

TVEGANJA V IT

Mag. Janko Uratnik, CISA, CISM

SICOS

Ljubljana, 19. maj 2007

1. UVOD

- Informacije predstavljajo eno najpomembnejših vrednot in imetja organizacije,
- Na informacije preži mnogo tveganj,
- Tveganja so zelo raznolika in kompleksna,
- Tveganja je zato potrebno prepoznavati in obvladovati,
- Ta proces je stalen, saj se okolje stalno spreminja (P-D-C-A)
 - Pa je temu v praksi vedno res tako ?

1. UVOD

Vsebina predstavitve v 48 slikah:

- Nekaj namigov o virih metodologij, pravil in dobrih praks,
- Nekaj besed o teoriji, predvsem bančni, saj je to področje najbolj regulirano,
- Več besed o praktičnih izkušnjah z različnih področij, nekaterih tudi iz bank

2. POTREBNO ZNANJE

Za uspešen spopad s tveganji v IT je dobro poznati naslednje:

Tujo strokovno literaturo s področja

- analize informacijskih tveganj,
- operativnih tveganj,
- upravljanja s tveganji,
- upravljanja z varnostjo informacij,
- upravljanja z neprekinjenim poslovanjem,

2. POTREBNO ZNANJE

- Dogovor BASEL II in zahteve po upravljanju z operativnimi tveganji,
- Standarde s področja varovanja informacij (ISI/IEC 17799:2005, ISO/IEC 27001:2005)
- Priporočila dobre prakse ITIL,
- Metodologijo preverjanja COBIT,

2. POTREBNO ZNANJE

- Metodologijo ocenjevanja in obravnave informacijskih tveganj v bankah (ZBS, 2006),
- Proces ocenjevanja tveganj (BS, 2007),
- Zakon o bančništvu (Ur.l. 131/06) in Sklep o upravljanju s tveganji in izvajanju procesa ocenjevanja ustreznega notranjega kapitala za banke in hranilnice

3. OBSEG IZKUŠENJ

OPOMBA

V nadaljevanju navedeni in opisani primeri so privzeti iz lastne izkušnje avtorja.

V večini primerov, še posebej pri sodnih primerih, dokončni razplet dogodkov ni vedno poznan v podrobnosti.

V primere so vključene delovne organizacije z različnih področij, banke, zavarovalnice, kot tudi posamezniki.

3. OBSEG IZKUŠENJ

Število vseh primerov: 61 100 %

- Število revizij IS: 17 28 %
- Število cenitev opreme: 19 31 %
- Število izvedenskih mnenj: 25 41 %
- Število kaznivih dejanj 5 oz. 8 % vseh primerov

3. OBSEG IZKUŠENJ

Izvedenska mnenja: 25 primerov 100 %

3.1 Pogodbeni odnosi	10	40 %
3.2 Avtorstvo	5	20 %
3.3 Internet	4	16 %
3.4 Zavarovanje podatkov	3	12 %
3.5 Zloraba bankomatov	1	4 %
3.6 Nezakonito pridobivanje podatkov	1	4 %
3.7 Funkcionalnosti strojne opreme	1	4 %

3.1 POGODBENI ODNOSI

Kratek opis primerov:

3.1.1 Funkcionalnosti programske opreme:

Naročnik ni zadovoljen z obsegom in vsebino funkcionalnosti programske opreme, katere razvoj je naročil.

3.1.2 Funkcionalnosti strojne opreme:

Naročnik ne verjame, da je nameščena strojna oprema ob dobavi bila nova in delujoča.

3.1 POGODBENI ODNOSI

3.1.3 Vzdrževanje programske opreme:

Naročnik se z izvajalcem ni dogovoril za vzdrževalno pogodbo, zato je prišlo do opustitve aktivnosti vzdrževanja, kar naj bi povzročilo gospodarsko škodo.

3.1.4 Funkcionalnosti razvojnega projekta programske opreme:

Razvojni projekt se je zaradi visoke formalizacije zavlekel in naročnika zanima kaj od projekta je še uporabno v bodočem razvoju.

3.1 POGODBENI ODNOSI

3.1.5 Kakovost programske opreme:

Kakovost nameščene programske opreme in delovanje sistema po mnenju naročnika nista bila ustrezna in zato zahteva odpravo pomanjkljivosti ozoroma odškodnino.

3.1.6 Funkcionalnosti programske opreme:

Dopolnitve standardnega ERP paketa ne izpolnjujejo naročnikovih pričakovanj po vsebini in po rokih izdelave.

3.1 POGODBENI ODNOSI

3.1.7 Funkcionalnosti programske opreme:

Razvoj novega programskega paketa po mnenju naročnika ni ustrezen tako glede funkcionalnosti kot glede izvedbenih rokov.

3.1.8 Funkcionalnosti programskega paketa:

Funkcionalnosti in delovanje programske opreme v povezavi z ERP ni ustrezno.

3.1 POGODBENI ODNOSI

3.1.9 Plačilo opravljenega dela:

Notranji izvajalec je po osmih letih dela zahteval plačilo za opravljeno delo.

