SLOVENSKI INŠTITUT za REVIZIJO

ISACA®
Strokovnjaki upravljanja storitev IT
Slovenia Chapter

19. mednarodna konferenca

O REVIDIRANJU IN KONTROLI

INFORMACIJSKIH SISTEMOV

zbornik referatov

26. in 27. september

2011

Justin Clark[1*]

PRIHAJAJOČI STANDARDI IN ZAGOTAVLJANJE VAROVANJA INFORMACIJ

Emerging Standards in Software Security Assurance

POVZETEK | *Realno je težko oceniti ali je proces razvoja v organizaciji, ne glede na to ali gre za lastni razvoj ali za razvoj z zunanjimi izvajalci, tak da promovira razvoj vranih rešitev, saj ne obstaja veliko standardov ali uveljavljenih praks. V predavanju bo predavatelj izpostavil nujnost več uporabe novih standardov na tem področju OpenSAMM – Zrelostni model zagotavljanja varnosti (Software Assurance Maturity Model), BSI-MM – Izgradnja varnosti po modelu zrelosti (Building Security In Maturity Model) in ASVS – Standard za preverjanje varnosti v rešitvah (Application Security Verification Standard) in kako bi v teh standardih predstavljen okvir lahko uporabili za oceno stanja razvojnih procesov v neki organizaciji, za načrtovanje bodočega stanja. Predavatelj bo govoril o možnih virih najboljše prakse v sedanjem času ter predstavil primere iz svoje prakse pridobljene v velikih finančnih in maloprodajnih organizacijah. sinergijo, kakšne dobre prakse in dopolnitve procesov na eni ali drugi strani. Mogoče bo tudi izpostavitev našega dela koristno za kakšnega revizorja in bo v njem našel kakšno dodatno motivacijo, ki bo lahko potem koristna za njegovo prihodnje revizorsko delo.*

Ključne besede | *Standardi, zrelostni model zagotavljanja varnosti, preverjanje, varnost, informacijski sistem.*

SUMMARY | *A difficulty in evaluating whether an organization's software development process (whether in-house or outsourced) promotes the development of secure software is the lack of standards or accepted practice in this area. In this talk, Justin will discuss the emergence of several new standards in this area – OpenSAMM (Software Assurance Maturity Model), BSI-MM (Building Security In Maturity Model) and ASVS (Application Security Verification Standard), and how these can be used as a framework for evaluating the current state of an organization's development process, planning a future state, and as sources of leading practice in this area. Examples will be drawn from work Justin has performed in this area at large UK financial and retail organizations*

Key Words | *Standards, Software Assurance Maturity Model, information system, evaluations, security.*

1 [*] Gotham Digital Science, UK.

Mag. Boštjan Delak[*], Mladen Terčelj[2]**

RAČUNALNIŠTVO V OBLAKU – VAROVANJE OSEBNIH PODATKOV

Cloud Computing and Personal Data Protection

POVZETEK | *Računalništvo v oblaku (oblak) je nova nastajajoča oblika storitev za zagotavljanje informacijskih sistemov (IS), infrastrukture in virov v okviru informacijske tehnologije (IT). Namesto da se s programsko opremo izvaja in upravlja podatke na namiznih računalnikih ali strežnikih, uporabniki lahko za izvedbo aplikacij in dostopov do svojih podatkov na zahtevo uporabljajo storitve iz oblaka kjerkoli na svetu. Veliko tveganj, ki so pogosto povezana z oblakom, ni novih in jih lahko najdemo v večini podjetjih tudi danes. Prispevek se osredotoča le na eno majhno, vendar zelo pomembno tveganje v zvezi z osebnimi podatki v oblaku – na skladnost z zakonodajo. Glede na teoretični opis možnih izzivov za to področje tveganja, prispevek predstavlja študijo primera in možne izzive skladnosti s slovenskim Zakonom o varstvu osebnih podatkov (ZVOP-1). Predstavljene so ugotovitve študijskega primera ter podani ukrepi, ki jih mora podjetje sprejeti, ko razmišlja o hrambi ali obdelavi osebnih podatkov v oblaku, bodisi svojih zaposlenih ali strank. Upoštevati je potrebno, da je odgovornost podjetja, da podatki zaupne narave, ki so bili predani v obdelavo ali nastali pri vodenju podjetja, ohranjajo svojo integriteto, zagotavljajo njihovo dostopnost in celovitost, se ne izgubijo in ne postanejo nedostopni v oblaku.*

Ključne besede | *Računalništvo v oblaku, osebni podatki, zakon o varstvu osebnih podatkov.*

