ME/PSO

DORACAK

Doracak për sigurinë e informacionit

Bazat, parimet dhe praktikat e përditshme për mbrojtjen e informacionit

Material shoqërues për trajnimin:
„Ngritja e vetëdijes për sigurinë e informacionit“

Dokument nr. MEPSO-PRI-IB-001 · Klasifikimi: Përdorim i brendshëm
Sektori i sigurisë informatike dhe kibernetike · MEPSO SHA Shkup

Përmbajtja

1. Hyrje

Informacioni është një nga pasuritë më të rëndësishme të çdo organizate. Në MEPSO, si operator i infrastrukturës kritike, mbrojtja e informacionit nuk është vetëm çështje teknike — ajo është përgjegjësi e çdo punonjësi.

Ky doracak i shpjegon konceptet themelore të sigurisë së informacionit në mënyrë të kuptueshme dhe jep udhëzime praktike që mund t'i zbatoni çdo ditë. Qëllimi nuk është t'ju bëjë ekspert, por t'ju japë njohuri dhe vetëdije për t'i njohur rreziqet dhe për të vepruar në mënyrë të sigurt.

Çdo ditë punojmë me të dhëna të ndjeshme — të dhëna operative për sistemin e transmetimit të energjisë elektrike, të dhëna personale të punonjësve, informacione afariste dhe dokumentacion teknik. Kompromet imi i këtyre informacioneve mund të shkaktojë pasoja serioze: nga dëmi financiar dhe çrregullimi i punës, deri te rrezikimi i sigurisë së infrastrukturës kritike.

> **Pse është e rëndësishme kjo për ju.** Pjesa më e madhe e incidenteve të sigurisë nuk ndodhin për shkak të sulmeve të sofistikuara teknike, por për shkak të gabimeve të thjeshta njerëzore — një fjalëkalim i dobët, klikimi në një link të dyshimtë, ose lënia e kompjuterit të pakyçur. Pikërisht për këtë, vetëdija juaj është linja e parë dhe më e rëndësishme e mbrojtjes.

2. Çfarë është siguria e informacionit

Siguria e informacionit është praktika e mbrojtjes së informacionit nga qasja, përdorimi, zbulimi, çrregullimi, ndryshimi ose shkatërrimi i paautorizuar. Ajo përfshin jo vetëm të dhënat digjitale, por edhe informacionet në formë letre, komunikimin me gojë dhe njohuritë e punonjësve.

2.1 Llojet e informacioneve që i mbrojmë

- **Të dhëna operative** — informacione për gjendjen dhe menaxhimin e sistemit të transmetimit të energjisë elektrike;
- **Të dhëna personale** — informacione për punonjësit, bashkëpunëtorët dhe palët e treta;
- **Informacione afariste** — kontrata, të dhëna financiare, plane strategjike;
- **Dokumentacion teknik** — skema, konfigurime, procedura të sigurisë;
- **Të dhëna qasjeje** — fjalëkalime, çelësa, certifikata.

2.2 Nga çfarë i mbrojmë

Kërcënimet mund të vijnë nga burime të ndryshme:

Burimi i kërcënimit	Shembull
Sulmues të jashtëm	Hakerë, grupe të organizuara të krimit kibernetik
Softuer keqdashës	Viruse, ransomware, programe spiunimi
Kërcënime të brendshme	Punonjës të pakënaqur ose të pakujdesshëm
Gabim njerëzor	Fshirje aksidentale, dërgim i gabuar i të dhënave
Kërcënime fizike	Vjedhje e pajisjeve, qasje e paautorizuar në hapësira
Fatkeqësi natyrore	Zjarr, përmbytje, ndërprerje e rrymës

3. Parimet: konfidencialiteti, integriteti, disponueshmëria

Siguria e informacionit bazohet në tre parime themelore, të njohura si „triada CIA“ (Confidentiality, Integrity, Availability).

3.1 Konfidencialiteti (Confidentiality)

Informacionet janë të disponueshme vetëm për personat që kanë autorizim për t’u qasur në to. Kjo arrihet përmes kontrollit të qasjes, enkriptimit dhe parimit të privilegjit më të vogël — secili përdorues merr vetëm ato të drejta që i janë të nevojshme për punën e tij.