3.1.10 Izpolnitev obveznosti plačila in vračilo medija:

Kupec programske opreme je odstopil od pogodbe, prodajalec zahteva celotno kupnino

3.1 POGODBENI ODNOSI

SKLEP:

- Neformalizirani ali premalo formalizirani postopki,
- Slabo definirane pogodbe,
- Slabo vodeni razvojni projekti,
- Nedefinirane odgovornosti udeležencev pogodbe,
- Navzkrižje interesov predstavnikov pogodbenih strank,
- Mešanje osebnih interesov, koristi in poslov.

3.1 POGODBENI ODNOSI

Kaj bi morali storiti udeleženci primerov:

- Preverili formalnost odnosov,
- Preverili natančnost pogodbe glede vsebine in odgovornosti,
- Spremljali potek razvoja projekta,
- Preverjali zapisnike sestankov in prevzemne zapisnike,
- Opozorili na neskladja v izvajanju projekta

3.1 POGODBENI ODNOSI

ISI/IEC 27001:

- A.6.2.1 prepoznavanje tveganj povezanih z zunanjimi strankami
- A.10.1.3 ločevanje nalog
- A.12.5.5 zunanji razvoj programske opreme

COBIT:

- PO 4 define IT processes, organisation and relationship
- PO 10 manage projects
- DS 2 manage third party services

3.2 AVTORSTVO

3.2.1 Nedefinirane avtorske pravice programskega paketa:

Skupina avtorjev je skupaj začela razvoj programskega paketa, nato so se razšli in vsak po svoje nadaljevali razvoj.

3.2.2 Nedefinirane avtorske pravice programskega paketa:

Skupina avtorjev je skupaj začela razvoj programskega paketa, nato so se razšli in vsak po svoje nadaljevali razvoj.

3.2 AVTORSTVO

3.2.3 Nelegalno kopiranje in razširjanje avtorskega dela:

Kopiranje CD in razširjanje iger za Play Station po pošti s povzetjem (KZ).

3.2.4 Nedefinirane avtorske pravice na podatkovnem modelu:

Po skupnem začetku razvoja sta se pogodbeni strani razšli in izvajalec zahteva avtorstvo za podatkovni model programskega paketa.

3.2 AVTORSTVO

3.2.5 Lastništvo vsebine in spletne strani:

Po skupnem začetku dela na ideji in vsebini internetne strani sta se avtorja razšla in eden je uporabil enako vsebino pod svojim imenom, drugi pa zahteva avtorstvo za vsebino in lastništvo spletne strani.

3.2 AVTORSTVO

SKLEP

- Ob začetku in ob prekinitvi sodelovanja premalo definirane avtorske pravice (pogodba),
- Kaznivo dejanje kopiranja in razširjanja avtorskega dela brez pravic,
- Izkoriščanje pogodbenega dela za avtorske zahteve (pogodba),
- Prilaščanje avtorskega dela.

3.2 AVTORSTVO

Kaj bi morali storiti udeleženci primerov:

- Preverili formalizem avtorstva
- Preverili ustreznost pravnih zaščit
- Vključili pravnega strokovnjaka

3.2 AVTORSTVO

ISI/IEC 27001

- A.7.1.2 lastništvo sredstev
- A.15.1.2 zaščita intelektualne zaščite

COBIT

- PO4 define IT processes, organisation and relationship
- PO10 manage projects
- AI2 acquire and maintain application software
- DS2manage third party services
- ME3 ensure regulatory compliance

3.3 INTERNET

3.3.1 Vdor v podatkovno bazo (KZ):

Mladoletnik je vdrl v tujo podatkovno bazo in povzročil DDS,

3.3.2 Razžalitev osebe na klepetalnici:

Žalitev dela in imena osebe preko klepetalnice,

3.3 INTERNET

3.3.3 Razžalitev osebe na klepetalnici:

Žalitev dela in imena osebe preko
klepetalnice,

3.3.4 Širjenje rasnega in etičnega nemira in žalitev na klepetalnici (KZ): dokazovanje storilca na brezžičnem spletu.

3.3 INTERNET

SKLEP

- Uporaba klepetalnic na internetu ni regulirana in je premalo nadzorovana,
- Administrator odloča o vsebini in trajanju sporočil na forumu,
- Podatkovne baze niso nikoli dovolj zaščitene,
- Dokazovanje storilca ni vedno mogoče.

3.3 INTERNET

Kaj bi morali storiti udeleženci primerov:

- Preverjati varnost podatkovne baze in zaščito pred vdori
- Klepetalnice ?

3.3 INTERNET

ISO/IEC 27001

- A.10.4.1 kontrole proti zlonamerni kodi
- A.10.6 upravljanje varovanja omrežja
- A.11.4 nadzor dostopa do omrežja

COBIT

- DS 5 ensure system security
- ME3 ensure regulatory compliance

3.4 ZAVAROVANJE PODATKOV

3.4.1 Zavarovanje podatkov zaradi suma uporabe službenih sredstev v privatne namene:

Delavka projektantskega podjetja je bila osumljena, da je v službenem času izdelovala projekte za osebni račun.

