SMART COM

Priporočila za učinkovito prilagoditev zahtevam direktive NIS 2

www.smart-com.si

IZJAVA

Poročilo je pripravljeno na osnovi podatkov, ki ste jih vnesli v vprašalnik za oceno, ali mora organizacija zagotoviti skladnost z Direktivo 2022/2555, ki določa visoko skupno raven varnosti omrežij in informacijskih sistemov v Evropski Uniji.

Poudarjamo, da je poročilo zgolj informativne narave in temelji na vnesenih podatkih.

Čeprav se trudimo zagotoviti natančnost in zanesljivost informacij, želimo poudariti, da nismo pravno zavezani rezultatom, ki ste jih prejeli na osnovi vnesenih podatkov v vprašalnik ali morebitnim posledicam, ki izhajajo iz uporabe teh informacij.

Uporabniki so sami odgovorni za preverjanje točnosti podatkov ter za morebitne dodatne korake, ki jih je treba sprejeti za doseganje skladnosti z evropsko direktivo.

KAZALO

Področja ukrepov za zagotavljanje skladnosti z direktivo NIS 2 4

1. Vključenost poslovodstva 4

2. Varnostna politika organizacije 5

3. Ozaveščanje osebja o varnostnih grožnjah 6

4. Upravljanje ključnih virov IKT 8

5. Posodabljanje programske opreme 9

6. Upravljanje dostopa do delovnih postaj in omrežja 10

7. Zaščita delovnih postaj in prenosnih naprav 12

8. Arhiviranje podatkov 13

9. Zaščita strežnikov in omrežnih komponent 14

10. Varen oddaljeni dostop 16

11. Zaščita pred zlonamerno programsko kodo 17

12. Zaščita pred drugimi grožnjami 18

13. Neprekinjenost poslovanja in upravljanje incidentov 19

Hitreje do skladnosti ter povišanja ravni kibernetske odpornosti 20

PODROČJA UKREPOV ZA ZAGOTAVLJANJE SKLADNOSTI Z NIS 2

Glede na to, da ste kot organizacija **zavezani k izpolnjevanju zahtev iz direktive NIS 2**, vam priporočamo, da preverite stopnjo zrelosti vaše organizacije z vidika kibernetske varnosti.

Stopnjo zagotavljanja skladnosti z direktivo NIS 2 **lahko ocenite s pomočjo trinajstih področij ukrepov**, ki so tudi del naše metodologije za ugotavljanje zrelostne ravni kibernetske varnosti v organizacijah in s tem skladnosti z direktivo NIS 2.

Na osnovi tehtnega premisleka se nato lahko odgovorno odločite za uvedbo ukrepov tam, kjer ugotovite, da vam preti največja grožnja oziroma na področju, kjer bo učinek spremembe največji.

1. Vključenost poslovodstva

Kibernetska varnost za organizacije predstavlja temelj uspešnega poslovanja. Tehnologija se neprestano razvija, kar pa prinaša tudi grožnje pred zlorabo podatkov in razkritjem informacij. **Poslovodstvo mora poskrbeti za varno obdelavo in učinkovito varovanje podatkov.** Ravno tako mora poslovodstvo oblikovati celovito strategijo varovanja informacij in nadzorovati raven pripravljenosti organizacije za uspešno obvladovanje kibernetskih groženj.

Predvsem je poslovodstvo tisto, ki določa način organiziranja, oblikuje varnostno politiko vključno s politiko usposabljanja zaposlenih na področju varovanja informacij in obvladovanja kibernetskih groženj ter na splošno predpisuje in nadzoruje ukrepe za dvig ravni kibernetske varnosti.

Direktiva NIS 2 namenja poslovodstvu ključno vlogo in posledično **nalaga neposredno odgovornost za posledice kibernetskih napadov**. Še posebej je to pomembno, kadar se posledice napada prelijejo preko meja napadene organizacije in ogrozijo širše kibernetsko okolje.

DOBRA PRAKSA

Poslovodstvo naj ukrepe sprejema šele po opravljeni celoviti analizi potreb, na osnovi katere bo postavilo zahteve glede ciljne ravni varnostne pripravljenosti in bo oblikovalo strategijo razvoja kibernetske varnosti.

Dobro izhodišče za oblikovanje učinkovitih procesov je uvedba upravljanja storitev IT skladno z eno od zbirk dobrih praks, kot na primer ITIL (Information Technology Infrastructure Library), priporočljiva pa je tudi vpeljava mednarodno priznanega standarda, kot je na primer ISO/IEC 9001 (mednarodni standard za vodenje kakovosti).

