РЕПУБЛИКА СРБИЈА
АУТОНОМНА ПОКРАЈИНА ВОЈВОДИНА
Покрајинска влада
УПРАВА ЗА ЗАЈЕДНИЧКЕ ПОСЛОВЕ ПОКРАЈИНСКИХ ОРГАНА

ИТ безбедност
Теорија и пракса

Др Милан Парошки, дипл.ел.инж.
Помоћник директора

Шта се деси у једној минути на интернету?

- 47.000 апликација се даунлодује
- 204 милиона мејлова се пошаље
- 61.141 сати музике се даунлодује
- 20 милиона фотографија се погледа
- 320 нових твитер налога се отвори
- 100.000 нових твитова се постави
- 6 нових чланака се постави на википедији
- 1300 нових мобилних корисника
- 277.000 логова на Фејсбук
- 2 милиона упита (search) на Google
- итд

Блиска будућност

- Сада : број мобилних уређаја је једнак светској популацији
- Крајем 2015: број мобилних уређаја ће бити два пута већи од светске популације
- 2015 ће бити потребно 5 година да се погледа сваки видео запис који се постави на интернет сваке секунде

Шта ће се десити 2017?

- Од 2012 до 2017 , мобилни саобраћај ће порасти 13 ПУТА
- 2017 ће бити 3 ПУТА више конектованих уређаја на мрежи неко светске популације
- 4 зетабајта података ће бити креирано сваког минута

Безбе дност?

Шта даље?

ИТ управљање
Теорија
Увод

- Информатичко друштво → **велика улагања у (ИКТ)** (информационо-комуникациону технологију).

↓

- **Утицај технологије** → потреба реструктуирања традиционалних организација у флексибилне организације засноване на процесном приступу.

↓

- Примена информатике није више довољна само на оперативном нивоу, већ се **од ИКТ улагања очекује и побољшање пословних процеса**.

De facto међународни оквир најбоље праксе за управљање ИТ услугама је ИТИЛ.

ITIL (*Information Technology Infrastructure Library*)

ITIL пружа оквир за управљање ИТ услугама и фокусира се на континуирано мерење и побољшање квалитета испоручених ИТ услуга с перспективе клијента и пружаоца ИТ услуге.

- Следеће четири карактеристике ИТИЛ-а су заслужне за глобалну препознатљивост тог стандарда

1. Власништво
2. Примењивост
3. Најбоља пракса
4. Добра пракса

Најбоља пракса

- ИТИЛ се састоји од најбољих пракси прикупљених од најуспешнијих и организација које пружају услуге са највећим учинком

Добра пракса

ИТИЛ садржи скуп најбољих и добрих пракси.

Најбоље праксе сазревају с временом и постају добре праксе, те постепено с временом постају замењене новим принципима

Дефиниција најбоље праксе

Најбоља пракса је низ смерница утемељених на искуствима најквалификованијих и стручних професионалаца из појединих подручја.

Најбоља пракса се базира на:

- Искуству и знању више под једне особе
- Искуству више од једне организације
- Искуству више од једне технологије
- Искуству више од једног догађаја

Различите стратегије пословања и стратегије ИС

Стратегија пословања	**Стратегија ИС**	**Метрике ИС**
Профит	Јефтина технологија	Укупни трошкови пословања и ИС
Купац	Канали приступа купцу	Анкете о задовољству купца
Глобално пословање	Робусна мрежа	Просечно време одзива
Висок квалитет	Висок квалитет ИС	Број инцидената
Брзина пословања	Флексибилан систем	Просечно време за имплементацију промена

Управљање ИТ ризицима и контрола и ревизија ИС-а

1. План управљања ИТ ризицима
2. Како одредити приоритетне ИТ ризике и ИТ контроле
3. Шта је ревизија ИС-а и чему служи?

Strategic Risks (Стратегијски ризици)

- Ризик је дефинисан као неизвесност исхода.
- Може бити негативна претња или позитивна прилика.
- Важно је идентификовати и управљати ризиком.

