EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PREDSTAVITEV NAČRTA VARNOSTNIH UKREPOV

VSEBINA

Splošno

Okvir skladnosti

Pregled varnostnih ukrepov(namen in ukrepi)

UVOD IN OKVIR SKLADNOSTI

NAČELA IN POVEZAVE NA SISTEME VODENJA

- **Usklajenost z varnostnimi standardi**

Načrt temelji na mednarodnih standardih ISO/IEC 27001, ISO/IEC 27002 in NIST SP 800-53 za informacijsko varnost.

- **Cilji načrta varnosti**

Glavni cilji so zagotovitev zaupnosti, celovitosti, razpoložljivosti in avtentičnosti informacijskih sredstev.

- **Povezava z ISMS in BCMS**

Načrt se izvaja skupaj z ISMS in BCMS, vključno s ciklom PDCA za nenehno izboljševanje varnostnih ukrepov.

- **Usklajevanje z zakonodajo in regulativami**

Vzorčna dokumentacija URSIV-a upošteva zakon o informacijski varnosti in EU uredbo 2024/2690 za skladnost in upravljanje kibernetskih tveganj.

DOLOČANJE OBSEGA UKREPOV

Glede na stopnjo izpostavljenosti posameznih sredstev in storitev različnim grožnjam oziroma

prepoznanim tveganjem;

- velikost in kompleksnost organizacije;

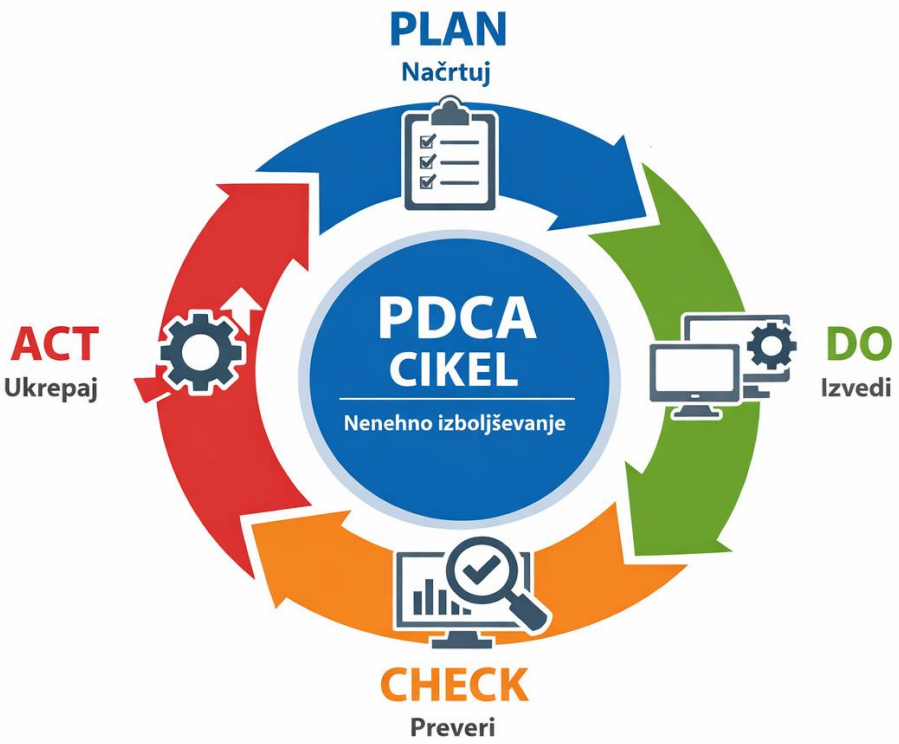
- verjetnost pojava različnih vrst incidentov ter

- potencialni vpliv incidentov na družbeno in gospodars okolje, v katerem organizacija

deluje.

Varnostni ukrepi se redno preverjajo, preizkušajo in nadgrajujejo v okviru cikla nenehnega

izboljševanja (Ang. ***Plan–Do–Check–Act***), s čimer se zagotavlja njihova skladnost, uspešnost in prilagodljivo spreminjajočim se tveganjem ter tehnološkemu razvoju.



Vir: ChatGpt

VARNOSTNI UKREPI

VARNOSTNI UKREPI

DELITEV NA:

- **Organizacijski ukrepi**
  (politike, postopki, vloge in odgovornosti, usposabljanja),
- **Tehnični ukrepi**
  (npr. večfaktorska avtentikacija, segmentacija omrežja, varovanje končnih naprav),
- **Operativni ukrepi**
  (upravljanje varnostnih kopij, testiranje obnovitve, postopki odzivanja),
- **Ukrepi varovanja sredstev in prostorov**
  (fizični dostop, nadzor prostorov).

PODPORA VODSTVA

- **Vloga vodstva v informacijski varnosti**

Vodstvo mora imenovati odgovorno osebo (CISO)
in jasno opredeliti pooblastila za učinkovitovarnostno upravljanje.

- **Vključitev v poslovni načrt**

Informacijska varnost mora biti del letnega poslovnega načrta in strateških usmeritev organizacije za uspeh.

- **Zagotavljanje virov in poročanje**

Vodstvo zagotavlja kadrovske, finančne in tehnične vire ter redno poroča o varnostnih incidentih in skladnosti.

- **Kultura varnosti in zmanjšanje tveganj**

Spodbujanje varnostne kulture in ozaveščanje zaposlenih povečuje odpornost organizacije proti kibernetskim grožnjam.

UKREPI

Vodstvo organizacije potrjuje vse ključne politike informacijske varnosti in zagotavlja ustrezne človeške, finančne in tehnične vire za njihovo izvajanje.

- Vodstvo imenuje odgovorno osebo za informacijsko varnost (ang. CISO), ki je tudi kontaktna oseba za informacijsko varnost in ima jasno opredeljena pooblastila in odgovornosti ter neposredno poroča in odgovarja vodstvu.

- Informacijska in kibernetska varnost sta vključeni v letni načrt in strateške usmeritve organizacije

- Uveden je proces rednega poročanja vodstvu o stanju varnosti (vsaj četrtletno), ki vključuje kazalnike skladnosti in incidentov.

- Vloge, odgovornosti in pooblastila v povezavi z informacijsko varnostjo so jasno določene in se redno revidirajo

- Politike in postopki varnosti vključujejo določitev meril uspešnosti in ukrepov za spremljanje ravni zrelosti informacijske in kibernetske varnosti

ODGOVORNOST VODSTVA

Vodstvo organizacije je odgovorno za skladnost z zakonodajo s področja informacijske in kibernetske varnosti ter za uspešnost oziroma učinkovitost sistema upravljanja varovanja informacij.

Najmanj enkrat letno preveri uspešnost in ustreznost ukrepov informacijske varnosti, presoja dosežene cilje, sprejema odločitve o izboljšavah in potrjuje ukrepe za obvladovanje tveganj.

Vir: https://care.gmu.edu/nsf-bridging-the-cybersecurity-leadership-gap-assessment-competencies-and-capacity-building-project/g" Project – Center for Assurance Research and Engineering

ZAGOTAVLJANJE INTEGRITETE KADROV

NAMEN

Z zagotovljenimi postopki preverjanja, pogodbenimi obveznostmi in nadzorom življenjskega cikla zaposlitve se zmanjšujejo tveganja človeškega faktorja in preprečujejo morebitna zlonamerna ali nenamerna dejanja oseb z dostopom do informacijskih sredstev.

