje niso priključene.

Strežniki in delovne postaje morajo biti zaščiteni s programsko opremo za protivirusno zaščito. Nameščena programska oprema mora omogočati preverjanje ob dostopu in preverjanje na zahtevo. Omogočati mora redno, najmanj enkrat mesečno, nadgradnjo in izredne (vmesne) nadgradnje za posamezne vrste virusov.
Postopki nameščanja, posodabljanja in preverjanja delovanja programske opreme za protivirusno zaščito se morajo izvajati skladno s postopki, ki so določeni v poglavju o postopkih.
Izredni dogodki se morajo obravnavati v skladu s postopki, ki so določeni za hitro ukrepanje in razkuževanje v poglavju o postopkih.
Zasebne naprave (BYOD) morajo zadostiti zahtevam te kontrole v enaki meri kot naprave v lasti TBP.

Na požarnih pregradah TBP morajo biti vzpostavljeni vsi potrebni mehanizmi, ki preprečujejo oziroma omejujejo odvečen mrežni promet. Zaprti morajo biti vsi protokoli in/ali vrata, ki so nepotrebni za izvajanje funkcionalnosti predpisane in za splošno uporabo odobrene elektronske pošte, dostopa do interneta in/ali v TBP dopustnih oddaljenih dostopov.

Uporabnik ne sme onemogočiti protivirusne zaščite na delovni postaji, programska oprema za protivirusno zaščito pa naj bo nameščena tako, da v največji možni meri preprečuje možnost, da bi jo uporabnik onemogočil.

2.8. UPRAVLJANJE TEHNIČNIH RANLJIVOSTI

V TBP pravočasno pridobimo vse informacije o tehničnih ranljivostih našega informacijskega sistema. Ob tem ocenimo izpostavljenost različnim ranljivostim ter sprejmemo ustrezne ukrepe za obravnavanje tveganj. Učinkovit nadzor tehničnih ranljivosti zagotavljamo z ažurnim in popolnim popisom informacijskih sredstev. V zvezi s prepoznavanjem tehničnih ranljivosti izvajamo naslednje aktivnosti:

- opredelimo in vzpostavimo vloge in odgovornosti, povezane z nadzorom tehničnih ranljivosti, vključno s spremljanjem ranljivosti in oceno tveganja,
- za vsa informacijska sredstva zagotovimo potrebne vire, ki jih bomo uporabljali za prepoznavanje posameznih tehničnih ranljivosti,
- definiramo časovni potek odzivov na obvestila o možnih pomembnih tehničnih ranljivostih,
- ko ugotovimo možno tehnično ranljivost, določimo tveganja in potrebne ukrepe, ki vključujejo posodabljanje in/ali uvedbo ustreznih kontrol,
- popravke testiramo in ovrednotimo, preden jih namestimo.

Sisteme, ki jih ogroža visoko tveganje, obravnavamo prednostno. Za upravljanje tehničnih ranljivosti so odgovorni sistemski skrbniki posameznega sistema.

2.9. UPRAVLJANJE KONFIGURACIJ

Proces upravljanja konfiguracij je upravljan. Kjer je smiselno, se pripravijo, vzdržujejo in uporabijo standardne konfiguracije.
Za le-te uporabimo orodja za upravljanje konfiguracij. Pri pripravi in konfiguriranju se naslonimo na priporočila proizvajalca in dobre prakse, kakor tudi varnostne zahteve TBP.
Število privilegiranih računov je minimizirano. Privzeti računi so ali onemogočeni ali pa se jim dodeli dovolj kompleksno geslo.
Vse funkcionalnosti ki jih ne uporabljamo, se onemogočijo.
Samo privilegirani računi lahko upravljajo z neposrednimi dostopi do podatkovnih baz.
Privzete informacije za identifikacijo je potrebno spremeniti.
Standardne konfiguracije se varno hrani in omejuje dostope.
Vse spremembe konfiguracij se izvajajo skozi proces upravljanja sprememb. Zagotoviti moramo upravljanje različic. Zagotoviti moramo sinhronizacijo ur na vseh napravah.

