Microsoft

Security Days 2008

Vrijeme**VIRTUALIZACIJE**je**SADA**

29-30. rujna 2008. Hotel Antunović, Zagreb

Pod pokroviteljstvom Središnjeg državnog ureda za *e*-Hrvatsku

ISO 27001 – izazov implementacije sigurnosnih kontrola

Dalibor Uremović, Andro Galinović
KING ICT d.o.o.

Generalni sponzori

INSIG2 integra2group

Sponzori

ALGEBRA UČILIŠTE

INFIGO information security

it sistemi nove tehnologije

KING ICT INFORMATION & COMMUNICATION TECHNOLOGIES

TRILIX

Partner konferencije

itSMF Hrvatska

Microsoft Security Days 2008

Microsoft Security Days 2008

Sadržaj

- Zašto uvodimo ISMS
- Gdje "*leže*" problemi uvođenja ISMS-a
- Kako rješavamo najčešće probleme
- Rješavanje kontrola Microsoft-ovim tehnologijama

Razlozi za uvođenje ISMS-a

- Osiguranje ključnih poslovnih procesa,
- Certifikacija prema ISO/IEC 27001:2005,
  - Reputacija,
  - Povećanje kreditnog rejtinga,
- Zahtjevi vlasnika (Grupe),
- Zakon o informacijskoj sigurnosti,
- Odluka HNB-a o primjerenom upravljanju informacijskim sustavom,…

Faze uvođenja ISMS-a

- **Planiranje** – PLAN faza
  - Snimke procesa,
  - Određivanje opsega,
  - Popis informacijske imovine,
  - Procjena rizika
  - Način i plan obrade rizika
  - Izrada SOA dokumenta






Faze uvođenja ISMS-a

- **Provedba** – DO faza
  - Izrada obavezne ISMS dokumentacije 
  - Provedba edukacije 
  - Implementacija kontrola i nadzornih mehanizama 

Faze uvođenja ISMS-a

- **Nadzor** – CHECK faza
  - Mjerenje učinkovitosti primijenjenih mjera
  - Revizije sustava
    - Interna revizija
    - Vanjska revizija

Faze uvođenja ISMS-a

- **Unaprjeđenje** – ACT faza
  - Korektivne mjere
  - Preventivne mjere
  - Revizija ciljeva ISMS-a



DO faza najveći problem - zašto

- Do sad se pričalo, analiziralo i planiralo
- Sad je potrebno **MIJENJATI**
  - **IT sustave** - *tehničke kontrole*
  - **Načine rada** - *proceduralne kontrole*
  - **Organizaciju** - *nove odgovornosti*
- Svaka promjena košta (*€, vrijeme, ljudi*)
- Otpor promjenama je dio ljudske prirode

DO faza - najčešće greške

- ISO/IEC 27002 kontrole vrlo općenite
- Ne postoje jasne smjernice za implementaciju kontrola
- Često:
  - se pribjegava stranim praksama,
  - se krene preširoko i preambiciozno,
  - se krene u provedbu bez potrebne podrške,
  - sve izgleda nedostižno.

Najvažnija područja

- Kontrola pristupa
- Upravljanje dokumentacijom
- Upravljanje zapisima
- Upravljanje zakrpama i nadogradnjama
- Upravljanje promjenama
- Upravljanje sigurnosnim incidentima
- Održavanje popisa informacijske imovine
- Alat za procjenu rizika
- Upravljanje kontinuitetom poslovanja

Kontrola pristupa

- Mnoštvo aplikacija, baza, operativnih sustava i veza među njima
- **Pitanje: Kojim sve sustavima djelatnik X ima pristup u ovom trenutku?**
- Odlazak zaposlenika iz tvrtke, promjena radnog mjesta, zamjena aplikacija, privremena dodjela (bolovanja, godišnji odmori), veze među aplikacijama
- Testni sustavi – najbolnija točka
- Nitko periodično ne provjerava korisnička prava
- Odgovornost? Tko određuje prava?

