

# **Sigurnost informacijskih sustava**

mr.sc. Kristian Saletović, v.pred.  
nositelj kolegija  
[kristian.saletovic@gmail.com](mailto:kristian.saletovic@gmail.com)

# Obaveze studenata

## **UVJETI ZA DRUGI POTPIS I PRISTUPANJE ISPITU:**

- 1) Redovito pohađanje nastave (minimum nazočnosti 20%)
- 2) Pripremljenost za vježbe i aktivno sudjelovanje u nastavi

**ISPIT:** PISMENI (višestruki izbor i otvorena pitanja) i prema potrebi USMENI

Na ispitu se ne smiju koristiti elektronički uređaji osim, ako nije izričito dozvoljeno.

## **ELEMENTI OCJENE**

- 1) Aktivno sudjelovanje u nastavi – 10%
- 2) Pristupni rad – 20%
- 3) Pismeni ispit – 60%
- 4) Usmeni ispit – 10%

# Motivacija za predmet

Zašto je zaposlenicima IT industrije bitno poznavati osnove područja sigurnosti informacijskih sustava?

Sony Corporation

- krađa informacija o korisnicima online servisa
- brojevi kartica
- imena i ostali podaci
- utjecaj na dionice - www.nyse.com – 20.4.2011.



# Motivacija za predmet

Zašto je zaposlenicima IT industrije bitno poznavati osnove područja sigurnosti informacijskih sustava?

Eqifax – kreditna agencija

- Barataju podacima cca 820 mil korisnika
- Ukradeni podaci od cca 145 mil korisnika
  - Ime, prezime, datum rođenja, broj osiguranja, adrese i ostali osobni podaci
- Ukradeno 210 000 brojeva kartica
- Iskorištena slabost Apache Struta za web app development
- Provaljeno u svibnju 2017., a primijećeno tek 29.7.2017.
- Dva dana poslije uprava prodaje svoje dionice (!!???)



# Što je informacija?

Da li je 24519 informacija? Zašto?

- Podatak koji nije smješten u kontekst nema značenje i radi toga nije informacija.
- Kada podatak stavimo u kontekst, koji može biti čak i naša pretpostavka, određujemo mu značenje i postaje informacija.
- Informacija ima vrijednost.



**Definicija:**

**Informacija** je svaki **podatak** koji u određenom **kontekstu** ima **vrijednost** za vlasnika i korisnike.

# Što je informacijski sustav?

Informacijski sustav je komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike. (NN 79/07)

## Pitanje

IS = IT ili IS  $\neq$  IT



# Zašto je potrebno štititi informaciju?

Informacija:

- ima **vrijednost** za njenog vlasnika
- je **imovina** i treba ju štititi kao i svaku drugu imovinu



**Informacijska sigurnost** je stanje **povjerljivosti, cjelovitosti i raspoloživosti** podataka, koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera i standarda (NN 79/07)

# Svojstva informacije – C I A

Glavna funkcionalna svojstva informacije – C I A

- C (*confidentiality*) – povjerljivost
- I (*integrity*) – cjelovitost
- A (*availability*) – raspoloživost



Povjerljivost je svojstvo po kojem informacija nije dostupna ili otkrivena neovlaštenim osobama, entitetima ili procesima.

Cjelovitost je svojstvo očuvanja točnosti i kompletnosti informacije.

Raspoloživost je pravo na dostupnost i upotrebljivost informacije na zahtjev ovlaštenog entiteta.

# Svojstva informacije – povjerljivost

Povjerljivost je svojstvo po kojem informacija nije dostupna ili otkrivena neovlaštenim osobama, entitetima ili procesima.

- Često se koristi i izraz tajnost
- Najočitije svojstvo informacije
- Vojna upotreba prije više od 2000 g. – Cezarov enkripcijski algoritam za očuvanje povjerljivosti informacija
  - pomaknuti slova za 1 u lijevo; zamijeniti A sa C ...
- Nitko osim onoga kome je namijenjena ne bi smio dobiti informaciju.
  - Prijenos poruka u računalnim mrežama – samo za ciljno računalo
  - Pohrana i arhiviranje
- Dvije metode osiguranja povjerljivosti informacije:
  - Kontrola pristupa (fizička i logička)
  - Enkripcija
  - U praksi se često koriste zajedno
- Narušavanje povjerljivosti podataka



# Svojstva informacije – cjelovitost

Cjelovitost je svojstvo očuvanja točnosti i kompletnosti informacije.

- Često se koristi i izraz integritet
- Cjelovitost podrazumijeva nemogućnost promjene informacije bez odgovarajućeg ovlaštenja
  - Informaciju ne smije mijenjati neovlaštena osoba
  - Ovlaštena osoba ne smije unositi neovlaštene promjene
- Dvije metode osiguranja cjelovitosti podataka:
  - Kontrola pristupa (fizička i logička)
  - Enkripcija – provjera da li je informacija promijenjena ili nije
- Narušavanje cjelovitosti podataka – primjeri
  - Obrisati datoteku ili dio sadržaja datoteke (npr. tekst iz dokumenta)
  - Maliciozni kod obriše/izmijeni dio datoteke (npr. virus)
  - Namjerna ili nenamjerna greška u radu uz ovlašten pristup informaciji

# Svojstva informacije – raspoloživost

Raspoloživost je pravo na dostupnost i upotrebljivost informacije na zahtjev ovlaštenog entiteta (korisnik, rač. sustav, vladina organizacija ili tvrtka).

- Često se koristi i izraz dostupnost
- Cilj raspoloživosti je osigurati dostupnost i upotrebljivost informacije
- Očuvanje raspoloživosti
  - Visoko raspoloživi sustavi (*high availability*)
  - Informacija ne mora biti trenutačno raspoloživa

# „High availability”

Availability %	Downtime per year	Downtime per month	Downtime per week
90% ("one nine")	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
97%	10.96 days	21.6 hours	5.04 hours
98%	7.30 days	14.4 hours	3.36 hours
99% ("two nines")	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes
99.9% ("three nines")	8.76 hours	43.2 minutes	10.1 minutes
99.95%	4.38 hours	21.56 minutes	5.04 minutes
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	25.9 seconds	6.05 seconds
99.9999% ("six nines")	31.5 seconds	2.59 seconds	0.605 seconds

# Suprotnosti svojstvima informacije

- D (*disclosure*) – razotkrivanje informacija – predstavlja narušavanje povjerljivosti informacije
- A (*alternation*) – narušavanje cjelovitosti informacije promjenom
- D (*disruption*) – prekid koji uzrokuje neraspoloživost informacije

# Potreba za informacijskom sigurnošću

Informacija ima određenu vrijednost:

- Intelektualno vlasništvo
- Komercijalne informacije
- Podaci o zaposlenicima, kupcima, dobavljačima
- ...



Regulatorni zahtjevi:

- Zaštita podataka i privatnost
- Održavanje kontinuiteta poslovanja
- Zakonska regulativa za pojedine vrste organizacija
  - odluka HNB-a o eksternalizaciji (izdvajanje dijela poslovanja) kojim moraju nadzirati svoje dobavljače
  - GDPR obvezuje uvođenje nadzora podugovarača
  - ...
- Međunarodna suradnja



Ovisimo o IT-u:

- Greške u IT-u su poslovne greške (neadekvatna oprema, napajanje, prirodna djelovanja...)
- IT nije sigurna tehnologija
- Povezivanje raznih sustava – nekompatibilnost tehnologije



# Zakonska regulativa

- 1) Zakon o informacijskoj sigurnosti (NN 79/07)
- 2) Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018)
  - a) Uredba o kibernetičkoj sigurnosti
- 3) Opća uredba o zaštiti podataka (GDPR)
  - Zakon o provedbi Opće uredbe o zaštiti podataka (NN 42/2018)
- 4) HNB – Odluka o primjerenom upravljanju informacijskim sustavom (2010)
- 5) Zakon o tajnosti podataka (NN 79/07)
- 6) Uredba o mjerama informacijske sigurnosti (NN 79/07)
- 7) Zakon o arhivskom gradivu i arhivima (NN 61/18)
- 8) Zakon o zaštiti i spašavanju (NN 174/04, 79/07, 38/09, 127/10)
- 9) Zakon o elektroničkoj ispravi (NN 150/05)
- 10) Zakon o elektroničkom potpisu (NN 10/02)
  - Zakon o izmjenama i dopunama Zakona o elektroničkom potpisu (NN 10/02)
- 11) Zakon o sigurnosnim provjerama (NN 85/08)
- 12) Zakon o elektroničkim komunikacijama (NN 73/08, NN 90/11)
- 13) ...



# Poslovna tajna

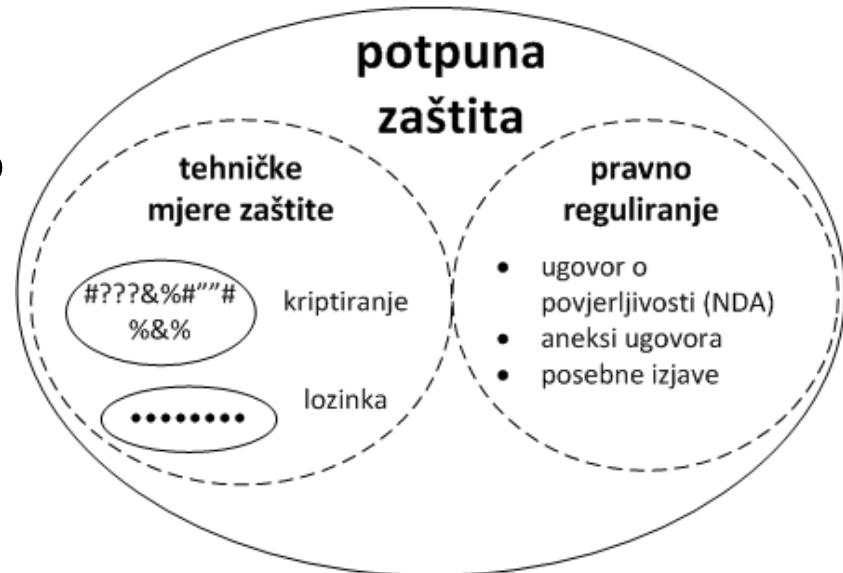
Poslovnu tajnu potrebno je regulirati internim aktom organizacije – pravilnikom.

Definicija: poslovnu tajnu predstavljaju podaci koji su regulirani kao poslovna tajna određenim zakonom, drugim propisom ili općim aktom trgovackog društva, ustanove ili druge pravne osobe, a koji predstavljaju proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada te druge podatke zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine gospodarske interese.

Ukoliko poslovna tajna nije regulirana na odgovarajući način ne mogu se sankcionirati osobe koje ju učine javno dostupnom ili otuđe.

Tehnička zaštita podataka – OK ali nedovoljno bez pravnog djela.

Pravno nije regulirano → podaci nezaštićeni



# ISMS

**ISMS (Information Security Management System) – sustav upravljanja informacijskom sigurnošću**

Zašto se ISMS uvodi u poslovanje?

- Kao regulatorna obaveza (npr. odluka HNB-a o eksternalizaciji, ZKS i UKS)
- Minimizira poslovnu štetu
  - Gubitak poslovanja
  - Gubitak tržišne vrijednosti marke (brand)
  - Novčane kazne
  - ...
- Osigurava kontinuitet poslovanja
- Podizanje povjerenja kupaca
- Održavanje konkurentnosti
- Smanjen rizik zbog provođenja politika i postupaka
- Osiguravanje svijesti o sigurnosti informacija
- Potencijalno niža cijena za osiguranje
- ...

# ISO/IEC 27000 obitelj standarda

ISO – *International Organization for Standard*

IEC – *International Electrotechnical Commission*

## ISO/IEC 27000

- obitelj standarda sastoji se od najbolje prakse i preporuka za dizajn, uvođenje i održavanje sustava za upravljanje informacijskom sigurnošću (ISMS)
- Sadrži obvezujuće standarde:
  - ISO/IEC 27001 – obvezna sa sve poslovne subjekte koji žele certificirati svoj ISMS
  - ISO/IEC 27006 – obvezna samo za certifikacijske tvrtke
- Sadrži neobvezujuće standarde
  - ISO/IEC 27002 – smjernice za zadovoljavanje kriterija ISO/IEC 27001 standarda
  - ISO/IEC 27003 – smjernice za uvođenje ISMS-a
  - ISO/IEC 27004 – smjernice za mjerjenje ISMS-a
  - ISO/IEC 27005 – smjernice za upravljanje rizikom
  - ISO/IEC 27011 – smjernice za uvođenje ISMS-a u telekomunikacijskoj industriji

## ISO/IEC 27001

- dio je obitelji standarda ISO/IEC 27000
- ISO/IEC 27001 – generičkog je karaktera → neovisan je o tehnologiji i zato ima široku primjenu u različitim industrijama

# ISO/IEC 27001

ISO 27001 norma čini okvir za:

- uspostavu,
- uvođenje,
- primjenu,
- nadzor,
- provjeru (reviziju),
- održavanje i
- poboljšavanje ISMS sustava.