Ta organizaciji pomaga prepoznavati, spremljati in izboljševati ključne procese, katere oblikuje na način, da v največji meri izpolnjujejo dejanske potrebe organizacije. Hkrati uvedba standarda zahteva redne neodvisne presoje organizacijske zrelosti, kar pomaga organizaciji k stalnemu izboljševanju.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. Pooblaščenec za informacijsko oz. kibernetsko varnost naj deluje neodvisno in ni del ekipe IT.
2. Cilje spremljanja sistemov in omrežja je potrebno jasno določiti.
3. Redno naj se izvaja ocena varnostnih tveganj in analiza poslovnih učinkov.
4. Ključni rezultat stalnega spremljanja je akcijski plan, s katerim poslovodstvo določa strategijo in opredeli nadaljnje ukrepe za dvig ravni kibernetske varnosti.

2. Varnostna politika

Dobro zasnovana in premišljena varnostna politika je ključnega pomena za vsako organizacijo, saj **določa smernice, pravila in postopke za zaščito njenih informacij in sredstev**. Učinkovita varnostna politika zagotavlja okvir za prepoznavanje, preprečevanje in obvladovanje tveganj v kibernetskem okolju. Z vzpostavitvijo jasnih smernic za varno ravnanje s podatki in informacijskimi sistemi organizacija zmanjšuje možnost kibernetskih napadov ter ohranja zaupnost, integriteto in razpoložljivost ključnih virov. Poleg tega dobro delujoča varnostna politika pomaga pri izpolnjevanju regulativnih zahtev,

krepitvi zaupanja deležnikov in vzpostavitvi kulture ozaveščenosti o kibernetski varnosti med zaposlenimi. **Varnostna politika deluje kot temeljni dokument**, ki usmerja vsa prizadevanja za ohranjanje kibernetske varnosti organizacije in vzpostavljanje njene odpornosti na sodobne grožnje.

DOBRA PRAKSA

Organizacija naj opravi analizo varnostne pripravljenosti in oceni tveganja ter vpliv groženj na poslovanje. Pri tem je lahko v pomoč zunanji pogled delovanja organizacije in prenos dobrih praks iz drugih okolij. Vpeljava mednarodnega standarda, kot je ISO/IEC 27001 (Informacijska varnost), oziroma sorodnih standardov organizaciji pomaga k prenosu dobrih praks v svoje okolje, hkrati pa zagotovi redne neodvisne presoje organizacijske zrelosti na področju varovanja informacij.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. V organizaciji naj se vpelje koncept "potrebe po vedenju".
2. V organizaciji naj se vpelje koncept "čiste mize".
3. Organizacija naj pripravi in predstavi pravilnik o odgovornem razkritju ranljivosti.
4. Če je možno, naj se vpelje koncept varnega tiskanja. Še posebej, če organizacija uporablja skupne tiskalnike.

3. Ozaveščanje osebja o varnostnih grožnjah

Kot najpomembnejši vektor kibernetskega napada prevladuje socialni inženiring. Večina napadov se začne pri zaposlenih ali zunanjih sodelavcih ali partnerjih, ki z napačnim ravnanjem ali opustitvijo dolžnega ravnanja dopustijo napadalcu,

da prodre do vitalnih sistemov v omrežju organizacije.

Zato je naloga in odgovornost poslovodstva, da poskrbi za neprestano usposabljanje in dvig ravni varnostne ozaveščenosti osebja. Tako zaposleni kot zunanji sodelavci in partnerji se morajo seznaniti s pomenom in zahtevami zagotavljanja kibernetske varnosti.

Organizacija naj prilagojeno različnim vlogam v organizaciji in glede na ocenjeno tveganje, vezano na vlogo posameznika ali skupine, zagotovi redno ozaveščanje o kibernetski varnosti in jih seznanja z aktualnimi grožnjami ter načini, kako se z dobro prakso ubraniti pred njimi. Osebje je potrebno seznaniti s postopki za ravnanje v primeru zaznave varnostnega dogodka in ukrepanjem v primeru varnostnega incidenta.

Vsaka organizacija mora poskrbeti za jasne in pregledne postopke ravnanja ob varnostnih dogodkih in incidentih, s katerimi mora biti seznanjeno osebje, da se bodo posamezniki, službe za ukrepanje in organizacija kot taka pravilno odzvali in pravočasno ter na primeren način znali preprečiti oziroma omejiti škodo v primeru kibernetskega napada.

