



UDRUGA
HRVATSKIH
MENADŽERA
SIGURNOSTI

I. RADIONICA UHMS-a

"Primjena tehničke zaštite u ostvarivanju
ušteda u poslovanju"

Velika dvorana Ministarstva gospodarstva, rada i poduzetništva RH,
Zagreb 27.05.2010.

NOVE TEHNOLOGIJE U PRIMJENI SUSTAVA TEHNIČKE ZAŠTITE

Predavači:

Zoran Bogadi, Hrvatski Telekom d.d.

Mladen Petrinović, Hrvatski Telekom d.d.

KRATKI INFO O PREDAVAČIMA

Zoran Bogadi

- rođen 1972. u Vinkovcima, RH;
- dipl. ing. PT prometa, Fakultet prometnih znanosti, Zagreb;
- od 2000. zaposlen u Hrvatskom Telekomu d.d.;
- 2000. - 2004. - Sektor za *informacijske tehnologije*;
- 2004. - 2010. - *Odjel za korporativnu sigurnost*,
 - 2008. ovlašteni interni revizor informacijskih sustava (RIF Zagreb);
 - 2009. ISO 27001:2005 *internal auditor training* (ZIK, Zagreb);
 - od 01/2010 rukovoditelj *Radne jedinice za poslovnu sigurnost*.

Područje djelovanja poslovne sigurnosti

- izrada/implementacija sigurnosni standarda, politika, pravilnika, procedura;
- nadzor provedbe sigurnosnih standarda/politika/zakonskih obveza unutar Tvrte;
- praćenje sigurnosnih rizika te provedba mjera za njihovo smanjenje/uklanjanje;
- podrška poslovanju, provedbi projekata (ISO 27001, PCI DSS, BCM...);
- ad hoc kontrole te sigurnosne revizije (tjelesno-tehničke zaštita, zaštita podataka);
- interne sigurnosne istrage;
- međunarodna suradnja u okviru DTAG.

KRATKI INFO O PREDAVAČIMA

Mladen Petrinović

- Rođen 1966. u Slavonskom Brodu, RH;
- Prof. obrane i zaštite, Fakultet političkih znanosti, Zagreb;
- od 1990. zaposlen u Hrvatskom Telekomu d.d.;
- 1990- 2003- *Odsjek obrane sigurnosti i zaštite*;
- 2003- 2010 - *Odjel za nekretnine*:
 - Suradnik za zaštitu i sigurnost nekretnina;
 - Voditelj tima za sigurnost nekretnina;
 - Voditelj sigurnosti i zaštite od požara;

Područje djelovanja zaštita i sigurnost zaposlenika i objekata

- Sudjelovanje u izradi/implementaciji sigurnosnih standarda, politika, pravilnika, procedura;
- Upravljanje i organiziranje provedbe sigurnosnih standarda/politika/zakonskih obveza unutar Tvrte.

SIGURNOST I NOVE TEHNOLOGIJE – TROŠAK ILI UŠTEDA?

Neki od načina ostvarivanja ušteda u poslovanju:

- promjena dobavljača usluga/sirovina;
- optimizacija poslovnih procesa;
- *outsourcing* (distribucija, održavanje, poslovi čišćenja, zaštitari ≠ IT sustav) – ušteda/rizik;
- *shared services* (dijeljene usluge);
- primjena novih tehnologija...

Ulaganje u nove sigurnosne tehnologije ostvaruje uštede:

- direktne (područje tjelesno tehničke zaštite kad prema procjeni stariju tehnologiju zamjenjujemo novim učinkovitijim tehnologijama);
- indirektne/prevencija smanjenjem rizika nastanka neželjenih događaja sa štetnim posljedicama - ozljede ili smrt osoba, šteta na imovini tvrtke, gubitak prihoda, narušavanje povjerenja/ugleda tvrtke (npr. gubitkom podataka) i dr.

INFORMACIJSKA SIGURNOST

INFORMACIJSKA SIGURNOST

- definicijski aspekti: oblik interne kontrole, tehnička procedura, poslovni proces
- primarni strateški cilj – ispunjenje 3 poslovna cilja zaštitom informacijske imovine, privatnosti pojedinca, legalne pozicije tvrtke (usuglašenost sa zakonima i ugovorima) te zaštita njenog javnog ugleda.