SUMMARY | *Cloud computing (the Cloud) is positioning itself as a new emerging platform for delivering information system (IS) infrastructure and resources as information technology (IT) services. Rather than running software and managing data on a desktop computer or servers, users are able to execute software applications and access their data on demand from the Cloud anywhere in the world. Many of the risks frequently associated with the Cloud are not new, and can be found in enterprises today. This paper focuses only on one small, but very important risk regarding personal data in the Cloud: compliance with law and regulation. In view of supporting the theoretical description of the issues related to this type of risk, the paper illustrates one case study related to this risk and the Slovene Personal Data Protection Act (PDPA). Findings describe what measures have to be taken when an enterprise is considering moving personal data (either on its employees or clients) to the Cloud. Be aware that it is the enterprise's responsibility to keep its data confidential, maintain their integrity, and assure their availability, to meet its compliance obligations and not to get lost in the Clouds.*

Key Words | *Cloud computing, personal data, Personal Data Protection Act.*

2 [*] Mag. elektrotehnike; CISA, preizkušeni revizor informacijskih sistemov, CIS; samostojni svetovalec, ITAD; Revizija in svetovanje, d.o.o., 4207 Cerklje na Gorenjskem; Bratovševa ploščad 27, 1131 Ljubljana.
[**] Univ. dipl. ing; CISM, preizkušeni revizor informacijskih sistemov; vodilni presojevalec sistema upravljanja varovanja informacij ISO/IEC 27001; pooblaščenec za varovanje informacij, Nova Ljubljanska banka d.d., 1520 Ljubljana; Jakčeva 19, 1000 Ljubljana.

Stanka Šalamun[3*]

BELEŽENJE MARIJE NOVAK

Tracking Mary Smith

POVZETEK | *V preteklem letu je skupina državljanov začela izvajati projekt, ki smo ga poimenovali "SLED". Zanimalo nas je, kdo vse v naši državi ve o nas skoraj več, kot vemo sami: kdo ima zabeleženo, katera zdravila uporabljamo, kje se je gibal naš mobilni telefon, kdo ve, kdaj smo imeli na bančnem računu tako veliko denarja, da bi se nas splačalo okrasti, kje vse so pospravljeni naši biometrični podatki in podobno. Iskali smo digitalne sledi osebnih podatkov (OP), ki jih čisto navadna "Marija Novak" ali "Jože Horvat" preprosto občasno morata zaupati popolnim neznancem - v zameno, da lahko živita času primerno življenje. Tako smo na množico naslovov organizacij poslali obrazec z zahtevo o seznanitvi z lastnimi osebnimi podatki, ki dosledno upošteva zahteve zakona ZVOP-1. Povpraševali smo po tem, katere osebne podatke hranijo in v katerih zbirkah, komu in zakaj so jih posredovali, zakaj jih zbirajo, do kdaj jih bodo hranili, kako jih varujejo in obdelujejo ter ali so jih izvažali – vse jasno opremljeno s sklicevanjem na člene zakona. Ključni nauki projekta, pa tudi njegova zgodba skupaj z zapleti in razpleti projekta, so zanimivi in poučni, zato jih razgrinjam v prispevku.*

Ključne besede | *Zasebnost, osebni podatki.*

SUMMARY | *Last year a group of private citizens started a project that we named »SLED« (»TRACE«)). We wanted to know who in this country knows more about us than ourselves: who has notes on which medications we take, or knows the whereabouts of our mobile phone or the exact time frame when our bank account is 'heavy' and interesting enough to be robbed, or where our biometric data are stored, and similar. We were looking for digital footprints of personal data that a common »Marija Novak (Mary Smith)« or »Jože Horvat (John Smith)« occasionally has to provide to a total stranger – so that they (we), in exchange, can live a normal life. Our request form, fully consistent with the 'Personal Data Protection Act', was sent to more than 75 organisations, asking them to provide some information on our own personal data that they store in their database. We specifically asked them which personal data exactly they are keeping and in which record, for which purpose they are storing the data, we asked them to provide a list of data recipients to whom personal data were supplied and for what purpose, to certify whether our personal data are being processed or not and to provide information on the purpose of processing – all with reference to relevant legal basis. The main (key) lessons of this project as well as the story with the tangling and untangling of the project, both interesting and informative, will be revealed in my conference contribution.*

Key Words | *Privacy, personal data.*

3 [*] Univ. dipl. ing. rač.; CISM; ACROS d.o.o.