UKREPI

Preverjanje pred zaposlitvijo

Zaupnost in zaveze

Pogodbeni pogoji

Ob zaposlitvi

Spremembe vlog

Tretje osebe

Obravnavanje kršitev

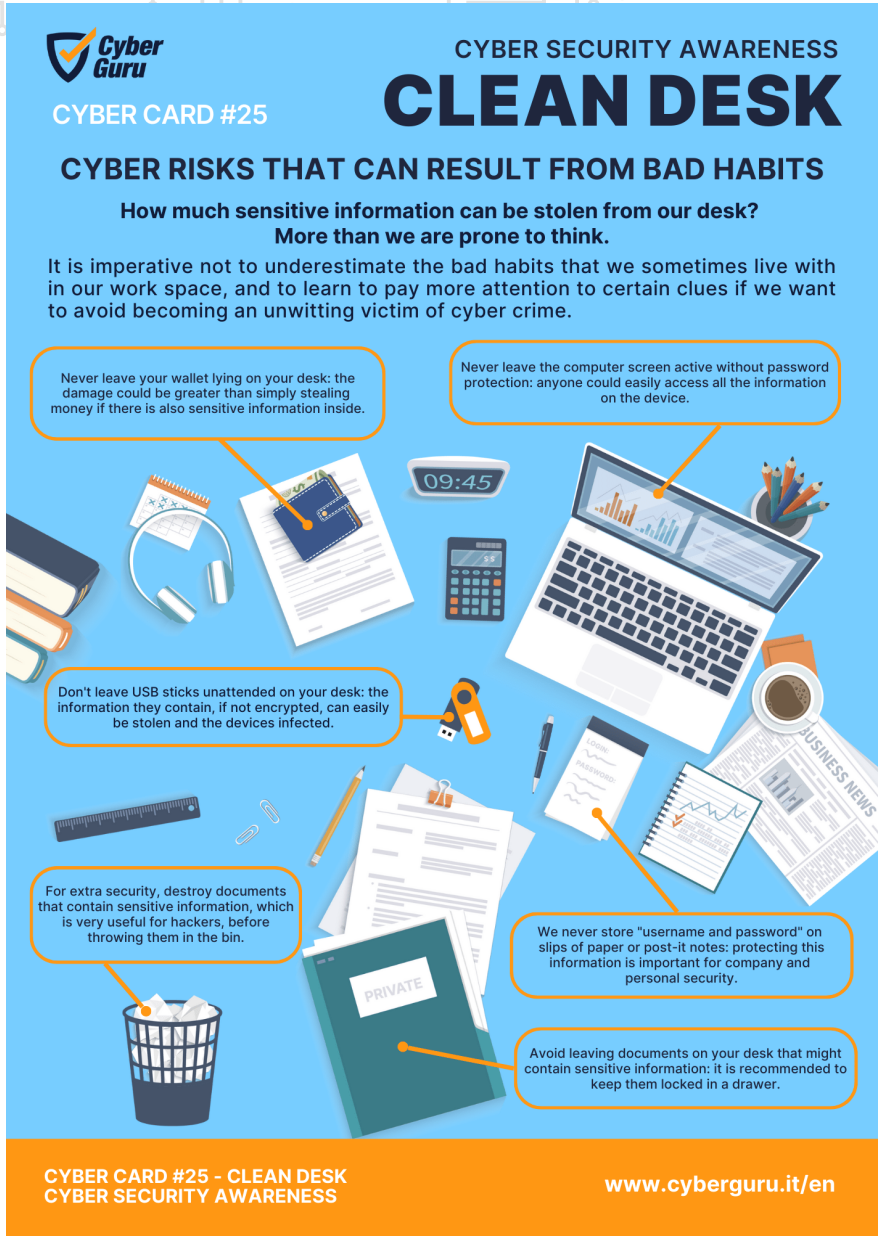
Ob prenehanju zaposlitve

OSNOVNE PRAKSE KIBERNETSKE HIGIENE IN USPOSABLJANJE

Namen

Z izvajanjem politike čiste mize in kontinuiranim usposabljanjem in ozaveščanjem zaposlenih ter pogodbenih izvajalcev se zagotavljajo osnovne prakse kibernetske higiene.

Namen ukrepov je zmanjšati tveganja socialnega inženiringa, lažnega predstavljanja ter nenamernega razkritja informacij organizacije.



Vir: https://www.cyberguru.it/en/2023/03/08/cyber-card-25-clean-desk/sk

UKREPI

Organizacija vzpostavi program ozaveščanja, ki zajema varno uporabo e-pošte, pomen večfaktorske avtentikacije, prepoznavanje poskusov socialnega inženiringa, varno delo na daljavo in zaščito pred lažnim predstavljanjem

Program je obvezen za vse zaposlene in druge uporabnike informacijskih sistemov organizacije; smiselno se uporablja tudi za pogodbene izvajalce.

Uspešnost oziroma učinkovitost programa se preverja najmanj enkrat letno; usklajuje se z rezultati analize tveganj ter priporočili pristojnih organov in izkušnjami iz lastnih zaznanih incidentov ali znanih sektorskih ali panožnih dogodkov

Program je kontinuiran, se redno preverja in posodablja, vanj so smiselno vključeni tudi dobavitelji in pogodbeni izvajalci.

Vključeno je tudi tehnično osebje (npr. skrbniki informacijskih sistemov, lokalni administratorji, upravljavci mrež, skrbniki dostopov ipd.) in vodstvo se usposablja glede na svoje vloge in ocenjena tveganja

Izvaja se politika čiste mize in zaklepanja zaslona iz krovne politike informacijske varnosti.

UPRAVLJANJE DOSTOPA IN VARNOST ČLOVEŠKIH VIROV

Namen

Nadzor dostopa na podlagi vlog in odgovornosti ščiti informacijska sredstva pred nepooblaščenim dostopom, ukrepi pa zagotavljajo upravljanje dostopov in privilegijev na varen, nadzorovan in sledljiv način

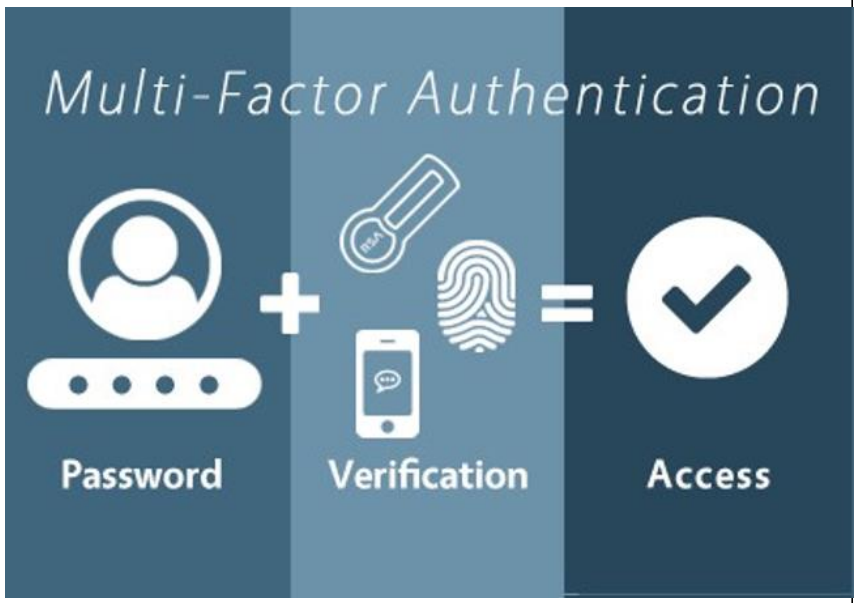
Vir: https://www.shutterstock.com/search/cyber-security-training?image_type=vector