Kontrola pristupa

- Problemi pri implementaciji:
  - Ukoliko se ide na “papirnate” obrasce – puno zapisa, zaborav nakon nekog vremena, overhead za IT djelatnike
  - Popis svih pristupnih točaka (uloge, sustavi, djelatnici, …)
  - Tehničko rješenje – dugotrajno, skupo, obuhvaćen mali dio sustava (zbog potrebe za konektorima) - **IAM**

Kontrola pristupa

- MS podrška:
  - Active Directory
  - **Identity Life Cycle Manager**
- Dokumenti:
  - Procedura za upravljanje korisničkim pravima pristupa
  - Obrasci dodjele i ukidanje prava
  - Zapisi periodične provjere prava pristupa

Najpravilnije je automatizirati procedure

- Kontrola pristupa
- **Upravljanje dokumentacijom**
- Upravljanje zapisima
- Upravljanje zakrpama i nadogradnjama
- Upravljanje promjenama
- Upravljanje sigurnosnim incidentima
- Održavanje popisa informacijske imovine
- Alat za procjenu rizika
- Upravljanje kontinuitetom poslovanja

Upravljanje dokumentacijom

- Jedna od rijetkih obaveznih stvari (zahtjev norme)
- Sve više dokumentacije, kompleksnost održavanja
- Djelatnici ne znaju da dokumentacija uopće postoji, procedura brzo padne u zaborav
- Distribucija i povlačenje kopija
- Najčešće potrebna dedicirana osoba
- Implementacija “normalnog” rješenja podrazumijeva – **DMS**

Upravljanje dokumentacijom

- MS podrška:
  - **SharePoint Server**
  - Rights Management Services
- Dokumenti:
  - Procedura za upravljanje dokumentima i zapisima
  - Glavni popis dokumenata
  - Predlošci dokumenata i zapisa

Najpravilnije za upravljanje tehničkim područja

- Kontrola pristupa
- Upravljanje dokumentacijom
- Upravljanje zapisima
- Upravljanje zakrpama i nadogradnjama
- Upravljanje promjenama
- Upravljanje sigurnosnim incidentima
- Održavanje popisa informacijske imovine
- Alat za procjenu rizika
- Upravljanje kontinuitetom poslovanja

Upravljanje zapisima

- velik popis aplikacija, operativnih sustava, mrežnih uređaja...
- “home made” aplikacije, zastarjele aplikacije za koje nema podrške
- količina podataka – kako to obraditi odnosno što će vam to? (preventivno i korektivno)
- čuvanje zapisa (zakoni)
- MS podrška: **MS System Center Operations Manager**

Upravljanje zakrpama i nadogradnjama

- nedostatak vremena – “PM je overhead!”
  - istraživanje ranjivosti
  - raspoloživost zakrpa
  - ispitivanje primjenjivosti na sustave
- frekvencija izdavanja zakrpa
- procedura testiranja prije krpanja
- **SC Configuration Manager, SC Essentials, Windows Server Update Services**

Najpravodobnije aktivnosti upravljanja promjenama

- Kontrola pristupa
- Upravljanje dokumentacijom
- Upravljanje zapisima
- Upravljanje zakrpama i nadogradnjama
- **Upravljanje promjenama**
- Upravljanje sigurnosnim incidentima
- Održavanje popisa informacijske imovine
- Alat za procjenu rizika
- Upravljanje kontinuitetom poslovanja

Upravljanje promjenama

- Dobro poznati pojam iz ITIL-a, CobiT-a, SDLC-a, MOF,...
- Mnogo naziva *change management*, *change control, configuration management, release management*
- Temelj svih je umanjenje potencijalnih problema prilikom promjene ili uvođenja novih tehnologija i sustava
- Principi koji vrijede sve od *patch management-a* do zamjene legacy sustava novim sustavom

Upravljanje promjenama

- Uključuje postupke (*pisane i nepisane procedure*), tehnologije (*alate*), zapise (*obrasce, RFC, odluke, trenutna stanja*) i odgovornosti (*change manager, change control analyst,...)*

- ISO kaže da se proces mora tako implementirati da se ne unose nove nekontrolirane ranjivosti u sustave
  - Ovo ne znači implementacija ITIL-a ili CobiT-a

Upravljanje promjenama – KAKO?