DOBRA PRAKSA

Organizacija naj redno preverja raven varnostne ozaveščenosti skozi izvedbo preizkusov ozaveščenosti, kot so preizkus ribarjenja (phishing) ali pregled z izkoriščanjem socialnega inženiringa. Pri tem se priporoča pogosta menjava metodologije in po potrebi tudi izvajalca.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. Naj bo poznavanje in spoštovanje pravil ravnanja del postopka ocenjevanja osebja.
2. Občasno ocenite varnostno ozaveščenost in odzivnost uporabnikov.
3. Organizacija naj zbira, spremlja in obravnava tudi potencialne grožnje (grožnje, ki se niso uresničile).
4. Organizacija naj načrtuje redna izobraževanja in preverjanja zaposlenih kot partnerjev oz. podizvajalcev o pomembnosti kibernetske varnosti.

4. Upravljanje ključnih virov IKT

Sodobnega poslovanja si ne moremo predstavljati brez uporabe elektronskih naprav, programske opreme in drugih kibernetskih sistemov ter informacijskih storitev, ki so bodisi osebne oziroma jih uporablja le ena oseba ali so v souporabi več uporabnikov. Priporočljivo je, da ima organizacija izdelan popis vseh sredstev IKT, kar velja tako za strojno kot programsko opremo. Pri tem naj bodo vključeni tudi informacijski viri, ki jih organizacija uporablja v obliki spletne ali oblačne storitve.

Organizacija naj zagotovi primeren nadzor nad svojim informacijskim okoljem, kar vključuje tako ustrezno organiziranost kot razpoložljivost primernih orodij za izvajanje nadzora. **Za višjo raven zaščite naj organizacija razmisli o orodjih, ki omogočajo nadzor nad sumljivimi dogodki in korelacijo dogodkov iz različnih informacijskih virov**, spremljanje prenosa večjih količin podatkov izven omrežja organizacije, samodejno analizo in odzivanje na zaznane varnostne dogodke ter orodja za ugotavljanje skladnosti na različnih področjih.

DOBRA PRAKSA

Organizacija lahko za varovanje in upravljanje ključnih virov IKT lastne vire nadomešča z najemom storitev zunanjih organizacij, ki so usposobljene za določen vidik varovanja oziroma svetovanja pri organiziranju varovanja. Ob tem je zelo pomembno, da se predhodno premisli in določi primeren obseg sporazuma o ravni storitev, ki jih organizacija najema pri zunanjem izvajalcu.

Prav tako naj organizacija zagotovi spremljanje dela zunanjih izvajalcev in redno ocenjuje doseganje ključnih parametrov storitev.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. Organizacija naj uporablja primerno orodje za upravljanje konfiguracij.
2. Organizacija naj določi osnovno varnostno konfiguracijo.
3. Organizacija naj zagotovi jasnost in preglednost ravni storitev, ki jih zagotavljajo zunanji izvajalci, ter jih redno preverja tudi s stališča zagotavljanja kibernetske varnosti.

4 Raven varovanja naj bo sorazmerna in enakomerno porazdeljena po celotnem omrežju.

5 Organizacija naj redno preverja skladnost s sistemom za upravljanje informacijske varnosti za vsa informacijska sredstva, izvajalce del, dobavitelje.

5. Posodabljanje programske opreme

Posodabljanje programske opreme je ključnega pomena za pravilno in varno delovanje programske opreme. Organizacije morajo s posodabljanjem programske opreme seznaniti zaposlene oziroma zagotoviti samodejno posodabljanje. Pri tem je priporočljiva uvedba mehanizmov, ki onemogočajo delo naprav ali sistemov z neustrezno programsko opremo v omrežju organizacije.

Organizacije naj spremljajo informacije o kritičnih varnostnih grožnjah, ki jih objavljajo proizvajalci in druge pristojne organizacije kot je npr. SI-CERT. Pri tem morajo pravočasno posodabljati programsko opremo ali pa preko drugih mehanizmov obvladovati grožnje.

Kjer je to tehnično izvedljivo in dovolj varno, naj se programska oprema posodablja samodejno.

DOBRA PRAKSA

Organizacija naj redno preverja varnost informacijskega sistema z izvajanjem zunanjih in notranjih varnostnih pregledov, pregledov brezžičnega omrežja, pregledov svojih spletnih strani in aplikacij.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1 Organizacija naj pripravi testno okolje in postopke za varno preverjanje nadgradenj preden le-te prenese v delovno okolje.