UKREPI

- Vsi dostopi so odobreni, dokumentirani in sorazmerni z nalogami (načelo najmanjših privilegijev, ločevanje dolžnosti);

- Vzpostavljena je politika upravljanja privilegiranih računov (ang. PAM); za skrbniške dostope se uporablja ločene skrbniške račune, namenski upravljavski/administrativni ločen segment omrežja z nadzorom dostopa do tega segmenta, podeljevanje privilegijev po sistemu JIT (Ang. just-in-time; samo takrat, ko je nujno potreben) in sejno beleženje;

- Večfaktorska avtentikacija je obvezna za vse skrbniške račune in občutljive dostope (npr. oddaljene dostope, delu na daljavo ali dostope do storitev v oblaku);



Vir: https://www.xcitium.com/knowledge-base/mfa/

UKREPI

- Izvaja se redna revizija dostopov (npr. četrtletno za privilegirane, najmanj letno za ostale) in takojšnja ukinitev neuporabljenih ali odvečnih računov;

- Uporablja se centralni imenik ali sistem za upravljanje identitet (npr. AD/LDAP/SSO), ki omogoča samodejno spremljanje sprememb, beleženje dostopov in pripravo tehničnih poročil o dodeljenih pravicah; interaktivni dostop s storitvenih ali strežniških računov ni dovoljen; njihove poverilnice (gesla, ključi, certifikati, API-žetoni) se hranijo v nadzorovanem varnostnem sistemu (npr. Vault ali HSM); menjava poverilnic se izvaja ob zaznani ali domnevni kompromitaciji, ob spremembi osebja ali pred iztekom njihove veljavnosti;

- Dostopi tretjih oseb (dobavitelji/izvajalci) so časovno omejeni, namenski, nadzorovani in pogodbeno urejeni; za oddaljen dostop se uporabljajo varni prehodi/zapisovanje sej

- Proces vstop-sprememba-izstop (aktivacija/spreminjanje/ukinitev pravic) je vezan na kadrovske dogodke in odobritve.

UPRAVLJANJE VARNOSTNIH KOPIJ

- **Varnostno kopiranje podatkov**

Načrtno in redno kopiranje podatkov omogoča neprekinjenoposlovanje in hitro obnovo po inciden tih.

- **Zahteve RTO in RPO**

Varnostne kopije izpolnjujejo zahteve RTO in RPO, ki temeljijo na analizi vpliva na poslovanje.

- **Dokumentacija in sledenje**

Formalno opredeljeni postopki in zapisniki zagotavljajo sledljivost in dokazljivost varnostnih ukrepov.

Vir: https://www.netinet.si/samodejne-varnostne-kopije

- **Povezava z varnostnimi ukrepi**

Strategija vključuje nadzor dostopa, šifriranje in usklajenost z analizo tveganj za popolno zaščito.

OPREDELITEV OBSEGA, POGOSTOSTI IN HRAMBE

- **Opredelitev obsega podatkov**

Jasno določite, katere podatke je treba varnostno kopirati glede na analizo tveganj in poslovni vpliv.

- **Pogostost in način kopiranja**

Določite pogostost kopiranja ter vrste kopij: polna, diferencialna ali inkrementalna, za ustrezno zaščito podatkov.

- **Roki hrambe in skladnost**

Roki hrambe morajo upoštevati zakonodajo, interne politike in pogodbe, z rednim preverjanjem skladnosti.

- **Preverjanje in posodabljanje postopkov**

Vzpostavite postopke za redno preverjanje in posodabljanje varnostnih kopij glede na spremembe v poslovanju.

NAMEN VARNOSTNIH KOPIJ

Namen varnostnih kopij

Zagotoviti načrtno in preverljivo kopiranje podatkov za hitro obnovo po incidentih in neprekinjeno poslovanje.

Zahteve RTO in RPO

Doseganje časovnih ciljev obnovitve in točk obnovitve temelji na analizi vpliva na poslovanje in neprekinjenosti.

Varnostni ukrepi in sledljivost

Uporaba nadzora dostopa, šifriranja in revizijskih sledi za zaščito in dokazovanje varnostnih kopij.

Ključne tehnologije in prakse

Načelo 3-2-1, WORM, KMS/HSM, večfaktorska avtentikacija in redno testiranje obnovljivosti zagotavljajo odpornost.

UKREPI

Za vse vrste podatkov so določeni obseg, pogostost, način kopiranja in roki hrambe, skladno z rezultati analize tveganj, oceno vpliva na poslovanje ter zahtevami RTO/RPO;

Varnostne kopije vključujejo podatke in konfiguracijske nastavitve (npr. aplikacij, omrežnih naprav) ter se testirajo in dokumentirajo;

Uporablja se načelo 3-2-1 (vsaj tri kopije, na dveh medijih, ena geografsko ločena/«offsite«); kjer je izvedljivo, se vzpostavi nespremenljive (ang. WORM/immutable) kopije in logična/omrežna ločitev »backup« okolja od primarne domene;

ELEMENT	OPIS
3 kopije	Primarna + 2 dodatni varnostni kopiji
2 medija	Dva različna fizična ali logična me dija
1 off-site	Kopija na geografsko ločeni lokaci ji
Immutable	Kopije, ki jih ni mogoče spreminjati ali bris ati

UKREPI

Varnostne kopije so šifrirane v prenosu in mirovanju; ključi se upravljajo in hranijo ločeno (KMS/HSM), z dokumentiranimi postopki za obnovo ključev;

SaaS/oblak: podatki v storitvah v oblaku (npr. e-pošta, datotečne storitve, CRM/ERP) so vključeni v strategijo kopiranja ali imajo izbran produkt, ki zagotavlja enakovredno varnostno kopiranje;

Dostop do »backup« infrastrukture se nadzira po načelu najmanjših privilegijev, z MFA na konzolah, segmentacijo (ločen upravljavski segment) in revizijskimi sledmi;

Izvaja se redno testiranje obnovljivosti (npr. četrtletni »sample restore«, letni celotni preizkus kritičnih sistemov), vključno s scenariji obnavljanja (posamezna datoteka, baza, celoten sistem); uspešnost, časi obnov (RTO) in integriteta podatkov se dokumentirajo

Določene so odgovornosti za izvajanje in nadzor nad kopijami; rezultati testov in zaznane pomanjkljivosti so del rednega poročila osebe pristojne za informacijsko varnost (CISO).

DNEVNIŠKI ZAPISI IN REVIZIJSKE SLEDI

NAMEN

Sistematično beleženje in hramba

Vzpostavitev centraliziranega in varnega sistema za shranjevanje dnevnikov je ključna za sledljivost varnostnih dogodkov.

Podpora preiskavam in skladnosti

Dnevniški zapisi pomagajo pri preiskavah varnostnih incidentov in zagotavljajo skladnost z zakonodajo ter notranjimi predpisi.

Avtomatizirano zaznavanje anomalij

Uporaba SIEM sistemov omogoča korelacijo dogodkov in hitro odkrivanje varnostnih anomalij v realnem času.

Organizacijski nadzor in postopki

Določitev jasnih postopkov, odgovornosti in rednih pregledov zagotavlja stalno spremljanje varnostnega stanja.

UKREPI

Sistemi za spremljanje dogodkov

Vzpostaviti je treba sisteme za beleženje dogodkov iz strežnikov, omrežne opreme, aplikacij in varnostnih rešitev.

Sinhronizacija časa in atributi zapisov

Vsi sistemi morajo biti usklajeni prek varnih NTP virov, zapisi morajo vključevati časovni žig, izvor in rezultat akcij.