Spremembe konfiguracij je potrebno nadzorovati z ustreznimi orodji za sledenje spremembam.

Pri konfiguracijah moramo zagotoviti licenčno skladnost.

2.10. BRISANJE INFORMACIJ

Informacije, ki niso več potrebne za izvajanje poslovnih procesov, je potrebno izbrisati. Pri rokih hrambe upoštevamo veljavno zakonodajo.
Za vsako izločanje in brisanje mora obstajati zapis, ne glede na to, ali brisanje izvaja TBP ali zunanji izvajalec.

V izogib tehničnim težavam pri brisanju (selektivno brisanje in brisanje vseh kopij) je potrebno že pri klasifikaciji in upravljanju informacij predvideti omejitve pri brisanju (varnostne kopije, arhivi, skupni mediji, idr.).

Glede na pomembnost informacij izberemo ustrezen način brisanja (uničevanje fizičnih dokumentov, uničevanje medijev za hrambo, nepovratno brisanje z večkratnim prepisovanjem…)

V primeru servisnih posegov in iznosu opreme, se mediji za shranjevanje odstranijo iz naprav. Če to ni mogoče, je potrebno ustrezno zagotoviti kontrole pred nenadzorovanim dostopom do informacij.

2.11. VARNOSTNO KOPIRANJE INFORMACIJ

V TBP izdelujemo varnostne kopije informacij in programske opreme, ki jih redno testiramo. Zagotovili smo ustrezne zmogljivosti za varnostno kopiranje, tako da lahko po okvari na nosilcu podatkov ali kritičnem incidentu rešimo vse pomembne informacije in programsko opremo. S tem namenom nosilce varnostnih kopij redno testiramo, tako da zagotovimo njihovo zanesljivost. Varnostne kopije tudi ustrezno fizično in okoljsko ščitimo.
Varnostne kopije shranjujemo tudi na oddaljeni lokaciji, ki je dovolj daleč, da incident na lokaciji nanjo ne more vplivati.
Varnostno kopiranje se v TBP izvaja samodejno, tako da je olajšan proces kopiranja in obnove. Pred vpeljavo samodejno varnostno kopiranje ustrezno testiramo, redno pa ga testiramo tudi po sami uvedbi.

Za varnostno kopiranje podatkov se uporablja namenska strojna in programska oprema. Konfiguracije se hranijo v samem sistemu. Parametri varnostnega kopiranja (pogostost, število verzij, retenzija…) je nastavljena skladno s poslovnimi zahtevami, ugotovljenimi preko ocene vpliva na poslovanje. Vsa programska oprema za varnostno kopiranje podatkov mora biti prilagojena (nastavljena) tako, da zagotavlja predpisani nivo zaščite.
Programsko opremo za centralno varnostno kopiranje podatkov sme nameščati in/ali posodabljati le administrator varnostnega kopiranja in zunanji ali notranji izvajalci, ki so zadolženi in usposobljeni za vzdrževanje naprav izven standardnega programskega okolja.

Administrator varnostnega kopiranja je dolžan redno preverjati delovanje sistema za varnostno kopiranje podatkov in najmanj enkrat tedensko tudi delovanje sistema za obveščanje in beleženje dogodkov.

Kadar se ugotovi potreba po dodatnem enkratnem ali rednem varnostnem kopiranju podatkov, je to potrebno sporočiti odgovorni osebi (opredeliti natančneje osebo / funkcijio) . Ta lahko predlog odobri ali pa zavrne v odvisnosti od razpoložljivosti sistema za izvajanje varnostnega kopiranja.

Vsi zaposleni morajo biti seznanjeni s pogoji izvajanja varnostnega kopiranja. Ob tem se morajo posebej zavedati dejstva, da se podatki, shranjeni lokalno na delovnih postajah, varnostno ne shranjujejo. Vse pomembne podatke so zaposleni dolžni shranjevati na mesta, ki varnostno kopiranje zagotavljajo.