- Postupci, zapisi i odgovornosti
  - Identificirati i proanalizirati postojeće neformalne postupke
  - Identificirati poboljšanja (*ugledati se na druge*)
  - Izradi formalne i pismene procedure
  - Definirati workflow koji će osigurati provedbu istih

- SharePoint sa svojom workflow podrškom je idealna tehnologija za implementaciji

  ili budući System Centar Service Manager

Upravljanje promjenama – KAKO?

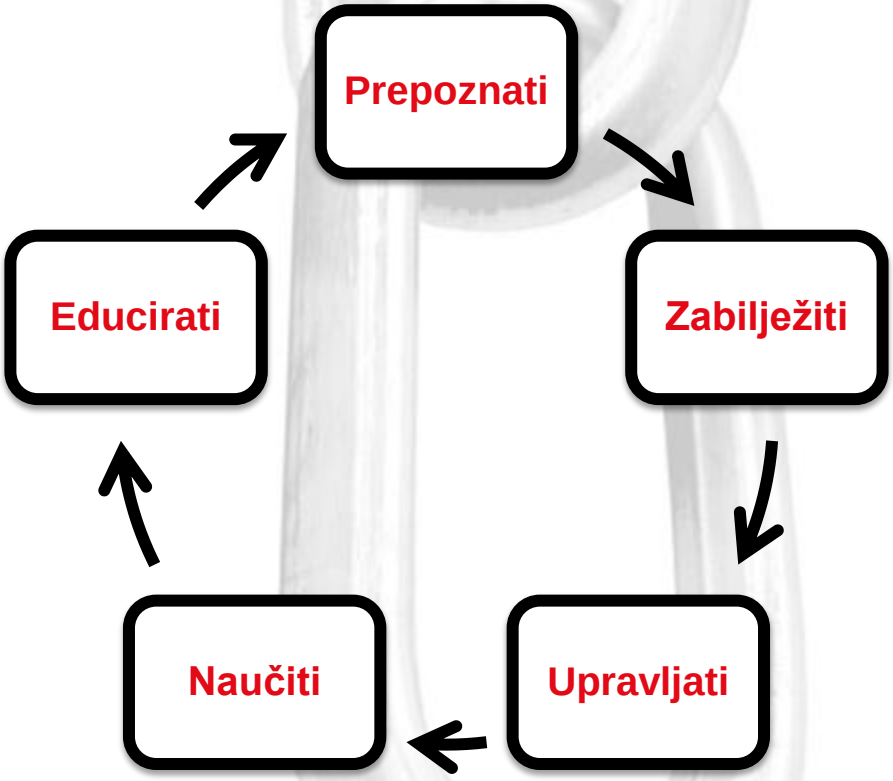
- Tehnologije
  - Za testiranje i Quality Assurance
    - System Center Virtual Machine Manager & Virtual Server
  - Za uniformnu distribuciju, instalaciju i nadogradnju softvera (Software Update Management, Software Distribution, Patch management)
    - System Center Configuration Manager

Upravljanje sigurnosnim incidentima

- Kontrola pristupa
- Upravljanje dokumentacijom
- Upravljanje zapisima
- Upravljanje zakrpama i nadogradnjama
- Upravljanje promjenama
- **Upravljanje sigurnosnim incidentima**
- Održavanje popisa informacijske imovine
- Alat za procjenu rizika
- Upravljanje kontinuitetom poslovanja

Upravljanje sigurnosnim incidentima

- Iznimno bitan dio upravljanja informacijskom sigurnošću



Upravljanje sigurnosnim incidentima

- Radne upute
  - Za zaposlenike, IT administratore, Help desk operatere
- Baza znanja
  - Za ljude i sustave (automatsko prepoznavanje)
  - *Problem management*
- Uniformirani način prijave
  - Prijave i zapisi - *Issue Logs*
- Postupak rješavanje – *workflow*
  - Procedure i odgovornosti