3.4.2 Zavarovanje podatkov zaradi suma razkrivanja poslovnih skrivnosti:

Delavec podjetja je bil osumljen, da je preko interneta razkrival poslovne skrivnosti podjetja.

3.4 ZAVAROVANJE PODATKOV

3.4.3 Zavarovanje podatkov o lastnostih strojne opreme:

Stranki sta bili v sporu glede lastništva strojne opreme, ki je bila shranjena pri prvi stranki, druga stranka pa je hotela dobiti zagotovilo, da prva stranka te opreme v času spora ne bo spreminjala.

3.4 ZAVAROVANJE PODATKOV

SKLEP

- Večino incidentov izvedejo notranji storilci
- Lastniki podatkov so postali pozorni šele na govorice o dogajanju
- Občutljiv postopek zaradi varovanja zasebnosti delavcev

3.4 ZAVAROVANJE PODATKOV

Kaj bi morali storiti udeleženci primerov:

- Preverjanje ustreznosti varnostnih politik,
- Preverjanje ustreznosti notranjih aktov,
- Preverjanje prometa na elektronski pošti ?

3.4 ZAVAROVANJE PODATKOV

ISO/IEC 27001

- A.5.1.1 politika varovanja informacij
- A.15.1 združljivost z zakonskimi zahtevami

COBIT

- DS5 ensure system security
- DS7 educate and train users
- ME2 monitor and evaluate internal control
- ME3 ensure regulatory compliance

3.5 ZLORABA BANKOMATOV

3.5.1 Skimming (KZ):

Storilec je pridobil podatke o magnetnih zapisih na bančnih karticah in ustrezne kode PIN ter lastnike oškodoval za večjo vsoto denarja.

3.5 ZLORABA BANKOMATOV

SKLEP

- Bančne kartice v tehnologiji brez čipa so zelo tvegane
- Uporabniki so premalo pozorni na svoje kartice in na promet na računih

3.5 ZLORABA BANKOMATOV

Kaj bi morali storiti udeleženci primerov:

- Osveščanje uporabnikov za previdno uporabo bančnih kartic,
- Osveščanje uporabnikov za stalno preverjanje stanja na računu
- Preverjanje bankomatov in terminalov POS

3.5 ZLORABA BANKOMATOV

ISO/IEC 27001

- A.5.1 politika varovanja informacij
- A.10.6 upravljanje varovanja omrežja

COBIT

- DS5 ensure system security
- DS7 educate and train the users
- ME2 monitor and evaluate internal control

3.6 NEZAKONITO PRIDOBIVANJE PODATKOV

3.6.1 Pridobitev podatkov telefonskega operaterja in izdelava razpredelnice klicev:

Dokazovanje možnosti izdelave razpredelnice s podatki o klicih v določenem času in s tem dokazovanje nezakonnosti pridobivanja podatkov.

3.6 NEZAKONITO PRIDOBIVANJE PODATKOV

SKLEP

- Nezakonitosti so mogoče tudi tam, kjer jih ne pričakujemo

3.6 NEZAKONITO PRIDOBIVANJE PODATKOV

Kaj bi morali storiti udeleženci primerov:

- Preverjali prisotnost ustreznih procesov in izvajanje postopkov
- Preverjali formalizacijo postopkov

3.6 NEZAKONITO PRIDOBIVANJE PODATKOV

ISI/IEC 27001

- A.5.1 politika varovanja informacij
- A.15.1 združljivost z zakonskimi zahtevami

COBIT

- PO4 define the IT processes, organisation and relationship
- ME2 monitor and evaluate internal control
- ME3 ensure regulatory compliance

3.7 FUNKCIONALNOSTI OPREME

3.7.1 Ugotavljanje lastnosti in delovanja strojne opreme zaradi odškodninskega zahtevka kupca do prodajalca.

3.7 FUNKCIONALNOSTI OPREME

SKLEP

- Včasih se prodajalci ne pustijo motiti
- Potrebni so argumenti

3.7 FUNKCIONALNOSTI OPREME

Kaj bi morali storiti udeleženci primerov:

- Preveril postopek izbire in nakupa
- Preveril postopek prevzema opreme

3.7 FUNKCIONALNOSTI OPREME

ISO/IEC 27001

- A.7.1 odgovornost za sredstva

COBIT

- AI3 acquire and maintain technology infrastructure
- AI6 manage changes
- DS2 manage third party services
- ME2 monitor and evaluate internal control

4. KOMENTAR

- Večina prikazanih primerov se je zgodila v okoljih, ki nimajo revizorja IT ali ne uporabljajo njegovih storitev
- Primeri po vzrokih niso enolični in so med seboj prepleteni in pogojeni

5. SKLEP

- Katere izkušnje nosijo opisani primeri
- Kako bomo te izkušnje uporabili pri naslednjih pregledih IT
- Standardi in metodologije niso čarobna paličica za upravljanje s tveganji, so pa zelo dobra pomoč

HVALA ZA POZORNOST

V / O ?