2.12. RAZPOLOŽLJIVOST NAPRAV ZA OBDELAVO INFORMACIJ

Za vse kritične sisteme, ki jih TBP prepozna preko ocene vpliva na poslovanje in ocene tveganja, je potrebno zagotoviti ustrezno razpoložljivost. V ta namen se uporabi podvajanje opreme, nameščanje gruč, deljenje bremen, rezervna oprema na skladišču, rezervna lokacija ali ustrezna pogodba z dobaviteljem, ki zagotavlja razpoložljivost nadomestne opreme.

2.13. BELEŽENJE DOGODKOV

Vse dejavnosti uporabnikov, izjeme v delovanju sistemov in dogodkih, povezanih z informacijsko varnostjo, se beležijo.
Obseg določimo z oceno tveganja, v osnovi pa dnevniški zapisi obsegajo:

- uporabniške identifikacije,
- datume, ure in podrobnosti o ključnih dogodkih, kot sta prijava in odjava iz sistema,
- identiteto ali lokacijo terminalov,
- zapise o uspešnih in zavrnjenih poskusih dostopa do sistema,
- zapise o uspešnih in zavrnjenih poskusih dostopa do podatkov in drugih virov,
- spremembe pri konfiguraciji sistema,
- uporabo privilegiranih računov,
- uporabo sistemskih pripomočkov in aplikacij,
- datoteke, pri katerih je prišlo do dostopa, in vrsto dostopa,
- omrežne naslove in protokole,
- alarme, ki jih sproži sistem za nadzor dostopa,
- aktiviranje in deaktiviranje zaščitnih sistemov.

Ker dnevniški zapisi praviloma vsebujejo občutljive in/ali zaupne osebne podatke, zagotavljamo zaščito zasebnosti v skladu s politiko varovanja osebnih podatkov.
Beleženje se izvaja najprej s privzetimi vrednostmi proizvajalca opreme, ki se po potrebi prilagodijo.
Za beleženje uporabimo centralni sistem za beleženje informacij.

Dnevniki delovanja sistemov vsebujejo številne informacije, ki so za vodenje varovanja nepomembne. Da bi lahko prepoznali dogodke, ki so pomembni, uporabljamo ustrezne sistemske pripomočke, filtre ali orodja za pregledovanje in racionaliziranje zapisov v dnevnikih.
Informacije v dnevnikih ščitimo pred nepooblaščenimi spremembami ali brisanjem s kontrolo dostopa in beleženjem spreminjanja ali brisanja datotek.
Nekatere dnevnike tudi arhiviramo; na podlagi zahteve stranke, druge regulative ali potreb po zbiranju in shranjevanju dokazov.
Da bi preprečili okvaro zapisov v dnevnikih, poskrbimo, da ne pride do prekoračitev shranjevalnih zmogljivosti nosilca, na katerem so shranjeni posamezni dnevniki.

Posebno pozornost posvečamo beleženju dogodkov, povezanih s privilegiranimi računi.

Datoteke dnevniških zapisov strežnikov mora dnevno pregledovati sistemski administrator.
Datoteke dnevniških zapisov se morajo varnostno kopirati.
Onemogočeno je ročno brisanje dnevniških zapisov.

2.14. USKLADITEV UR

Sinhronizacija ur je avtomatska s protokolom omrežnega časa, tako da so vse ure na strežnikih in delovnih postajah usklajene.
Pravilna nastavitev računalniške ure je pomembna za zagotovitev natančnosti dnevnikov, ki bi jih lahko uporabili pri preiskavah ali kot dokazno gradivo v pravnih in disciplinskih postopkih. Nepravilni zapisi v dnevnikih lahko onemogočijo takšne postopke in niso verodostojni dokazi. Posebno pozornost pri sinhronizaciji posvetimo oblačnim storitvam.

Strežniški sistemski čas se sinhronizira na 3.si.pool.ntp.org, 0.europe.pool.ntp.org, 2.europe.pool.ntp.org.

2.15. UPORABA POSEBNIH POMOŽNIH PROGRAMOV

V delovnih oz. operativnih navodilih so opredeljeni podatki o tem kdo, kdaj in katere pomožne programe je dovoljeno uporabljati. Posebne pomožne programe lahko uporabljajo izključno skrbniki sistemov. Vsaka uporaba posebnega pomožnega programa mora biti zabeležena.