4 типа ризика :

- **Уговорни ризици** (Contract risks) - повезани са непрецизно уговореним споразумима

- **Ризици дизајна** (Design risks) – произилазе из грешака при конвертовању захтева у атрибуте сервиса

- **Функционални ризици** (Operation risks) – произилазе из техничких или административних промашаја у подршци сервиса у живом окружењу

- **Ризици тржишта** (Market risks) – повезани са брзомењајућим и све комплекснијим пословним окружењем.

Управљање континуитетом ИТ услуга (IT Service Continuity Management

- Процес **управљања континуитетом ИТ услуга је део** целокупног процеса **управљања континуитетом пословања** (Business Continuity Management -BCM).
- Примарни **циљ** процеса управљање континуитетом ИТ услуга је **подржати континуитет пословања** – у случају непогоде у оптималном времену вратити ИТ инфраструктуру и ИТ услуге у нормално стање.
- **Непогодама се сматрају догађаји који доводе до прекида пословања** и захтевају велике напоре за повратак пословања у нормално стање. Примери непогода су: пожар, поплава, земљотрес, крађа, рачунарски криминал, итд.

- Процес управљања континуитетом пословања **укључује процене ризика** за пословање.

- Фокус му је на **развоју планова за опоравак пословања** (како би се потенцијални ризик смањио на најмању могућу меру или пак потпуно елиминисао).

- Управљање континуитетом ИТ услуга настоји :
  - **вратити ИТ услуге у нормално стање**,
  - **препознати ризике** и
  - **елиминисати ризике** који прете ИТ систему.

Главне активности управљања континуитетом ИТ услуга су:

- **Процена последица прекида** ИТ услуга за пословања
- **Идентификација услуга битних за пословање** а за које се траже додатне превентивне мере
- **Развој, тестирање и одржавање планова за повратак услуга у нормално стање** након непогоде
- **Дефинисање периода у којем се може остварити опоравак** ИТ сервиса
- **Примена мера за спречавање и смањивање непогода**

- Управљање континуитетом реализује се у четири фазе:

- **Увођење** – дефинисање опсега и услова, планирање

- **Захтеви и стратегија** – анализа утицаја на пословање, процена ризика

- **Извођење** – извршавање мера за смањење ризика, тестирање планова

- **Стална активност** – едукација и подизање свести о управљању континуитетом, стално тестирање

IT Service Continuity Management - Сврха

- Дефинисати приоритете у опоравку ИТ сервиса.
- Дефинисати План непрекидности ИТ услуге (IT Service Continuity Plan.
- Требало би извршити и процену ризика (Risk Assessment) како би се утврдиле вероватноће и очекивани утицаји значајнијих инцидената на ИТ инфраструктуру.

ITSCM – Опције опоравка(Recovery options)

Disaster recovery plan: смештање података/апликације на удаљеној локацији, стратегија прављења сигурносних копија (инкрементални/потпуни бекап итд), тестирање опоравка

- **Тренутни опоравак** (hot – split site – mirroring)
  Тренутно!
- **Брзи опоравак** (Hot)
  <24 сата
  Подаци/апликације пресликани са операционалних сервера
- **Средње брз опоравак** (Warm)
  24-72 сата
  Функционална опрема
  Губитак података/апликација, коришћење сигурносних копија за опоравак
- **Постепени**(Cold)
  >72 сата
  Губитак опреме

Управљање информационом сигурношћу(Information Security Management)

Треба осигурати да су информације сигурне и да се ефикасно управља на следећи начин:

- Информације су расположиве и искористиве кад је то потребно (**расположивост**)
- Информације су доступне онима који на то имају право (**поверљивост**)
- Информација је комплетна, тачна и заштићена од неауторизованих промена (**неповредивост**)
- Размени информација и пословним трансакцијама се може веровати (**непорецивост**)

- Сигурносне мере које се користе могу се класификовати у следеће скупине:

- Превенција
- Детекција
- Корекција
- Евалуација

Information Security Management - Сврха

- Одговорност за успостављање, одржавање и примену **политике сигурности информација** (Information Security Policy – ISP).
- **Заштита података од грешака** повезаних са мањком расположивости, интегритета или сигурности.
- **Осигурање поверљиве размене информација** са другим странама.