ISO 27001 norma je:

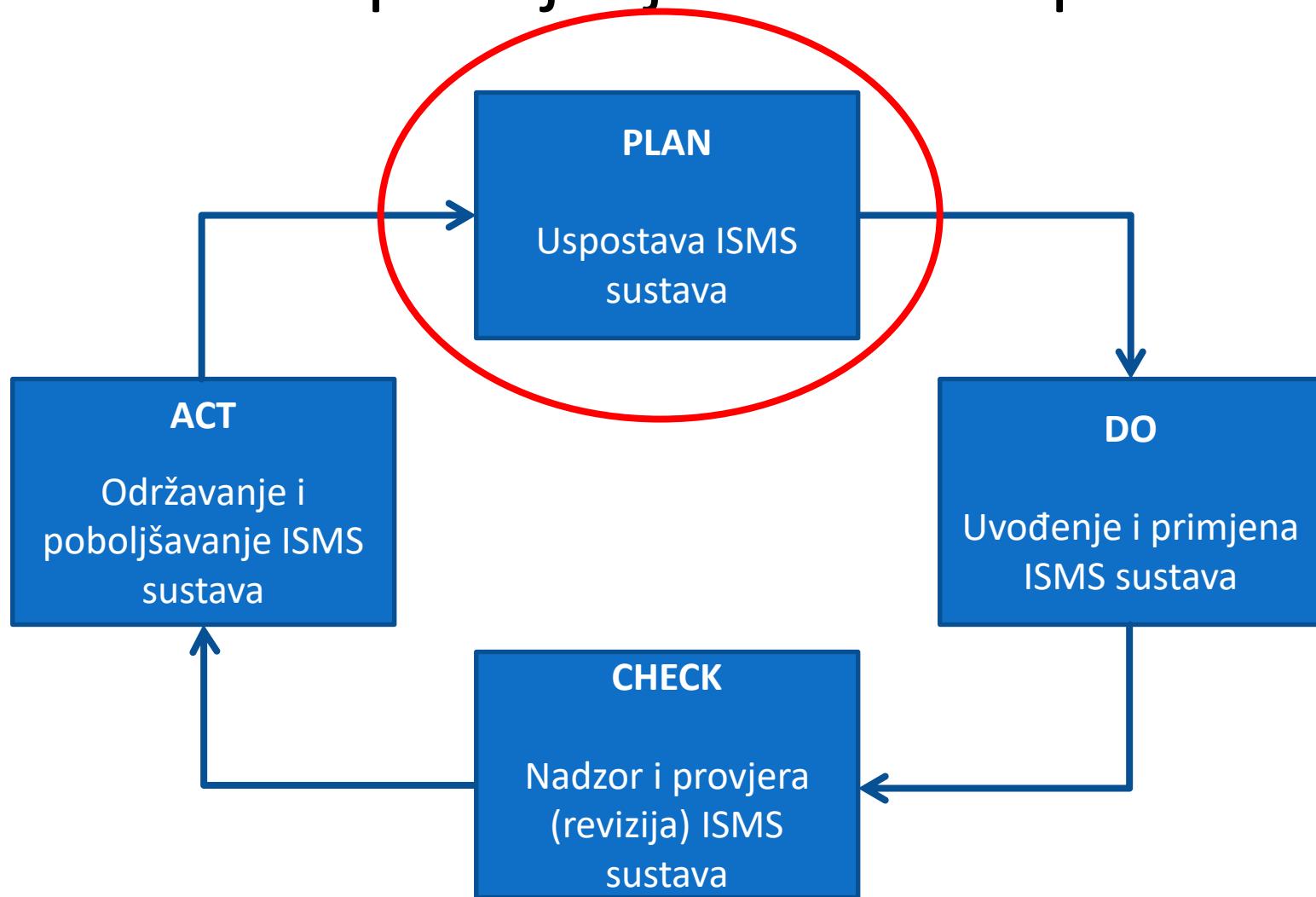
- specifikacija ISMS sustava
- generičkog karaktera,
- ukoliko je uvedena u poslovanje moguće je provođenje postupka certifikacije.

# Put do certifikata

1. Uvesti ISMS u poslovanje
2. Provesti vanjsku provjeru ISMS sustava
  - Provodi ovlaštena certifikacijska tvrtka
  - Provjera usklađenosti ISMS sustava s zahtjevima norme ISO/IEC 27001
3. Provesti korektivne mjere
4. Certifikat se dobiva ukoliko su korektivne mjere adekvatno provedene



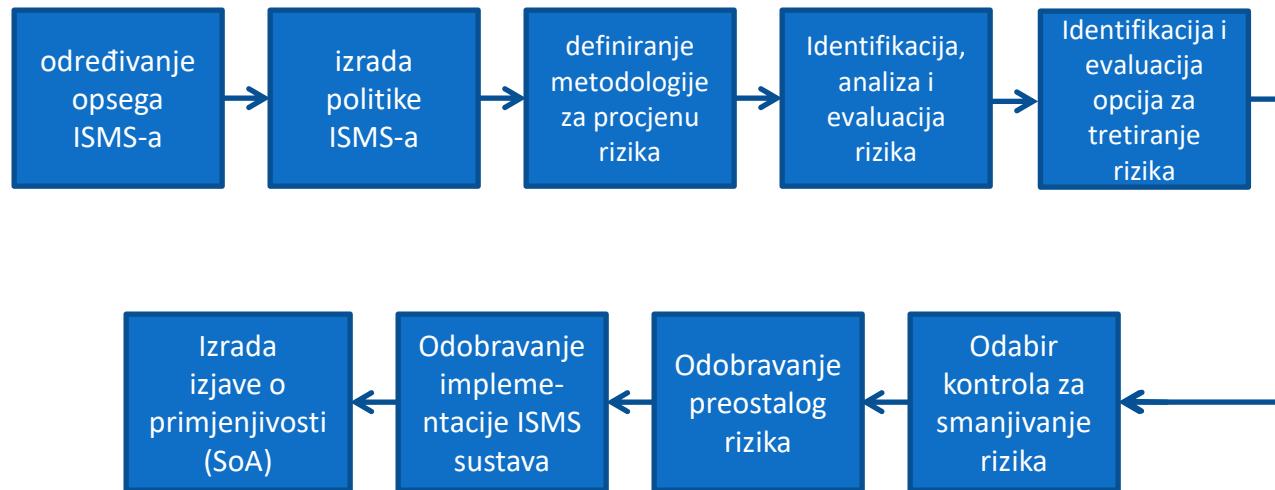
# PDCA model primijenjen na ISMS procesima



# Uspostava ISMS sustava – PLAN faza

Zahtjevi za uspostavu ISMS sustava:

- Prikazani u dijagramu
- Nalaze se u ISO 27001 normi
- Obvezujući su



# Uspostava ISMS sustava – određivanje opsega

Definiranjem opsega:

- Određuju se granice ISMS sustava
- Precizno se određuje područje nad kojim se može provesti ISO 27001 certifikacija
- Stvara se popis imovine



Prilikom definiranja opsega ISMS sustava moguće je obuhvatiti:

- Cjelokupno poslovanje (sve poslovne procese ili usluge)
- Dijelove poslovanja – čest primjer u praksi
  - Npr. pojedini poslovni procesi ili usluge
  - Npr. razvoj, sistemsala...

# Vježba – određivanje opsega

Studenti --> 5-10 min pripreme (pretraživanje interneta)

Zadatak: Kreirati dokument koji opisuje opseg projekta ISMS-a.

Pronaći:

- Savjete za određivanja opsega s obzirom na broj zaposlenika tvrtke, godišnji promet, organizacijsku strukturu ...
- Što je početak dokumenta? Odakle krenuti?
- Koji je sadržaj dokumenta?
- Što je to popis informacijske imovine i kako izgleda? Pronaći primjer.
- Može li se opseg mijenjati tijekom projekta uvođenja ISMS-a u poslovanje?

# Uspostava ISMS sustava – izrada politike ISMS-a



ISMS politika:

- Ključan dokument ISMS-a!
- Definira ciljeve ISMS-a i smjernice za uspostavu ISMS-a
- Usklađena je sa strategijom upravljanja rizikom ISMS-a
- Uzima u obzir poslovne i zakonske obvezе, te uredbe i odluke državnih tijela
- Odobrava ju Uprava (npr. potpisuje predsjednik Uprave)

# Uspostava ISMS sustava – definiranje metodologije za procjenu rizika

Kriteriji odabira metodologije:

- Jednoznačnost – rezultate je moguće usporediti, ne daje dvosmislene rezultate
- Ponovljivost – može se provoditi više puta (zahtjev norme je procjena rizika minimalno jednom godišnje ali provodi se i nakon svake značajne promjene imovine u opsegu ISMS-a)
- Prikladna za ISMS tvrtke (kvalitativna ili kvantitativna metoda)



# Uspostava ISMS sustava – identifikacija, analiza i evaluacija rizika

Procjena rizika na imovini ISMS-a:

- Ključna aktivnost u projektu uspostave inf. sig.
- Na osnovi procjene rizika donose se odluke o ulaganjima



Identificiraju se:

- prijetnje za imovinu
- ranjivosti imovine (prijetnja iskorištava ranjivost)

Procjenjuje se utjecaj na:

- C I A
- poslovanje (uzeti u obzir moguće posljedice)
- realne mogućnosti sigurnosnog incidenta
- rizik → prihvatljiv ili ga je potrebno tretirati (kriterije potrebno odrediti unaprijed)

# Uspostava ISMS sustava – identifikacija i evaluacija opcija za obradu rizika

Moguće opcije za obradu (tretiranje, ovladavanje) rizika:

- 1) Smanjivanje rizika – primjena prikladnih kontrola
- 2) Prihvaćanje rizika – svjesno i objektivno prihvaćanje rizika u skladu s politikom sigurnosti i kriterijima za prihvaćanje rizika
- 3) Izbjegavanje rizika – izbjegavanje situacija u kojima može doći do pojave rizika
- 4) Prenošenje rizika – prenošenje poslovnih rizika na nekog drugog (npr. osiguravatelje, dobavljače...)



# Uspostava ISMS sustava – odabir sigurnosnih kontrola za smanjivanje rizika



Odabir kontrola:

- Na osnovi odluke o smanjenju rizika odabiru se kontrole
- Kontrole se odabiru iz poglavlja Anex A u ISO 27001 standardu
- Broj kontrola nije konačan i po potrebi može se proširiti
- Odabir mora biti u skladu s kriterijima za prihvaćanje rizika te pravnim, regulatornim i ugovornim zahtjevima

# Uspostava ISMS sustava – odobravanje preostalih rizika i uvođenja ISMS-a

Rizici preostali nakon odabira kontrola za obradu rizika moraju biti odobreni.

Uprava mora odobriti:

1. Preostale (rezidualne) rizike
2. Uvođenje sigurnosnih kontrola (uvođenje ISMS-a) tj. primjenu mjera za obradu rizika



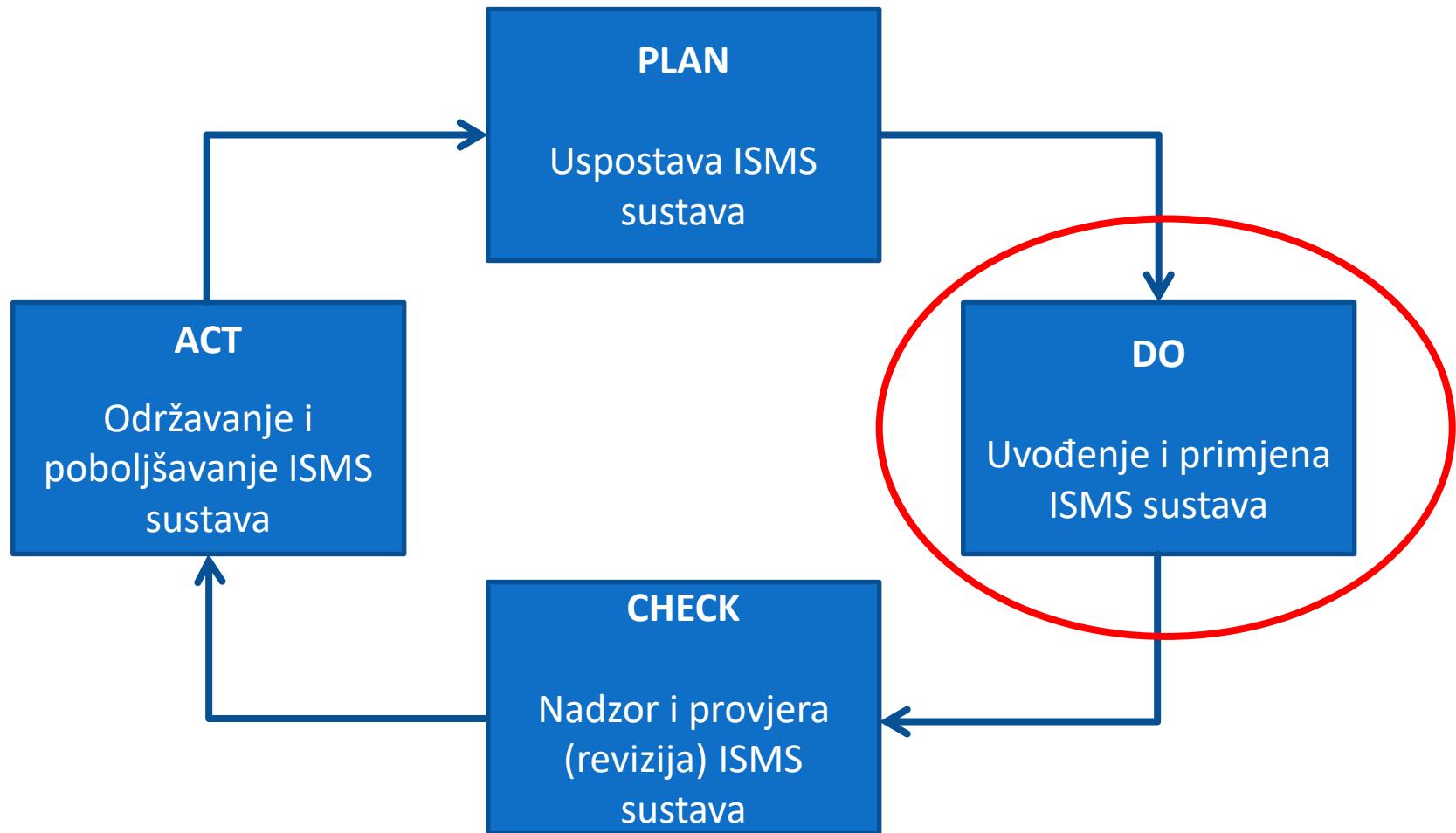
# Uspostava ISMS sustava – izrada izjave o primjenjivosti (SoA)

Izjava o primjenjivosti (*Statement of Applicability* – SoA):

- Formalan zahtjev norme
- Sadrži ciljeve i razlog upotrebe kontrola
- Sadrži razlog isključenja kontrola



# PDCA model primijenjen na ISMS procesima



# Uvođenje i primjena ISMS sustava – DO faza

Zahtjevi za uvođenjem i primjenom ISMS sustava:

- Prikazani u dijagramu
- Nalaze se u ISO 27001 normi
- Obvezujući su



# Uvođenje i primjene ISMS sustava – izrada plana obrade rizika, uvođenje kontrola i mjerjenje

Plan obrade rizika (*risk treatment plan*):

- Dokument koji sadrži:
  - Odabrane kontrole u PLAN fazi (povezati ih sa imovinom iz popisa)
  - Aktivnosti i resurse
  - Odgovornosti
  - Prioritete
- Planirati i organizirati aktivnosti uvođenja kontrola (dugotrajan postupak)

Mjerenje:

- Nadzor primjene kontrola
- Učinkovitost primijenjenih kontrola
- Redovita analiza mjerenja



# Uvođenje i primjena ISMS sustava – program sigurnosnog osvjećivanja

Cilj sigurnosnog osvjećivanja:

- Upoznati zaposlenike s politikama i procedurama ISMS-a te pravilima propisanim zakonom
- Utjecati na način razmišljanja („*state of mind*“)
- Podići razinu svijesti o vrijednosti informacija i načinu kako ih treba štititi (CIA)
- Upoznati zaposlenike sa sigurnosnim prijetnjama, rizicima i kontrolama kojima se tretiraju rizici
- Utjecati na zaposlenike da prilikom obavljanja poslovnih aktivnosti donose odluke uzimajući u obzir sigurnost informacija

# Uvođenje i primjena ISMS sustava – upravljanje resursima i radom ISMS sustava

Potrebno je osigurati resurse za:

- Cijeli PDCA ciklus
  - Uspostava ISMS-a
  - Uvođenje i primjenu
  - Nadzor i provjeru (revizija)
  - Održavanje i poboljšavanje
- ISMS je projekt u koji je potrebno trajno ulagati!
  - Sustavno upravljanje sigurnošću informacija zahtjeva održavanje i ulaganja (*state-of-the-art technology*)



# Uvođenje i primjena ISMS sustava – proces upravljanja sigurnosnim incidentima

Potrebno je uvesti proces upravljanja sigurnosnim incidentima!