2.16. NAMEŠČANJE PROGRAMSKE OPREME NA OPERACIJSKE SISTEME

Nenadzorovano nameščanje programske opreme s strani uporabnikov povečuje varnostna tveganja in ranljivost IKT okolja. Posledica tega je lahko izguba celovitosti, zaupnosti in razpoložljivosti informacij, poveča se verjetnost incidentov, lahko pa pride tudi do kršitev avtorskih in sorodnih pravic.
V TBP lahko uporabniki sami namestijo le naslednje vrste programske opreme:

- posodobitve obstoječe programske opreme,
- varnostne popravke obstoječe programske opreme.

Izrecno je prepovedano nameščanje kakršnekoli programske opreme, katere izvor je neznan in nepreverjen s strani sistemskih administratorjev.
Pri določenih uporabnikih, za katere velja povečano tveganje, upoštevamo načelo najmanjših možnih pravic. Z ustrezno konfiguracijo informacijske opreme uporabnikom onemogočimo nameščanje kakršnekoli programske opreme. Za nameščanje programske opreme na informacijsko opremo uporabnikov je v TBP zadolžena služba IT.

Služba IT je odgovorna za preverjanje programske opreme pred namestitvijo (licenciranje, testiranje, konfiguracija).

Pri posodobitvah operacijskih sistemov je potrebno pripraviti povrnitvene procedure, testni sistem ter testiranje z ustreznimi zapisi.

2.17. VARNOST V OMREŽJIH

V TBP so uvedene različne kontrole, ki zagotavljajo varovanje informacij oziroma podatkov v omrežju.
Za upravljanje in nadzor omrežja je odgovoren skrbnik omrežja. Skrbnik je odgovoren za pripravo postopkov in navodil za upravljanje omrežne opreme. Skrbi tudi za ažurno shemo omrežja.

Glede na vrsto informacij, ki se posredujejo preko določenih delov omrežij ter namenom in dostopnosti le-teh, se vzpostavi dodatne kontrole.
Omrežja za goste so fizično ločena od poslovnega omrežja.
Proizvodna omrežja so ločena od ostalih omrežij in imajo omejen dostop do interneta.

Robna požarna pregrada, ki ločuje promet med zunanjim okoljem in notranjim omrežjem, mora biti ustrezno zmogljiva, nameščena, upravljana in nadzorovana.

V omrežje, razen v omrežje za goste, se lahko priključi samo odobrene naprave.
Občutljivi podatki, ki se prenašajo preko omrežja, morajo biti kriptirani z ustrezno metodo.

Upravljanje omrežnih naprav se loči od ostalih omrežij (glej 2.19).

2.18. VARNOST OMREŽNIH STORITEV

Vsi dostopi do pomembnih/občutljivih informacij morajo biti ustrezno zaščiteni z avtentikacijo. Dostopi do kritičnih sistemov morajo biti omogočeni samo z več-faktorsko avtentikacijo. Dostopi do posameznih omrežnih storitev se po potrebi onemogočijo. Ves čas spremljamo neuspešne poskuse dostopov.
Za oddaljene dostope se uporablja izključno VPN tehnologija, odobrena s strani oddelka IT.

2.19. LOČEVANJE OMREŽIJ

Glede na oceno tveganja ter performančne zahteve se uporabi ločevanje omrežja v ločene logične omrežne segmente. Ločujemo omrežja za goste, poslovna, proizvodna, upravljalska in servisna omrežja. Po potrebi se lahko posamezno omrežje dodatno ločuje. Za vzdrževanje sheme omrežja je odgovoren skrbnik omrežja (glej 2.17).
Med omrežji, ki se povezujejo, se vgradi varnostni prehod oziroma požarni zid, s katerim se nadzoruje dostop in pretok informacij.
Glede na potrebo po vedenju se prehodi med segmenti omejujejo.