Сигурност информација

- Многобројни су и разноврсни видови угрожености информационих ресурса организације.
- Извори угрожености се могу разврстати у унутрашње и спољашње
- Унутрашњи могу бити случајни и злонамерни
- Спољашњи могу да потичу од конкуренције и других уљеза у систем.

Сигурност информација

- Први корак у изградњи одговарајућег сигурносног система је **идентификација опасности** које му прете.
- Појмом уљез (intruder) или нападач (attacker) дефинишемо **особу или програм који настоје добити неовлашћен приступ подацима** или ресурсима рачунарског система.
- Постоји много начина угрожавања система, али уопштено говорећи, они се могу сврстати у две скупине – активни напади и пасивни напади.
  - **Активни напади**: вируси, црви итд.
  - За разлику од активних напада, пасивни не чине видљиву штету систему којег нападају, па их је веома тешко детектовати. Њихов основни задатак је **украсти информације из система**, не мешајући се при томе у његов рад.

Сигурност информација

- Неки од аспеката сигурности информација:
  - ***аутентификација корисника*** *(user authentication)* – дозволивши му физички приступ средству, ***систем мора проверити идентитет*** корисника пре него га он почне користити.
  - ***контрола приступа*** (*access control*) – рачунарски систем садржи многе ресурсе и типове информација. Очито је да они нису намењени свим корисницима. Стога, када корисник прође фазу аутентификације ***потребно је, некако му забранити приступ ресурсима и информацијама који му нису намењени***.
  - ***комуникациона сигурност*** (*communication security*) – комуникациони канали који се користе за повезивање рачунара су изложени нападачима који посматрањем, изменом или прекидом промета покушавају продрети у систем. ***Комуникациона сигурност штити од неовлашћеног мењања информација док се оне налазе унутар комуникационог пута.***