2 Organizacija naj jasno določi in pojasni izjeme pri samodejnih posodobitvah programske opreme.

3 Organizacija naj redno posodablja programsko opremo kot so brskalniki in vtičniki.

4 Pred vsako nadgradnjo strežnikov naj se naredi celovit arhiv, po nadgradnji pa kopijo za nujno popravilo.

6. Upravljanje dostopa do delovnih postaj in omrežja

Upravljanje dostopa do delovnih postaj in omrežja je ključno za zagotavljanje varnosti informacij v organizaciji.

S pravilnim upravljanjem dostopa organizacija nadzira, kdo ima dostop do določenih virov, zmanjšuje tveganje nepooblaščenega dostopa ter varuje občutljive podatke. Pri tem so na voljo različne oblike učinkovitih identifikacijskih in avtentikacijskih mehanizmov, kot so gesla, večfaktorska avtentikacija in biometrija. Gesla naj bodo najmanj 12-mestna in naj vsebujejo čim večji nabor znakov (male in velike črke, številke, posebni znaki). Sistematično dodeljevanje pravic, na osnovi potreb posameznika za opravljanje delovnih nalog, še dodatno krepi varnost.

Redno spremljanje in revizija uporabniških pravic ter hitro ukrepanje ob zaznanih nepravilnostih pripomoreta k agilnemu in odzivnemu upravljanju dostopa. Celovit pristop k temu vprašanju je ključnega pomena za vzpostavitev robustnega sistema kibernetske varnosti v organizaciji. Organizacija naj posebno pozornost posveti postopkom ob ukinitvi pravic in pa nadzoru nad zunanjimi izvajalci, ki se gibljejo v prostorih organizacije oziroma vstopajo v omrežje organizacije.

DOBRA PRAKSA

Uporaba dolgih in zapletenih gesel uporabnike sili v shranjevanje gesel na različnih platformah. Za nekaj ključnih gesel naj velja politika, da uporaba takšnih sistemov ni dovoljena, lahko pa organizacija vzpostavi interni sistem za upravljanje z gesli.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1 Organizacija naj zagotovi sistem, ki od uporabnika zahteva redno menjavanje gesel in zapoveduje primerno dolžino ter zapletenost gesel.

2 Del politike naj bo prepoved prijavljanja z administratorskimi pooblastili za izvajanje rednih nalog.

3	Uporabniki naj vedno uporabljajo le svoj račun, deljenje gesel za dostop do uporabniških računov naj bo izrecno prepovedano.
4	Uporabniki naj imajo dostop le do informacij, ki jih potrebujejo za opravljanje nalog. Organizacija naj vzpostavi in se ravna skladno s pristopom "potrebe po vedenju".
5	Uporablja naj se dvo ali večfaktorska avtentikacija.
6	Računi z administratorskimi pravicami naj imajo delno ali v celoti omejen dostop do interneta.
7	Organizacija naj vzpostavi sistem, ki bo samodejno preverjal, zaznaval in obveščal o neprimerni uporabi dostopov, nenavadne dostope do podatkov in podobne aktivnosti. Sistem naj hrani vse dogodke za določeno časovno obdobje (vsaj nekaj mesecev) in povzetke oz. zbirnike za daljše obdobje (več kot eno leto).
8	Organizacija naj zagotovi redno preverjanje centralnih sistemov za dostop (AD ali LDAP).

7. Zaščita delovnih postaj in prenosnih naprav

Zaščita delovnih postaj in prenosnih naprav je ključna za ohranjanje celovitosti, zaupnosti in razpoložljivosti informacij. To vključuje vpeljavo samodejnega zaklepanja naprav, učinkovite protivirusne programe, požarne zidove in redne varnostne posodobitve. **Uporaba stroge politike gesel, šifriranje podatkov ter izvajanje rednih varnostnih kopij prispevajo k odpornosti proti izgubi podatkov**. Določanje in nadzor dostopnih pravic preprečujeta nepooblaščen dostop do občutljivih informacij.

Izobraževanje zaposlenih o nevarnostih socialnega inženiringa ter pravilno ravnanje s podatki je ključno za preprečevanje napak zaposlenih. Dodatna zaščita se doseže z uporabo virtualnih zasebnih omrežij (VPN) pri delu na oddaljenih lokacijah.

S kombinacijo teh metod organizacija vzpostavlja celovit pristop k varovanju svojih delovnih postaj in mobilnih naprav pred različnimi kibernetskimi grožnjami.