2.20. SPLETNO FILTRIRANJE

TBP ima opredeljene dovoljene oz. nedovoljene spletne aktivnosti. Uporabnike je potrebno o tem obvestiti in jih ustrezno usposobiti. Za filtriranje se uporabljajo namenska orodja. V TBP je prepovedan dostop do spletnih strani z naslednjo vsebino:

- Kriminal
- Izogibanje proxy
- Igre na srečo
- Strani s sovražno vsebino (rasno, politično)
- Orožarske strani
- Pornografija
- Strani s škodljivo vsebino
- Strani, ki delijo nezakonite vsebine
- CnC strežniki

2.21. KRIPTOGRAFIJA

Kriptografske kontrole uporabljamo za doseganje naslednjih varnostnih ciljev:

- zaupnost informacij,

- celovitost informacij,
- razpoložljivost informacij.

Kriptografske metode uporabljamo pri informacijah v gibanju in informacijah v mirovanju. Vedno upoštevamo zakonske zahteve in omejitve ter veljavne mednarodne standarde.
Posebno pozornost posvečamo zaščiti in distribuciji šifrirnih ključev.

Za upravljanje ključev je odgovoren oddelek IT. Za odločitev o kriptografskih kontrolah je odgovorno vodstvo TBP.
V politiki so opredeljene vloge in odgovornosti. Upoštevana je veljavna zakonodaja, predpisi in mednarodni standardi s tega področja.

Na osnovi ocene tveganja določimo potrebno stopnjo zaščite, pri tem določimo vrsto, moč in kvaliteto šifrirnega algoritma,

Kriptiranje podatkov se brez izjeme uporabi, kadar se preko naprav ali telekomunikacijskih linij prenašajo občutljive oziroma pomembne ter zaupne informacije.
Odločitev o tem, katere zaupne podatke je potrebno kriptirati, sprejme vodstvo TBP in to opredeli s klasifikacijo informacij, razen tam, kjer je uporaba kriptografije obvezna z zakonom.
V kolikor posameznik, ki izmenjuje podatke s stranko, presodi, da so ti izredno pomembne in zaupne narave, jih lahko zaščiti s kriptiranjem.

Za zaposlenega na delovnem mestu, ki potrebuje službeno digitalno potrdilo, vodja organizacijske enote poda zahtevek v IT, ki poskrbi za izpolnitev ustreznih obrazcev in pošiljanje pristojnemu organu.
Ko zaposleni prejme digitalno potrdilo, ga kadrovska služba vpiše v ustrezno evidenco. Nosilec digitalnega potrdila je sam odgovoren za njegovo pravočasno podaljšanje.
Ob prekinitvi delovnega razmerja je kadrovska služba dolžna vodjo organizacijske enote opozoriti, da poskrbi za preklic digitalnega potrdila. Prav tako je dolžna vodjo organizacijske enote opozarjati na ostale spremembe, ki jih je treba sporočiti pristojnemu organu.

2.22. VARNA RAZVOJNA POLITIKA

Varen razvoj je pogoj za izgradnjo varne storitve, arhitekture, programske opreme in sistema.
Za zagotavljanje varnega razvoja:

- ločujemo razvojno, testno in proizvodno okoljo (glej 2.28);
- za razvoj uporabljamo priznana orodja in programske jezike, ki zagotavljajo varne razvoj
- že v fazi načrtovanja opredelimo varnostne zahteve
- uporabljamo sistemsko in varnostno testiranje, kot je regresijsko testiranje, skeniranje kode in penetracijski testi (glej 2.26);
- uporabljamo varna skladišča za izvorno kodo in konfiguracijo (glej 2.4 in 2.9);
- ustrezno upravljamo različice (glej 2.29)
- razvijalci morajo biti ustrezno usposobljeni in izobraževani;

2.23. APLIKACIJSKE VARNOSTNE ZAHTEVE

Dostop do vseh aplikacij je omogočen le z ustrezno avtentikacijo. Za dostop do kritičnih informacij se uporablja več-faktorska avtentikacija. Vse aplikacije morajo imeti možnost granuliranega upravljanja pravic dostopa. Priporoča se uporaba skupinskih pravic. Vse aplikacije morajo biti ustrezno varno razvite brez znanih ranljivosti (npr. OWASP Top 10). Obdelava informacij mora biti zakonita. Podatki morajo biti ustrezno zaščiteni pri obdelavi, prenosu in v mirovanju.
Vnosna polja morajo imeti ustrezne validacije, da se prepreči škodljive vnose.
Za kritične transakcije je potrebno deljenje dolžnosti (glej Politiko organizacije informacijske varnosti 2.1.2.).