> **Shembull.** Raportet financiare duhet të jenë të disponueshme vetëm për sektorin financiar dhe udhëheqjen, jo për të gjithë punonjësit. Nëse secili ka qasje në gjithçka, rreziku i keqpërdorimit ose rrjedhjes rritet në mënyrë dramatike.

3.2 Integriteti (Integrity)

Saktësia dhe tërësia e informacioneve mbrohen nga ndryshimet e paautorizuara ose aksidentale. Çdo ndryshim i të dhënave kritike duhet të evidentohet dhe të jetë i gjurmueshëm, që të mund t’u besojmë se informacionet janë të sakta dhe të pandryshuara.

> **Shembull.** Nëse dikush i ndryshon pa autorizim parametrat e konfigurimit të një sistemi, kjo mund të shkaktojë funksionim të gabuar. Mekanizmat e integritetit (evidenca, shumat kontrolluese, versionet) na mundësojnë ta zbulojmë dhe ta kthejmë një ndryshim të tillë.

3.3 Disponueshmëria (Availability)

Informacionet dhe sistemet janë të disponueshme kur u nevojiten përdoruesve të autorizuar. Kjo sigurohet përmes kopjeve rezervë, planeve për vazhdimësi të punës, sistemeve redundante dhe mbrojtjes nga sulmet që synojnë ta pamundësojnë qasjen.

> **Ekuilibri.** Tre parimet ndonjëherë janë në tension — kontrolli tepër i rreptë (konfidencialiteti) mund ta zvogëlojë disponueshmërinë. Qëllimi është të gjendet ekuilibri i duhur sipas rëndësisë së informacionit.

4. Klasifikimi i informacionit

Jo të gjitha informacionet janë njësoj të ndjeshme. Klasifikimi na ndihmon të dimë si të veprojmë me secilin lloj informacioni.

Niveli	Përshkrimi	Shembull
Publik	Mund të publikohet lirisht	Njoftime për shtyp, raporte publike
Përdorim i brendshëm	Vetëm për punonjësit	Procedura të brendshme, skema organizative
Konfidenciale	Rreth i kufizuar personash	Kontrata, të dhëna financiare
Rreptësisht konfidenciale	Më rreptësisht të mbrojtura	Konfigurime sigurie, plane strategjike

4.1 Rregullat e veprimit

- ✓ Shënoni dokumentet sipas nivelit të klasifikimit
- ✓ Mos ndani informacione konfidenciale përmes kanaleve të pambrojtura
- ✓ Shkatërrojini dokumentet e ndjeshme në mënyrë të sigurt (jo në shportën e zakonshme)
- ✓ Në rast dyshimi për nivelin, trajtojeni informacionin si më të klasifikuar

5. Menaxhimi i fjalëkalimeve

Fjalëkalimet janë çelësat e botës digjitale. Një fjalëkalim i dobët është si ta lini derën të pakyçur — një ftesë për qasje të paautorizuar.

5.1 Karakteristikat e një fjalëkalimi të fortë

- ✓ Së paku 12 karaktere — sa më i gjatë, aq më i sigurt
- ✓ Kombinim i shkronjave të mëdha dhe të vogla, numrave dhe simboleve
- ✓ Pa të dhëna personale (emri, data e lindjes, emri i kafshës shoqëruese)
- ✓ Pa fjalë të zakonshme ose vargje të parashikueshme (123456, password)
- ✓ Unik për çdo llogari — mos e përsëritni të njëjtin fjalëkalim

5.2 Teknika e frazës

> **Këshillë.** Në vend të një vargu të vështirë për t’u mbajtur mend, përdorni një frazë që vetëm ju e dini dhe zëvendësoni disa shkronja me simbole. Për shembull, një fjali që ka kuptim personal për ju, e shndërruar në kombinim shkronjash, numrash dhe shenjash — e gjatë, komplekse, por e lehtë për t’u mbajtur mend.

