KOMPLEMENTARNE METODE ZA ZAGOTAVLJANJE VARNOSTI INFORMACIJSKIH SISTEMOV

Denis Trček
Laboratorij za e-medije, Katedra za informatiko
Fakulteta za računalništvo in informatiko
Univerza v Ljubljani
Tržaška cesta 25, 1000 Ljubljana
denis.trcek@fri.uni-lj.si

Borut Likar
Fakulteta za management
Univerza na Primorskem
Cankarjeva 5, 6000 Koper
borut.likar@guest1.arnes.si

Povzetek. Zagotavljanje varnosti je postala ena osrednjih nalog pri obvladovanju informatike oz. upravljanju informacijskih sistemov (IS). Klasični pristopi na tem področju na eni strani izhajajo iz tehničnih osnov, kjer prek varnostnih mehanizmov in z njimi realiziranih varnostnih storitev ščitimo informacijske vire in sredstva, na drugi strani pa izhajajo iz poslovnih osnov, kjer so v ospredju varnostne politike in sistemi za obvladovanje varnosti kot organizacijske strukture in procesi. Ti klasični, v znatni meri standardizirani pristopi pomenijo velik korak, žal pa ima vsaka organizacija svoje specifike, ki jih standardizirani pristopi ne morejo pokriti, ali pa jih ne pokrijejo v zadostni meri, poleg tega pa se operativno stanje spreminja hitreje, kot nastajajo nove standardizirane rešitve. Da bi zagotovili kar največjo stopnjo varnosti tako v prispevku predstavljamo dva komplementarna pristopa. Eden je relativno poznan, to je t.i. penetracijsko testiranje, kjer operativno poskušamo najti možne načine vdora, drugi pa je metoda, imenovana MIS^2 (Management Method for Integrative Information Systems Security). Pri slednji metodi z inovativnimi tehnikami poskušamo identificirati potencialne grožnje ter ranljivosti in na ta način slabosti IS ter zagotoviti višjo stopnjo varnosti ob upoštevanju specifik organizacije in skritega znanja s strani njenih zaposlenih, ki jih na ta način aktivno vključimo v proces informacijske varnosti. Nenazadnje s tem dosežemo večjo prisotnost proaktivnega in ne le pretežno (re)aktivnega načina varovanja IS.

Ključne besede: obvladovanje tveganj, upravljanje informacijske varnosti, varnostna politika, inovativne tehnike, človeški dejavnik.

Uvod – namen in cilji

Varnost informacijskih sistemov je postala ena ključnih dejavnosti pri upravljanju informacijskih sistemov in obvladovanju informatike nasploh. Zadnja leta se je na tem področju vzpostavilo tudi kar nekaj standardov. Eden temeljnih je BS 7799 [BSI 1995], ki je iz svojih začetnih okvirov sredi devetdesetih let botroval standardoma ISO 117799-1/2 [ISO 2000], nato pa družini ISO 27000 [ISO 2005a, 2005b, 2007], ki zelo obsežno pokriva

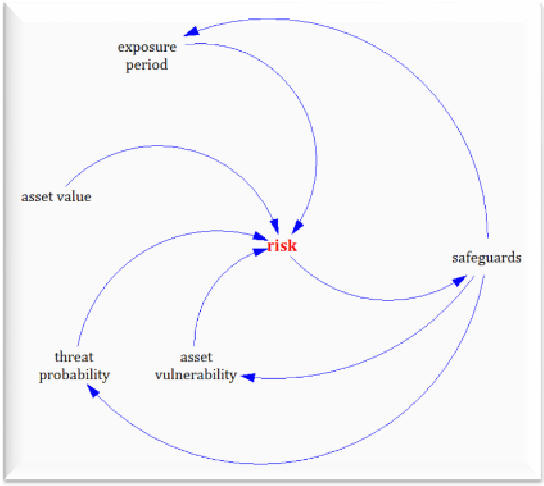
problematiko od sistemov za upravljanje varnosti na eni strani, prek obvladovanje tveganj do operativnih varnostih politik.

Vendar pa ima pokrivanje varnosti IS s standardi inherentne omejitve. Kot prvo, standardi stremijo k generaliziranim rešitvam, ki ne morejo pokriti specifik posamezne organizacije bodisi zaradi njenih specifičnih poslovnih procesov v celoti, bodisi zaradi specifične kulture v celoti – vsekakor pa vsaj v manjših segmentih vsaka organizacija ima svoje specifike in teh s standardi ni moč pokriti. Nadalje, nabor tehnoloških rešitev, ki jih uporablja organizacija in njihova konfiguracija nosijo specifičen pečat. Tudi - in nenazadnje - standardi tipično s časovno zakasnitvijo nekaj let sledijo razvoju v realnem okolju.

