МЕПСО

ПРИРАЧНИК

Прирачник за информациска безбедност

Основи, принципи и секојдневни практики за заштита на информациите

Придружен материјал за обуката:
„Зголемување на свест за информациска безбедност"

Документ бр. МЕПСО-ПРИ-ИБ-001 · Класификација: Интерна употреба
Сектор за информатичка и сајбер безбедност · МЕПСО АД Скопје

Содржина

1. Вовед

Информациите се едно од најважните средства на секоја организација. Во МЕПСО, како оператор на критична инфраструктура, заштитата на информациите не е само техничко прашање — таа е одговорност на секој вработен.

Овој прирачник ги објаснува основните концепти на информацискатa безбедност на разбирлив начин и дава практични насоки што можете да ги применувате секој ден. Целта не е да ве направи експерт, туку да ви даде знаење и свест за да ги препознаете ризиците и да постапувате безбедно.

Секој ден работиме со чувствителни податоци — оперативни податоци за електропреносниот систем, лични податоци на вработени, деловни информации и техничка документација. Компромитирањето на овие информации може да предизвика сериозни последици: од финансиска штета и нарушување на работењето, до загрозување на безбедноста на критичната инфраструктура.

Зошто е важно ова за вас. Најголем дел од безбедносните инциденти не се случуваат поради софистицирани технички напади, туку поради едноставни човечки грешки — слаба лозинка, кликнување на сомнителен линк, или оставање на незаклучен компјутер. Токму затоа вашата свест е првата и најважна линија на одбрана.

2. Што е информациска безбедност

Информацискатa безбедност е практика на заштита на информациите од неовластен пристап, употреба, откривање, нарушување, измена или уништување. Таа опфаќа не само дигиталните податоци, туку и информациите во хартиена форма, усната комуникација и знаењето на вработените.

2.1 Видови информации што ги штитиме

- **Оперативни податоци** — информации за состојбата и управувањето со електропреносниот систем;
- **Лични податоци** — информации за вработените, соработниците и трети лица;
- **Деловни информации** — договори, финансиски податоци, стратешки планови;
- **Техничка документација** — шеми, конфигурации, безбедносни процедури;
- **Пристапни податоци** — лозинки, клучеви, сертификати.

2.2 Од што ги штитиме

Заканите можат да дојдат од различни извори:

Извор на закана	Пример
Надворешни напаѓачи	Хакери, организирани сајбер криминални групи
Малициозен софтвер	Вируси, ransomware, шпионски програми
Внатрешни закани	Незадоволни или невнимателни вработени
Човечка грешка	Случајно бришење, погрешно испраќање податоци
Физички закани	Кражба на уреди, неовластен пристап до простории
Природни катастрофи	Пожар, поплава, прекин на струја

3. Принципи: доверливост, интегритет, достапност

Информацискатa безбедност се темели на три основни принципи, познати како „ЦИА тријада" (Confidentiality, Integrity, Availability).

3.1 Доверливост (Confidentiality)

Информациите се достапни само за лицата кои имаат овластување да пристапат до нив. Ова се постигнува преку контрола на пристап, шифрирање и принципот на најмала привилегија — секој корисник добива само оние права што му се неопходни за неговата работа.

> **Пример.** Финансиските извештаи треба да бидат достапни само за финансискиот сектор и раководството, не за сите вработени. Ако секој има пристап до сè, ризикот од злоупотреба или истекување расте драматично.

3.2 Интегритет (Integrity)

Точноста и целовитоста на информациите се заштитени од неовластена или случајна измена. Секоја промена на критичните податоци мора да биде евидентирана и следлива, за да можеме да веруваме дека информациите се точни и непроменети.

> **Пример.** Ако некој неовластено ги измени конфигурациските параметри на систем, тоа може да предизвика погрешно работење. Механизмите за интегритет (евиденција, контролни суми, верзии) ни овозможуваат да откриеме и вратиме таква измена.

3.3 Достапност (Availability)

Информациите и системите се достапни кога се потребни на овластените корисници. Ова се обезбедува преку резервни копии, планови за континуитет на работењето, редундантни системи и заштита од напади што целат да го оневозможат пристапот.