Zaščita dnevnikov in dostop

Dostop do dnevnikov naj bo omejen, zaščiten z WORM tehnologijo in hash integriteto, ločevanje dolžnosti pa nujno.

Analiza in arhiviranje dnevnikov

Redni pregledi, avtomatizirana korelacija dogodkov in varna hramba dnevnikov najmanj 12 mesecev sta ključna.

UPRAVLJANJE OMREŽNIH IN INFORMACIJSKIH SISTEMOV

- **Zagotavljanje varnega upravljanja**

Zagotavlja varno, stabilno in sledljivo delovanje omrežij in informacijskih sistemov z jasno določenimi odgovornostmi.

- **Nadzor sprememb in revizijska sled**

Formalni postopki evidentirajo vsa sredstva in zagotavljajo revizijsko sled za vsako spremembo ter preprečujejo nepooblaščene spremembe.

- **Ločena razvojna okolja**

Vzpostavitev razvojnih, testnih in produkcijskih okolij preprečuje vpliv sprememb na kritične sisteme in zmanjšuje tveganja napak.

- **Redno nameščanje popravkov**

Varne posodobitve in popravki se namestijo po preverjanju združljivosti, kar zagotavlja skladnost in varnost sistemov.

UKREPI

Določitev odgovornosti lastnikov sredstev

Organizacija mora imenovati lastnike, ki skrbijo za razpoložljivost, celovitost in zaupnost informacijskih sredstev.

Vzpostavitev celovite evidence sredstev

Evidenca mora zajemati identifikator, lokacijo, lastnika, klasifikacijo in življenjski cikel sredstev.

Postopki za spremembe in nadzor

Vzpostaviti je potrebno postopke za dokumentiranje sprememb, spremljanje konfiguracij in nadzor različic za varnost.

Sledljivost in varnostna skladnost

Jasno definirani procesi zagotavljajo odobritve, testiranje in revizijsko sled za skladnost z zakonodajo.

UKREPI ZA SPREMEMBE IN POSODOBITVE

Redne varnostne posodobitve

Varnostne popravke je treba redno nameščati hitro glede na kritičnost ranljivosti in priporočila proizvajalcev.

Testiranje združljivosti

Pred uvedbo v produkcijo je nujno preveriti združljivost v testnem okolju, da preprečimo motnje v delovanju.

Dokumentacija in odobritev sprememb

Vsaka sprememba mora biti dokumentirana, testirana in odobrena s strani odgovorne osebe.

Ločevanje okolij in revizijska sled

Spremembe potekajo v ločenih okoljih z revizijsko sledjo, kar zmanjšuje tveganja in zagotavlja sledljivost.

UKREPI ZA REVIZIJSKO SLED IN NADZOR

Vzdrževanje revizijske sledi

Za vse spremembe je potrebna revizijska sled z datumom, opisom, izvajalcem in potrditvijo odgovorne osebe.

Redni pregledi in nadzor

Pregledi konfiguracij, sistemskih dnevnikov in ranljivosti odkrivajo odstopanja od varnostnih politik.

Ločevanje dolžnosti

Odgovornosti so razdeljene, da nobena oseba ne nadzoruje celotnega procesa sprememb.

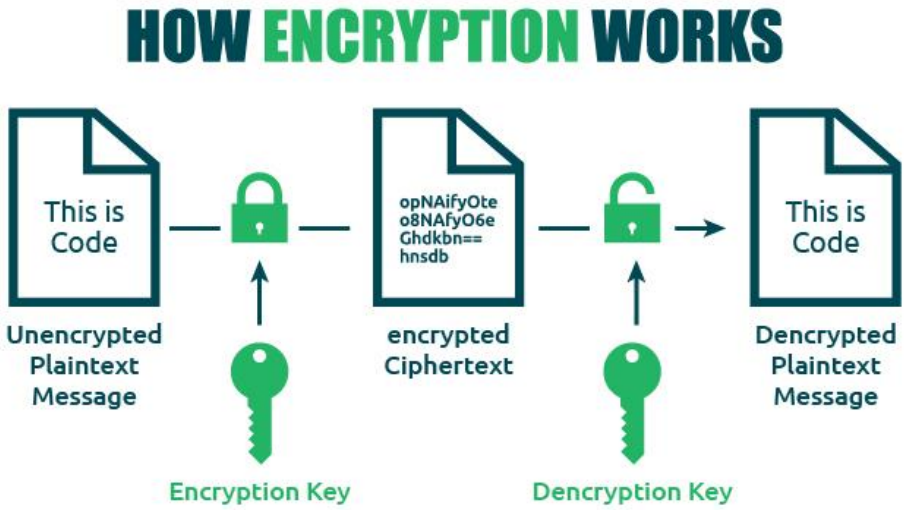
Transparentnost in poročanje

Vse spremembe se redno poročajo CISO, kar zagotavlja skladnost z internimi politikami in zakonodajo.

KRIPTOGRAFIJA IN ZAŠČITA PODATKOV

NAMEN

Kriptografija ščiti podatke med prenosom in obdelavo ter v mirovanju, zagotovljeno mora biti varno upravljanje kriptografskih ključev skozi celoten življenjski cikel



Vir: https://www.clickssl.net/blog/what-is-asymmetric-encryption

UKREPI

Zaščita podatkov s kriptografijo

Kriptografija ščiti podatke pri prenosu, shranjevanju in obdelavi z uporabo varnih protokolov in digitalnih podpisov.

Sodobni varnostni algoritmi

Uporaba preverjenih< algoritmov kot so AES-256, RSA 2048+, ECC in SHA-2 zagotavlja visok nivo varnosti.

Upravljanje življenjskega cikla ključev

Postopki vključujejo generiranje, distribucijo, rotacijo, revizijsko sled in varno uničenje kriptografskih ključev.

Redno preverjanje skladnosti

Konfiguracije in algoritmi se vsaj enkrat letno preverjajo glede skladnosti z mednarodnimi standardi in priporočili.

UPRAVLJANJE PROMETA IN OMREŽNE KOMUNIKACIJE

Namen

Z varnim načrtovanjem, segmentacijo in nadzorom omrežnega prometa se ščitijo komunikacijske poti in omrežje pred nepooblaščenimi dostopi in zlorabami.

Vir: https://learn.g2.com/network-traffic-analysis

Ukrepi

dokumentirana je arhitektura omrežja (logični in tehnični diagram) z označenimi zaupanimi conami, vmesniki do interneta in tretjih oseb ter točkami nadzora prometa;
notranje domene in storitve so zaščitene z logično in fizično segmentacijo (VLAN, VRF, mikrosegmentacija) in načelom najmanjših privilegijev na ravni omrežnih pravil;
omrežni promet se omejuje na dovoljene poti in storitve (allow-list); privzeto je vse ostalo zavrnjeno; uporabljajo se šifrirani protokoli, stare in ranljive različice so onemogočene;
oddaljeni dostop se izvaja prek VPN z večfaktorsko avtentikacijo in preverjenimi standardi; povezave dobaviteljev in skrbniški dostopi so namenski, časovno omejeni, odobreni in beleženi;
vzpostavljeni so sistemi zaznavanja in preprečevanja anomalij/vdorov (NDR/IDS/IPS) z alarmi in, kjer je primerno, avtomatiziranimi odzivi; dogodki se centralizirano beležijo;
omrežna oprema in varnostne pregrade se upravljajo skladno s standardi konfiguracije; izvaja se port security; spremembe pravil so dokumentirane in redno pregledane;
ključne omrežne storitve in protokoli (DNS, DHCP, NTP, e-pošta, proxy) so zaščiteni in nadzorovani; nepotrebne storitve so onemogočene;
glavno komunikacijsko ožičenje, omarice in telekomunikacijske točke so fizično zaščiteni in dostopno kontrolirani;
izvedeni so ukrepi za odpornost in razpoložljivost komunikacij (redundanca, zaščita pred DDoS, sodelovanje s ponudnikom storitev).