Mag. Pavle Golob[4*], Maja Hmelak[**]

POSTOPKI ZA PREVERJANJE OSEBJA

Security Vetting

POVZETEK | *Upravljanje človeških virov je pomemben element okvira za nadzor vodenja IT, predvsem pri zagotavljanju varnosti podatkov in informacij. Upravljavski okvir vodenja storitev IT se je pogosto izkazal za ranljivega tam, kjer nastopajo ljudje, bodisi zaposlenci, zunanji izvajalci ter drugi deležniki v teh procesih. To velja tako za razpoložljivost sistemov in podatkov, kot tudi za njihovo zaupnost in celovitost.*

V prispevku predstavljava primere iz prakse kako upravljati s človeškimi viri, s poudarkom na njihovem preverjanjem pred njihovo vključitvijo v izvajanje procesov upravljanja z IT, spremljanjem njihovih aktivnosti ter zagotavljanjem usposabljanja in ozaveščanja. Predstavljeni primeri iz prakse se bodo nanašali na upravljanje človeških virov s ciljem zagotoviti varovanje osebnih podatkov, občutljivih podatkov in tajnih podatkov, saj se prakse na teh področjih razlikujejo glede na različne zakonske osnove, ki določajo in zahtevajo ustrezne ukrepe na strani organizacij.

Ključne besede | *Varnostno preverjanje, izbor kadrov, varovanje informacijskih virov.*

SUMMARY | *Human resource management is an important element of the corporate IT control framework, especially when safeguarding the data and information. It was proved many times, that the weakest element of the IT service management framework are humans, whether employees, outside contractors and other stakeholders. This applies to both the availability of systems and data, as well as to its confidentiality and integrity of information.*

In this paper we discuss practical examples how to manage human resources, with emphasis on the security vetting during the recruitment, monitoring staff activities and providing training and awareness. The examples presented are related to the human resources management in order to ensure the protection of personal data, sensitive data and classified information, as practices in these areas.

Key Words | *Security screening, recruitment, safeguarding information assets.*

4 * Magister organizacije dela; vršilec dolžnosti, vodja oddelka Corporate Services, Eurojust, Den Haag, Nizozemska.
** Univ. dipl. ekon.; CISA, CIA; preizkušena revizorka informacijskih sistemov, Računsko sodišče RS.

Renato Burazer[5*], Albert W. Kisjes[6]**

CELOVITO, NEPREKINJENO REVIDIRANJE VARNOSTI IN KONTROL V SAP

Integrated Continuous Security and Controls Auditing in SAP

POVZETEK | *Izzivi revidiranja kompleksnih informacijskih sistemov, stroka ter pritiski regulatornih inštitucij kažejo na trend in potrebo po sprotnem, stalnem in celovitem revidiranju informacijskega sistema. Količina transakcij ter vpliv prepozne identifikacije odstopanj na področju upravljanja, tveganj ali skladnosti, narekujejo uporabo sodobnih integriranih pristopov za revidiranje IS. Prispevek obravnava razvoj stroke in tehničnih rešitev na področju celovitega revidiranja ter nove tehnologije za povečanje operativne učinkovitosti in operativne uspešnosti upravljanja, varnosti in nadzora v okoljih SAP. Namen prispevka je:*

predstaviti najnovejše pristope in rešitve za celovito upravljanje GRC (Governance, Risk, Compliance) v SAP okoljih

pomagati pri razumevanju vpeljave kontrol kot je to opisano v ISACA Security, Audit and Controls features SAP ERP 3rd edition

pomagati strokovnjakom pri načrtovanju usmeritev na področju neprekinjenega revidiranja in izvajanju neprekinjenega revidiranja

Podan je vpogled v primer sodobnega orodja za izvajanje neprekinjenega revidiranja v SAP okolju. Prikazani so primeri pristopov, najboljše prakse in priporočila s tega področja.

Ključne besede | *GRC, Governance, Risk, Compliance, upravljanje, upravljanje tveganj, skladnost, SAP, ERP, neprekinjena revizija, neprekinjeno spremljanje kontrol, neprekinjeno kontroliranje, IT, notranja revizija, notranjerevizijski predstojnik, korporativno upravljanje, trend, revizijsko podatkovno skladišče, kazalniki tveganj, kontrolni parametri, transformacija notranje revizije, G42 Continuous Assurance.*

5 * CISA, CISM, CGEIT, CRISC, CISSP; AREM d.o.o.
6 ** RE, RA; Agilos COE4GRC2.

SUMMARY | *Challenges of Auditing complex information systems, profession and the pressure from regulators resulted in trend and the need for ongoing, regular and integrated auditing of information systems. Number of transactions and the influence of late detection in the domains of management, risks or compliance demand the use of modern integrated approach in auditing information systems. Article is focusing on development of the profession and technical solutions in the domain of integrated information system audit. We are commenting new technologies that can enhance operational effectiveness and efficiency management, security and controls in SAP environments. The goal of the article is to:*

present the latest approach and solutions for integrated GRC management (Governance, Risk, Compliance) in SAP environments

provide help with the understanding of the implementation of controls as it is described in ISACA Security, Audit and Controls features SAP ERP 3rd edition

help professionals at planning and execution of continuous audit

Article is providing an insight into an example of modern tool for continuous audit in SAP environment as well as audit approach, best practices and recommendations.