DOBRA PRAKSA

Organizacija naj poskrbi, da so prenosne naprave zaščitene pred krajo in nepooblaščenim dostopom s programsko opremo, ki zagotavlja šifriranje podatkov shranjenih v napravi in oddaljeno brisanje podatkov.

Uporabnik teh nastavitev sam ne more spreminjati. Ravno tako naj bo glede na potrebe uporabnikov nastavljena zaščita pred uporabo zunanjih medijev, priporoča pa se, da sistem ne dovoli funkcije samodejnega zagona zunanjih medijev.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. Organizacija naj zagotovi, da so podatki na vseh prenosnih računalnikih kriptirani in ustrezno zaščiteni v primeru nepooblaščenega dostopa ali kraje naprave.
2. Podatki, shranjeni v oblaku, naj bodo šifrirani.
3. Odrabljeni podatkovni mediji naj se fizično uničijo.
4. Organizacija naj onemogoči uporabo osebnih naprav v poslovnem okolju. Kjer je dovoljena deljena uporaba informacijskih sredstev, naj bo naprava last organizacije in kot taka v celoti podvržena varnostni politiki organizacije.
5. Organizacija naj zagotovi ustrezne tehnične ukrepe, da bo delo na daljavo potekalo zgolj po šifriranih povezavah in da bo prenos podatkov nadzorovan, karakteristike prenosa pa ustrezno hranjene. Organizacija naj vzpostavi primeren sistem za preprečevanje nepooblaščenega prenosa podatkov izven organizacije (DLP).
6. Raven zaščite podatkov, ki jo zagotavljajo ponudniki storitev v oblaku, naj bo ustrezna kritičnosti podatkov, ki se hranijo v oblaku.
7. Uporabniki naj se redno izobražujejo o varni uporabi delovnih postaj in prenosnih naprav. Znanje naj se preverja, rezultat preverjanja pa naj bo del postopka ocenjevanja zaposlenih.

8. Arhiviranje podatkov

Arhiviranje podatkov je ključnega pomena za dolgoročno upravljanje informacij in izpolnjevanje zakonskih zahtev. Pomaga ohranjati zgodovinsko kontinuiteto organizacije, hkrati pa optimizira prostor na aktivnih sistemih. Učinkovite metode vključujejo redno klasificiranje podatkov glede na njihovo pomembnost, s čimer se določi, katere podatke arhivirati. Uporaba varnih in trajnostnih medijev za shranjevanje arhivskih podatkov ter njihovo pravilno označevanje pospešuje iskanje in obnavljanje informacij. Zasnovati je treba tudi jasno politiko zbiranja, hrambe in uničenja arhivskih podatkov v skladu z regulativnimi smernicami. S pravilnim arhiviranjem podatkov organizacija ne le **izpolnjuje zakonodajne zahteve, pač pa tudi izboljšuje upravljanje z informacijami ter pripomore k učinkovitemu in preglednemu delovanju**.

DOBRA PRAKSA

Arhivske kopije naj bodo shranjene na oddaljeni lokaciji. Podatki v arhivu naj bodo šifrirani. Organizacija naj redno izvaja preverbo povrnitve arhiviranih podatkov.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. Organizacija naj zagotovi redno izdelavo arhivskih kopij po vnaprej določeni časovnici, hrambo na varni lokaciji, primerno oddaljeni od centralne lokacije in občasno izdelavo časovnega posnetka kritičnih podatkov za obnovitev poslovanja, ki so po izdelavi hranjeni brez neposrednega dostopa z omrežja.
2. Preizkusi obnovitve podatkov naj se izvajajo v rednih presledkih, da se s tem preverja kakovost podatkovnih kopij.
3. Organizacija naj dokumentira in skrbno preverja izvajanje ravni storitev ponudnika oblačnih storitev ter redno preverja primernost ponudnika upoštevajoč evolucijo lastnih zahtev.

9. Zaščita strežnikov in omrežnih komponent

Zaščita strežnikov in omrežnih komponent je ključna za ohranjanje stabilnosti in varnosti informacijskih sistemov.

Učinkovite metode vključujejo **uporabo požarnih zidov, sistematično posodabljanje programske opreme in izvajanje rednih varnostnih pregledov**. Šifriranje podatkov med prenosom in hranjenjem dodatno zmanjšuje tveganje nepooblaščenega dostopa. Vzpostavljanje politik dostopa in dodeljevanje pravic zgolj glede na dejanske potrebe uporabnikov omejuje možnost zlorabe. Redno spremljanje omrežnih aktivnosti s pomočjo varnostnih informacijskih in dogodkovnih sistemov ter uvedba sistemov za zaznavanje vdorov prispevajo k hitremu prepoznavanju morebitnih groženj.