VARNOST DOBAVNE VERIGE

Namen

Z vključitvijo informacijske in kibernetske varnosti v celoten življenjski cikel sodelovanja z dobavitelji, od izbire in pogodbenih zahtev do nadzora izvajanja in prenehanja sodelovanja se zmanjšujejo tveganja na področju varnosti dobavnih verig.

Vir: https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

Ukrepi
vodi se ažuren seznam ključnih dobaviteljev in pogodbenih izvajalcev, ki lahko vplivajo na informacijsko ali kibernetsko varnost organizacije oziroma na izvajanje njenih storitev;
pred sklenitvijo pogodbe se izvede ocena tveganj dobavitelja ali izvajalca, ki vključuje pregled varnostne zrelosti (npr. certifikat ISO/IEC 27001, SOC 2), zgodovino incidentov, finančno stabilnost ter postopke neprekinjenega poslovanja in obnove po katastrofi (merila izbire dobavitelja)
pogodbe vsebujejo obvezne varnostne klavzule: varovanje zaupnosti podatkov, takojšnje obveščanje o incidentih ali ranljivostih, zahteve glede varnosti izdelkov in storitev skozi celoten življenjski cikel, določitev RTO/RPO in načrta neprekinjenosti, pravico naročnika do presoje ter zahteve za hrambo, predajo in uničenje podatkov po prenehanju pogodbe
pogodbe lahko, glede na tveganje, vsebujejo tudi zahteve za SBOM, varni razvoj programske opreme (SDLC), podpisovanje kode in varnost v oblačnih okoljih
pogodbeni pogoji veljajo tudi za podizvajalce; vključitev podizvajalca je mogoča le ob predhodni odobritvi in skladno z enakimi varnostnimi zahtevami;
varnostne zahteve dobavne verige so vključene v postopke nabave in upravljanja pogodb; vodja informacijske varnosti sodeluje pri oceni tveganj in nadzoru skladnosti dobaviteljev
izvajajo se redni pregledi in nadzor izvajanja pogodbenih varnostnih določil; ključni dobavitelji morajo omogočiti vpogled v dokazila o skladnosti (npr. certifikate, rezultate presoj, poročila o vdornih in drugih testih)
organizacija spodbuja dobavitelje, da izvajajo postopke za razkritje ranljivosti (Ang. vulnerability disclosure), redno odpravljajo znane ranljivosti in dokazujejo uporabo varnostnih praks (SDLC, nadzor dostopov, varnost v oblaku)
ob prenehanju sodelovanja mora dobavitelj varno odstraniti ali vrniti vse podatke in kopije, preklicati vse dostope in poverila ter predložiti potrdilo o uničenju podatkov
za ključne dobavitelje je določen načrt izstopa (Ang. exit plan), ki zagotavlja možnost nemotene zamenjave ponudnika, vključno s prenosom konfiguracij in podatkov v ustreznem formatu.

FIZIČNA IN OKOLJSKA VARNOST

Namen

Omrežja in informacijski sistemi morajo biti fizično zaščiteni pred okoljskimi tveganji, nepooblaščenim dostopom in fizičnimi poškodbami, s čimer se zagotavlja razpoložljivost, celovitost, zaupnost in avtentičnost informacijskih sredstev.

Vir: https://www.securingpeople.com/physical-security-access-control/

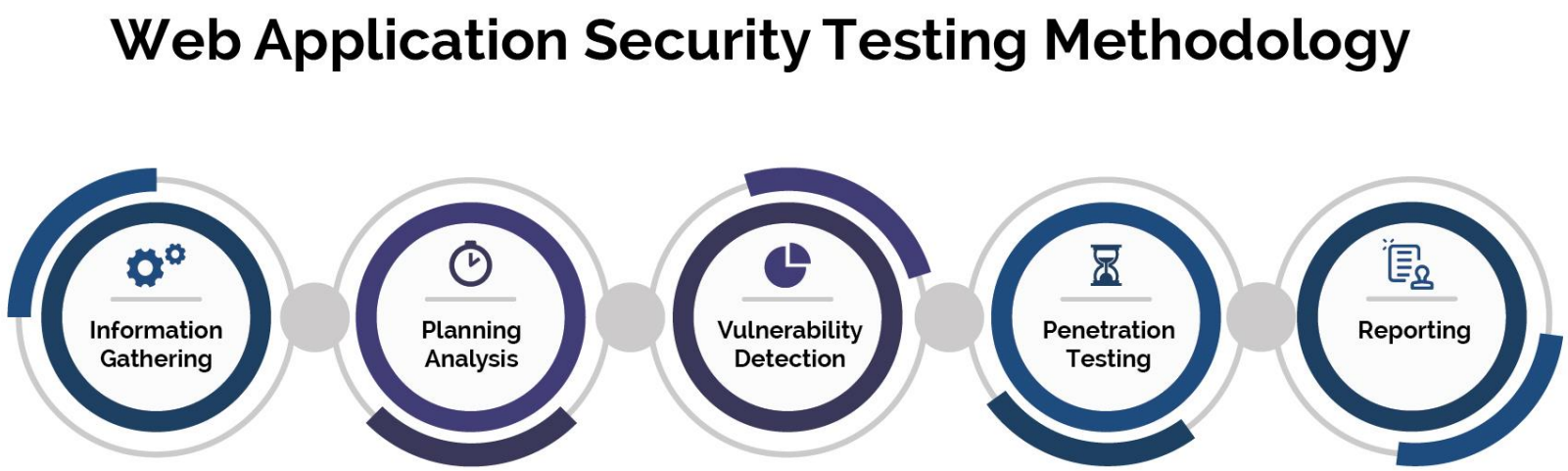
UKREPI

- določene so fizične meje in varovana območja, kjer se nahajajo ključni deli informacijskih sistemov in omrežne opreme, dostop v ta območja je fizično omejen in jasno označen;
- dostop do varovanih območij je dovoljen le pooblaščenim osebam; uporablja se večfaktorska avtentikacija (MFA) ter beleženje vseh vstopov in izstopov; evidence se hranijo najmanj 12 mesecev, razen če predpisi določajo drugačen rok;
- varovana območja so opremljena s sistemi za zaznavo požara, dima, izliva vode, sprememb temperature in vlage ter fizičnega vdora; alarmi so povezani z odzivnimi postopki;
- nameščeni so ustrezni sistemi napajanja in zaščite (UPS, agregati, zaščita pred prenapetostjo) in načrtovani postopki za varno zaustavitev sistemov ob daljših izpadih električne energije;
- glavno komunikacijsko in napajalno ožičenje je fizično zaščiteno in neprekinjeno nadzorovano; servisni in tehnični dostopi do omrežne infrastrukture so dovoljeni le po odobritvi in se morajo beležiti;
- izvaja se 24/7 video nadzor na dostopnih točkah varovanih območij in ključnih prostorih; posnetki se hranijo skladno s politiko varovanja osebnih podatkov in predpisi s področja varstva osebnih podatkov;
- redno se izvajajo požarne in evakuacijske vaje, pregledi delovanja varnostnih sistemov (požarni alarmi, detektorji, UPS, agregati, hlajenje) ter vzdrževanje varnostne in klimatske opreme;
- določene so odgovorne osebe za vzdrževanje in nadzor fizične varnosti, njihova pooblastila in postopki za poročanje incidentov ter
- obiskovalci in vzdrževalci se morajo prijaviti, nositi identifikacijo na vidnem mestu in morajo biti ves čas pod nadzorom pooblaščene osebe; obiski se evidentirajo

APLIKACIJSKA VARNOST IN RAZVOJ

Namen

Z vključevanjem informacijske in kibernetske varnosti v celoten življenjski cikel razvoja programske opreme in aplikacij se omejuje oziroma preprečuje vnos ranljivosti v produkcijsko okolje.