2.24. NAČELA VARNEGA SISTEMSKEGA INŽENIRINGA

Pri načrtovanju informacijskih sistemov je potrebno določiti varnostne zahteve, ki se vgradijo v sistem (ločevanje vlog, avtentikacija, kriptiranje, granulirane pravice, onemogočanje nepotrebnih storitev…). Za informacijske sisteme se v TBP uporabi znane rešitve ter upošteva dobre prakse.
Spremembe informacijskih sistemov se preverja na notranjih presojah, kjer se ugotavlja, ali so bile spremembe primerno vpeljane in zadostujejo primernemu nivoju informacijske varnosti. TBP za preverjanje uporablja predvsem mehanizme varnostnih pregledov.

Varnostni pregled informacijskega sistema se izvaja enkrat letno. Namen pregleda je ugotoviti stopnjo varnosti in ranljivosti informacijskih sistemov. Varnostni pregled obsega:
- preverjanje zasnove informacijskega sistema s stališča varnosti,
- analizo konfiguracij strežnikov in mrežnih naprav,
- analizo ustreznosti uporabljenih varnostnih mehanizmov,
- preverjanje varnostne politike požarnih pregrad,
- preverjanje varnostne politike sistemov za zaznavanje in preprečevanje vdorov,
- varnostno preverjanje poslovnih aplikacij.

Obseg varnostnega pregleda določa vodstvo. Rezultate varnostnega pregleda se dokumentira v zapisniku vodstvenega pregleda.

2.25. VARNO KODIRANJE

Obvezna je uporaba dobrih praks razvoja programske opreme. Prepovedana je uporaba neodobrenih knjižnic in ostalih komponent programske kode neznanih virov. Za kodiranje se uporablja ustrezna orodja.
Vsi razvijalci morajo biti ustrezno izobraževani in ozaveščani.

Pred spremembami in migracijami se izdela varnostno kopija sistema, stari sistem pa se ohrani, da je možna povrnitev v prvotno stanje. Razvojno okolje mora biti ločeno od produkcijskega.

Vsa programska oprema mora ustrezati zahtevam in pogojem licenčnih predpisov.
Vse čas razvoja je potrebno uporabiti ustrezne varnostne principe (validacija polj, OWASP Top 10 …).
Načela varnega kodiranja veljajo za notranji ter zunanji razvoj.

2.26. TESTIRANJE VARNOSTI IN PREVZEM SISTEMA

Vsa programska oprema mora ustrezati zahtevam in pogojem licenčnih predpisov.
Namestitev strojne opreme mora biti izvedena s strani pooblaščenih oseb, ki skupaj s skrbniki sistemov preverijo delovanje sistema po namestitvi. Pred spremembami strojne opreme se izdela varnostno kopijo sistema, stari sistem pa se ohrani, da je možna povrnitev v prvotno stanje. Kakršnekoli spremembe na strojni opremi s strani nepooblaščenih oseb so prepovedane.
Vsa programska in sistemska oprema ter strojna oprema mora biti nameščena s strani pooblaščenih oseb in mora biti usklajena z varnostnimi zahtevami politike varovanje informacij.
Testiranje sistemov mora biti izvedeno po vnaprej opredeljenih scenarijih, kjer se določi obseg in pričakovane rezultate. Po vsakem testiranju se pripravi zapisnik, ki ga obravnava skupina za prevzem (člani projektne skupine). Odstopanja od pričakovanih rezultatov se ocenijo, pripravi se načrt popravkov, tako funkcionalnih kot varnostnih zahtev.
Za kritične aplikacije se pred prevzemom izvede vdorno testiranje. Rezultate obravnava skupina za prevzem (člani projektne skupine). Sprejemljivost sistema potrdi vodstvo TBP.