5.3 Gabime të shpeshta

Bëni	Shmangni
Përdorni menaxher fjalëkalimesh	Shkrimin në një letër mbi tavolinë
Fjalëkalim të ndryshëm për çdo llogari	Të njëjtin fjalëkalim kudo
Ndryshojeni në rast dyshimi për kompromet im	Ndarjen me kolegët
Aktivizoni autentifikimin me dy faktorë	Dërgimin e fjalëkalimeve me postë elektronike

6. Autentifikimi me dy faktorë

Edhe fjalëkalimi më i fortë mund të kompromet ohet. Autentifikimi me dy faktorë (2FA) shton një shtresë të dytë mbrojtjeje — përveç diçkaje që e dini (fjalëkalimi), nevojitet edhe diçka që e keni (kod nga telefoni, aplikacioni ose një çelës fizik).

6.1 Si funksionon

Kur kyçeni, pas vendosjes së fjalëkalimit, sistemi kërkon konfirmim shtesë — më së shpeshti një kod që gjenerohet në telefonin tuaj. Edhe nëse dikush e mëson fjalëkalimin tuaj, nuk mund të qaset pa faktorin e dytë.

> **Rekomandim.** Sa herë që është i disponueshëm, aktivizoni autentifikimin me dy faktorë — veçanërisht për llogaritë afariste, postën elektronike dhe qasjen administrative në sisteme.

7. Mbrojtja e stacionit të punës

Kompjuteri juaj është porta drejt informacioneve të organizatës. Mbrojtja e tij është përgjegjësia juaj e përditshme.

7.1 Zakonet e përditshme

- ✓ Kyçeni ekranin sa herë që largoheni (edhe për pak kohë)
- ✓ Mos instaloni softuer të pamiratuar
- ✓ Përditësoni rregullisht sistemin operativ dhe aplikacionet
- ✓ Mos i çaktivizoni programet e sigurisë (antivirusi, muri mbrojtës)
- ✓ Mos lidhni pajisje USB të panjohura

> **Kujdes.** Pajisjet USB janë një mënyrë e shpeshtë e përhapjes së softuerit keqdashës. Një USB i gjetur në parking ose i dhuruar nga një i panjohur — kurrë mos e lidhni në kompjuterin e punës.

8. Siguria gjatë punës në distancë

Puna nga shtëpia ose gjatë udhëtimit zyrtar sjell rreziqe shtesë. Vlejnë të njëjtat rregulla, por me kujdes më të madh.

- ✓ Bëni kopje rezervë të të dhënave të rëndësishme
- ✓ Qasuni në sistemet e brendshme vetëm përmes VPN-së
- ✓ Përdorni lidhje të besueshme interneti, shmangni Wi-Fi publik të hapur
- ✓ Mos e lini pajisjen pa mbikëqyrje në vende publike
- ✓ Kini kujdes kush e sheh ekranin tuaj (shoulder surfing)
- ✓ Ndajeni pajisjen e punës nga ajo private ku është e mundur

9. Siguria fizike

Siguria e informacionit nuk është vetëm digjitale. Qasja fizike në hapësira, pajisje dhe dokumente është po aq e rëndësishme.

- ✓ Mbani kartën e identifikimit dhe mos ia huazoni askujt
- ✓ Mos lejoni persona të panjohur të hyjnë pas jush (tailgating)
- ✓ Mbyllini dokumentet e ndjeshme me kyç
- ✓ Zbatoni politikën e „tavolinës së pastër“ — mos lini dokumente konfidenciale të dukshme
- ✓ Raportoni personat e panjohur në zonat e mbrojtura

10. Menaxhimi i incidenteve

Pavarësisht sa të kujdesshëm jemi, incidentet ndodhin. E rëndësishme është të dimë si të reagojmë.

10.1 Çfarë është një incident

Çdo ngjarje që mund ta rrezikojë sigurinë e informacioneve — një email i dyshimtë, një pajisje e humbur, një fjalëkalim i kompromet uar, sjellje e pazakontë e një sistemi.

10.2 Si të reagoni

1. Mos u panikosni — reagimi i shpejtë dhe i qetë është kyç
2. Mos u përpiqni ta „rregulloni“ problemin vetë
3. Raportoni menjëherë te Sektori i sigurisë informatike
4. Dokumentoni çfarë keni vërejtur dhe çfarë keni bërë
5. Bashkëpunoni me ekipin e sigurisë

> **Raportimi nuk është dënim.** Raportimi në kohë i një incidenti është sjellje e përgjegjshme që e mbron tërë shoqërinë. Më mirë është të raportoni një alarm të rremë sesa të humbisni një sulm të vërtetë.