Vir: https://www.suntechnologies.com/service/security-testing/

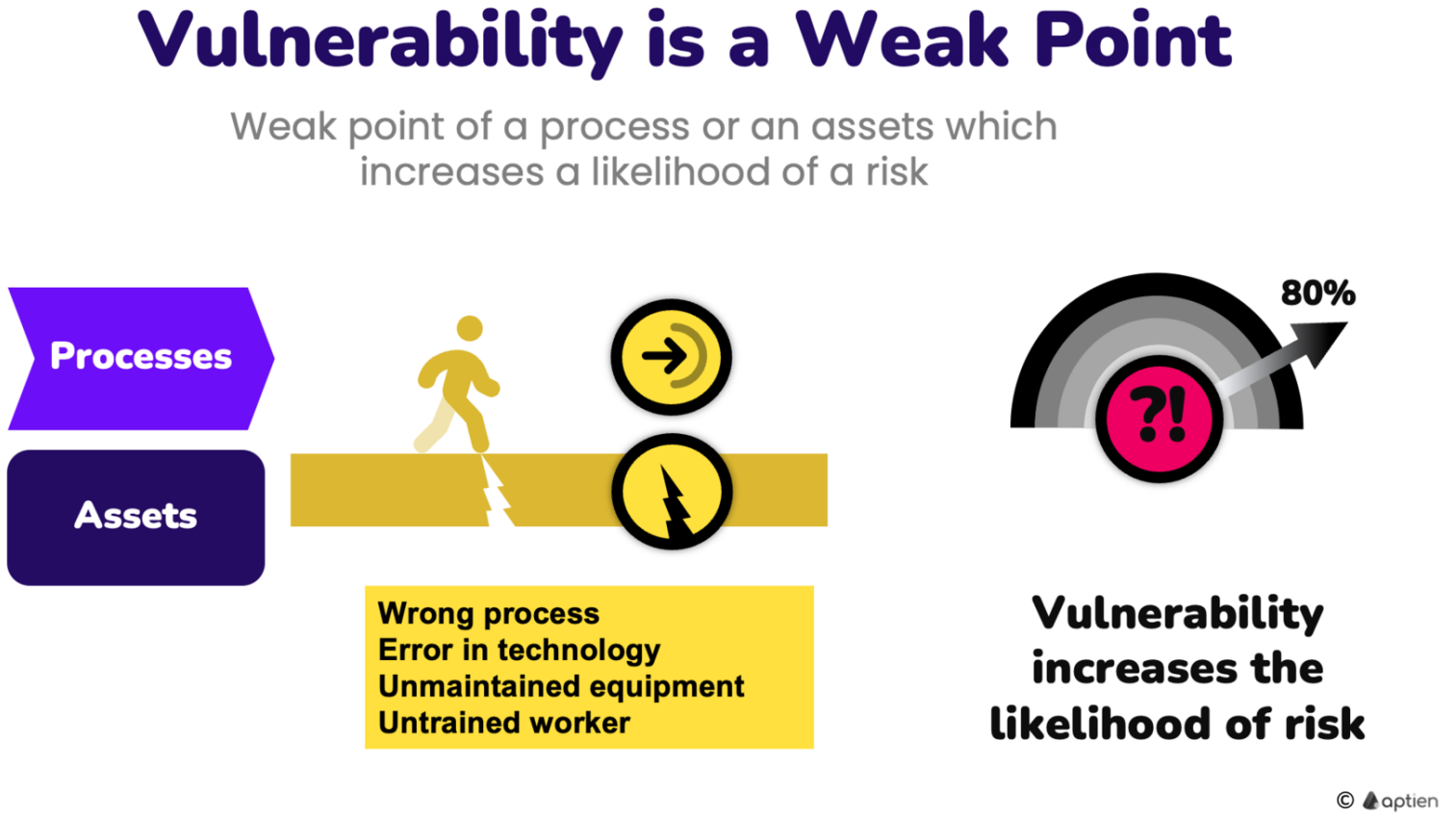
UKREPI

- vse faze razvoja programske opreme (načrtovanje, razvoj, testiranje, uvajanje, vzdrževanje) vključujejo oceno varnostnih tveganj in preverjanje skladnosti z varnostnimi zahtevami;
- razvoj in vzdrževanje aplikacij temelji na načelih varne kode (ang. secure coding), arhitekture ničelnega zaupanja (ang. zero trust) ter vključenosti varnosti v razvojne procese (Ang. SDLC/DevSecOps);
- uporabljajo se samo preverjene in zaupanja vredne knjižnice, moduli in zunanje komponente; njihovo izvorno zanesljivost in licenčne pogoje se preveri pred uporabo;
- dostop do izvorne kode, razvojnih repozitorijev in orodij za gradnjo programske opreme je omejen na pooblaščene osebe, z uporabo večfaktorske avtentikacije in beleženjem dostopov;
- vzpostavljeno je ločeno razvojno, testno in produkcijsko okolje; spremembe se testirajo in odobrijo pred uvedbo v produkcijo;
- preskušanje vključuje statično in dinamično analizo kode (Ang. SAST – static application security testing/DAST – dynamic application security testing) ter, kjer je primerno, vdorno testiranje pred uvedbo v produkcijsko okolje;
- ranljivosti, odkrite v fazi razvoja ali v obratovanju, se odpravljajo brez odlašanja; vzpostavljen je postopek za odgovorno razkritje ranljivosti (ang. vulnerability disclosure policy);
- rezultati varnostnih preskusov, popravki in odpravljene ranljivosti se dokumentirajo in hranijo zaradi morebitnega dokazovanja skladnosti in ugotavljanja odgovornosti
- za zunanje izvajalce, ki sodelujejo pri razvoju programske, veljajo enake zahteve glede varnosti kode, testiranja in odgovornega razkritja kot za interne razvijalce

UPRAVLJANJE IN PREPREČEVANJE RANLJIVOSTI

Namen

S proaktivnim spremljanjem, ocenjevanjem in odpravo tehničnih ranljivosti v informacijskih sistemih se zmanjšuje tveganje zlorabe znanih ranljivosti



Vir: https://aptien.com/en/kb/articles/what-is-vulnerability

UKREPI

- vzpostavljen je centralni sistem za spremljanje virov o ranljivostih (npr. CISA KEV, CVE, obvestila proizvajalcev, skupine CSIRT, ENISA), oceno vpliva na sredstva organizacije in ocenjevanje prioritet odprave ranljivosti;

- izvajajo se redni avtomatizirani pregledi ranljivosti z ustreznimi pooblastili (ang. credentialed scanning) za interno omrežje in javno izpostavljene sisteme; vse zaznave se vodijo v enotnem registru ranljivosti, ki omogoča sledljivost celotnega postopka od zaznave do zaprtja;