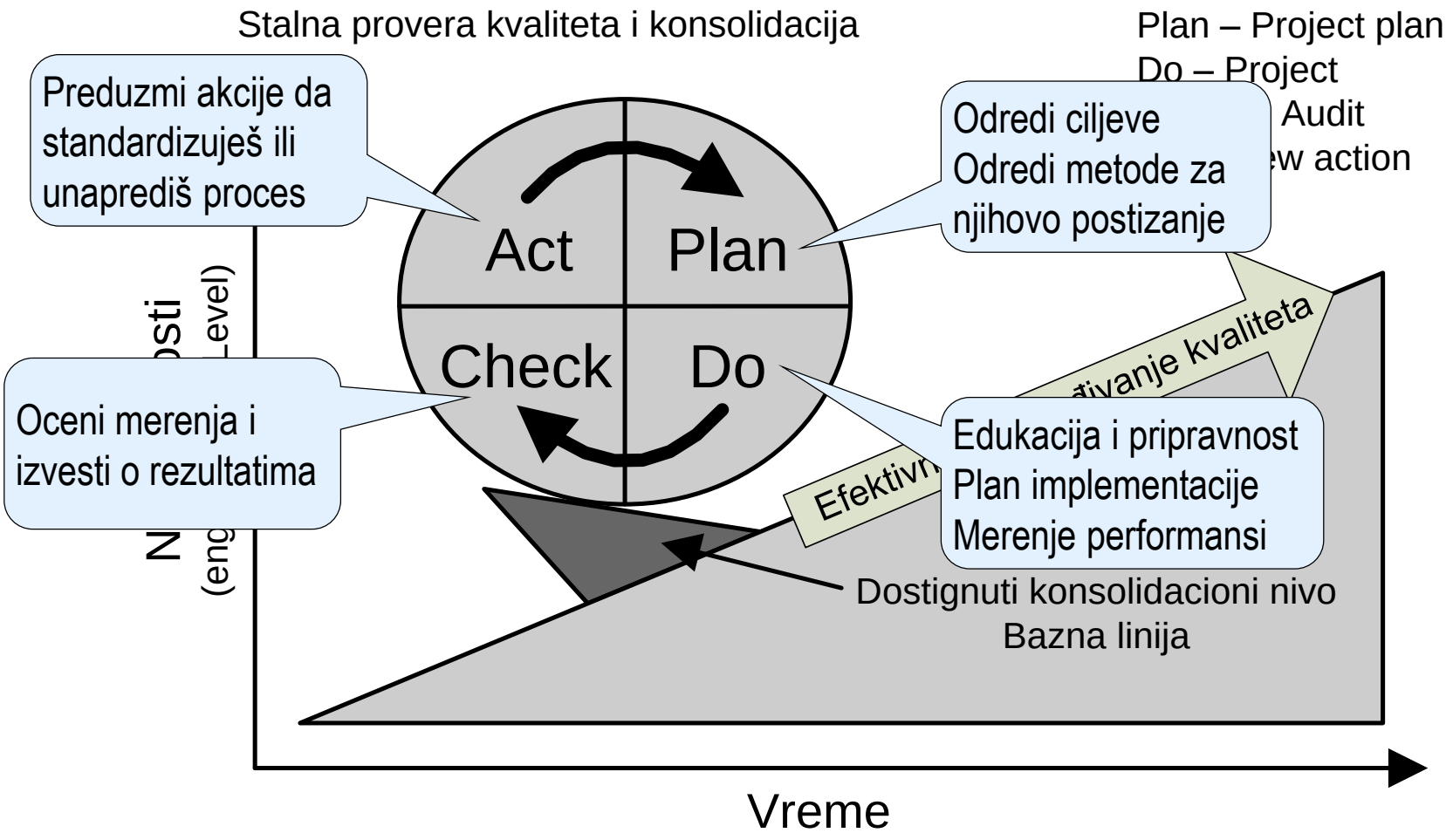
Сигурност информација

- Општи циљеви у остварењу сигурности система су:
  - **поверљивост** (*privacy, confidentiality*) – садржај података, постојање одређених података, садржај комуникације и идентитет корисника у комуникацији ***морају остати тајни.***
  - **веродостојност** (*authenticity*) ***– корисници у комуникацији морају доказати свој идентитет.***
  - **целовитост** (*integrity*) – информација унутар система, као и поруке које се измењују морају се ***штитити од неовлашћених промена.***
  - **признавање** (*nonrepudiation*) – ***нити једна страна не може оспорити да је учествовала у размени порука.***
  - **тајност** (сецрецу) – ***информација унутар система мора бити доступна само овлашћеном кориснику.***

Incident Management
Циљ и делокруг

- Примарни циљ је поновно успостављање нормалног функционисања сервиса :
  - што је брже могуће и
  - минимизирање негативног утицаја на функционисање посла.

Демингов круг



Пракса

Искуства Сектора за ИТ у коришћењу серверске инфраструктуре указују на следеће:

- Сервере треба приликом набавке узимати са **предимензионираним карактеристикама** јер се врло брзо серверски ресурси троше.
- Важне ресурсе сервера (напајање, дискови, мрежна картица) узимати у **редунданси.**
- За све инсталације на серверима користити **легалне софтвере**.
- Пратити нове технологије у овој области (**виртуелизација сервера** итд).
- На серверима **подизати само неопходне серверске сервисе**.
- **Серверску инфраструктуру надоградити системским софтверима** који омогућавају лакше праћење рада и активности сервера (имплементирани CISCOWORKS, IBM Tivoli, Dameware, Service desk, Backupexec итд итд)
- Неопходно **стално праћење и анал**иза мрежног и серверског саобраћаја.

- Неопходна припрема свих предуслова за просторије у којој се налазе сервери, мрежна опрема итд:
  - Климатизована просторија,
  - Агрегатско напајање,
  - УПС-еви,
  - Видео надзор,
  - Мерење температуре
  - Електронске браве - евиденција улазака у просторију
  - итд
  - итд.

- Имплементиран је сложен **систем видео надзора** са 248 IP камера, 20 сервера и видео кластером.

- Користе се **системски софтвери за надзор уређаја** у мрежно серверском окружењу

- **Коришћењем смарт UPS-ева** се спречава осциловање напајања и премошћава рад опреме од нестанка напајања до укључења дизел агрегата.

- Сви уграђени УПС-еви аутоматски шаљу мејлом систем администраторима помене у раду.

Практична реализација у имплементацији безб.

• Урађена је **физичко техничка заштита просторија** са комуникационом опремом.