Upravljanje sigurnosnim incidentima

- repozitorij dokumenata
- baza znanja
- issue logs
- workflow
- taskovi

SharePoint (MOSS)

- Automatsko prepoznavanje kroz incidenta System Center Operations Manager
- Do 2010 System Centar Service Manager

Najproblematičnija područja

- Kontrola pristupa
- Upravljanje dokumentacijom
- Upravljanje zapisima
- Upravljanje zakrpama i nadogradnjama
- Upravljanje promjenama
- Upravljanje sigurnosnim incidentima
- Održavanje popisa informacijske imovine
- Alat za procjenu rizika
- Upravljanje kontinuitetom poslovanja

Održavanje popisa informacijske imovine

- Održavanje popis informacijske imovine (*engl.* ***asset registar***)
- Ako je organizacija veća alat je obavezan!
- Idealni alat – ***pruža ažurnost***
  - automatska nadopunu hardvera i softvera
  - ručna nadopuna kritičnih informacija i lokacija
  - distribuirani ručni unos
  - praćenje CIA parametra
  - integracija sa alatom za procjenu rizika
    - **Takav ne postoji!!**

Održavanje popisa informacijske imovine

- Ono što nam može pomoći je neka vrsta CMDB-a
  - Ažurni popis HW i SW je ½ posla
- Prestaju kritične informacija i lokacije

- AR se koristi prilikom upravljanja rizikom
  - nije nužno da bude ažuran cijele godine (makar je preporučljivo)

Održavanje popisa informacijske imovine

- System Center Configuration Manager, Operations Manager i Active Directory, mogu pomoći u održavanju jednog dijela popisa imovine
- System Centar Service Manager će donijeti CMDB
- Naravno ostaju karakteristični ISMS atributi: CIA parametri i katalog informacija

Alat za procjenu rizika

- Odabir/implementacija alata za procjenu rizika
  - svaki alat ujedno diktira metodologiju procjene rizika
  - mali broj alata je projektirano za ISO27001
  - većina je preorijentirana za potrebe ISO27001
  - Više-manje svi imaju integrirani popis imovine
  - Mnogi kažu "*ensures ISO 27001 compliance*"

Upravljanje kontinuitetom poslovanja

- Upravljanje kontinuitetom poslovanja (BCM) je iznimno opširno područje koje uvijek nadilazi IT i informacijsku sigurnost
- ISO traži
  - integraciju informacijske sigurnosti u BC procese
  - Analizu posljedica kriznih situacija na IS
  - Razvoj i testiranje planova koji vode računa od IS

Upravljanje kontinuitetom poslovanja

- Ovo NE znači
  - pokretanje novog projekta,
  - povećanje opsega šire od ISMS-a
  - implementaciju kriznog stožera i testiranje preseljenja uredske opreme u nedjelju ujutro,
  - izrada alternativnog datacentra

Upravljanje kontinuitetom poslovanja

- Ovo znači:
  - provedbu analize utjecaja na poslovanje (BIA) i procjenu rizika – najlakše prevesti istovremeno sa ISMS procjenom rizika
  - definiranje opsega, strategije i odgovornosti za BCM u skladu sa prevedenom analizom
  - Izradu, održavanje i testiranje planova oporavka
  - Izradu plana za upravljanje oporavkom (framework-a ili master plana)

Zaključak

- ISO 27001 se temelji na najboljima i provjerenim praksama, ali se također poziva na mnoge druge najbolje praske
- Ne mora svaka kontrola biti novi jednako složeni projekt
- Treba se ići korak po korak, postepena nadogradnja
- Treba pronaći i iskoristiti ono dobro i poznato u organizaciji!

Microsoft Security Days 2008

Microsoft Security Days 2008

HVALA!