- roki odprave so določeni glede na tveganje in kritičnost sredstva: kritične internetno izpostavljene v 72 urah; kritične interne v 7 dneh; visoke v 14 dneh; srednje v 30 dneh; nizke v 90 dneh; 2.13.4 kadar popravka ni mogoče takoj uporabiti, se izvedejo kompenzacijski ukrepi skladno z oceno tveganja (npr. segmentacija, izolacija v IDMZ, »whitelisting«, »virtual patching«, dodatni nadzor), izjeme od rokov pa pisno odobri vodja informacijske varnosti za časovno omejeno obdobje;

- nameščanje popravkov poteka po postopku upravljanja sprememb; za kritične ranljivosti z aktivno izrabo se lahko uporabi nujni postopek (ang. emergency change) z naknadnim poročilom vodji informacijske varnosti;

- po namestitvi popravkov se izvede ponovni pregled (ang. rescan) najpozneje v 7 dneh; če ranljivost po ponovnem pregledu ni odpravljena, se določijo dodatni ukrepi ali eskalacija lastniku sistema;

- prepovedana je uporaba informacijskih rešitev z aktivno izkoriščanimi ranljivostmi brez predhodne ocene tveganja in določenih kompenzacijskih ukrepov

- zunanji izvajalci in ponudniki storitev morajo spoštovati enake ali strožje roke in postopke; obveznosti so opredeljene v pogodbah/SLA, izvajalci pa na zahtevo predložijo dokazila (poročila skeniranj, potrditve o posodobitvah).

ZAŠČITA PRED ZLONAMERNO PROGRAMSKO KODO TER NAČIN ZAZNAVANJA POSKUSOV VDOROV IN PREPREČEVANJA INCIDENTOV

Namen

Informacijski sistemi, naprave in omrežje morajo biti zaščiteni pred zlonamerno programsko kodo ter napadi in poskusi vdorov, omogočeno mora biti pravočasno zaznavanje, odzivanje in preprečevanje incidentov oziroma skorajšnjih incidentov (ang. near miss).

Vir: https://www.europeanfiles.eu/digital/revamped-enisa-eus-cybersecurity-agency

UKREPI

- na vseh končnih napravah (strežniki, delovne postaje, prenosniki, mobilne naprave) je implementirana aktivna zaščita z EDR/XDR rešitvami, ki omogočajo sprotno zaznavanje, analizo in odzivanje na grožnje;
- omrežje je zaščiteno z napredno požarno pregrado, sistemi za zaznavanje in preprečevanje vdorov (ang. IDS/IPS), nadzorom spletnega prometa in filtriranjem elektronske pošte;
- protivirusni in »antimalware« programi so centralno upravljani, samodejno posodabljani in ne smejo biti samoiniciativno onemogočeni ali izključeni;
- vsi zunanji mediji (USB, prenosni diski, SD kartice) se ob priklopu samodejno preverijo z zaščitno programsko opremo;
- prepovedana je uporaba neodobrene ali piratske programske opreme; nameščanje programske opreme je dovoljeno le s soglasjem skrbnika informacijskega sistema;
- sistemi in omrežje se redno pregledujejo z orodji za zaznavanje anomalij in znakov kompromitacije; zaznani incidenti se takoj evidentirajo in obravnavajo po postopkih iz načrta odzivanja na incidente;
- dogodki, povezani z zaznavo zlonamerne programske opreme, se beležijo v centralnem sistemu za spremljanje varnostnih dogodkov (SIEM) in analizirajo v okviru rednega nadzora;
- vzpostavljen je postopek za forenzično analizo kompromitiranih sistemov, ki vključuje zavarovanje dokazov, izolacijo prizadetih sistemov in dokumentiranje ugotovitev
- uporabniki so seznanjeni z odgovornostjo za varno ravnanje pri odpiranju elektronske pošte, priponk, zunanjih povezav in drugih potencialno nevarnih vsebin

AVTENTIKACIJA IN NADZOR DOSTOPOV

Namen

Z uporabo močne in večfaktorske avtentikacije se ščitijo dostopi do informacijskih sistemov in preprečujejo nepooblaščeni dostopi ali zlorabe poverilnic

Vir: https://www.info-sol.co.uk/why-you-need-multi-factor-authentication/

UKREPI

obvezna je uporaba večfaktorske avtentikacije za vse oddaljene dostope (VPN, VDI, e-pošta v oblaku), vse administrativne in sistemske račune ter druge sisteme, kjer to določa ocena tveganja;
večfaktorska avtentifikacija uporablja najmanj dve neodvisni komponenti (npr. geslo + biometrija ali geslo + FIDO2 varnostni ključ);
gesla uporabniških računov morajo biti dolga najmanj 12 znakov, gesla administrativnih računov pa najmanj 16 znakov; priporočena je uporaba geselnih fraz (ang. passphrases) in odobrenih upravljavcev gesel (ang. password manager);
gesel ni treba menjati periodično, temveč le ob sumu ali potrjeni kompromitaciji, ob spremembi vloge, incidentu ali izgubi naprave;
gesla se preverjajo glede na sezname kompromitiranih gesel (ang. blacklist); šibka ali javno objavljena gesla se zavrnejo;
gesla se hranijo v zgoščeni obliki z uporabo kriptografskih algoritmov (bcrypt, scrypt ali Argon2) in naključne soli (ang. salt); prepovedano je obrezovanje gesel;
vzpostavljena je omejitev prijav na največ 5 zaporednih neuspešnih poskusov, po čemer se račun zaklene za najmanj 15 minut ali do ročnega odklepa;
sejna politika določa samodejno prekinitev uporabniške seje po največ 15 minutah nedejavnosti in največ 10 ur dejavnosti;
uporabniški računi morajo biti individualni, neprenosljivi in vezani na osebo; deljenje poveril je prepovedano;
administrativni računi so ločeni od navadnih uporabniških računov in se uporabljajo izključno za upravljavska opravila;
“super-admin” gesla se hranijo ločeno, v fizično zavarovanem sefu pod nadzorom vodje informacijske varnosti in z dostopom po postopku dvostopenjske odobritve;
vodja informacijske varnosti spremlja učinkovitost oziroma uspešnost ukrepov nadzora dostopa ter predlaga izboljšave na podlagi analiz incidentov, notranjih presoj in tehnološkega razvoja.

UPORABA VARNIH KOMUNIKACIJ IN SISTEMOV KOMUNIKACIJE V SILI

Namen

V primeru motenj ali nedostopnosti običajnih komunikacijskih poti je treba zagotoviti varne in redundantne komunikacijske kanale ter določiti postopke za pravočasno, usklajeno in odobreno obveščanje v kriznih situacijah.

Vir: https://www.linkedin.com/pulse/cybersecurity-communication-systems-challenges-solutions-vikaas-s-v--arsgc/

