SECURITY 2011

19. ročník konference o bezpečnost v ICT

Riadenie informačnej bezpečnosti vo wiki

Vladimír Luknár

Orange CorpSec

Agenda CSO

- Chief Security Officer trvale zápasí s
  - definovaním ucelenej stratégie bezpečnosti
  - určovaním priorít (krátko-strednodobých)
  - plným pochopením svojich zodpovedností
  - demonštrovaním prínosu pre business
  - deklarovaním súčasného „stavu bezpečnosti“ a preukazovaním zlepšenia tohto stavu
  - dokumentovaním tých zdrojov „neistoty“ (rizík), ktoré môžu mať dopad podnikanie spoločnosti
  - demonštrovaním zhody („compliance“) s rastúcim počtom legislatívnych, odvetvových, firemných „štandardov“
    - ktoré prapôvodný zmysel existencie komerčnej firmy (podnikanie) komplikujú/predražujú

Governance Risk Compliance (1)

- v nedávnej minulosti to mal management ťažké - komu veriť, že bezpečnosť je taká, aká má byť?
  - vlastnému CSO?
  - nezávislým expertom?
  - dodávateľom bezpečnostných riešení?
  - odborným časopisom, novinárom, konferenciám ☺?
  - štátnym úradom a vládnym iniciatívam?
- dnes je trendom spoločná platforma GRC, kde
  - G = všetky aktivity, ktoré zaručia, že kritické, pre rozhodovanie nevyhnutné, informácie sa k top managementu dostanu včas, úplne a neskreslene
  - R = proces riadenia (identifikácie, minimalizácie atď) rizík, ktoré by mohli mať zásadný dopad na (podnikateľské) ciele spoločnosti
  - C = zhoda s deklarovanými požiadavkami (legislatívou, priemyselným odvetvím, obchodnými dohodami a ICT praxou)
    - SOX, COBIT, ITIL, ale aj ISO/IEC, PCI DSS atď

Governance Risk Compliance (2)

požiadavky na „compliance“ z rôznych oblastí:

- duplicitné, decentralizované, off-line
- typicky riešené inými ľuďmi v rôznych organizačných jednotkách
- overovanie súladu sa vykonáva auditormi s rôznym backgroundom, s rôznymi skúsenosťami a s rôznou podporou top manažmentu
  - a (hlavne) nekoordinovane

Preto je celé riadenie aj plnenie neefektívne

(o 30-50% viac nákladov ako je potrebné)

Kupovať komerčný nástroj?

s ISMS ale hlavne „GRC“ nástrojmi sa v posledných rokoch roztrhlo vrece

- sú tieto komerčné produkty dobré?
  - nie všetky ale mnohé áno
- vyriešia bezpečnosť?
  - (za vás ju) nevyriešia...
    - lebo riadenie bezpečnosti nie je o nástroji, ale o danej organizácii
      - každá je iná, každá je unikátna
- skôr vy sa prispôsobíte nástroju ako nástroj vám
    - komerčný nástroj vás pravdepodobne bude nútiť robiť veci inak, ako by ste ich vo svojej organizácii robili
    - jednotný robustný nástroj má zmysel vo veľkej organizácii, ktorej pobočky majú rovnakú štartovaciu čiaru, rovnakú alebo aspoň podobnú organizačnú hierarchiu a rovnaké podnikateľské prostredie a ciele

Komponenty ISMS

- ISMS / GRC typicky pracuje s kategóriami, atribútmi:
- aktíva – informácie, zariadenia, ľudia, procesy
- riziká - hrozby, zraniteľnosti, opatrenia
  - atribúty (hrozieb, opatrení) ako
    - dôvernosť/integrita/dostupnosť, základné/pokročilé/špecializované, riadiace/procesné/technické
- udalosti - incidenty, nálezy auditov, zistenia z iných aktivít
- prostredie - stakeholders, legislatíva, priemysel, odvetvie
- metrika - benchmarky na meranie účinnosti opatrení
- reporting - dashboards, live reportovanie ne/súladu pre top manažment

Prečo w(iki)ISMS (1)

- “najjednoduchšia online databáza, ktorá by mohla fungovať”
  - Ward Cunningham, autor prvého wiki systému WikiWikiWeb
- informácie a vzťahy medzi nimi dynamicky modeluje používateľ priamo cez web browser
  - pomocou označovania kľúčových slov (tagging), dynamického odkazovania cez wiki syntax
- databázová schéma back-endu je fixná
  - v našom prípade ide o server-side variant wiki využívajúci cross-platformový web server balík (Apache, MySQL, PHP)
  - MySQL databáza sa používa len na uloženie dát
- modulárny javascript kód umožňuje o.i.
  - jednoduchý “data-mining” cez priamo editovateľné skripty
    - používateľ vytvára pseudo-databázové “query” sám
  - full-textové prehľadávanie