• Сви уређаји су **заштићени од пренапона**.

• **Заштита од пожара** (хлађење просторија, коришћење незапаљивих материјала, коришћењем материјала који приликом горења ослобађају малу количину дима, коришћење детектора и јављача пожара, аутоматско гашење пожара и поштовање свих стандарда из ове области.

•**Заштита од поплава** - уграђене пумпе за аутоматско избацивање воде и обезбеђено аутоматско искључивање напајања у тим случајевима.

Access листама су врло прецизно дефинисана права приступа и мрежи

Имплементиран **антивирус**

Стално се прате безбедносне рупе и врши се **инсталирање закрпа** (patch).

Кориснике стално информишемо о безбедоносним проблемима

Дефинисана **стратегија backup**-а (врши се седмично нормални full backup и свакодневни инкрементални backup).

- **Резервне копије** података складиштимо удаљено.
- Не покреће се ниједан непотребан мрежни сервис.
- Код корисника се подстиче коришћење тешких лозинки
- Периодично процењујемо и проверавамо стање ИКТ инфраструктуре.
- Урађен је пројекат и реализација интерног ПКИ за Владу Војводине.

Спецификација модела

Примењени модел информационе безбедности омогућава:

- управљање системом заштите,
- анализу ризика,
- обуку,
- евалуацију система заштите и
- сертификацију и акредитацију.

Обрађени механизми заштите

Дефинисане вредности и власници

1. Углед покрајинске владе
2. HW
3. SW
4. Запослени
5. Итд

Пример1:углед покрајинске владе

Идентификовано укупно 217 вредности

ПРЕТЊЕ

Дефинисане претње за сваку вредност

- Укупно 1567 претњи
- За сваку претњу дефинисани параметри (осетљивост, значај итд)
- Формулом формирана вредност претње
- Сортиране претње

- Пример1: одавање информација, напад

РИЗИЦИ

- Од 1567 претњи дефинисано 295 ризика
- Максимална вредност за ризик 5000
- Дефинисана вредност за сваки ризик
- Сортирани ризици

- Пример 1: 900 и 1000

МЕХАНИЗМИ

- Дефинисани механизми за заштиту од ризика
- Укупно 30 механизама

- Примери:
  - Рад ФТО
  - Видео надзор
  - бекап

ВЕЗА РИЗИК-МЕХАНИЗАМ

- Сваком од 195 ризика додељен један или више механизама

- Пример 1:
  - Заштита веб сајта
  - Поступање са материјалом
  - итд

Планови

- Дефинисани планови за сваки ризик
- За сваки ризик дефинисано:
  - Ресурс
  - Одговорност
  - Запис

Пример 1:

Одбрана од DOS напада

Правила поступања са материјалом

Процедура рада ФТО

итд

Урађен каталог сервиса

- Дефинисано 58 сервиса
- За сваки сервис одређено:
  - Припадност: пословни, технички ...
  - Категорија: апликативни, инфраструктурни итд
  - Припадност одељењу ИТ сектора
  - Документи
  - итд

Тип сервиса (Пословни, Технички, Професионални)
Статус сервиса
Приоритет сервиса (Висок, Средњи, Низак)
Менаџер сервиса
Бизнис менаџер сервиса
Пословни опис услуге
ИТ опис услуге
Категорија услуге
Информације за крајњег корисника
Радно време сервиса
Распоред редовног одржавања
Подршка
СЛА/ОЛА
Цена услуге
Пословно релевантна документација и ресурси
Сервиси зависни од овог сервиса
Подупирући сервиси
Корисници

Урађене карте процеса

- За свако одељење дефинисани:
  - Процеси
  - Циљеви процеса
  - Улазни подаци
  - Излазни подаци
  - Документа
  - Мерење, мерне величине
  - остало

Неке препоруке за безбедност:

- Вршити сталну процену система како би осигурало спровођење безбедносних мера.
- Редовно копирање података и складиштење резервних копија на посебној локацији.
- Када је реч о личним подацима, држати прикупљање информација на минимуму и не откривати личне податке без претходне сагласности.
- Обезбедити обуке запослених у вези безбедности рачунара.