> **Рамнотежа.** Трите принципи понекогаш се во тензија — премногу строга контрола (доверливост) може да ја намали достапноста. Целта е да се најде вистинската рамнотежа според важноста на информацијата.

4. Класификација на информации

Не сите информации се подеднакво чувствителни. Класификацијата ни помага да знаеме како да ракуваме со секој вид информација.

Ниво	Опис	Пример
Јавно	Може слободно да се објави	Прес-соопштенија, јавни извештаи
Интерна употреба	Само за вработени	Интерни процедури, организациски шеми
Доверливо	Ограничен круг лица	Договори, финансиски податоци
Строго доверливо	Најстрого заштитено	Безбедносни конфигурации, стратешки планови

4.1 Правила за ракување

- ✓ Означувајте ги документите според нивото на класификација
- ✓ Не споделувајте доверливи информации преку незаштитени канали
- ✓ Уништувајте ги чувствителните документи безбедно (не во обична корпа)
- ✓ При сомнеж за нивото, третирајте ја информацијата како повисоко класифицирана

5. Управување со лозинки

Лозинките се клучевите на дигиталниот свет. Слаба лозинка е како да оставите отклучена врата — покана за неовластен пристап.

5.1 Карактеристики на силна лозинка

- ✓ Најмалку 12 знаци — колку подолга, толку побезбедна
- ✓ Комбинација од големи и мали букви, бројки и симболи
- ✓ Без лични податоци (име, датум на раѓање, име на милениче)
- ✓ Без вообичаени зборови или предвидливи низи (123456, password)
- ✓ Уникатна за секоја сметка — не ја повторувајте истата лозинка

5.2 Техника на фраза

Совет. Наместо тешко памтлива низа, користете фраза што само вие ја знаете и заменете некои букви со симболи. На пример, реченица која ви значи нешто лично, претворена во комбинација од букви, бројки и знаци — долга, сложена, но лесна за паметење.

5.3 Чест грешки

Направете	Избегнувајте
Користете менаџер за лозинки	Запишување на ливче на бирото
Различна лозинка за секоја сметка	Иста лозинка насекаде
Менувајте при сомнеж за компромис	Споделување со колеги
Вклучете двофакторна автентикација	Испраќање лозинки преку е-пошта

6. Двофакторна автентикација

Дури и најсилната лозинка може да биде компромитирана. Двофакторната автентикација (2FA) додава втор слој заштита — покрај нешто што знаете (лозинка), потребно е и нешто што имате (код од телефон, апликација или физички клуч).

6.1 Како функционира

Кога се најавувате, по внесувањето на лозинката, системот бара дополнителна потврда — најчесто код што се генерира на вашиот телефон. Дури и ако некој ја дознае вашата лозинка, не може да пристапи без вториот фактор.

Препорака. Секогаш кога е достапна, вклучете двофакторна автентикација — особено за деловни сметки, е-пошта и административен пристап до системи.

7. Заштита на работната станица

Вашиот компјутер е портата кон информациите на организацијата. Неговата заштита е ваша секојдневна одговорност.

7.1 Секојдневни навики

- ✓ Заклучувајте го екранот секогаш кога се оддалечувате (дури и на кратко)
- ✓ Не инсталирајте неодобрен софтвер
- ✓ Редовно ажурирајте го оперативниот систем и апликациите
- ✓ Не исклучувајте ги безбедносните програми (антивирус, заштитен sид)
- ✓ Не поврзувајте непознати USB уреди

- ✓ Правете резервни копии на важните податоци

Внимание. USB уредите се чест начин за ширење на малициозен софтвер. Најден USB на паркинг или подарен од непознат — никогаш не го приклучувајте на работниот компјутер.

8. Безбедност при работа од далечина

Работата од дома или на службен пат носи дополнителни ризици. Истите правила важат, но со поголемо внимание.