Zaradi tega je realna potreba po iskanju komplementarnih načinov za obvladovanje varnosti IS in ta prispevek podaja dve od njih, s katerima imamo tudi vse več izkušenj. Prva je operativno penetracijsko testiranje, drugi pa je metoda, ki izhaja iz širokega angažmaja članov organizacije in metod inovativnega mišljenja za identifikacijo tveganj in ustrezno prilagajanje varnostnih politik (metoda se imenuje Management Method for Integrative Information Systems Security, MIS^2). V naslednjem razdelku je tako najprej podana osnova obvladovanja tveganj, ki ji v tretjem razdelku sledi predstavitev zgoraj omenjenih komplementarnih metod, sestavek pa se konča z zaključki in navedbo literature.

Izhodišča - obvladovanje tveganj

Obvladovanje tveganj bi najširše lahko definirali kot nabor dejavnosti, s pomočjo katerih opredelimo grožnje, ranljivosti sredstev v odnosu do identificiranih groženj, in iz te interakcije izhajajoča tveganja. Na podlagi opredelitve teh tveganj sledi njihovo rangiranje in določanje protiukrepov, s katerimi bodisi zmanjšamo ranljivosti ali tveganja. Shematsko je proces obvladovanja tveganj prikazan na sliki 1.



Slika 1: Procesna predstavitev obvladovanja tveganj (povzeto po [Trček 2006]).

Seznanjanje z omenjenimi principi obvladovanja tveganj je ključno tudi za komplementarne pristope zagotavljanja varnosti, predvsem postopka MIS^2. Omenjeno problematiko podrobno obravnavata standarda [ISO 2008] in [NIST 2007].

Uporabljene metode za komplementarno zagotavljanje varnosti IS

Ta razdelek podaja najprej osnovne principe in načine izvedbe penetracijskih testov, zatem pa predstavi metodo MIS^2.

Penetracijsko testiranje

Penetracijsko testiranje služi kot način odkrivanja operativnih pomanjkljivosti v IS s poskušanjem nadzorovanega vdora v IS tako po tehnično tehnološki plati kot prek človeškega dejavnika (družbeni dejavniki). Vsi tovrstni testi morajo biti skrbno načrtovani in metodološko dorečeni – navajamo osnovna izhodišča [Trček 2006]:

- testi ne smejo načeti operabilne sposobnosti preverjanega IS;
- testi morajo biti taki, da je zagotovljena točnost rezultatov ter da je ob predpostavljeni nespremenjenosti IS možno teste ponoviti z identičnimi rezultati;
- rezultati morajo biti zadostni za izdelavo poročila (priporočil), ki določevalcem omogoča sprejemanjem konkretnih ukrepov.

Penetracijsko testiranje razdelimo v štiri faze. Najprej se opredeli okolje, v katerem bo potekalo testiranje (konkretna strojna oprema, programske rešitve in osebje). Ti podatki nato služijo v drugi fazi za kontrolirane načine vdora, kjer se tipično teži k pridobitvi najvišjih, sistemskih privilegijev. V tretji fazi sledi formiranje dokaznega materiala za dokaz uspešnega vdora (npr. postavitev t.i. zastavic v sistemske mape). Tekom tretje faze poteka intenzivno dokumentiranje za izdelavo končnega poročila, v odvisnosti od dogovora z naročnikom pa je lahko zahtevano, da se vsaka odkrita ranljivost naročniku sproti sporoča. V četrti fazi se izdela podrobno poročilo z eksplicitnimi koraki za eventualno ponovitev vdorov in predstavitev rezultatov naročniku, ki vsebujejo konkretna priporočila za odpravo slabosti.

Metoda MIS2

Namen metoda MIS^2 je predvsem ta, da omogoči proaktivno obvladovanje varnosti in to ob vidnem angažmaju zaposlenih v organizaciji (Likar in Trček, 2012). Na ta način pri obvladovanju tveganj zagotovimo večjo proaktivno komponento (in ne le reaktivno ali aktivno), poleg tega pa poudarek na soudeležbi zaposlenih prispeva k večji zavesti o pomeni varnosti IS v organizaciji. Ne nazadnje prav zaposleni poznajo mnogo specifik informacijskega sistema in kreativen način njihovega vključevanja lahko pomeni pomemben prispevek k zagotavljanju varnosti.