Sigurnosni incident je svaki događaj koji narušava povjerljivost, cjelovitost i raspoloživost informacija unutar opsega ISMS-a.

Cilj procesa je osigurati:

- prijavu
- dosljedno i učinkovito reagiranje
- upravljanje sigurnosnim incidentima vezanim uz slabosti informacijskih sustava na način koji omogućuje pravovremeno izvođenje korektivnih mjera



Sigurnosni incident može prijaviti:

- zaposlenik
- vanjski suradnik
- vlasnik imovine u opsegu ISMS-a
- nadzorni sustav
- vatrodojavni alarm
- ...

# Vježba – sigurnosni incident 1/3

Sigurnosni incident je ...

Primjer sigurnosnog incidenta:

Primijetili ste da vam lozinka ne radi (PayPal, Gmail, Windows login). Pretpostavljate da je vam je netko ukrao lozinku i izmijenio ili ju je resetirao administrator računalnog sustava.



Pitanja:

1. Koje svojstvo informacije je narušeno?
2. Što je potrebno napraviti u slučaju sigurnosnog incidenta?
3. Koji je redoslijed događaja?
4. Što se smije, a što se ne smije raditi u takvim situacijama?
5. Koga je potrebno informirati o cjelokupnom događaju i koje aktivnosti se poduzimaju?

# Vježba – sigurnosni incident 2/3

**Zadatak:** osmisliti proceduru za upravljanje sigurnosnim incidentima koja će zadovoljiti kontrole.

Cilj kontrola: Osigurati trajan i efikasan način upravljanja sigurnosnim incidentima. Na isti način omogućiti komunikaciju o događajima i slabostima vezanim za informacijsku sigurnost.

- Kontrola A.16.1.2 – Prijava sigurnosnih događaja

Sigurnosni događaji moraju se prijaviti putem odgovarajućih kanala komunikacije što je prije moguće.

- Kontrola A.16.1.3 – Prijava sigurnosnih slabosti

Od svih zaposlenika i podugovarača zahtijevati bilježenje i prijavu bilo koje uočene sigurnosne slabosti ili sumnje na sigurnosnu slabost u sustavima ili uslugama.

# Vježba – sigurnosni incident 3/3

**Zadatak:** osmisliti proceduru za upravljanje sigurnosnim incidentima koja će zadovoljiti kontrole.

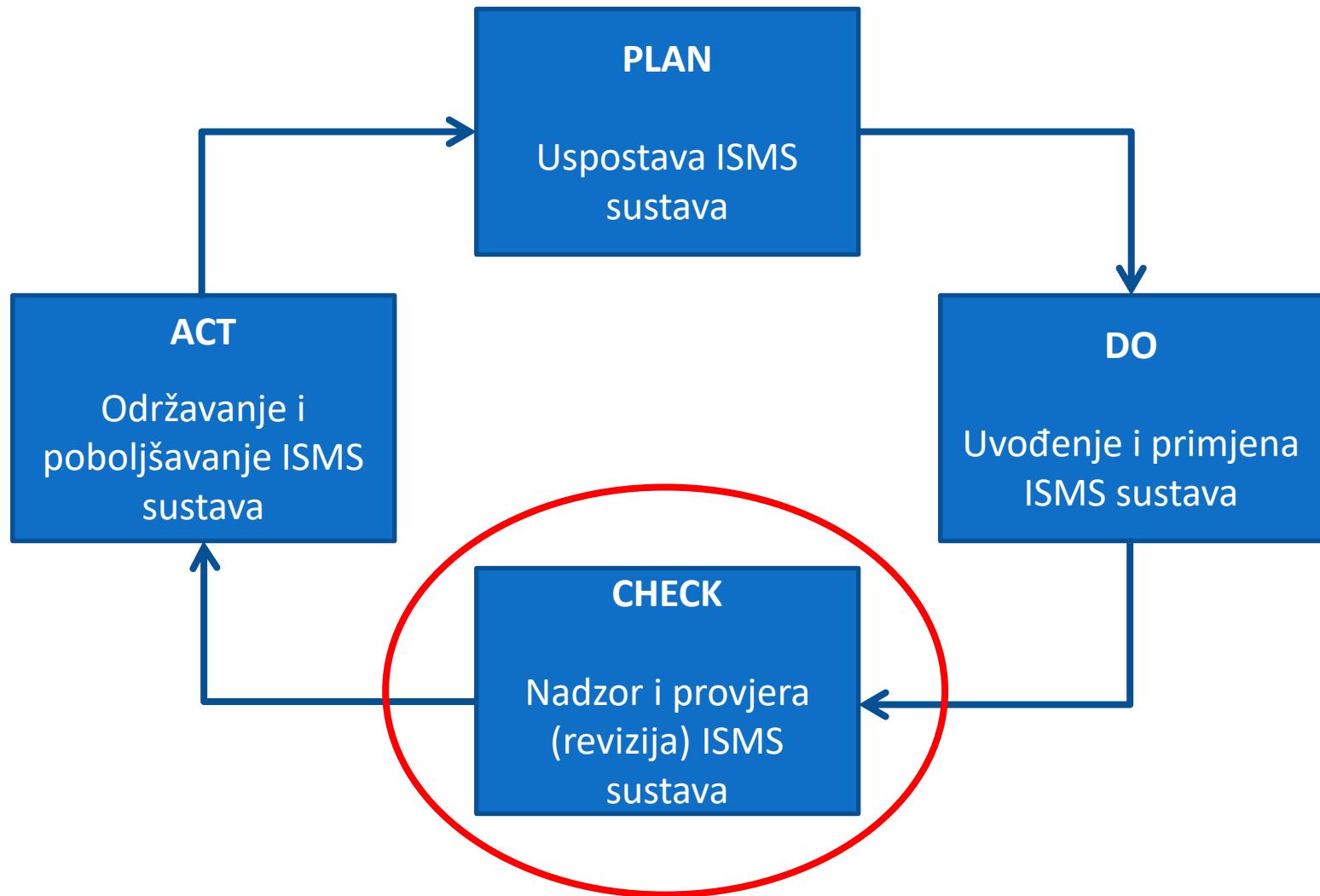
- Kontrola A.16.1.6 Učenje na sigurnosnim incidentima

Znanje prikupljeno analizom i rješavanjem sigurnosnih incidenata treba se iskoristiti za smanjenje vjerojatnosti i utjecaja budućih incidenata.

- Kontrola A.16.1.7 Prikupljanje dokaza

Potrebno je propisati proceduru za prepoznavanje, prikupljanje i očuvanje informacija koje se mogu koristiti za kao dokazi.

# PDCA model primijenjen na ISMS procesima



# Nadzor i provjera (revizija) ISMS sustava – CHECK faza

Zahtjevi za uvođenjem i primjenom ISMS sustava u CHECK fazi:

- Prikazani u dijagramu
- Nalaze se u ISO 27001 normi
- Obvezujući su



# Nadzor i provjera (revizija) ISMS sustava – kontinuiran nadzor i provjera ISMS-a

ISMS je uspostavljen i potrebno ga je nadzirati.

Promjene u organizaciji utječu na promjene u ISMS-u:

- Poslovni procesi
- Organizacija poslovanja
- Promjena kadrova
- Promjene HW-a i SW-a



Kako bi utjecaj promjena bio usklađen sa ISMS-om potrebno je:

- Nadzirati poslovne procese
- Pratiti promjene (zaposlenici, HW, SW, ...)
- Analizirati prijedloge za poboljšanja
- Pratiti utjecaj novih tehnologija

Potrebno je također nadzirati:

- Greške u radu (npr. prepoznati sigurnosni incident)
- Prepoznati pokušaj narušavanja ili narušavanje informacijske sigurnosti
- Provodenje postupka trajnog rješavanja sigurnosnog događaja

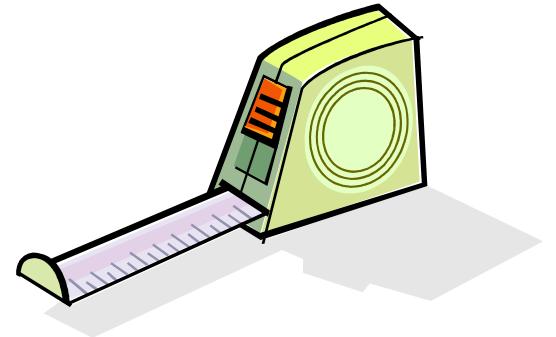
# Nadzor i provjera (revizija) ISMS sustava – mjerjenje učinkovitosti sigurnosnih kontrola i provjera procjene rizika

Metrika:

- Uspostava metrike – najbolja praksa i formalan zahtjev norme
- Mjeri se učinkovitost kontrola
- Izvodi se prema planiranim intervalima

Provjera procjene rizika:

- Provodi se periodički
- Provodi se nakon značajnih promjena:
  - Organizacijskih
  - Tehnoloških
  - Poslovnih ciljeva i procesa
  - ...
- Na kraju provedene procjene revidira se preostali rizik



# Nadzor i provjera (revizija) ISMS sustava – unutarnja provjera ISMS-a

Unutarnja provjera ISMS sustava:

- Često se koriste izrazi interna revizija i/ili interni audit
- Provodi se minimalno jednom godišnje
- Provode educirani zaposlenici firme, a dozvoljeno je da to bude i stručna osoba izvan firme.

Cilj unutarnje provjere:

- Utvrditi učinkovitost ISMS-a
- Provjeriti zadovoljava li ISMS propisane zahtjeve (definirane u ISMS politici)
- Procijeniti sukladnost ISMS sustava sa zahtjevima ISO 27001 standarda tj. da li su formalni zahtjevi zadovoljeni

# Vježba – unutarnja provjera ISMS-a 1/2

Zadatak 1 – odgovoriti na pitanja i napraviti proceduru za unutarnju provjeru

Osnovni okvir procedure:

- 1) Cilj unutarnje provjere
  - a) Što je cilj unutarnje provjere?
  - b) Što je potrebno provjeriti?
- 2) Općenite informacije o unutarnjoj provjeri
  - a) Koliko često se provodi?
  - b) Kada se provodi – u periodima smanjenih poslovnih aktivnosti ili pojačanih?
  - c) Tko ju provodi?
  - d) Tko određuje terminski plan provjere?
- 3) Podjela odgovornosti u postupku unutarnje provjere
  - a) Za što je zadužen direktor sigurnosti?
  - b) Dužnosti menadžera za sigurnost?
  - c) Dužnosti glavnog internog auditora?
  - d) Dužnosti internih auditora

# Vježba – unutarnja provjera ISMS-a 2/2

Zadatak 2 – pripremiti pitanja za unutarnju provjeru pojedinih odjela

Provjeravaju se odjeli:

- 1) Ljudski potencijali (HR)
- 2) Backup sustav
- 3) E-mail sustav
- 4) Prijava i obrada sigurnosnih incidenata

# Nadzor i provjera (revizija) ISMS sustava – provjera rukovodstva (uprave)

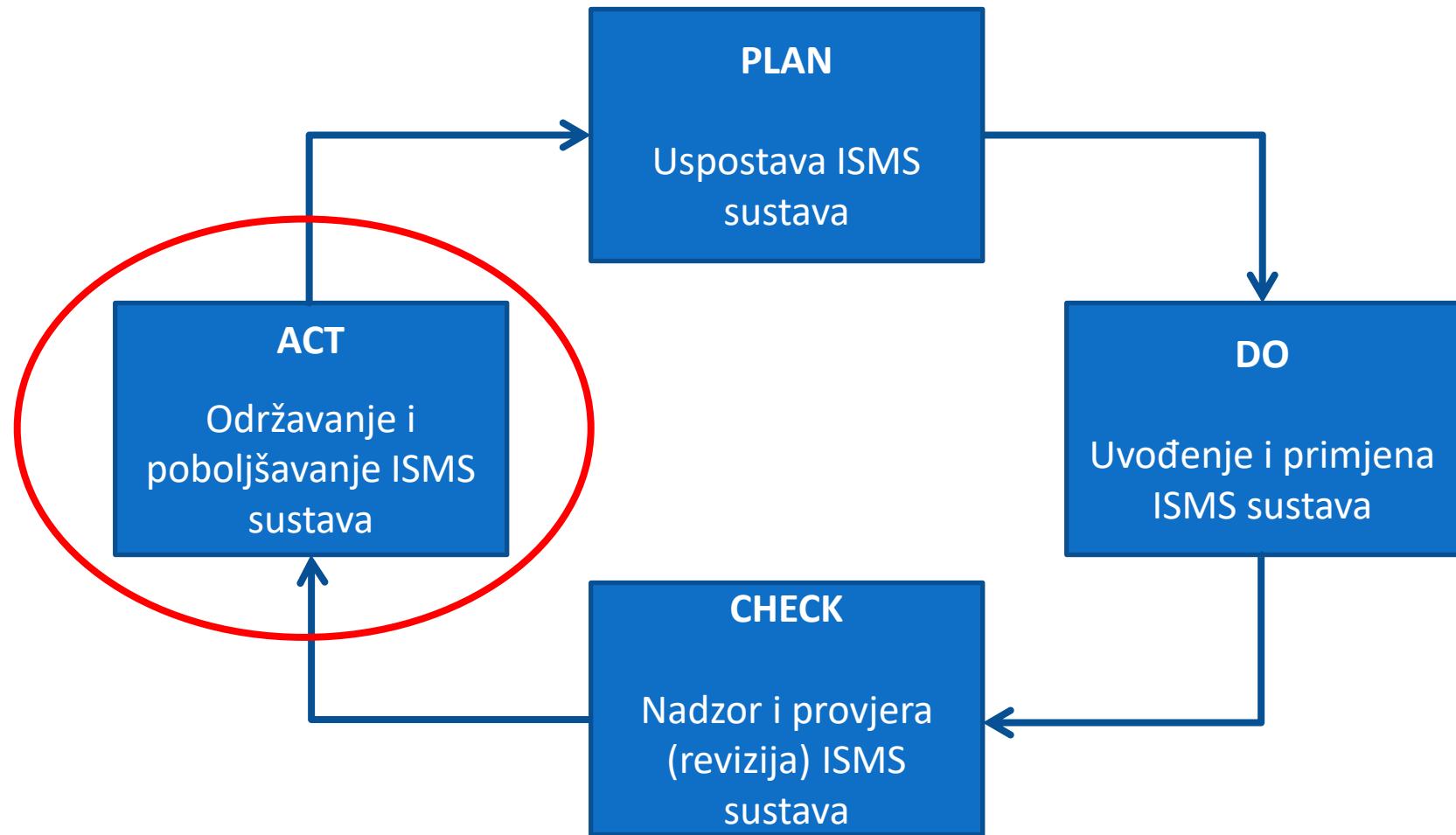
Provjera rukovodstava (revizija uprave):