- ✓ Пристапувајте до внатрешните системи само преку VPN
- ✓ Користете доверлива интернет врска, избегнувајте отворен јавен WiFi
- ✓ Не оставајте го уредот без надзор на јавни места
- ✓ Внимавајте кој гледа на екранот (shoulder surfing)
- ✓ Одвојте го работниот од приватниот уред каде е можно

9. Физичка безбедност

Информацискатa безбедност не е само дигитална. Физичкиот пристап до простории, уреди и документи е подеднакво важен.

- ✓ Носете ја идентификацискатa картичка и не ја позајмувајте
- ✓ Не дозволувајте непознати лица да влезат зад вас (tailgating)
- ✓ Заклучувајте ги чувствителните документи
- ✓ Применувајте политика на „чиста маса" — не оставајте доверливи документи видливи
- ✓ Пријавувајте непознати лица во заштитените зони

10. Управување со инциденти

Без разлика колку сме внимателни, инциденти се случуваат. Важно е да знаеме како да реагираме.

10.1 Што е инцидент

Секој настан што може да ја загрози безбедноста на информациите — сомнителна е-пошта, изгубен уред, компромитирана лозинка, невообичаено однесување на систем.

10.2 Како да реагирате

1. Не паничете — брзата и смирена реакција е клучна
2. Не се обидувајте сами да го „поправите" проблемот
3. Веднаш пријавете на Секторот за информатичка безбедност
4. Документирајте што сте забележале и што сте направиле
5. Соработувајте со тимот за безбедност

> **Пријавувањето не е казна.** Навременото пријавување на инцидент е одговорно однесување што го штити целото друштво. Подобро е да пријавите лажна тревога отколку да пропуштите вистински напад.

11. Одговорности на вработените

Секој вработен има улога во заштитата на информациите:

- ✓ Придржување кон безбедносните политики и процедури
- ✓ Заштита на пристапните податоци (лозинки, картички)
- ✓ Пријавување на сомнителни активности и инциденти
- ✓ Учество во обуки за безбедносна свест
- ✓ Внимателно ракување со чувствителни информации
- ✓ Известување при промена на работната позиција или заминување

Практични сценарија

Најдобар начин да се научи безбедноста е преку реални ситуации. Разгледајте ги следните сценарија и размислете како би постапиле.

Сценарио 1: Сомнителна е-пошта

Добивате е-пошта која изгледа дека е од ИТ Секторот, со барање итно да ја потврдите вашата лозинка преку линк, инаку сметката ќе биде блокирана за 24 часа.

> **Погрешна реакција:** Кликнувате на линкот и ја внесувате лозинката за да не ја изгубите сметката.
>
> > **Правилна реакција:** Застанувате. Ниту еден легитимен ИТ Сектор не бара лозинка преку е-пошта. Проверувате ја адресата на испраќачот, не кликате на линкот, и пријавувате на Секторот за безбедност преку официјален канал.
>
> ### Сценарио 2: Најден USB уред
>
> На паркингот пред зградата наоѓате USB уред. Љубопитни сте што има на него и размислувате да го приклучите на компјутерот за да видите на кого припаѓа.
>
> > **Погрешна реакција:** Го приклучувате USB-то за да видите содржината и да го вратите на сопственикот.
> >
> > > **Правилна реакција:** Не го приклучувате. Оставените USB уреди се чест начин за ширење на малициозен софтвер. Го предавате на Секторот за безбедност кој ќе го провери безбедно.
> >
> > ### Сценарио 3: Колега бара пристап
> >
> > Колега од друг сектор ве замолува да му ја позајмите вашата лозинка за да пристапи до систем, бидејќи неговиот пристап „не работи" и итно му треба.
> >
> > > **Погрешна реакција:** Му ја давате лозинката за да му помогнете, бидејќи е колега и делува итно.

Правилна реакција: Не ја споделувате лозинката — никогаш, со никого. Го упатувате да контактира со ИТ Секторот за да се реши проблемот со неговиот пристап. Споделувањето лозинки е повреда на безбедносните правила.

Сценарио 4: Работа во кафуле

Работите од кафуле и треба итно да пристапите до внатрешен систем на МЕПСО преку бесплатниот WiFi на локалот.

> **Правилна реакција:** Се поврзувате преку VPN пред да пристапите до било кој внатрешен ресурс. Внимавате кој гледа на вашиот екран. Ако VPN не е достапен, чекате додека не добиете безбедна врска.