DOBRA PRAKSA

Vsa prednastavljena gesla je potrebno zamenjati in odstraniti odvečne račune. Vstop napadalca skozi tovarniško nastavljen račun administratorja na omrežni napravi je žal še vedno zelo pogosta metoda vdora, ki napadalcu omogoča enostavno zlorabo sistema. Brezžično omrežje naj bo zaščiteno z ustreznim šifrirnim algoritmom, kot je WPA2-Enterprise.

Odvečni vhodi na omrežni napravi naj bodo blokirani, prav tako naj bodo onemogočene storitve, ki niso v uporabi. Administratorji naj do strežnikov dostopajo preko ločenega omrežja. Vsi komunikacijski protokoli v podjetju morajo biti varni, ravno tako pa mora biti za obiskovalce vzpostavljeno ločeno brezžično omrežje.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. Dnevniki dostopov naj se hranijo najmanj 6 mesecev.
2. Brezžično omrežje organizacije naj bo zaščiteno s protokolom WPA2-Enterprise z registracijo naprav.
3. Pri uporabi vseh sistemov naj se upoštevajo standardi in varnostna priporočila proizvajalcev.
4. Za administracijo strežnikov naj se uporablja ločeno omrežje.

5 Vzpostavijo naj se organizacijski ukrepi, ki bodo omogočali obravnavo vseh varnostnih obvestil za strežnike, požarne pregrade in kritične omrežne komponente.

6 Vzpostavi naj se sistemski nadzor vseh dnevniških zapisov, analiza in obveščanje v primeru nepredvidenih dogodkov.

7 Vzpostavi naj se sistem za zaznavo in preprečevanje vdorov, ki bo ščitil vse komunikacijske poti.

8 Zagotovljen naj bo nadzor nad fizičnim dostopom do strežnikov in mrežnih komponent. Vsak fizičen dostop oziroma poseg naj bo zabeležen.

9 Organizacija naj redno izvaja varnostno testiranje sistema (npr. penetracijski testi, testi ranljivosti).

10. Varen oddaljeni dostop

Varen oddaljeni dostop je pomemben za prilagodljivo delovno okolje. Uporaba navideznih zasebnih omrežij (VPN) omogoča šifriran in zaseben dostop do omrežja.

Dvo ali večfaktorska avtentikacija (2FA) dodatno utrjuje varnost in omejuje možnost zlorabe gesel.
S politikami dostopa, ki temeljijo na dejanskih potrebah, se omeji tveganje nepooblaščenega dostopa.

Osebje je treba izobraževati o varnih praksah pri delu na daljavo, kar povečuje ozaveščenost in omejuje grožnjo socialnega inženiringa. S skrbno izbranimi in ustrezno uporabljenimi varnostnimi ukrepi organizacija zagotavlja zanesljiv in varen oddaljeni dostop, ključen za sodobno delovno okolje.

DOBRA PRAKSA

Oddaljeni dostop naj se zapre po določenem času neaktivnosti uporabnika. Raven pravic naj bo prilagojena potrebam dela, pri čemer naj seoddaljeni dostop posebej omeji za administrativne posege. Oddaljeni dostop se lahko dodatno zaščiti z določitvijo dovoljenj glede na regijo in naslov IP ponudnika spletnih storitev.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. Organizacija naj dovoli uporabnikom izključno oddaljeni dostop preko navideznih zasebnih omrežij (VPN).
2. Za dostop iz zunanjih javnih omrežij naj se zahteva uporabo močne avtentikacije (2FA, varnost na prvem mestu, princip ničelnega zaupanja).
3. Oddaljeni dostopi naj se omejujejo na ponudnikov naslov IP in regijo.

11. Zaščita pred zlonamerno programsko kodo

Zaščita pred zlonamerno programsko kodo je temeljna za varnost informacijskih sistemov.

Organizacija naj uporablja sodobne protivirusne rešitve ter redno posodablja programsko opremo. Zaščita naj bo nameščena na vseh delovnih postajah, mobilnih napravah in strežnikih.

Filtriranje e-pošte, preverjanje pristnosti prenosov in omejevanje uporabe nepreverjenih aplikacij so učinkoviti ukrepi za preprečevanje okužb.