- Provodi se minimalno jednom godišnje
- Opseg provjere je cijelokupan ISMS (politike, procedure, kontrolni ciljevi...)
- Radi se na osnovu prikupljenih podataka:
  - Unutarnje provjere
  - Vanjskih partnera
  - Djelatnika u opsegu ISMS-a

Cilj provjere rukovodstva:

- Strateško usmjeravanje ISMS-a
- Usklađenost s poslovnim ciljevima
- Kontinuirano poboljšanje ISMS-a
- Nadzor
  - Korektivne aktivnosti
  - Promjene politike

# PDCA model primijenjen na ISMS procesima



# Održavanje i poboljšanje ISMS sustava – ACT faza

Zahtjevi za uvođenjem i primjenom ISMS sustava:

- Prikazani u dijagramu
- Nalaze se u ISO 27001 normi
- Obvezujući su



# Održavanje i poboljšavanje ISMS sustava – uvodenje utvrđenih poboljšanja

Nesukladnosti s ISO 27001 normom definirane u prethodnom koraku u ovoj je fazi potrebno korigirati.

Uvedena poboljšanja mogu biti u:

- Procedurama
- Tehnologijama
- Načinu izvještavanja
- Bilješkama
- Ljudima
- Ugovornim obvezama
- ...



# Održavanje i poboljšavanje ISMS sustava – provođenje korektivnih i preventivnih mjera

Nesukladnosti se pojavljuju kada nije zadovoljen neki od zahtjeva:

- Zahtjev standarda (međunarodnog ili nacionalnog) prema kojem je ISMS uspostavljen
- Zahtjev internih politika, procedura, pravilnika i radnih uputa
- Zakonski, regulatorni i ugovorni zahtjevi

Korektivne mjere:

- Poduzimaju se kako bi se uklonili uzroci postojećih nesukladnosti, nedostataka ISMS-a i neželjenih situacija unutar opsega ISMS-a

Preventivne mjere:

- Poduzimaju se kako bi se uklonili uzroci potencijalnih nesukladnosti, nedostataka ISMS-a i neželjenih situacija unutar opsega ISMS-a

# Održavanje i poboljšavanje ISMS sustava – komuniciranje aktivnosti za poboljšanje

Komunikacija je ključan dio ISMS-a:

- Sve aktivnosti koje se provode s ciljem poboljšanja ISMS-a moraju biti kvalitetno iskomunicirane (svi moraju znati za to)
- Aktivnosti poboljšanja često dovode do promjena politika, procedura i ostale dokumentacije te je radi toga potrebno adekvatno provoditi kontrolu bilježaka (npr. verzioniranje → novo-zastarjelo)



# Vježba – pronalazak nesukladnosti

Primjer 1

Primjer 2

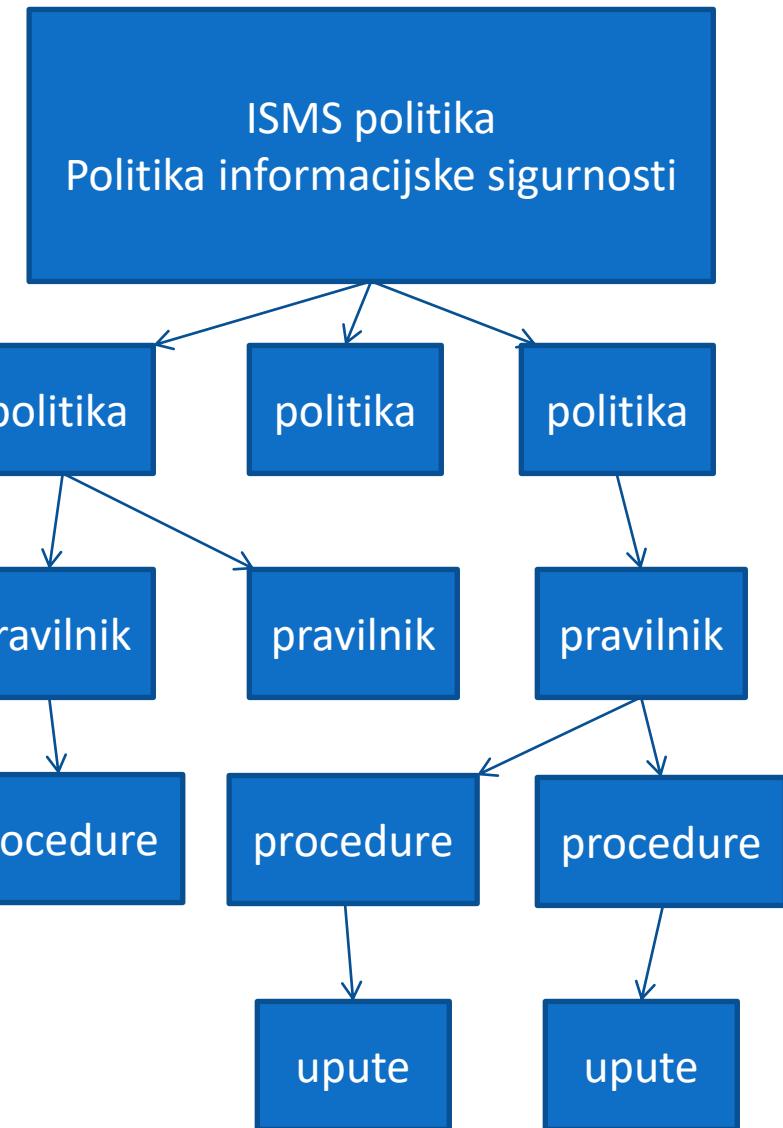
Primjer 3

Primjer 4

# Dokumentacija ISMS-a

## hijerarhija dokumentacije

- ISMS politika
  - Krovni dokument na području informacijske sigurnosti
  - Često je sadržana u jednom dokumentu sa Politikom informacijske sigurnosti tj. Sigurnosnom politikom
  - To su politike visoke razine
- Ostale politike niže razine bave se pojedinim područjima informacijske sigurnosti i namijenjene su za operativnu upotrebu:
  - Politika backupa
  - Politika kontrole pristupa
  - Politika čistog stola i čistog ekrana
  - Politika upotrebe prijenosnih uređaja
  - ...
- Pravilnici definiraju pravila koja proizlaze iz izjava u nadređenoj politici
- Procedure definiraju način provođenja aktivnosti
- Upute detaljno pojašnjavaju procedure



# ISMS politika tj. Politika informacijske sigurnosti

- Krovni dokument ISMS-a!
- Definira ciljeve i smjerove za uspostavu ISMS-a
- Uzima u obzir poslovne i zakonske obvezе, te uredbe i odluke državnih tijela
- Odobrava ju uprava (npr. potpisuje predsjednik uprave)
- Izražava očekivanja, smjernice i namjere rukovodstva organizacije u smislu informacijske sigurnosti
- Usklađena je sa strategijom organizacije
- Namijenjena je svim zaposlenicima
- Sadrži:
  - Osnovne *high level* koncepte informacijske sigurnosti
  - Prikazuje odnos organizacije prema informacijskoj sigurnosti
  - Prikazuje osnovne uloge u informacijskoj sigurnosti organizacije (npr. direktor sigurnosti, menadžer sigurnosti) bez previše detalja
  - Jasno definira svim zaposlenicima da je briga o informacijskoj sigurnosti djelokrug njihovog rada (npr. prijava uočavanja sigurnosnog incidenta)
  - Prijetnje informacijskoj sigurnosti dolaze izvana i iznutra pa je potrebno uspostaviti disciplinski mehanizam (upozoriti na posljedice)
  - Podršku edukacijama o podizanju razine svijesti o informacijskoj sigurnosti
  - Reference na ostale dokumente u opsegu ISMS-a (politike za područja, pravilnike, procedure...) kojih se treba pridržavati
  - ...



# Vježba – kreiranje politike informacijske sigurnosti → 1/2

## Politika informacijske sigurnosti

Uvod:

- opisati tvrtku – npr. vlasništvo, područje kojim se bavi
- Strateški se tvrtka opredjeljuje za:
  - Očuvanje svoje pozicije na tržištu
  - Usklađenost sa smjernicama iz najbolje prakse
  - Regulative
  - Očuvanje CI A sve informacijske imovine u opsegu ISMS-a
  - ...

Ciljevi i rizici:

- Navode se ciljevi i rizici firme
- Cilj sustava upravljanja informacijskom sigurnošću je osigurati operativno funkcioniranje u vrijeme ispada usluge...
- Cilj je potvrditi poslovnim partnerima opredijeljenost...
- Cilj je zadovoljiti sve regulatorne i zakonodavne obaveze...
- Cilj daljnog razvoja je proširenje...
- Procjena rizika nad definiranim opsegom je temelj uspostave ISMS-a ...
- Metoda procjene rizika kvalitativna/kvantitativna odgovara poslovanju ...

Namjena politike je zaštita informacijsku imovinu od svih prijetnji...

Povjerljivost informacija osigurava se...

# Vježba – kreiranje politike informacijske sigurnosti → 2/2

## Politika informacijske sigurnosti

Informacije moraju biti raspoložive...

Cjelovitosti informacija...

Plan kontinuiteta poslovanja (održanje poslovanja u kriznim situacijama)...

Edukacija, svijest i obuka o informacijskoj sigurnosti...

Incidenti i proboji informacijske sigurnosti...

Odgovornosti:

- Uprava se obvezuje...
- Uprava ovlašćuje...
- Pravo izmjene politika, procedura...
- Odgovornost svakog djelatnika i podugovarača je pridržavanje...
- Svako nepoštivanje sankcionirat će se...

# Pravilnici

## Pravilnici:

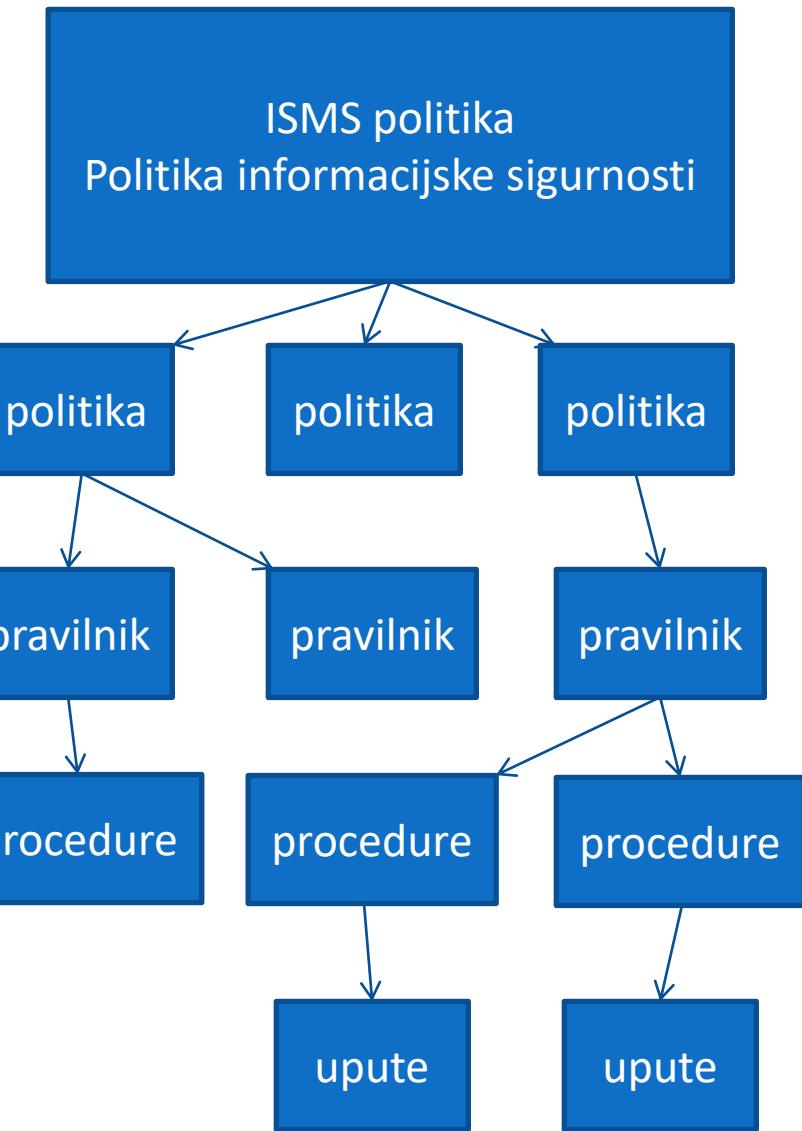
- Definiraju pravila u pojedinim segmentima inf. sigurnosti
- Jasno definiraju zahtjeve koji proizlaze iz politike

## Pravilnik vs politika

- Politika izražava namjeru i daje smjernice, a pravilnik uspostavlja granice u procesima i kontrolama
- Politike se rijetko mijenjaju, a pravilnici se mijenjaju u skladu s poslovnim procesima, tehnologijama...