Најчесто поставувани прашања

Дали навистина е важно да заклучувам екран ако одам само на кратко?

> Да. Дури и неколку минути се доволни некој да пристапи до вашиот компјутер и информациите. Заклучувањето на екранот е брза навика која спречува голем ризик.

Што ако заборавам сложена лозинка?

> Користете менаџер за лозинки — алатка која безбедно ги чува сите ваши лозинки, па треба да запаметите само една главна. ИТ Секторот може да препорача одобрена алатка.

Дали е безбедно да ја користам истата лозинка ако е многу силна?

> Не. Дури и најсилната лозинка, ако се користи на повеќе места и едно од нив биде компромитирано, ги изложува сите ваши сметки. Секоја сметка треба уникатна лозинка.

Кога треба да пријавам инцидент?

> Секогаш кога сте во дилема. Подобро е да пријавите нешто што се покажува како безопасно, отколку да пропуштите вистински инцидент. Тимот за безбедност е тука да помогне.

Дали моите лични уреди подлежат на овие правила?

> Ако ги користите за работа или пристап до системи на МЕПСО, да. Истите безбедносни принципи важат за секој уред што допира

> до информациите на организацијата.

Што ако сомневам дека колега прекршува безбедносни правила?

> Пријавете го вашето сознание на Секторот за безбедност. Ова не е „издавање" — тоа е заштита на целото друштво од потенцијален ризик.

Речник на поими

Кратко објаснување на клучните поими што се користат во оваа област.

Поим	Значење
Автентикација	Процес на потврдување на идентитетот на корисник
Авторизација	Определување на што има право да пристапи корисникот
Шифрирање	Претворање на податоци во нечитлив облик за заштита
Малициозен софтвер	Програм создаден да наштети или неовластено пристапи
Phishing	Измама преку лажни пораки за кражба на податоци
Ransomware	Малициозен софтвер што ги заклучува податоците и бара откуп
VPN	Виртуелна приватна мрежа за безбедна врска од далечина
2FA	Двофакторна автентикација — втор слој заштита при најава
Заштитен ѕид	Систем што ја контролира мрежната комуникација
Резервна копија	Копија на податоци за враќање при загуба
Социјален инженеринг	Манипулација на луѓе за откривање информации
Критична инфраструктура	Системи од суштинско значење за општеството

Дневна безбедносна чек-листа

Практична листа што можете да ја следите секој работен ден.

На почеток на работниот ден

- ✓ Проверете дали има безбедносни ажурирања за инсталирање
- ✓ Прегледајте ги е-пораките внимателно пред да кликате

Во текот на денот

- ✓ Заклучувајте го екранот секогаш кога се оддалечувате
- ✓ Внимавајте на сомнителни пораки и барања
- ✓ Не споделувајте пристапни податоци со никого
- ✓ Пријавувајте што било сомнително веднаш

На крај на работниот ден

- ✓ Заклучете ги чувствителните документи
- ✓ Применете политика на „чиста маса"
- ✓ Одјавете се или заклучете го компјутерот
- ✓ Проверете дека немате оставено доверливи материјали видливи

Навика над се. Безбедноста не е еднократна активност, туку секојдневна навика. Малите постојани дејства прават најголема разлика.

12. Заклучок

Информацискатa безбедност е заеднички напор. Технологијата обезбедува алатки, но вистинската заштита доаѓа од свесни и одговорни вработени. Секој ваш избор — од силната лозинка до пријавувањето на сомнителна порака — придонесува кон безбедноста на МЕПСО.

Овој прирачник е почеток. Продолжете да учите, останете внимателни и не двоумете се да побарате помош кога сте во дилема. Безбедноста е патување, не дестинација.

> **Клучна порака.** Не постои совршена безбедност, но постои одговорно однесување. Вие сте најважниот дел од одбраната на организацијата.

МЕПСО АД Скопје — Оператор на електропреносниот систем на Северна Македонија
Документ бр. МЕПСО-ПРИ-ИБ-001 · Класификација: Интерна употреба