USPOSTAVA SUSTAVA UPRAVLJANJA INFORMACIJSKOM SIGURNOŠĆU (ISMS - Information Security Management System) – ISO 2700x STANDARDI;

Provedba uporabom PDCA modela (*Plan Do Check Act*).

Upravljanje sigurnošću tvrtke - informacijske tehnologije neizostavna su podrška suvremenom poslovanju, među ostalim učinkovito se koriste za praćenje rizika unutar tvrtke:

- središnje prikupljanje i analiza informacija o sigurnosnim incidentima;
- praćenje sigurnosnih KPI-a (ključni pokazatelji uspješnosti);
- on-line kampanje “buđenja svijesti zaposlenika” - sigurnosne edukacije;
- on-line upitnici kojima periodički procjenujemo stanje sigurnosti;
- *firewall* (vatrozid);
- IDS (Intrusion Detection Systems) sustavi mreže;
- centralno praćenje i brzi odgovor na sigurnosne incidente.

INFORMACIJSKA SIGURNOST

Podaci kao informacijska imovina - rizici i zaštita

- zaštita podataka - CIA (confidentiality/povjerljivost, integrity/cjelovitost, availability/dostupnost) + accountability/odgovornost, auditability/otvorenost prema reviziji, non-repudiation/neporecivost;
- olakšano kopiranje/zlouporaba;
- rizici zlouporabe podataka - odgovornost;
- vlasništvo nad podacima/klasifikacija podataka/zaštita podataka;
- edukacija korisnika - zaštita podataka odgovornost svih zaposlenika;
- zaštita podataka - PKI sustavi za kriptiranje i digitalno potpisivanje mail-a;
- kriptiranje diskova računala (posebno laptopi);
- primjena biometrije;
- backup podataka;
- upravljanje servisom/otpisom/donacijom informacijske imovine (diskovi...);
- ukidanje admin. prava korisnicima/ograničena uporaba računala;
- praćenje mrežnog prometa;
- zaštita od virusa/trojanaca.

INFORMACIJSKA SIGURNOST

Podrška internalim istragama

Kvalitetno implementirane nove tehnologije daju bitan doprinos sprječavanju prijevarnih postupanja te olakšavaju forenziku ukoliko se prijevarno postupanje ipak dogodi.

- aplikacije s kontrolnim mehanizmima;
- međusobna povezanost aplikacija u svrhe kontrole;
- korisnički računi i role unutar aplikacija;
- baze podataka;
- važnost datoteka zapisa;
- centralni log management sustav/sustav datoteka zapisa...



“Potrebno je učiniti, potrebno je znati.”