## Primjer:

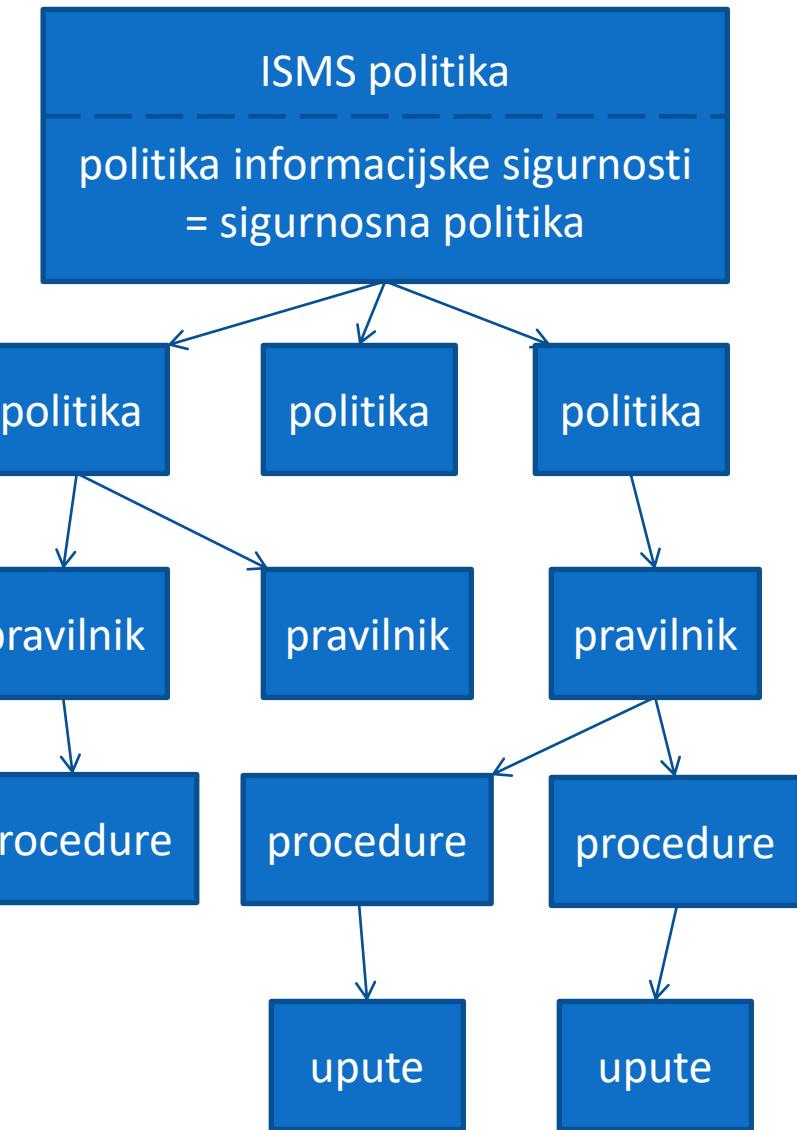
- Politika upotrebe zaporki propisuje da su svi djelatnici u opsegu ISMS sustava odgovorni za odabir sigurnosne zaporce i brigu o njoj
- Pravilnik precizno definira kako zaporka treba izgledati (minimalan broj znakova, velika i mala slova, specijalni znakovi, brojevi...)



# Procedure i upute

## Procedure:

- Opisuju korake kako se treba provoditi određena aktivnost
- Korisnik procedure mora imati dovoljno detalja za njeno provođenje
- Npr. procedura za promjenu zaporke opisuje korake promjene – prijava u sustav, odabir postavki korisničkog računa, unos stare zaporke, unos nove zaporke



## Upute:

- Detaljno opisuje proceduru ako je to potrebno
- Upute su često za pojedine korake
- Npr. upute proizvođača, alati koji se mogu koristiti ...

# Upravljanje rizikom

Sigurnosni rizik – mogućnost realizacije neželjenog događaja koji može štetno utjecati na povjerljivost, cjelovitost i raspoloživost informacijske imovine.



Upravljanje rizikom (*Risk Management*):

- Osnovni je preduvjet za upravljanje informacijskom sigurnošću
- Cijeli ISMS se oslanja na proces upravljanja rizikom
- Omogućuje postizanje ravnoteže između ostvarenja poslovnih ciljeva i minimiziranja štete

# Postupak procjene rizika

Postoji više načina procjene rizika i različite preporuke (ISO 27005, NIST ...)

Prema preporukama NIST-a (*National Institute of Standards and Technology*) postupak procjene rizika sastoji se od 8 koraka:

- 1) Identifikacija imovine
- 2) Identifikacija ranjivosti pojedine imovine
- 3) Identifikacija prijetnji koje mogu iskoristiti pojedine ranjivosti
- 4) Identifikacija i analiza pojedinih sigurnosnih kontrola nad imovinom
- 5) Procjena vjerojatnosti ostvarivanja prijetnje
- 6) Procjena štete koja nastaje realizacijom prijetnje
- 7) Izračun rizika
- 8) Prijedlog kontrola za umanjivanje rizika



# Postupak procjene rizika

- 1) Identifikacija imovine
  - Potrebno je definirati imovinu nad kojom će se vršiti procjena rizika
  - U tu svrhu koristi se popis imovine definiran u početnoj fazi projekta kod određivanja opsega ISMS-a
- 2) Identifikacija ranjivosti
  - Ranjivost je svojstvo imovine
  - To je slabost imovine i ne odnosi se samo na tehničke karakteristike (loš dizajn ili implementacija) već i na procesne (loša procedura, loše definirana sigurnosna politika...)
  - Ranjivost se promatra u kombinaciji sa prijetnjom – ako ne postoji prijetnja koja bi mogla iskoristiti ranjivost tada ne postoji niti rizik
  - Primjeri ranjivosti:
    - Nezaštićeno spremište
    - Nekontrolirano kopiranje
    - Ne radi se „logout“ nakon odlaska s radnog mjesta
    - Nedostatak dokumentacije
    - Loše kabliranje
    - ...



# Postupak procjene rizika

## 3) Identifikacija prijetnji

- Prijetnja iskorištava ranjivost i nanosi štetu imovini
- Nezadovoljan djelatnik – jedna od najvećih prijetnji
- Primjeri prijetnji za prethodno definirane ranjivosti:
  - Otuđivanje dokumenata ili medija
  - Zloupotreba prava
  - Greška prilikom upotrebe
  - Ispadi komunikacijske opreme
  - ...



## 4) Identifikacija i analiza postojećih sigurnosnih kontrola

- Primjenom sigurnosnih kontrola umanjuje se vjerojatnost da će prijetnja iskoristi ranjivost ili se smanjuje šteta ako prijetnja iskoristi ranjivost
- Kontrole po svojoj prirodi mogu biti:
  - Tehničke (npr. vatrozidi, enkripcija, kontrola pristupa...)
  - Administrativne (dokumenti kojima se definiraju pravila; npr. politike, procedure...)
  - Fizičke (npr. videonadzor, alarmni sustav, protupožarni sustav...)

# Postupak procjene rizika

## 5) Procjena vjerojatnosti

- Vjerojatnost da prijetnja iskoristi ranjivost najčešće se izražava skalom s određenim brojem razina vjerojatnosti
- Primjer kvalitativnog izražavanja vjerojatnosti:

vjerojatnost	opis
1 – niska	<ul style="list-style-type: none"><li>• postoje adekvatne sigurnosne kontrole</li><li>• niska motivacija potencijalnog napadača</li><li>• dešava se rijetko (manje od jednom godišnje)</li></ul>
2 – srednja	<ul style="list-style-type: none"><li>• postoji mogućnost za iskorištavanje ranjivosti</li><li>• postojanje sigurnosnih kontrola to otežavaju</li><li>• srednja motivacija potencijalnog napadača</li><li>• dešava se do dva puta godišnje (poznati su slučajevi u prošlosti)</li></ul>
3 – visoka	<ul style="list-style-type: none"><li>• ne postoje implementirane sigurnosne kontrole ili nisu adekvatne</li><li>• visoka motivacija potencijalnog napadača</li><li>• dešava se češće od dva puta godišnje.</li></ul>

# Postupak procjene rizika

## 6) Procjena štete

- Procjenjuju se mogući gubici ako prijetnja iskoristi ranjivost
- Prilikom procjene štete važno je uzeti u obzir:
  - Namjenu imovine u poslovnim procesima
  - Važnosti imovine za organizaciju
  - Osjetljivost informacija kojima imovina raspolaže
  - Vrijednost imovine iz popisa imovine (ako je tamo iskazana)
- Zahtjevan postupak – potrebno razmotriti sve moguće posljedice
- Kvantitativne metode izražavaju štetu u finansijskim gubicima ali se osim finansijskih gubitaka treba uzeti u obzir i npr. gubitak ugleda, gubitak kredibiliteta...

šteta	opis
1 – niska	utjecaj ostvarenja prijetnje na C I A je malen ili zanemariv: <ul style="list-style-type: none"><li>• zanemariva šteta na imovini</li><li>• nisu narušeni poslovni ciljevi organizacije</li></ul>
2 – srednja	utjecaj ostvarenje prijetnje na C I A postoji, ali nije kritičan: <ul style="list-style-type: none"><li>• djelomični gubitak ili oštećenje imovine</li><li>• djelomično narušeni poslovni ciljevi organizacije</li></ul>
3 – visoka	utjecaj ostvarenje prijetnje na C I A je vrlo velik: <ul style="list-style-type: none"><li>• gubitak ili uništenje imovine</li><li>• potpuno narušavanje poslovnih ciljeva organizacije</li></ul>

# Postupak procjene rizika

## 7) Izračun rizika

- Izračunom određujemo razinu rizika za pojedinu imovinu
- Prilikom određivanja razine rizika potrebno je uzeti u obzir:
  - Vjerojatnost da prijetnja iskoristi ranjivost
  - Posljedicu (štetu) u slučaju realizacije prijetnje
  - Implementirane sigurnosne kontrole koje mogu umanjiti vjerojatnost ostvarenja prijetnje ili štetu
- Pogledati slideove od 26 do 30



## 8) Prijedlog kontrola za umanjivanje rizika

- Rizik za pojedinu imovinu je procijenjen te je potrebno analizirati i predložiti mjere za umanjivanje sigurnosnog rizika
- Prilikom odabira kontrola potrebno je uzeti u obzir niz čimbenika:
  - Sigurnosnu politiku
  - Učinkovitost kontrola
  - Troškove uvođenja i održavanje kontrola
  - Kulturu organizacije
  - Reakcije korisnika
  - ...



# Tretiranje (obrada) rizika

Tretiranje (obrada) rizika podrazumijeva:

- Izradu plana obrade rizika
- Analizu, evaluaciju i uvođenje kontrola predloženih u prethodnoj fazi

Rizik se najčešće umanjuje

- Uglavnom se ne može u potpunosti ukloniti
- Umanjuje se do razine koja je prihvatljiva u organizaciji (najčešće financijski)
- Menadžment organizacije odlučuje na koji način i u kojoj mjeri se rizik umanjuje



**Moguće opcije za tretiranje (obradu) rizika:**

- 1) Smanjivanje rizika – primjena prikladnih kontrola
- 2) Prihvatanje rizika – svjesno i objektivno prihvatanje rizika u skladu s politikom sigurnosti i kriterijima za prihvatanje rizika
- 3) Izbjegavanje rizika – izbjegavanje situacija u kojim može doći do pojave rizika
- 4) Prenošenje rizika – prenošenje poslovnih rizika na nekog drugog (npr. osiguravatelje, dobavljače...)

# Evaluacija i nadzor rizika

Imovina u opsegu ISMS-a podložna je promjenama te je potrebno:

- Periodički evaluirati rizike
- Konstantno nadzirati rizike

Često je u praksi potrebno provoditi procjenu rizika nakon određenih promjena unutar opsega ISMS-a:

- Na mrežnoj opremi (promjene u arhitekturi mreže)
- Na serverskoj opremi
- Nakon promjene djelatnika (najčešće rukovodstva)
- ...

# Vježba - jedna od metoda procjene rizika

Potrebno je proračunati rizik za navedenu imovinu i napraviti plan obrade rizika.

## Kvalitativna metoda procjene rizika

- Prikladna za poslovne procese i tehnologiju
- Daje usporedive i ponovljive rezultate

# Klasifikacija informacija

Potreba za klasifikacijom informacija očituje se u slijedećim činjenicama:

- Sve informacije u nekoj organizaciji nisu jednako vrijedne (osjetljive)
- Ukoliko su vrijedne (osjetljive) informacije otkrivene mogu nanijeti štetu organizaciji
- Ako se nad svim informacijama primjenjuju jednake mjere zaštite neke će biti premalo, a neke previše zaštićene
- Primjena adekvatnih kontrola na informaciji obzirom na njezinu vrijednost

Klasifikacija informacija je postupak utvrđivanja stupnja tajnosti, odnosno klasifikacijskih razina tajnosti.

Vlasnik informacije je osoba odgovorna za:

- Klasifikaciju informacije u skladu s njenom vrijednošću
- Zaštitu informacije – primjenu mehanizama zaštite
- Periodičku provjeru klasifikacije informacije obzirom na promjene u poslovnim procesima, zakonima i dr.
- Odobravanje prava pristupa informaciji
- Označavanje informacije prema stupnju tajnosti – klasifikacija treba biti vidljiva svima kojima je informacija dostupna



Vlasnik se često definira u popisu informacijske imovine.

# Proces klasifikacije informacija

Proces klasifikacije informacija obuhvaća 4 koraka:

- 1) Identifikacija informacije
- 2) Definiranje klasifikacijskih razina
- 3) Definiranje kontrola za klasifikacijske razine
- 4) Pridruživanje klasifikacijskih razina

# Proces klasifikacije informacija

## 1) Identifikacija informacije

Napraviti registar informacija u organizaciji:

- Pomoću anketa
- Poslovnom analizom
- Većina organizacija će iskoristiti popis imovine definiran na početku uvođenja ISMS-a – odnosi se na informacijsku imovinu (ugovori, baze podataka, dokumenti, a ne na fizičku imovinu, softver, usluge...)