11. Përgjegjësitë e punonjësve

Çdo punonjës ka rol në mbrojtjen e informacioneve:

- ✓ Respektimi i politikave dhe procedurave të sigurisë
- ✓ Mbrojtja e të dhënave të qasjes (fjalëkalime, karta)
- ✓ Raportimi i aktiviteteve të dyshimta dhe incidenteve
- ✓ Pjesëmarrja në trajnime për vetëdijesësim për sigurinë
- ✓ Veprim i kujdesshëm me informacionet e ndjeshme
- ✓ Njoftimi në rast ndryshimi të pozitës së punës ose largimi

Skenarë praktikë

Mënyra më e mirë për ta mësuar sigurinë është përmes situatave reale. Shqyrtoni skenarët në vijim dhe mendoni si do të vepronit.

Skenari 1: Email i dyshimtë

Merrni një email që duket se është nga Sektori i TI-së, me kërkesë urgjente ta konfirmoni fjalëkalimin tuaj përmes një linku, përndryshe llogaria do të bllokohet brenda 24 orëve.

Reagimi i gabuar: Klikoni në link dhe e vendosni fjalëkalimin që të mos e humbisni llogarinë.

Reagimi i drejtë: Ndaleni. Asnjë Sektor legjitim i TI-së nuk kërkon fjalëkalim përmes emailit. E kontrolloni adresën e dërguesit, nuk klikoni në link dhe raportoni te Sektori i sigurisë përmes kanalit zyrtar.

Skenari 2: Pajisje USB e gjetur

Në parkingun para ndërtesës gjeni një pajisje USB. Jeni kurioz çfarë ka në të dhe mendoni ta lidhni në kompjuter për të parë kujt i përket.

Reagimi i gabuar: E lidhni USB-në për ta parë përmbajtjen dhe për t’ia kthyer pronarit.

Reagimi i drejtë: Nuk e lidhni. Pajisjet USB të lëna janë mënyrë e shpeshtë e përhapjes së softuerit keqdashës. Ia dorëzoni Sektorit të sigurisë, i cili do ta kontrollojë në mënyrë të sigurt.

Skenari 3: Kolegu kërkon qasje

Një koleg nga një sektor tjetër ju lut t’ia huazoni fjalëkalimin tuaj për t’u qasur në një sistem, sepse qasja e tij „nuk punon“ dhe i nevojitet urgjentisht.

Reagimi i gabuar: Ia jepni fjalëkalimin për t’i ndihmuar, sepse është koleg dhe duket urgjente.

Reagimi i drejtë: Nuk e ndani fjalëkalimin — kurrë, me askënd. E udhëzoni të kontaktojë Sektorin e TI-së për ta zgjidhur problemin me qasjen e tij. Ndarja e fjalëkalimeve është shkelje e rregullave të sigurisë.

Skenari 4: Puna në kafene

Punoni nga një kafene dhe ju duhet urgjentisht të qaseni në një sistem të brendshëm të MEPSO-s përmes Wi-Fi-t falas të lokalit.

Reagimi i drejtë: Lidheni përmes VPN-së para se të qaseni në cilëndo resurs të brendshëm. Kini kujdes kush e sheh ekranin tuaj. Nëse VPN-ja nuk është e disponueshme, prisni derisa të keni lidhje të sigurt.

Pyetjet më të shpeshta

A është vërtet e rëndësishme ta kyç ekranin nëse largohem vetëm për pak kohë?

Po. Edhe disa minuta janë të mjaftueshme që dikush të qaset në kompjuterin tuaj dhe në informacionet. Kyçja e ekranit është një zakon i shpejtë që parandalon një rrezik të madh.

Po nëse e harroj një fjalëkalim kompleks?

Përdorni menaxher fjalëkalimesh — një mjet që i ruan në mënyrë të sigurt të gjitha fjalëkalimet tuaja, kështu që duhet ta mbani mend vetëm një kryesor. Sektori i TI-së mund të rekomandojë një mjet të miratuar.

A është e sigurt ta përdor të njëjtin fjalëkalim nëse është shumë i fortë?

Jo. Edhe fjalëkalimi më i fortë, nëse përdoret në disa vende dhe njëri prej tyre komprometohet, i ekspozon të gjitha llogaritë tuaja. Çdo llogari kërkon fjalëkalim unik.