Pomembno je tudi izboljšanje ozaveščenosti zaposlenih o nevarnostih socialnega inženiringa ter usposabljanje za prepoznavanje sumljivih dejavnosti.

Kombinacija teh pristopov oblikuje celovito strategijo za zmanjšanje tveganj in krepitev odpornosti organizacije pred zlonamernimi kibernetskimi napadi.

DOBRA PRAKSA

Protivirusna zaščita se mora samodejno posodabljati, pri čemer uporabnik ne sme imeti dovoljenj za izklop zaščite. Prenosno napravo z neustrezno protivirusno zaščito je potrebno zaustaviti pred prijavo v delovno omrežje organizacije in ji dostop odobriti šele po podrobnem pregledu in posodobitvi protivirusne zaščite.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. Obvestila, ki jih pošilja protivirusna zaščita, naj se zbirajo, kategorizirajo in preverjajo s strani strokovnega osebja za kibernetsko varnost.
2. Organizacija naj redno preverja pravilnost namestitev protivirusne zaščite in poskrbi za usposabljanje uporabnikov.
3. Organizacija naj pri neodvisnih virih redno spremlja primerjave in poročila o kakovosti in zmogljivosti protivirusne zaščite, ki jo uporablja.

12. Zaščita pred drugimi grožnjami

Organizacija se učinkovito zaščiti pred raznolikimi grožnjami kibernetske varnosti z implementacijo celovite strategije.

Za preprečevanje izsiljevalske programske opreme in lažnega predstavljanja je ključno izvajanje stalnih izobraževanj zaposlenih o teh grožnjah ter uvedba filtrov za prepoznavanje sumljivih e-poštnih sporočil. Notranje grožnje se naslavljajo s striktnimi politikami dostopa, nadzorom uporabniških pravic in sistematičnim spremljanjem aktivnosti zaposlenih.

Napredne dolgotrajne grožnje zahtevajo napredne varnostne rešitve, kot so sistemi za preprečevanje vdorov, zaznavanje groženj in redno izvajanje varnostnih testiranj.

DOBRA PRAKSA

Stalno sodelovanje z zunanjimi strokovnjaki za kibernetsko varnost in redno prilagajanje ukrepov glede na najnovejše grožnje so ključni za vzpostavitev odpornega kibernetskega okolja.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. Organizacija naj identificira vse sisteme za zagotavljanje kibernetske varnosti, ki jih uporablja, popiše raven storitev, ki jih zagotavljajo proizvajalci programske opreme in posebej raven storitev, ki jo zagotavljajo zunanji izvajalci.

2. **Organizacija naj oceni potreben obseg dela za posamezen sistem na treh ravneh upravljanja:**
   - osnovna raven - osnovno upravljanje za delovanje sistema (administracija sistema, upravljanje sistemskih nastavitev, posodabljanje, obnova, poročanje);
   - napredna raven - napredno upravljanje sistema (integracija sistema v okolje IKT, napredne nastavitve, evolucija delovanja v smislu večjih posodobitev, dograditev, načrtovanje in izvedba menjav);
   - strateška raven - priprava politik in obravnava zaznav (razumevanje sistemskih obvestil, načrtovanje ukrepov in eskalacij, organizacijski ukrepi in nadzor, razumevanje logične umestitve sistema v poslovanje podjetja v smislu priprave zahtev za poročanje, priprave zahtev za povezovanje med sistemi, priprave zahtev za evolucijo obratovanja).

3. Organizacija naj oceni potreben obseg dela in oblikuje zahtevano raven storitev, ki bi jo prepustila zunanjemu izvajanju.

13. Neprekinjenost poslovanja in upravljanje incidentov

Kljub delujočemu sistemu kibernetske varnosti lahko pride do varnostnih dogodkov, ki prerastejo v varnostni incident. Zaradi tega morajo imeti organizacije vzpostavljen načrt neprekinjenega poslovanja, ki zagotavlja, da organizacija kljub nepričakovanim dogodkom ohranja neprekinjenost poslovanja. To vključuje **izdelavo načrtov za obvladovanje motenj, vzpostavitev varnostnih kopij podatkov in redno preizkušanje postopkov obnovitve**.

Upravljanje incidentov pa je ključno za hitro in organizirano odzivanje na kibernetske napade ali druge izredne dogodke. Učinkovite metode vključujejo vzpostavitev ekipe za odziv na incidente, sistematično analizo napadov in neprestano izboljševanje odzivnih postopkov.