2.27. ZUNANJE IZVAJANJE RAZVOJA

Pravno razmerje z izvajalcem storitev se natančno opredeli s pogodbo. Pogodba o zunanjem izvajanju storitev predstavlja pravno podlago za dostop izvajalca do določenih podatkov oziroma informacijskih sistemov v okviru TBP in njegovo uporabo podatkov. Pred sklenitvijo pogodbe z zunanjim izvajalcem skrbnik pogodbe ugotovi, če je potrebno opraviti analizo tveganj v zvezi s predvideno pogodbo oziroma storitvijo oziroma dobavami blaga po tej pogodbi ter glede na pomen teh storitev oziroma dobav predvidi morebitne preventivne ukrepe ter zagotovi njihovo izvajanje. Pogodba mora poleg ostalih predpisanih vsebin vključevati vsaj:

- opis storitve in predviden rok trajanja oziroma dobo opravljanja te storitve; pri opisu storitve se opredelijo ciljne in tudi nesprejemljive ravni izvajanja storitev, vključno z opredelitvijo preverljivih meril za doseganje teh ravni oziroma delovni učinek ter pravica pregleda in nadzorovanja pogodbenih obveznosti, lahko tudi s strani usposobljenih tretjih oseb;
- določilo, da nesprejemljiva raven opravljanja storitve, ki se ponavlja določen čas, šteje za kršitev pogodbe;
- jasno razmejitev nalog in odgovornosti med podjetjem kot naročnikom in izvajalcem oziroma dobaviteljem;
- opredelitev obveznosti v zvezi s pravnimi zahtevami področne veljavne zakonodaje, kot so na primer predpisi na področju varovanja podatkov (npr. osebnih, tajnih...) in varstva pravic intelektualne lastnine;
- druge določbe, če so potrebne za čim bolj jasno definirano poslovno, organizacijsko, operativno in varnostno sodelovanje med izvajalcem in naročnikom.
- Pogodba mora vsebovati dogovor o spoštovanju varnostnih zahtev za izvajalce, ki so določene z varnostnimi politikami. V pogodbo se vključijo še drugi varnostni ukrepi kot:
- fizični in logični ukrepi za omejitev dostopa uporabnikom do varovanih podatkov (upravljanje z dostopnimi pravicami in nadzorom);
- struktura in oblike poročanja ter obveščanje in preiskave varnostnih dogodkov in kršitev;
- način vzdrževanja razpoložljivosti storitev v primeru izrednih dogodkov oziroma zagotavljanje primerne ravni neprekinjenega poslovanja;
- poročila o testiranjih sistemov;
- pravico do revizije pri izvajalcu.

2.28. LOČEVANJE RAZVOJNIH, TESTNIH IN PRODUKCIJSKIH OKOLIJ

Programsko opremo je treba pred namestitvijo v produkcijsko okolje ustrezno testirati v testnem okolju, pri tem pa je pomembno, da se predvidi vse okoliščine, ki se bodo pojavile v produkcijskem okolju. Pred spremembami in migracijami se izdela varnostno kopija sistema, stari sistem pa se ohrani, da je možna povrnitev v prvotno stanje.
Okolja morajo biti ločena na način, da ima vsak sistem ločeno upravljanje pravic dostopa. Po potrebi se razvojno, testno in produkcijsko okolje namesti na ločenih strežnikih in v ločenih virtualnih omrežjih.
Načini prenosa iz razvojnega v testno in produkcijsko okolje morajo biti natančno opredeljeni. Vsak prehod mora biti potrjen s strani lastnika vira.
Razvijalci ne smejo imeti dostopa do produkcijskega okolja.