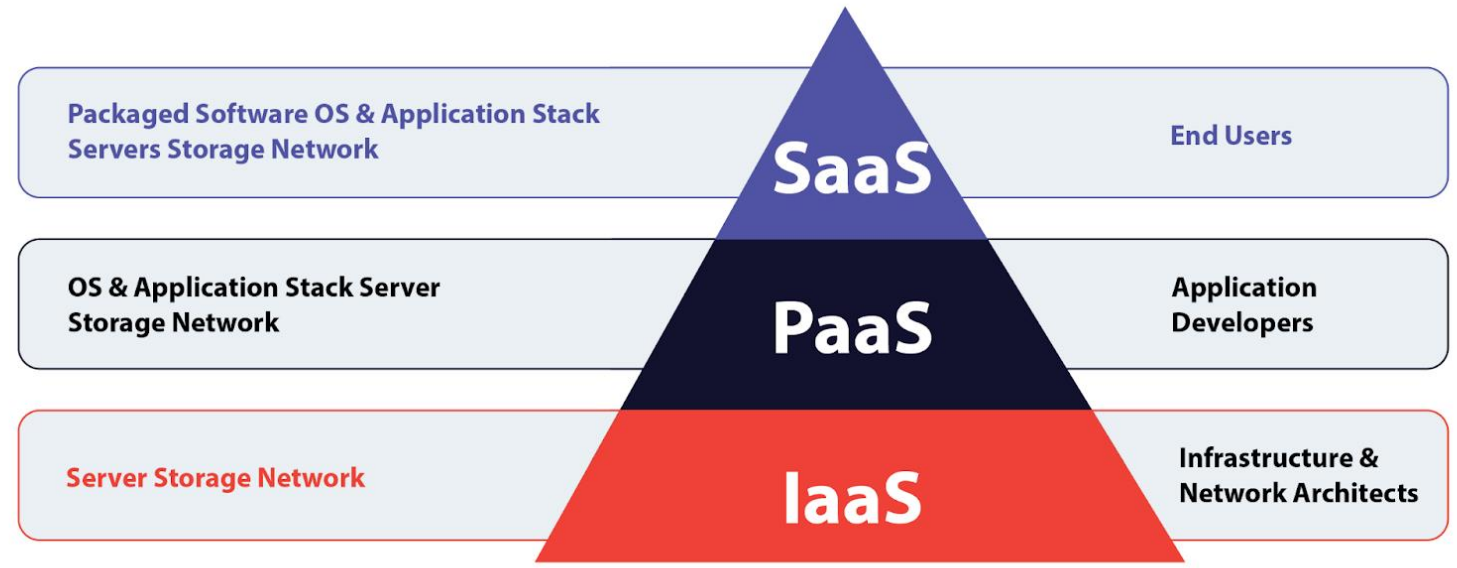
UKREPI

rezervni komunikacijski kanali so določeni v komunikacijskem načrtu (npr. satelitski telefoni, varne aplikacije z E2E šifriranjem, SMS »gateway«, alternativni ponudnik mobilne telefonije); seznam kanalov se vzdržuje in redno posodablja;
komunikacijski načrt vključuje vnaprej pripravljene kontaktne sezname (vodstvo, zaposleni, ključni dobavitelji, stranke, pristojni organi) ter predloge sporočil (e-pošta, SMS, spletna stran, družbena omrežja);
določeni so pripravljavec izjave, govorec in odobritvena pot (krizna ekipa → vodja neprekinjenega poslovanja → direktor); brez odobritve se javne izjave ne objavljajo;
opredeljen je protokol internega obveščanja (eskalacijska veriga, časovne meje za obveščanje, odgovornosti); vsi koraki obveščanja se dnevniško beležijo;
pri uporabi komunikacijskih kanalov (običajnih ali rezervnih) se uporabljajo varni protokoli in kriptografija (npr. TLS 1.2+; E2E za klepet/glas), občutljive informacije se posredujejo le po odobrenih kanalih skladno s klasifikacijo informacij;
v primeru nedostopnosti primarnih kanalov se uporabljajo redundantni kanali iz komunikacijskega načrta (mobilne zveze, satelitski telefoni, fizični stiki), z jasnimi navodili za preklop in povratek na primarni kanal;
vzpostavljena so navodila za uporabo komunikacijskih kanalov v sili (kdo, kdaj, kako, vsebina, potrditev prejema) in postopek preverjanja točnosti kontaktov (npr. četrtletno);
izvajajo se redna testiranja kriznega obveščanja in komunikacij (npr. polletne vaje BC/IR); po vsaki vaji ali dejanskem dogodku se izvede pregled uspešnosti in posodobitev kontaktov, vlog, kanalov in postopkov;
komunikacija z dobavitelji in pristojnimi organi poteka po vnaprej določenih kanalih; roki in načini obveščanja o incidentih so usklajeni z načrtom odzivanja na incidente in pogodbenimi določili ter
dostop do orodij in seznamov za krizno komunikacijo je omejen na pooblaščene osebe (MFA, revizijska sled), varnostne kopije ključnih seznamov in predlog sporočil so hranjene tudi »offline« oziroma na neodvisni lokaciji.

OBLAČNE STORITVE

Namen

Varnost oblačnih storitev se zagotavlja s postavljenimi varnostnimi zahtevami in postopki za varno izbiro, uporabo, nadzor in izstop iz oblačnih storitev ob upoštevanju načela deljene odgovornosti.



Vir: https://www.appviewx.com/education-center/cloud-services/

UKREPI

uporaba oblačnih storitev temelji na načelu deljene odgovornosti; pred uvedbo se določijo varnostne zahteve glede modela storitve (ang. IaaS/PaaS/SaaS), klasifikacije podatkov, lokacije hrambe ter poslovnih zahtev (RTO/RPO);
pred sklenitvijo pogodbe se izvede ocena tveganja in preveri zanesljivost ter odpornost ponudnika; pregledajo se in shranijo dokazila o skladnosti (npr. ISO/IEC 27001, ISO/IEC 27017, SOC 2 Type II, CSA STAR);
pogodba določa kraj hrambe in prenosa podatkov (GDPR, ZVOP-2, ZInfV-1), pravico do izvedbe poročil/revizije ali do vpogleda v rezultate poročil/revizij, roke obveščanja o incidentih, zahteve za posodobitve in odpravljanje ranljivosti, SLA z RTO/RPO ter postopke vračanja/izbrisa podatkov in prenos v prenosljivem formatu;
dostop do oblačnih storitev je po načelu najmanjših privilegijev z obvezno večfaktorsko avtentikacijo; prepovedana je uporaba osebnih ali neodobrenih računov/storitev (ang. shadow IT); izvajajo se najmanj letni pregledi dostopov;
podatki so šifrirani pri prenosu, med obdelavo in v mirovanju; za dostop do oblačnih storitev se uporablja večfaktorska avtentikacija; kjer je izvedljivo se uporabljajo ključi pod nadzorom organizacije (CMK/KMS/HSM); varnostne kopije in konfiguracije so vključene v strategijo varnostnega kopiranja;
uveljavljeni so enotni standardi varnostnih nastavitev (ang. hardening/baselines) za izbrana oblačna okolja; organizacija redno odpravlja ranljivosti in napačne konfiguracije ter spremlja varnostna obvestila ponudnika;
pomembne aktivnosti (prijave, spremembe, administrativna dejanja, prenos podatkov) se beležijo in po možnosti posredujejo v centralni sistem (npr. SIEM); dnevniki se hranijo najmanj 12 mesecev (razen, če predpisi določajo drugače) in so zaščiteni pred spremembami;
postopki in roki obravnave incidentov pri ponudniku so usklajeni z načrtom odzivanja na incidente in vključujejo protokol obveščanja pristojnih CSIRT;
dokumentiran je načrt izstopa, ki določa migracijo k nadomestnemu ponudniku ali vrnitev/izbris podatkov, preklic dostopov in potrdila o uničenju; po prenosu se preveri celovitost in razpoložljivost podatkov ter
periodično se preverja uporaba aktivnih oblačnih storitev in zaznava neodobrene storitve ali račune; ugotovljene neskladnosti se odpravijo v razumnem roku glede na tveganje.

VZDRŽEVANJE NAČRTA

KORAK	OPIS
Plan	Določitev ciljev, pregled politik, analiza tveganj
Do	Izvedba ukrepov in posodobitev načrta
Check	Redni pregledi, presoja skladnosti, analiza incidentov
Act	Izboljšave, prilagoditve glede na nove grožnje in tehnologije

HVALA

info@enisa.europa.eu

www.enisa.europa.eu