# Proces klasifikacije informacija

## 2) Definiranje klasifikacijskih razina

- Odabrati onoliko klasifikacijskih razina koliko je prikladno da bi organizacija zaštitila svoju informacijsku imovinu (primjer u tablici)
- Za državne ustanove propisano Zakonom o tajnosti podataka (NN 79/07)
- Opisati klasifikacijske razine tj. definirati njihovo značenje

klasifi- cijska razina	opis	primjer
javno	<ul style="list-style-type: none"><li>• informacije namijenjene javnoj objavi</li><li>• javna objava <u>ne može našteti</u> organizaciji</li></ul>	informacije na javnim web stranicama, objave za medije, newsletteri, ...
povjerljivo	<ul style="list-style-type: none"><li>• informacije čije otkrivanje neovlaštenim osobama može imati <u>štetne</u> posljedice za organizaciju</li><li>• ugled, manja finansijska šteta...</li></ul>	opće informacije o organizaciji, osobne informacije zaposlenika, informacije o partnerima...
tajno	<ul style="list-style-type: none"><li>• informacije čije otkrivanje neovlaštenim osobama može imati <u>značajne štetne</u> posljedice za organizaciju</li><li>• značajno narušavanje ugleda, veća finansijska šteta...</li></ul>	finansijske informacije, ugovori, informacije o klijentima...
vrlo tajno	<ul style="list-style-type: none"><li>• informacije čije otkrivanje neovlaštenim osobama može nanijeti <u>nepopravljivu štetu</u> za organizaciju</li><li>• tržišne, pravne...</li></ul>	Marketinške informacije i planovi, informacije o kritičnim tehničkim sustavima, finansijski planovi...

# Proces klasifikacije informacija

## 3) Definiranje kontrola za pojedine klasifikacijske razine

Kontrole za klasifikacijske razine definiraju se uz pomoć:

- Sigurnosnih politika organizacije
- Vlasnika informacijske imovine
- Regulatornih i ugovornih zahtjeva
- Voditelja odjela/sektora
- ...

Često upotrebljavane kontrole:

- Provjera identiteta osobe koja pristupa informaciji (autentifikacija)
- Pristup podacima prema radnom mjestu (uloge eng. *role based access*)
- Enkripcija
- Razne tehničke kontrole (segmentacija mreže, backup, antivirusni sustavi...)

# Proces klasifikacije informacija

## 4) Pridruživanje klasifikacijskih razina

Za klasifikaciju informacija zadužen je vlasnik informacije.

Potrebno je:

- Klasificirati informacijsku imovinu prema definiranim razinama
- Provoditi periodičke provjere razine klasifikacija pojedine informacijske imovine

# Vježba - klasifikacija informacija

Zadatak: odgovoriti na pitanja (informacije s predavanja ili pronaći na internetu)

Pravilnik ili procedura za klasifikaciju imovine ima slijedeću formu:

- 1) Odgovornosti
  - a) Tko sve sudjeluje u klasifikaciji imovine i koja mu je uloga?
  - b) Tko periodički radi kontrolu?
- 2) Klasifikacijske razine
  - a) Koliko će ih biti?
  - b) Opis svake razine – da li ćemo sami kreirati ili preuzeti iz zakona?
- 3) Način označavanja klasifikacijske razine
  - a) Kako se mogu označiti mediji poput traka ili DVD-ova?
  - b) Kako treba izgledati klasificirani dokument? Gdje se nalazi klasifikacija?
- 4) Način rukovanja
  - a) Kako se barata klasificiranom imovinom? Npr. slanje, primanje, čuvanje i uništavanje klasificiranih informacija.
  - b) Što je deklasifikacija i kada je informacija deklasificirana?

# Fizička sigurnost

Informacijski sustav siguran je onoliko koliko je sigurna njegova najslabija karika.

Fizička sigurnost često je zanemarena.

Fokus informacijske sigurnosti na logičke kontrole više nego na fizičke:

- politike, procedure, pravilnici
- password (4 uvjeta kompleksnosti, redovita promjena)
- *firewall* uređaji, antivirusna zaštita, *antispam* filteri
- zakrpe (*security & critical patches*)

# Fizička sigurnost – prijetnje

Prijetnje fizičkoj sigurnosti mogu narušavati sva svojstva informacije (CIA):

## 1) Prirodne prijetnje

Poplave, potresi, oluje, šumski požari, ekstremne temperature

## 2) Infrastrukturne prijetnje (prijetnje iz okoline)

Požari, prekidi napajanja električnom energijom, problemi sa instalacijama (plin, voda...), curenje klima uređaja

## 3) Ljudske prijetnje

Neovlašten pristup, šteta uzrokovana nepažnjom (npr. prolijevanje tekućine po opremi), vandalizam, krađa, industrijska špijunaža

## 4) Društveno uzrokovane prijetnje

Štrajk, rat, teroristički napad...

# Fizička zaštita informacijskih resursa

Fizičke mjere zaštite najčešće se provode nad imovinom:

1. Građevine i okoliš (zgrade i grupe zgrada s okolišem)
2. Prostorije (uredi, prostor s posebnom namjenom, prostor s javnim pristupom)
3. Računalna i mrežna oprema
4. Papirnati i elektronički mediji

# Fizička zaštita – građevine i okoliš

Građevine i okoliš prva su razina zaštite od prijetnji (ljudskih, prirodnih, društveno uzrokovanih i iz okoline).

Stručnjak za informacijsku sigurnost mora uzeti u obzir:

1. Dizajn građevine i okoliša
  - utjecaj na ljudsko ponašanje
  - smanjenje rizika od kriminalnih aktivnosti (npr. kamere, jaka rasvjeta, uklanjanje stabala i grmlja...)
2. Dodatne mjere
  - Ograde
  - Klupe na javnim površinama
  - Položaj sigurnih prostorija i server sobe (npr. u sredini zgrade)
  - Materijala od kojih je prostorija građena (npr. protupožarni knauf, antistatički premaz na podu...)
  - Raspored prozora i vrata
  - Izvedba infrastrukture (grijanje, ventilacija, klima)
  - Instalacije (vodovod, električne, telekom instalacije)

# Fizička zaštita – građevine i okoliš

Prilikom procjene rizika za građevine i okoliš potrebno je uzeti u obzir:

## 1. Okoliš i vanjski utjecaji

- a) Izgled zgrade (ne smije odavati dojam da je nešto važno u zgradi)
- b) Izgled terena (npr. stara gradska jezgra često ima drvene kuće – opasnost od požara)
- c) Stopa kriminaliteta u području
- d) Blizina policije, vatrogasaca...
- e) Položaj industrije ili skladišta (zapaljivi materijali, opasne kemikalije i sl.)

## 2. Dostupnost

- a) Cestovni pristup – dostupnost i više pristupnih putova povećava sigurnosni rizik
- b) Gustoća prometa
- c) Blizina aerodroma

## 3. Prirodne nepogode

- a) Rizik od potresa, poplava i oluja (utjecaj kod odabira sekundarne lokacije)
- b) Rizičan teren (klizišta, odroni kamenja, lavine...)

# Fizičke kontrole za građevine i okoliš

- 1) Ograde – analizom rizika određuju se gabariti ograde (npr. namjena je odvratiti slučajnog provalnika, namjernog provalnika...)
- 2) Videonadzor – efikasan za odvraćanje i naknadne analize
- 3) Konstrukcija zgrade, zidovi i podovi
  - a) Zapaljivost i otpornost na vatru zidova, stropova i podova
  - b) Otpornost zidova (dvostruki zidovi, posebne armature...)
  - c) Nosivost stropova i podova (bitno za sistem sale i prostore za arhivu i sebove)
- 4) Vrata – protuprovalna i protupožarna (s atestom)
- 5) Prozori – ojačana stakla ili zaštita metalnim šipkama
- 6) Infrastrukturne instalacije
  - a) Predstavljaju prijetnju; nije fokus menadžera za sigurnost
  - b) Osigurati redovito održavanje
  - c) Saznati gdje su ventili u slučaju nužde
- 7) Ostale kontrole
  - a) Npr. redoviti obilasci zaštitara imaju snažan efekt odvraćanja
  - b) Npr. trenirani psi

# Fizičke kontrole za prostorije

- 1) Kontrola pristupa
  - a) Identifikacija posjetitelja
  - b) Ograničavanje pristupa (npr. dozvola za kat ili sobe)
- 2) Sustavi za detekciju i alarmni sustavi
  - a) Široka primjena – otkrivanje provala i drugog neovlaštenog pristupa
  - b) Podrazumijeva ljudsku intervenciju nakon alarma
- 3) Sustavi za zaštitu od požara
  - a) Detektori dima, prašine i temperature
- 4) Napajanje električnom energijom
  - a) Ispravno kabliranje (utjecaj EM zračenja; odvojiti od ICT instalacija)
  - b) UPS (*Uninterruptable Power Supply*) – osigurava napajanje i smanjuje fluktuacije napona
  - c) Generatori – koriste se u slučaju duljih prekida napajanja

# Fizičke kontrole za računalnu i mrežnu opremu

- 1) Serverske sobe (sistemske sobe, sistem sale)
  - a) Kontrola pristupa – isključivo ljudi koji imaju potrebu pristupa
  - b) Protupožarna zaštita – vatrootporni zidovi i detekcija/gašenje požara moraju biti sastavni dio sobe
  - c) Protuprovalna vrata
  - d) Klimatizacija – osjetljivost računalne opreme na vlagu (40-60%) i temperaturu (< 25°C)
  - e) Senzori za detekciju tekućine
  - f) Antistatički podovi i uzemljenja
  - g) Poslužiteljski ormari (*rack*) – osiguravaju pravilan smještaj i hlađenje
  - h) Seizmička zaštita – gumena postolja i seizmički ormari smanjuju osjetljivost na vibracije
- 2) Kabliranje i zaštita komunikacijske infrastrukture
  - a) Ispravno kabliranje vrlo je bitno
  - b) Upotreba adekvatnih kablova – UTP (*unshielded*), FTP (*foiled*), STP (*shielded*)
- 3) Zaštita prijenosnih računala
  - a) Ne ostavljati na javnim mjestima, koristit sigurnosne brave, detektori pokreta
  - b) Preporuka je kriptirati diskove

# Fizičke kontrole za papirnate i elektroničke medije

- 1) Sefovi – tradicionalno rješenje
  - a) Zaštita od provale
  - b) Vatrootpornost
  - c) Zaštita od uvjeta iz okoline
- 2) Rezači papira – uništavanje na konfete i trake
- 3) Uništavači elektroničkih medija
  - a) Demagnetizacija
  - b) Fizičko uništavanje

## Uništavanje podataka na magnetskim medijima (*degaussing*)

[http://www.youtube.com/watch?feature=player\\_embedded&v=nJ3oqDytutc](http://www.youtube.com/watch?feature=player_embedded&v=nJ3oqDytutc)

EMP

Što je sa SSD diskovima ili USB flash memorijama?

# Podatkovni centar

- Izgled podatkovnog centra

[https://www.youtube.com/watch?v=iuqXFC\\_qlvA](https://www.youtube.com/watch?v=iuqXFC_qlvA)

- Dizajn podatkovnog centra

[https://www.youtube.com/watch?v=kfvbCggY\\_nl](https://www.youtube.com/watch?v=kfvbCggY_nl)

- Višeslojna zaštita

# Održavanje poslovanja u kriznim situacijama

Što može onemogućiti odvijanje poslovanja (potpuno ili djelomično)?

- Dugotrajan nestanak napajanja
- Kvar ključne opreme (npr. servera ili *core switcha*)
- Gubitak bitne dokumentacije (npr. projekt, ugovori...)
- Požar ili poplava u prostoriji sa serverima (sistem sala/server soba...)
- Vandalizam (namjerno uništenje opreme)
- Potres
- Poplava

Cilj sustava upravljanja kontinuitetom poslovanja (BCM – *Business Continuity Management*) je držati posljedice pod kontrolom ili ih spriječiti.

U sklopu ISMS sustava razvija se plan kontinuiteta poslovanja (BCP – *Business Continuity Plan*).

Koje svojstvo informacije želi očuvati plan kontinuiteta poslovanja?

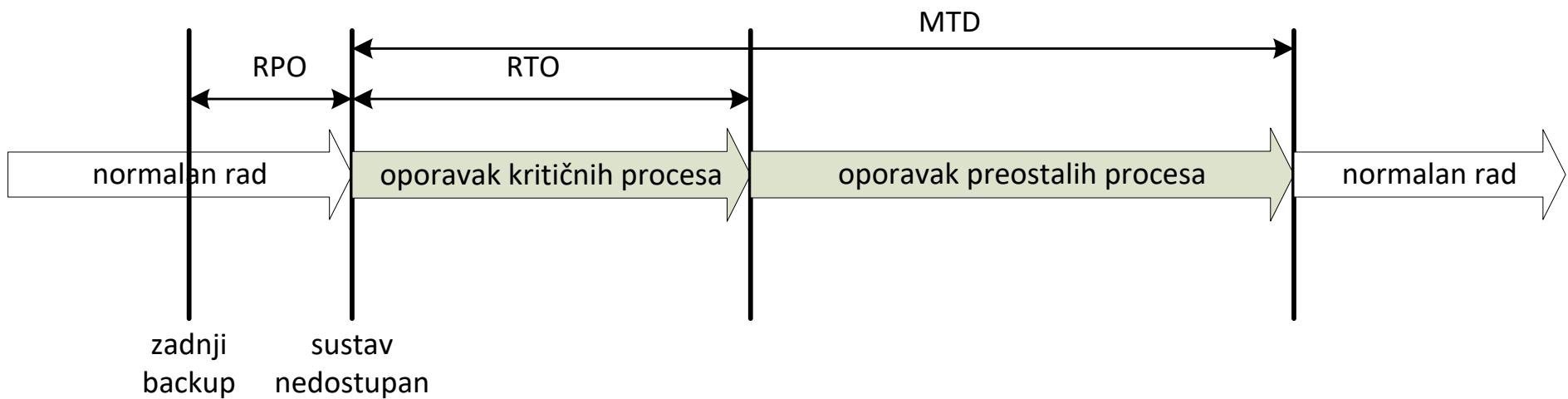
# Plan kontinuiteta poslovanja (BCP)

Proces planiranja kontinuiteta poslovanja ima slijedeće korake:

- 1) Procjena rizika
- 2) Analiza učinka na poslovanje (BIA – *Business Impact Analysis*)
  - a) Ključni IT sustavi, aplikacije i ostali resursi
  - b) MTD (*Maximum Tolerable Downtime*) parametar
  - c) RTO (*Recovery Time Objective*) i RPO (*Recovery Point Objective*)
- 3) Izrada strategije kontinuiteta poslovanja
  - a) Alternativne lokacije za obavljanje posla, lokacije za rad BCP tima, mjesto susreta nakon neželjenog događaja...
  - b) Ključni infrastrukturni sustavi i infrastruktura, alternative
  - c) Ključni podaci, njihov smještaj (zapisi, diskovi, trake, sefovi...)
- 4) Izrada plana kontinuiteta poslovanja
- 5) Testiranje planova kontinuiteta poslovanja
- 6) Održavanje planova kontinuiteta poslovanja

# Vremenski parametri utjecaja na poslovanje

- RPO (*Recovery Point Objective*) – označava vremenski period prihvatljive količine izgubljenih podataka
- RTO (*Recovery Time Objective*) – označava vrijeme do oporavka ključnih resursa
- MTD (*Maximum Tolerable Downtime*) – označava maksimalno prihvatljivo vrijeme do oporavka na uobičajenu razinu



# Izrada plana kontinuiteta poslovanja (BCP)

Cilj plana je omogućiti uspostavljanje ključnih poslovnih procesa u određenom vremenskom periodu nakon što nastupi neželjeni događaj.