INFORMACIJSKA SIGURNOST

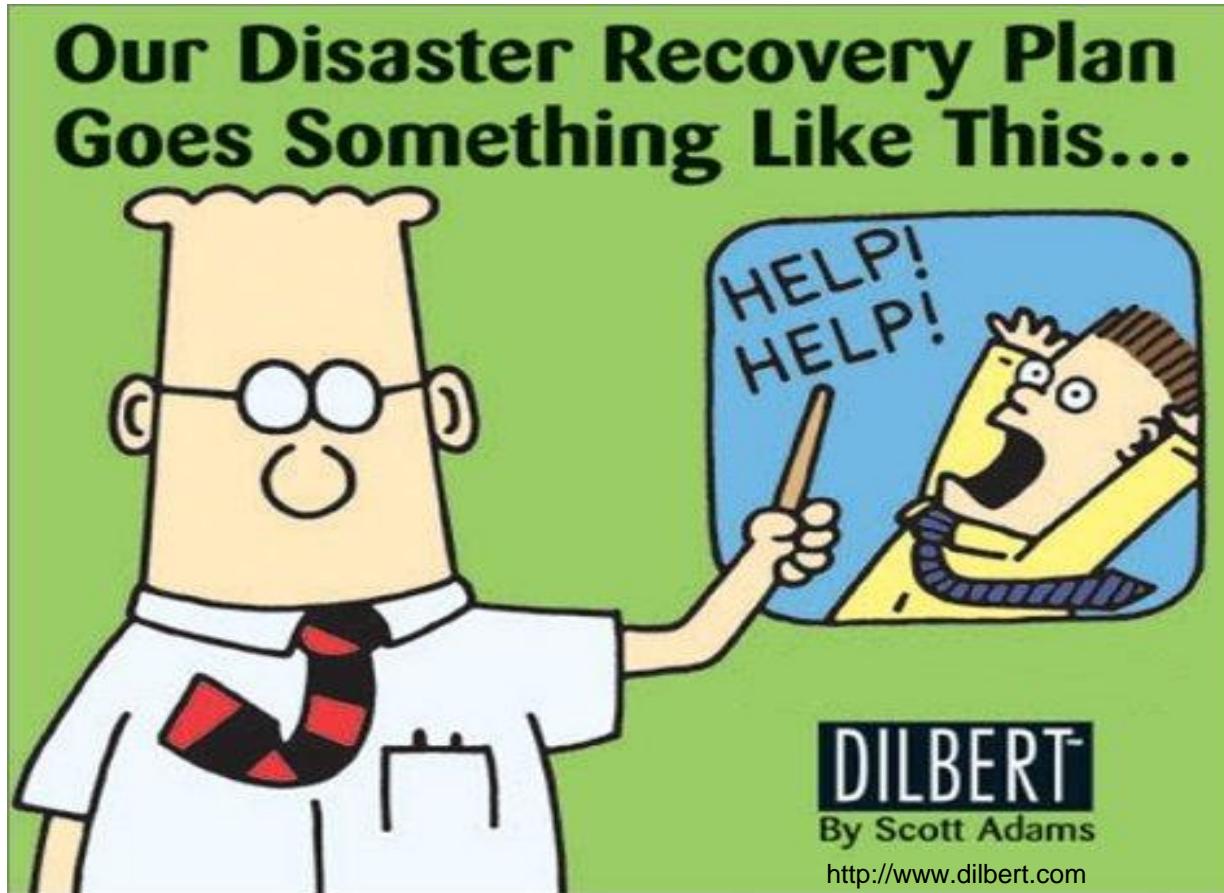
Direktne uštede

- ICT (Information and Communication Technologies);
- standardizacija procesa nabave, tipska računala;
- virtualizacija servera;
- primjena antivirusnih rješenja;
- primjena sustava za automatsku instalaciju sigurnosnih nadogradnji;
- SPAM filtering sustavi;
- web filtering sustavi – pristup Internet sadržajima...

Pravni okvir– ušteda

- osobni/službeni podaci/IT resursi u Tvrcti;
- pokriće za istražnje radnje/uvide u računala/vožnje sl. vozilima, upoznatost zaposlenika, njihova suglasnost; *Ugovori o povjerljivosti s trećim stranama...*

OSIGURANJE KONTINUITETA POSLOVANJA



- svrha - osiguranje dostupnosti ključnih procesa/usluga/proizvoda tvrtke u slučaju "katastrofe";
- primjena BS 25999 standarda za očuvanje kontinuiteta poslovanja;
- BCM (Business Continuity Management), DR (Disaster Recovery) planovi;
- povezanost s kriznim menadžmentom/upravljanje incidentima i krizama.

UPRAVLJANJE VOZNIM PARKOM

FLEET MANAGEMENT (FM) SUSTAV – upravljanje voznim parkom



Telargo On-Board Unit

foto: <http://www.telargo.com>



Telargo Handset

- HT d.d. Pokrenuo je implementaciju TELARGO FM sustava 2007.;
- inicijalno ulaganje za cca. 1500 vozila - povrat investicije u cca. 2 godine;
- koristi:
 - web baziran sustav s mogućnošću povezivanja s drugim sustavima Tvrte - smanjenje papirologije/olakšana kontrola;
 - optimizacija uporabe voznog parka kroz detaljne analize/statistike;
 - smanjena zlouporaba vozila/korištenja u privatne svrhe;
 - olakšana provjera i analiza pri sumnji u zlouporabu;
 - smanjena potrošnja goriva i troškovi održavanja.

UPRAVLJANJE OBJEKTIMA

FACILITY MANAGEMENT SUSTAV – energetska učinkovitost objekata



- HT d.d. primjenjuje automatizirane sustave u pojedinim objektima;
- isplativost pri izgradnji novih objekata (trošak cca. 10% investicije, povrat 3-5 g.);
- centralni nadzor i upravljanje (napajanje, grijanje/hlađenje, osvjetljenje, kontrola pristupa osoba/vozila, protuprovala, video nadzor);
- uz centralni nadzor na lokaciji, moguće i udaljeno upravljanje/nadzor nad objektom/objektima.