Z usmerjenim pristopom k neprekinjenemu poslovanju in upravljanju incidentov organizacija zagotavlja odpornost ter zmanjšuje škodo ob morebitnih kibernetskih napadih.

DOBRA PRAKSA

Dobra praksa vključuje redne vaje za usposabljanje zaposlenih, vzpostavitev centralnega sistema za zaznavanje in odzivanje na incidente ter sodelovanje z zunanjimi strokovnjaki za kibernetsko varnost. Morebitno škodo v primeru uspešnega kibernetskega napada lahko organizacija omeji tudi s sklenitvijo ustreznega zavarovanja, pri čemer pa se mora zavedati, da slednje ne more odvrniti vseh posledic uspešnega napada, niti zmanjšati odgovornosti poslovodstva za nastalo škodo.

Pomembni ukrepi, ki naj jih organizacija uveljavi:

1. Organizacija naj načrte za neprekinjeno poslovanje redno preverja in obravnava najmanj enkrat letno.
2. Organizacija naj razmisli o možnosti sklenitve zavarovalnega kritja za kibernetske varnostne incidente.
3. Organizacija naj razmisli o možnostih vzpostavitve nadomestnih virov električnega napajanja, komunikacijskih povezav, lokacije za začasno delo.

Hitreje do skladnosti ter povišanja ravni kibernetske odpornosti

Analizo stopnje kibernetske zrelosti organizacije lahko opravite sami, lahko pa poiščete pomoč pri zunanjih strokovnjakih za posamezno tehnološko področje oziroma presojo in oblikovanje procesov. Smart Comovi strokovnjaki za kibernetsko varnost in procese vam pri tem znamo pomagati.

Oblikovali smo storitev procesnega svetovanja za prilagoditev organizacije zahtevam direktive NIS 2, ki zajema:

1. Vrednotenje trenutnega stanja in ravni kibernetske varnosti (tako v poslovnih kot industrijskih okoljih)
2. Prepoznavanje potreb
3. Pomoč pri pripravi strategij in postavitev zahtev glede na poslovne cilje organizacije
4. Svetovanje pri vzpostavitvi procesov
5. Pomoč pri oblikovanju zahtev za spremembe v smeri skladnosti z direktivo NIS 2

Organizacijam na poti do sprememb pomagamo tudi v obliki strukturiranega vprašalnika, s pomočjo katerega določimo potrebe posamezne organizacije.

Vprašanja po predhodnih razgovorih in izvedeni analizi prilagodimo konkretni organizaciji.

S tem poslovodstvo organizacije ob pomoči svetovalca kar najbolj učinkovito **pridobi vpogled v dejanske potrebe svojega poslovanja** in nato oblikuje zahteve za uvedbo potrebnih sprememb v organizaciji, procesih in sistemih.

SMART COM

Smo specializirani za vzpostavljanje kibernetske varnosti tako v poslovnih kot industrijskih okoljih. In kot taki zanesljiv partner podjetjem in organizacijam pri doseganju skladnosti z direktivo NIS 2. Naša strokovnost in specializacija na področju kibernetske varnosti nam omogočata, da nudimo celovito storitev ter rešitve za podporo procesu prilagajanja zakonodaji.

Dodatne informacije

Igor Mlakar
Direktor operative

igor.mlakar@smart-com.si

01 530 82 60

Strateški partner pri načrtovanju in integraciji IKT infrastrukture

Smo neodvisen sistemski integrator in zagotavljamo razvoj, skladnost in izgradnjo celotnega informacijsko – komunikacijskega ekosistema. Nastopamo kot svetovalec kibernetske varnosti v poslovnih in industrijskih okoljih in načrtovalec sodobnih omrežij, v kasnejši fazi pa tudi lahko kot dobavitelj, integrator, vzdrževalec ali upravljalec omrežnih ali varnostnih sistemov.

Obvladovanje najsodobnejših razvojnih in tehnoloških rešitev, številne partnerske naveze in usposobljeni strokovnjaki omogočajo najboljše rešitve po meri naročnika.

Vizija

Utrditi položaj enega izmed vodilnih partnerjev pri izvajanju sodobnih, kompleksnih in informacijsko varnih IKT infrastruktur na trgu. To dosegamo samostojno s krepitvijo dolgoročnih poslovnih povezav in partnerskih odnosov na področju razvoja, izobraževanja, storitev in trženja.

Poslanstvo

Razvijati, načrtovati, uvajati in upravljati celovito ter informacijsko varno IKT infrastrukturo po meri uporabnika.

#skupaj je bolje

www.smart-com.si