Plan se izrađuje kako bi:

- Imali pripremljene procedure i smjernice za oporavak ključnih poslovnih procesa
- Izbjegli donošenje odluka o uspostavi poslovanja u kriznom trenutku

Plan je potrebno testirati jednom godišnje – primjer dobre prakse, zakonska obaveza ili formalan zahtjev norme.

# Vježba – Sadržaj plana kontinuiteta poslovanja 1/4

Plan je različit u svakoj organizaciji, ali neki osnovni elementi su zajednički svima.

- 1) Opseg i svrha plana
  - a) Svrha – umanjiti posljedicu radi nastanka neželjenog događaja
  - b) Opseg – operativna i tehnička područja organizacije:
    - Lokacije
    - **Definirati ključne poslovne procese i usluge**
    - Poslovne jedinice (funkcije/odjeli)
    - Alternativne lokacije (smještaj backup medija, IT opreme...)
    - Poslovni partneri i klijenti
    - Javne službe (vatrogasci, hitna pomoć...)
- 2) Što je za našu organizaciju neželjeni događaj?
  - a) Definirati neželjeni događaj
  - b) Razlikovati od uobičajenog sigurnosnog incidenta da se ne pokreće BCP plan bez razloga

# Vježba – Sadržaj plana kontinuiteta poslovanja 2/4

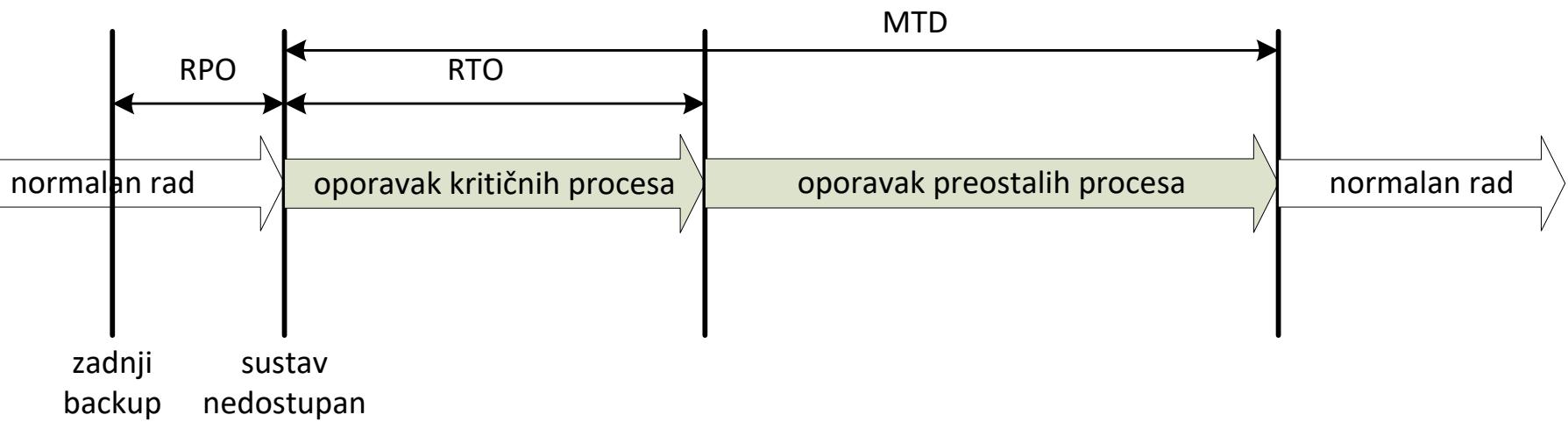
## 3) Procjena rizika

Naziv imovine	Opis kombinacije prijetnja/ranjivost	Vjerojatnost da prijetnja iskoristi ranjivost	Opis učinka/posljedice	Procjena posljedice	Razina rizika
Server	Vandalizam/uništenje opreme	1	Ispad ključnih poslovnih procesa	2	3
Server	Eksplozija/uništenje opreme	1	Ispad ključnih poslovnih procesa	2	3
Soba	Potres/uništenje opreme ili jednog dijela	2	Ispad ključnih poslovnih procesa	2	4
Switch	Požar/uništenje opreme	2	Ispad ključnih poslovnih procesa	3	5
Soba	Poplava/zastoj funkcija poslovanja - djelomično ili potpuno	2	Ispad ključnih poslovnih procesa	3	5
Soba	Dugotrajan nestanak struje/zastoj djelomično ili potpuno	1	Ispad ključnih poslovnih procesa	3	4

# Vježba – Sadržaj plana kontinuiteta poslovanja 3/4

## 4) Definirati ciljana vremena

- RPO
- RTO
- MTD



# Vježba – Sadržaj plana kontinuiteta poslovanja 4/4

## 5) Definirati članove BCP tima i odgovornosti

- Koordinator svih aktivnosti i zamjenik – odgovoran za izvršavanje plana, proglašavanje katastrofe i pokretanje plana
- Tim za procjenu štete – odgovoran za procjenu nakon koje se donosi odluka hoće li se pokrenuti BCP plan i hoće li se npr. aktivirati sekundarna lokacija
- Tim za provedbu plana (tehničko osoblje i njihova zamjena)
- Tim za odnos s medijima

# Tipične faze provedbe BCP plana 1/3

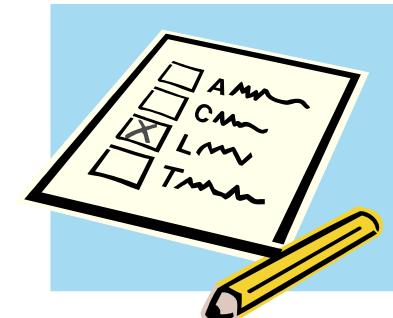
## Faza 1: Inicijalni odgovor

- Neželjeni događaj se dogodio
- Obavještava se koordinatora BCP aktivnosti (bilo tko iz organizacije, zaštitar, vatrogasac...) o neželjenom događaju
- Gruba procjena posljedica
- Obavještavaju se ostali članovi BCP tima



## Faza 2: Procjena događaja i eskalacija

- Procjena štete
- Izrada detaljnog izvještaja o šteti
- Odluka o eskalaciji u slijedeću fazu



# Tipične faze provedbe BCP plana 2/3

## Faza 3: Proglašavanje katastrofe

- Odluka na osnovu detaljnog izvještaja iz prethodne faze
- Odabir strategije oporavka (npr. aktiviranje sekundarne lokacije, oporavak u istoj zgradi, zakup *cloud* usluge...)
- Priprema izjave o proglašenju katastrofe
- Priprema izjave za javnost
- Okupljanje BCP tima



## Faza 4: Priprema nove lokacije

- Priprema okruženja za oporavak svih poslovnih aktivnosti (nabava hardvera, instalacija softvera, ...)

# Tipične faze provedbe BCP plana 3/3

## Faza 5: Oporavak i obnavljanje aktivnosti

- Obnavljaju se ključni resursi
- Uspostavljaju se poslovni procesi



## Faza 6: Normalizacija

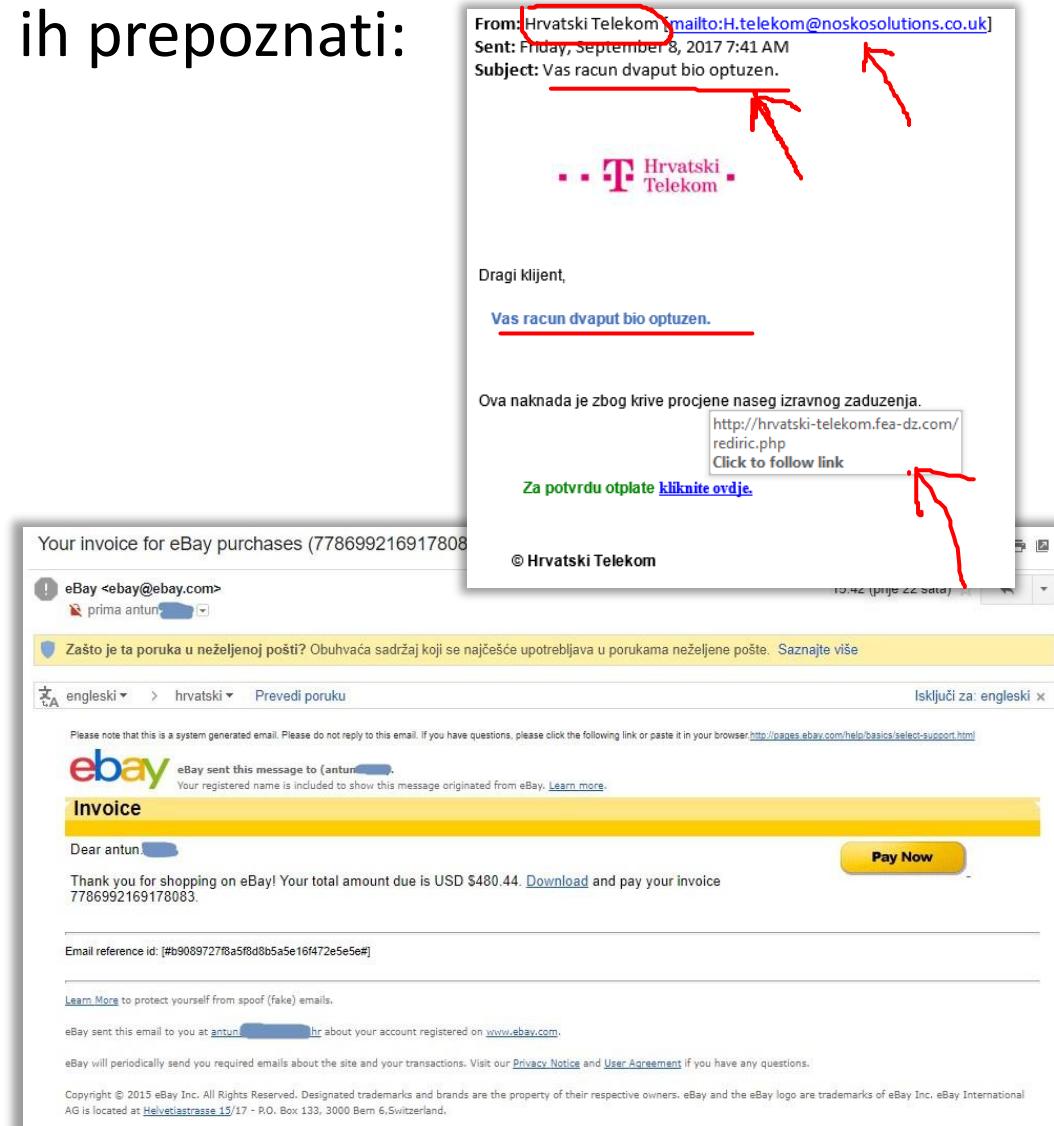
- Povratak u stanje prije neželjenog događaja (gašenje sekundarne lokacije, povrat hardvera, ...)



# Kibernetička (računalna) sigurnost

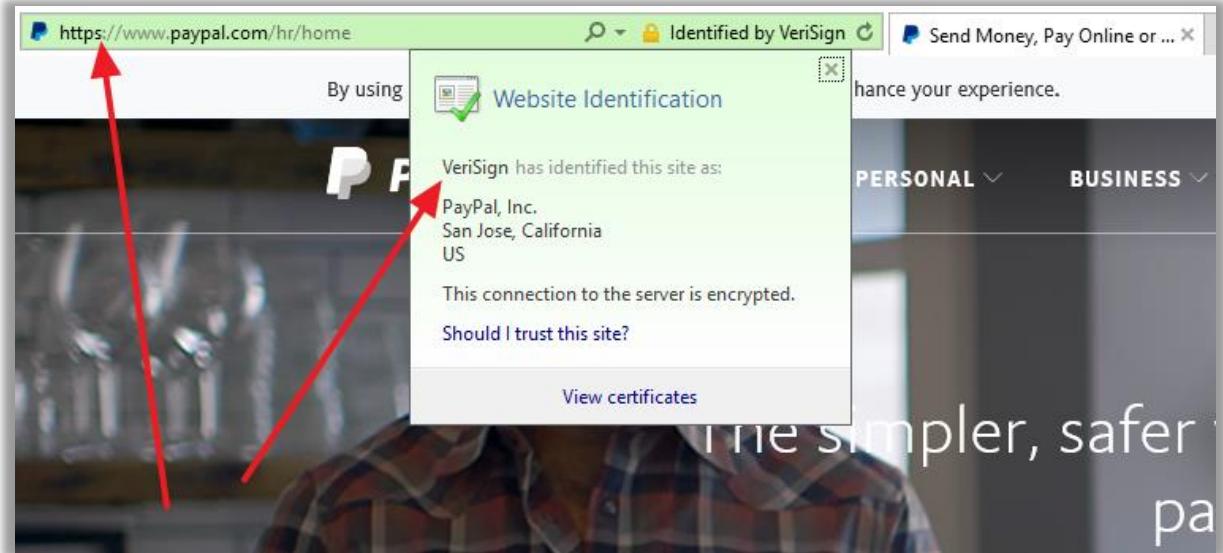
Sigurnosne prijetnje i kako ih prepoznati:

- Varljivi mailovi
  - stvaraju privid legitimnih poruka
  - linkovi ili dokumenti koji sadrže linkove (docx, xlsx, zip i rar s passwordom)
  - često loše prevedeno na hrvatski
- Sumnjivi privitci u mailovima
  - najčešće *phishing* za krađu identiteta ili ransomware softver kojim se kriptiraju podaci

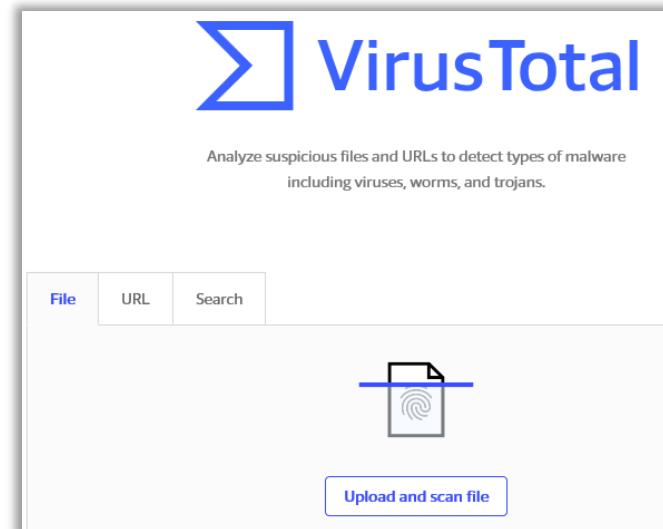


# Provjera linkova

- https
- Certifikat:
  - PayPal,
  - ZABA...