I. RADIONICA UHMS-a

"Primjena tehničke zaštite u ostvarivanju ušteda u poslovanju", Zagreb 27.05.2010.

ZAŠTITA PROSTORA

Sigurnost osoba, radnih prostora, imovine i poslovnih interesa, obveza je i jedan od prioriteta
HT

- standardi sigurnosti su definirani 2003.
- pristup radnim prostorima moraju biti kontrolirani, a svaki pristup mora se evidentirati
- prava pristupa na principu "pristup jedino kad je nužno"
- zaposlenici mogu koristiti radne prostore sukladno radnom mjestu i dobivenim ovlaštenjima
- ovlaštenja pristupa trećim osobama moraju biti ograničena na minimum i stalno nadzirana
- ovlaštenja pristupa moraju biti ukinuta istog trenutka kad više ne postoji razlog za njihovo postojanje

ZAŠTITA PROSTORA

SUSTAVI ZA KONTROLU PRISTUPA

RIZICI

- nekontrolirani ulaz vanjskih izvođača / konkurencije
- nekontrolirani ulaz djelatnika
- nedovoljno brzi pristup opremi
- nepravovremena dojava o nasilnom ulasku ili provali

“ON LINE” SUSTAVI

- kartični sustavi, biometrijski sustavi
- sustav sastoji se od individualnih uređaja koji imaju stalnu mogućnost slanja informacija prema i od centralne lokacije u stvarnom vremenu.
- centralizirano prikupljanje i obrada podataka
- centralni i/ili regionalni nadzorni centri
- nedostatak sustava je cijena

ZAŠTITA PROSTORA

“OFF LINE SUSTAVI”

- sigurnosni sustavi zaključavanja (“sistemske brave i ključevi”)
- kombinacija sigurnosnog sustava zaključavanja i elektronike
- cijena je prednost
- ne omogućuju trenutnu informaciju o kretanjima/ulascima, boravku u prostoru

ZAŠTITA PROSTORA

SUSTAVI VIDEO NADZORA

- autonomni sustavi
- integracija sa ostalim sustavima zaštite
- nadzor prostora
- klasična tehnologija
- pixelna tehnologija
- HD tehnologija

PROTUPROVALNI SUSTAVI

- centralni nadzor,
- intervencije
- direktne uštede, tjelesna zaštita

ZAŠTITA PROSTORA

SUSTAVI ZA ZAŠTITU OD POŽARA

- zakonska regulativa
- interna regulativa
- ljudske žrtve
- materijalne štete
- sustavi za dojavu požara, vatrodojava, grafički prikaz
- sustavi za sprječavanje širenja, zaklopke, grafički prikaz

SUSTAVI ZAŠTITE T CENTARA

- video nadzor, (mrežni)
- protuprovala,
- vatrodojava,
- sustav zaštite proizvoda
- protuprepad
- integracija na CDS zaštitarskih tvrtki

SIGURNOSNI PORTFOLIO

Sigurnosni portfolio:

- Upravljanje sigurnošću
- Informacijska sigurnost
- Upravljanje incidentima i krizama
- Upravljanje kontinuitetom poslovanja
- Upravljanje sigurnosnim rizicima
- Usklađenost poslovanja
- Utvrđivanje zlouporaba i istrage
- Sigurnost zaposlenika
- Tehnička sigurnost objekata
- Sigurnost u području ljudskih resursa
- Sigurnost sustava
- Sigurnost komunikacija

NOVE TEHNOLOGIJE – ZAKLJUČAK

Prednosti primjene novih tehnologija u sustavima tehničke zaštite:

- visoka učinkovitost i pouzdanost;
- razvojem tehnologija one svakom novom generacijom postaju učinkovitije;
- mogućnosti prilagodbe zahtjevima korisnika;
- cijene visoko sofisticiranih tehnologija postale su prihvatljive širem tržištu, standardne sigurnosne tehnologije su dostupnije.

Primjena novih tehnologija je potreba, a ne luksuz, jer smanjuje rizik nastanka neželjenih događaja i daje ključan doprinos podršci poslovanja i osiguranju kontinuiteta poslovanja.

**HVALA
NA
PAŽNJI!**