2.29. UPRAVLJANJE SPREMEMB

Spremembe informacijskih sistemov lahko povzročijo nestabilnost ali povečano ranljivost glede na nameščeno različico.
Vse spremembe morajo biti načrtovane in potrjene s strani IT.
Varnostno posodabljanje je naloga IT oddelka.
Pri načrtovanju sprememb je potrebno predvideti morebitne posledice posamezne spremembe.
Vse spremembe na sistemski ali aplikativni programski opremi izvedemo le, ko za to obstaja upravičen razlog, kot je npr. zmanjšanje ogroženosti ali izboljšanje delovanja sistema.
Za izvajanje sprememb morajo biti vzpostavljeni ustrezni postopki, ki morajo biti formalizirani, nadzorovani, konsistentni med različnimi platformami in v celoti dokumentirani.
Spremembe se izvajajo v določenih terminih oz. v skladu z veljavnimi SLA (Service-level agreement) pogodbami do končnih uporabnikov,
Pred vsako izvedbo spremembe morajo biti preverjene varnostne kontrole in izvedeni postopki za preverjanje pravilnosti delovanja sistema po spremembi. Preveriti je treba, ali je kot posledica spremembe potrebna dodatna prilagoditev kateregakoli dela sistema (programska in strojna oprema, baze podatkov, datoteke …),
Vse spremembe, ki bi lahko vplivale na delovanje sistema, morajo biti, preden se izvedejo v produkcijskem okolju, preverjene v testnem okolju.
Pri vsaki zahtevani in izvedeni spremembi mora biti zagotovljeno vodenje dnevnika dela in dopolnitev dokumentacije sistema oz. njegovih sestavnih delov (popis sredstev).
Zaradi morebitne potrebe po vrnitvi sistema v prejšnje delujoče stanje (pred izvedbo spremembe) – rollback scenarij – je treba pred vsako spremembo izvesti varnostno kopiranje stanja sistema.
Namestitev kritičnih popravkov naj se izvede najkasneje v 2 dneh po objavi le-teh. Kritičnih varnostnih popravkov ni treba namestiti v primeru, ko – zaradi specifičnosti arhitekture ali načina uporabe programske opreme – varnostna luknja, ki jo kritični varnostni popravek odpravlja, ne predstavlja realne grožnje informacijskemu sistemu.

Ob izvedbi posamezne spremembe, ki vpliva na delo uporabnikov, je treba uporabnike, na delo katerih sprememba vpliva, obvestiti o začetku veljavnosti spremembe, njenem namenu in morebitnih vplivih na njihovo delo; obveščanje o predvidenih akcijah (spremembah) kot tudi o incidentih je lahko v pisni ali elektronski obliki (zadošča tudi sporočilo po e mailu).

2.30. TESTNE INFORMACIJE

Kjer je le mogoče, se za razvoj in testiranje ne uporabi realnih (produkcijskih) podatkov. Kjer to ni mogoče, je potrebno zagotoviti enak nivo varnosti v razvojnem in testnem okolju, kot velja za produkcijsko. V primeru kopiranja podatkov iz produkcijskega v testno in/ali razvojno okolje, je potrebno zagotoviti revizijsko sled. V primeru uporabe takih podatkov je potrebno poskrbeti za ustrezno brisanje le-teh takoj, ko podatki več niso potrebni.

2.31. VAROVANJE INFORMACIJSKIH SISTEMOV MED REVIZIJO

Vse revizije sistemov morajo biti načrtovane. Potek revizije mora biti usklajen med izvajalcem in vodstvom TBP.
Vsa testiranja, revizije in pregledi, tako notranji kot zunanji, morajo kar najmanj motiti delovni proces.
Obseg pregleda mora biti določen vnaprej. Vsi sodelujoči morajo biti obveščeni, da lahko prilagodijo svoj delovni proces med samo izvedbo. V primeru, da je za revizijo potreben logični dostop do informacij, se kreira namenske uporabniške račune za čas trajanja revizije. Vsi uporabniški računi morajo imeti pravico vpogleda. Onemogočiti je treba možnost spreminjanja informacij. Če se pri izvedbi revizije uporablja namenska revizijska orodja, se le-ta namesti skladno s to politiko.

Lenart, 01.03.2024

Uprava TBP d.d.
Direktor družbe

Danilo ROJKO