- VirusTotal
- [www.virustotal.com](http://www.virustotal.com)

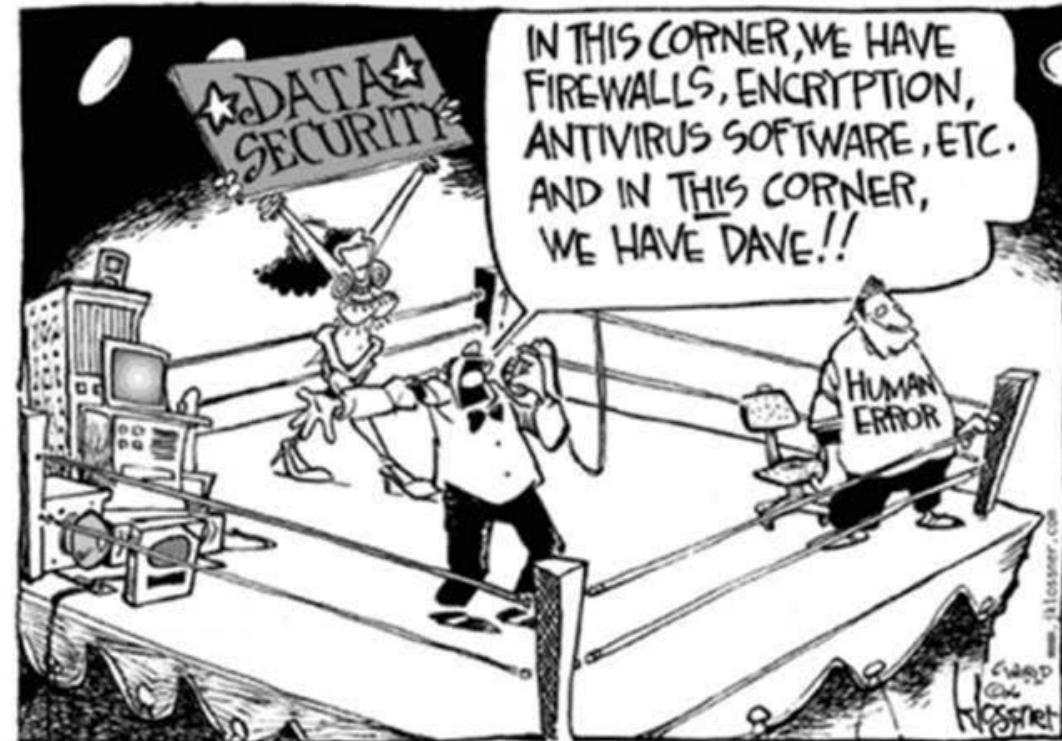


# Socijalni inženjering

- socijalni inženjering (eng. *social engineering*), ponekada prijevod društveni inženjering
- tehnika za iskorištavanje ljudskih pogrešaka i slabosti
- cilj napadača je otkrivanja povjerljivih informacija ili dobivanja pristupa određenim resursima
- napadač navodi žrtvu da učini nešto što nije u njegovom interesu koristeći metode zavaravanja (vješto kreirani scenariji):
  - lažno predstavljanje,
  - iskorištavanje osjećaja odgovornosti,
  - stvaranje osjećaja krivnje,
  - poticanje na žurnu reakciju,
  - ucjenjivanje, prijetnje i sl.
- priprema napada – proučavanje žrtve i prikupljanje podataka (društvene mreže, stranice tvrtke i sl.)
- način napada – telefonski pozivi i e-mail poruke kojima se pokušava zavarati žrtva
- primjeri scenarija:
  - lažno predstavljanje
    - direktor neke tvrtke koji podsjeća na plaćanje računa
    - policijski službenici koji istražuju prijevaru i navode žrtvu da im preda „lažan“ novac
  - podmetanje lažnog dokumenta (npr. Excel tablica s lažnim IBAN)
  - senzibiliziranje sugovornika radi preuzimanja ovlasti na računalu (npr. plač djeteta u pozadini)

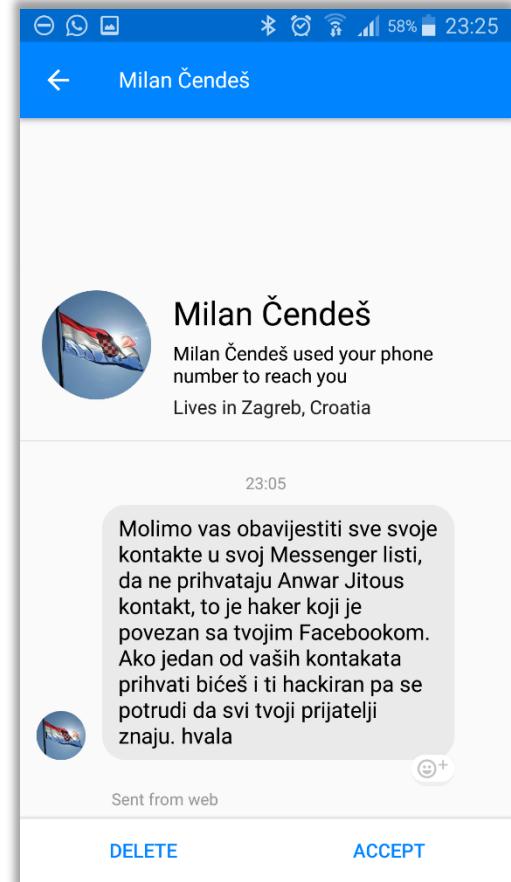
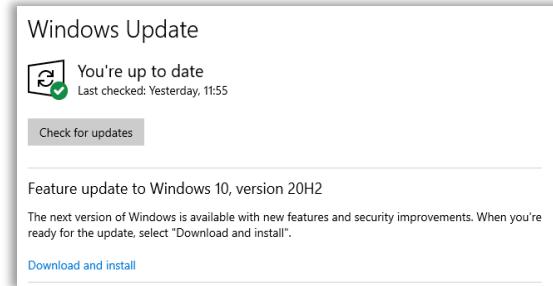
# Zaštita u tvrtkama

- Antispam
- Firewall
- Antivirus
- Redovite zatrpe
  - *sucurity & critical patches*
- Ljudski faktor
  - svijest o sigurnosti
  - odgovorna upotreba računala
  - nemojte biti Dave 😊



# Računalna zaštita u privatnom okruženju

- Zaštita „digitalnog života“ značajna poput zaštite vlastite imovine, obitelji, fizičke sigurnosti i zdravlja.
- Hakeri ne mare za zdravlje žrtve, etičnost ili moralne posljedice svojih postupaka već im je prvenstveni prioritet zarada.
- Preventivne mjere:
  - ažuriranje softvera (OS, aplikacije)
  - backup (na vanjski disk), isključiti disk nakon backupa
  - koristiti antivirusni alat i redovito ažurirati
    - Avast Free Antivirus
    - AVG Antivirus Free
    - Bitdefender Free
    - Sophos Home
  - pažljivo baratati s nepoznatim porukama
  - nemojte otvarati nepoznate linkove i dokumente prije provjere
  - koristite *adblocker*, nemojte otvarati reklame
  - nemojte biti Dave 😊



# Računalna zaštita u privatnom okruženju

- Desilo se – što sada?
  - Skeniranje antivirusom
  - *Guglati* rješenje
  - Skeniranje/očistiti zarazu s dodatnim antivirusnim alatom
  - Potražiti pomoć stručne osobe



# Ransomware

- Prijetnja prisutna nekoliko godina
- Kriptiranje podataka na zaraženom računalu i priključenim diskovima
- Svibanj 2017.
  - WannaCry, Wcry, Wanna Crypt
  - iskorištena poznata slabost (*by NSA*)
  - Redovito ažurirana računala nisu imala problema



# Ransomware

- Načini širenja
  - mail – linkovi, dokumenti s linkovima
  - portali – reklame, *banners*
- *Zero-day* napadi
  - sigurnosni rizici u operativnim sustavima i aplikacijama nepoznati javnosti i proizvođačima
  - uzrokuju veliku štetu
  - ne postoji „definicija“ u postojećim antivirus ili firewall zaštitama

## Malware

Major sites including New York Times and BBC hit by 'ransomware' malvertising

Adverts hijacked by malicious campaign that demands payment in bitcoin to unlock user computers



# Ransomware

- Ransomware-as-a-Service (Raas)
  - *custom made ransomware* – nisu potrebna posebna tehnička znanja da se dođe u posjed ransomware softvera
  - servis na internetu – preko sučelja mogu se odabrati opcije vlastitog ransomware softvera
  - nakon update dobije se vlastiti ransomware spremam za širenje
- Ucjenja objavom privatnih podataka
  - ne kriptira već uzima privatne podatke i prijeti njihovom objavom
  - npr. slike, povijest surfanja, povijest poziva...
  - LeakerLocker ugrađen u neke aplikacije za Android

Thread Tools ▾ Search this Thread ▾ Rate Thread ▾ Display Modes ▾ #1

Today, 16:05

**Cold\_As\_Ice** Satan is a free to use ransomware kit, you only need to register on the site to start making your viruses. Satan only requires a user name and password to create an account, although, if you wish, you can set a public key for two-factor authentication. Satan has a initial fee of 30% over the victim's payment, however, this fee will get lower as you get more infections and payments. All of the user transactions are covered by the server, you'll always get what the victim paid, minus the fee of course.

Junior Member

Join Date: Aug 2016

Posts: 1

Reputation: 0 [+/-]

Balance: 0.00\$

Satan is free. You just have to register on the site.  
Satan is very easy to deploy, you can create your ransomware in less than a minute.  
Satan uses TOR and Bitcoin for anonymity.  
Satan's executable is only 170kb.

If english is not your first language or you speak a second language you can translate the ransom notes to help your victims understand better what is happening.  
In case you're looking for a way to spread the ransomware, there is a droppers page, where you can generate a crude code for a Microsoft Word macro and CHM file.  
If you have any problem with the ransomware, you can report it using the leftmost button on the malwares table. The middle blue button is used to update the malware to a newer version, if available, and the green one is used to edit your malware configuration.

<http://satan6dII23napb5.onion>

QUOTE QUICK REPLY



Identity and Privacy LEAK

All personal data from your smartphone has been transferred to our secure cloud.  
© McAfee Labs

It contains:

- 和个人照片 ()
- 联系人号码 ()
- 已发送和接收的短信 ()
- 电话通话历史 ()
- Facebook 消息
- Chrome 浏览历史
- 完整电子邮件文本
- GPS 位置历史

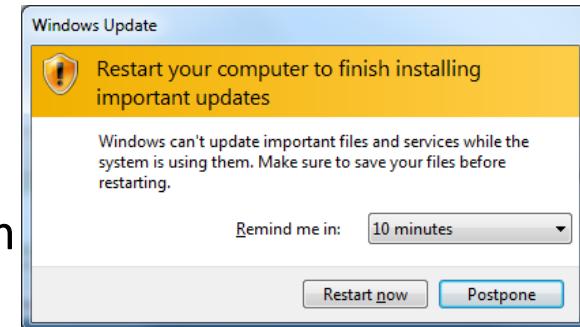
In less than 72 hours this data will be sent to every person from your telephone and email contacts list. To abort this action you have to pay a modest RANSOM of \$50.

PROCEED

© McAfee Labs

# Što možete sami poduzeti

- Preventiva – *backup & patch*
- Odgovorno koristite računalo
  - izbjegavajte instalacije iz neprovjerjenih izvora
- Pažljivo pristupajte s nepoznatom i neočekivanom
  - budite sumnjičavi prema nepoznatim pošiljateljima
  - provjerite neočekivane poruke poznatih pošiljatelja npr. banaka, PayPala, Amazona i sl.
    - izgledaju kao legitimne poruke
    - zahtijevaju unos korisničkog imena i zaporce
- Koristite *ad blocker*
- Provjera sumnjivih linkova i fileova – [virustotal.com](http://virustotal.com)
- Provjerite postoji li rješenje na [nomoreransom.org](http://nomoreransom.org)
- Napredniji korisnici mogu koristiti *sandbox* rješenja



# Upotreba zaporki (passwords)

- Zaporce su osnova sigurnosti u računalnom svijetu
- Opasnost od preuzimanja identiteta
  - kompromitiranje osobe
  - neugodne situacije
  - online plaćanje
- Preporuke:
  - dvofaktorska autentifikacija
  - kompleksnost
  - periodičke promjene
- Različite zaporce za različite servise
- Alati za čuvanje:
  - KeePass
  - LastPass
  - Dashline

Top 10 Worst Passwords You Should Never Keep	
Rank	String
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321



# Literatura

- 1) Saletović K. (2015): *Sigurnost poslovnih informacijskih sustava – priručnik*, nakladnik Vern, 2015, Zagreb
- 2) Grupa autora (2010): *Sigurnost informacijskih sustava – priručnik*, nakladnik Algebra d.o.o., Zagreb
- 3) Humphreys E. (2007): *Implementing the Information Security Management System Standard*, nakladnik Artech House, Boston, SAD
- 4) Međunarodni standard ISO/IEC 27001 – informacijska sigurnost
- 5) Međunarodni standard ISO/IEC 27002 – smjernice i dobra praksa
- 6) <http://blog.iso27001standard.com/hr/tag/isms-hr/> - pristupano 1.4.2012.
- 7) Međunarodni standard ISO/IEC 27005 – procjena rizika
- 8) Razna literatura dostupna na internetu