Prečo w(iki)ISMS (2)

- open source, nízka náročnosť na IT, používateľská prívetivosť
  - používateľovi stačí bežný browser a lokálna/centrálna autentifikácia
- ľahký export dát z wiki
  - RSS feeds (XML)
  - statické html dokumenty
  - dokonca s možným zachovaním plnej funkcionality pôvodnej aplikácie:
    - samostatný „samo-sa-editujúci“ html
- samotné wISMS nenarába s objemnými dátami
  - ide väčšinou o stavové informácie a metadáta (tags, links, fields, references)
- otvorené kolaboratívne prostredie je najlepší prístup k bezpečnosti
  - „security is everyone's business“ a zároveň je počet bezpečnostných zamestnancov limitovaný
  - vo wISMS viacerí vlastníci sledujú pomerne malý počet opatrení
    - daj bezpečnosti 5 min svojho denného času a uvidíš, aký veľký rozdiel to urobí
- takéto wiki prostredie je perfektným prototypovým nástrojom
  - koncepty, monitorovanie, progres atď. - je možné navrhnúť a odskúšať okamžite a bez nárokov na technické (programátorské) zručnosti

Špecifikácia w(iki)ISMS

- nosnou informačnou jednotkou je opatrenie (control)
  - opatrenia pochádzajú z ISO/IES 27002 a z IRAM/ISF
- štruktúra informácií je v zásade voľná, bez hierarchie
  - nechceme pevnú štruktúru, chceme voľnosť pri definovaní vzťahov medzi informáciami, súvis vzniká podľa potreby
- základným dizajnérskym prvkom je „visačka“ (tag)
  - pomocou tagov sa vytvárajú logické vzťahy medzi informáciami
    - napr. medzi hrozbami a opatreniami, vlastníkmi, doménami, rolami atď
  - aj riadenie prístupu k dátam využíva princíp tagov
- dáta sú nezávislé od aplikácie (skriptov)
  - je možné oddeliť prezentačnú vrstvu od samotných dát
- dáta sú dolované a prezentované v „reálnom čase“
  - umožňujú zostaviť aktuálne stavové ciferníky (dashboards)
  - dynamické reporty sú jedným z hlavných zmyslov wISMS

4 ciele wISMS

- dilema:
  - ako pracovať s - pre firmu špecifickými - vedomosťami využiteľnými bez ohľadu na to, kto je momentálne na pozícii CSO
  - ako často a podrobne dokumentovať čo a ako robíte
- 4 ciele wISMS
  - poskytovať ucelený pohľad na stav bezpečnosti bez vytvárania závislosti na proprietárnych, komerčných produktoch
  - priebežne mapovať úlohy, role a zodpovednosti ľudí a oblasti pokrývané bezpečnosťou
  - riadiť kompletný životný cyklus bezpečnostných opatrení
    - vyhodnocovať účinnosť opatrení (man, proc, tech)
    - plánovať a zabezpečovať nápravu nedostatkov
  - zabezpečiť viditeľnosť stavov a trendov pre top management
    - dashboards o stave
    - priebežné monitorovanie súladu

Čo tvorí wISMS

samostatné ale prepojené "pracoviská":

- high-level risk mapping
- security requirements „live“ document
- system security quality assurance
- control objectives and controls (SCOC)
- guides (on application of controls)
- key performance indicators
- risk assessment and threat modelling
- reports - on incidents and audits

SCOC (1)

Set of **C**ontrol **O**bjectives and **C**ontrols

- základná štruktúra podľa ISO 27002 s referenciami na ISF a COBIT
  - atribúty bezpečnostného cieľa:
    - strength, category, type, security property, threat link, reason, verified, owner
  - atribúty opatrenia:
    - strength, category, type, reason, domain, scope, status, change, metrics, verified, due, owner, auditor
- sledujú sa „bezpečnostné ciele“ (control objectives) prostredníctvom plnenia súvisiach opatrení (controls)
  - napĺňanie cieľov posudzované podľa stavu plnenia opatrení manažérmi („subjektívne“)
  - samotné opatrenia sú sledované ich vlastníkmi podľa stanovenej metriky („objektívne“)
- vyhodnocované v polročných obdobiach
- grafická prezentácia uľahčuje identifikáciu „nezrovnalostí“ vizuálne a okamžite

live demo

Děkujeme za pozornost.

Vladimír Luknár
Orange CorpSec s.r.o.
vladimir.luknar@orange.sk