Kur duhet ta raportoj një incident?

Sa herë që jeni në dilemë. Më mirë është të raportoni diçka që rezulton e padëmshme, sesa të humbisni një incident të vërtetë. Ekipi i sigurisë është aty për të ndihmuar.

A u nënshtrohen këtyre rregullave pajisjet e mia personale?

Nëse i përdorni për punë ose për qasje në sistemet e MEPSO-s, po. Të njëjtat parime të sigurisë vlejnë për çdo pajisje që prek informacionet e organizatës.

Po nëse dyshoj se një koleg i shkel rregullat e sigurisë?

Raportoni atë që dini te Sektori i sigurisë. Kjo nuk është „spiunim“ — kjo është mbrojtje e tërë shoqërisë nga një rrezik potencial.

Fjalorth i termave

Shpjegim i shkurtër i termave kyç që përdoren në këtë fushë.

Termi	Kuptimi
Autentifikimi	Procesi i konfirmimit të identitetit të një përdoruesi
Autorizimi	Përcaktimi se në çfarë ka të drejtë të qaset përdoruesi
Enkriptimi	Shndërrimi i të dhënave në formë të palexueshme për mbrojtje
Softuer keqdashës	Program i krijuar për të dëmtuar ose për qasje të paautorizuar
Phishing	Mashtrim përmes mesazheve të rreme për vjedhje të dhënash
Ransomware	Softuer keqdashës që i kyç të dhënat dhe kërkon shpërblim
VPN	Rrjet privat virtual për lidhje të sigurt në distancë
2FA	Autentifikimi me dy faktorë — shtresë e dytë mbrojtjeje gjatë kyçjes
Muri mbrojtës	Sistem që e kontrollon komunikimin në rrjet
Kopja rezervë	Kopje e të dhënave për rikthim në rast humbjeje
Inxhinieria sociale	Manipulimi i njerëzve për zbulim informacionesh
Infrastruktura kritike	Sisteme me rëndësi thelbësore për shoqërinë

Lista ditore e kontrollit të sigurisë

Listë praktike që mund ta ndiqni çdo ditë pune.

Në fillim të ditës së punës

- ✓ Kontrolloni a ka përditësime sigurie për t’u instaluar
- ✓ Shqyrtojini emailet me kujdes para se të klikoni

Gjatë ditës

- ✓ Kyçeni ekranin sa herë që largoheni
- ✓ Kini kujdes ndaj mesazheve dhe kërkesave të dyshimta
- ✓ Mos ndani të dhëna qasjeje me askënd
- ✓ Raportoni menjëherë çdo gjë të dyshimtë

Në fund të ditës së punës

- ✓ Mbyllini dokumentet e ndjeshme me kyç
- ✓ Zbatoni politikën e „tavolinës së pastër“
- ✓ Çkyçuni ose kyçeni kompjuterin
- ✓ Kontrolloni që nuk keni lënë materiale konfidenciale të dukshme

> **Zakoni mbi të gjitha.** Siguria nuk është aktivitet i njëhershëm, por zakon i përditshëm. Veprimet e vogla të vazhdueshme bëjnë ndryshimin më të madh.

12. Përfundim

Siguria e informacionit është përpjekje e përbashkët. Teknologjia siguron mjetet, por mbrojtja e vërtetë vjen nga punonjës të vetëdijshëm dhe të përgjegjshëm. Çdo zgjedhje e juaja — nga fjalëkalimi i fortë deri te raportimi i një mesazhi të dyshimtë — kontribuon në sigurinë e MEPSO-s.

Ky doracak është fillimi. Vazhdoni të mësoni, qëndroni të kujdesshëm dhe mos hezitoni të kërkoni ndihmë kur jeni në dilemë. Siguria është udhëtim, jo destinacion.

> **Mesazhi kyç.** Nuk ekziston siguri e përsosur, por ekziston sjellje e përgjegjshme. Ju jeni pjesa më e rëndësishme e mbrojtjes së organizatës.

MEPSO SHA Shkup — Operatori i sistemit të transmetimit të energjisë elektrike të Maqedonisë së Veriut
Dokument nr. MEPSO-PRI-IB-001 · Klasifikimi: Përdorim i brendshëm