Osrčje pristopa MIS^2 so tehnike kreativnega razmišljanja kot so možganska nevihta, Gordonova tehnika, itd. Izbrana tehnika tudi narekuje potrebno število udeležencev v postopku MIS2 (v primeru Gordonove tehnike je to od 5 do 15 udeležencev). Pri Gordonovi tehniki je prednost npr. tudi ta, da omogoča identifikacijo problemov, medtem ko večina drugih tehnik izhaja iz znanih problemov in išče kreativne rešitve (Pečjak, 1989).

Prvi korak pri MIS^2 je razdelitev sodelujočih zaposlenih v dve skupini, prvo s posamezniki, ki so dobro seznanjeni z delovanjem in podrobnostmi informacijskega sistema in so neposredno

vključeni v njegovo obvladovanje, in drugo, ki imajo le uporabniške izkušnje z IS. Zadnja skupina bo služila generiranju inovacij, prva pa jih bo evalvirala.

Zatem sledi izvajanje seje kreativnega mišljenja, ki jo vodi ekspert za tehnike inovativnega razmišljanja. V prvem koraku specialist za področje informacijske varnosti poda osnove informacijske varnosti, vendar brez podajanja podrobnih detajlov (podajo se osnove obvladovanja tveganj in osnove operativnega varovanja IS v organizaciji). Izogibanje detajlom je namenjeno temu, da se posamezniki iz kreativne skupine ne bi ujeli v ustaljene miselne vzorce specialistov za področje varnosti. Temu sledi seja kreativnega mišljenja, kjer se sistematično najprej obravnava grožnje in ranljivosti ter možne protiukrepe.

Ko je faza kreativnega procesa končana, se rezultati predajo v vrednotenje prvi skupini, ki se sestoji iz kreativnih posameznikov, ki so seznanjeni s podrobnosti upravljanja IS. Ti potem na podlagi svojega znanja in razpoložljivih podatkov ovrednotijo rezultate in sprejmejo tiste, ki ustrezajo kriterijem glede na izbrane kriterijske funkcije: imajo stik z realnostjo, so tehnični izvedljivi in finančno gledano smiselni glede na tveganja. Rezultati te evalvacije gredo potem v realizacijo bodisi kot konkretne implementacije ali pa v nadgradnjo varnostne politike.

Zaključki

Varnost IS postaja centralna točka upravljanja IS in obvladovanja informatike nasploh. Kljub vse večji prisotnosti standardov na tem področju, akreditacijskih postopkov in revizijskih postopkov pa standardizirani pristopi ne morejo vključiti vseh specifik IS posamezne organizacije. Zaradi tega in zaradi zagotavljanja pro-aktivnega pristopa k varovanju IS so potrebni komplementarni postopki in v tem prispevku sta prikazana dva, ki sodita tudi v ekspertno področje Laboratorija za e-medije Fakultete za računalništvo in informatiko Univerze v Ljubljani. Prvi je t.i. penetracijsko testiranje, ki ima že relativno uveljavljen status, drugi pa je tehnika MIS^2, ki je fokusirana na proaktivno varovanje IS ob znatnem angažmaju osebja v organizaciji. Slednja je osnovana na tehnikah kreativnega razmišljanja in z njo imamo že nekaj pozitivnih izkušenj v konkretnih organizacijah (Androjna, 2012). Glede na te izkušnje stremimo k temu, da bi metodo v bodoče implementirali v čimveč okoljih in jo tudi eventelno ustrezno nadgradili.

Viri

Androjna A. (2012), Innovative Approaches to Pro-Active Information Systems Security Provisioning, M.Sc. Thesis, Faculty of management, Koper, 2012.

British Standards Institute (1995), Code of Practice For Information Security Management, BS 7799, London.

International Standards Organization (1989), Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture, ISO 7498-2:1989, Geneva.

International Standards Organization (2000), IT - Code of Practice for Information Security Management. ISO 17799, Geneva.

International Standards Organization (2005a), IT - Security techniques - Information security management systems - Requirements, ISO ISO/IEC 27001, Geneva.

International Standards Organization (2005b), IT - Security techniques - Code of Practice for Information Security Management, ISO/IEC 27002, Geneva.

International Standards Organization (2008), Information Security Risk Management, ISO/IEC 27005, Geneva.

Likar and Trček (2012), Likar B., Trček D., A methodology for provision of sustainable information systems security. Cybernetics and Systems, 43:1, 22-33, Taylor & Francis.

NIST (2007), Managing Risk from Information Systems, NIST SP 800-39 Draft, US Dept. of Commerce, Washington D.C..

Pečjak V. (1989), Ways to ideas: Techniques of creative thinking, DZS, Ljubljana.

Trček D. (2006), Managing Information Systems Security and Privacy, Springer, Heidelberg / New York.