Key Words | *GRC, Governance,Risk, Compliance, Management, Risk Management, SAP, ERP, Continuous Audit - CA, Continius Controls Monitoring – CCM, Controls Monitoring – CM, IT, Internal Audit, Chief Internal Auditor, Corporate Governance, trend, Audit Data Warehouse, Key Risk Indicators, Control Parameters, Internal Audit Transformation, G42 Continuous Assurance.*

Dr. Uroš Godnov[7*]

MASTER DATA SERVICES KOT ORODJE ZA IZBOLJŠANJE KAKOVOSTI TER SLEDLJIVOSTI PODATKOV

Master Data Services as a Data Quality and Auditing Tool

POVZETEK | *Raziskava TDWI iz leta 2006 je pokazala, da imajo organizacije v ZDA letno več kot 600 milijard dolarjev stroškov, ki so posledica nekakovostnih podatkov. Pri procesu zagotavljanja kakovosti podatkov je potrebno upoštevati pravilo 1-10-100, ki pravi, da nas preprečevanje nekakovostnih podatkov stane 1 enoto, popravljanje nekakovostnih podatkov 10 enot, posledice nekakovostnih podatkov pa 100 enot. Namen članka je trojen, in sicer a) prikazati in podrobneje razdelati merila kakovosti podatkov b) podrobneje razdelati posledice nekakovostnih podatkov c) prikazati pomen upravljanja matičnih podatkov pri zagotavljanju kakovostnih podatkov ter uporabniške rešitve Microsoft Master Data Services (MDS) kot ustreznega orodja za izboljšanje kakovosti ter sledljivosti podatkov. Obstajajo različna merila za kakovost podatkov (kvantitativna ter kvalitativna), ki jih bomo v članku ustrezno predstavili in jih povezali v enotno opredelitev kakovosti podatkov. Jedro članka pa bo predstavljal prikaz upravljanja matičnih podatkov kot eno izmed možnosti, da se izboljša kakovost podatkov v organizacijah s poudarkom na predstavitvi Microsoftovega MDS, ki je izšel kot del MS SQL 2008 R2. MDS ponuja nadzor nad podatki predvsem v smislu določanja oz. spreminjanja modelov, entitet ter lastnosti. Hkrati nam MDS omogoča tudi sledljivost sprememb podatkov ter sprožanja različnih dogodkov v primeru spremembe določenega podatka.*

Ključne besede | *Upravljanje matičnih podatkov, Microsoft Master Data Services, kakovost podatkov, uspešnost.*

SUMMARY | *TDWI survey in 2006 showed that organizations in the U.S. have annually, more than 600 billion dollars of costs that result from bad quality data. In the process of data quality assurance is necessary to consider 1-10-100 rule, which states that prevention of bad quality data, costs an unit, correcting bad quality data 10 units and the consequences of bad quality data 100 units. The purpose of this article is threefold, namely: a) to demonstrate and further elaborate the criteria of data quality b) further elaborated the consequences of bad quality data c) show the importance of Master Data Management (MDM) in providing quality data and Microsoft Master Data Services (MDS) as a suitable tool for improving the quality and the traceability of data. There are different criteria for quality of data (quantitative and qualitative) that will be presented in the article and link them into a single definition of data quality. The core of the article will represent the review of MDM, as one of possibilities to improve data quality in organizations with an emphasis on presentation of Microsoft's MDS. Released as part of MS SQL 2008 R2 MDS offers control over information primarily in terms of defining or changing models, entities and properties. At the same time the MDS also allows us to trace changes in the data and triggers various events in the event of changes to certain data.*

Key Words | *Master Data Management, Microsoft Master Data Services, data quality, effectiveness.*

7 * Doktor informacijsko-upravljalskih ved; Inštitut za kakovost podatkov, Koroška cesta 28, 4290 Tržič.

Tadej Kosmačin[8]*

REVIZIJSKI NAČRT ZA MICROSOFT DYNAMICS CRM

Microsoft Dynamics CRM Audit Plan

POVZETEK | *V zadnjih nekaj letih je kar nekaj podjetij uvedlo CRM-rešitev in velik del tega predstavlja Microsoft Dynamics CRM različic 4.0 ali 2011. Po nekem obdobju uporabe rešitve prihaja tudi naš čas, ko bomo morali uvedeno rešitev revidirati. Glede na dejstvi, da gre za rešitev, v kateri se hranijo in obdelujejo podatki, ki so podvrženi različni zakonodaji, in da je rešitev sama po sebi dokaj kompleksna, obravnava prispevek revizijski načrt za uspešno in učinkovito revizijo. Revizijski načrt, ki je osnovan podobno kot že dobro poznani revizijski načrti združenja ISACA, obravnava vse vidike in področja varne, učinkovite in uspešne uvedbe CRM-sistema. Revizijski načrt je na voljo za uporabo pri izvedbah tovrstnih revizij, v prispevku pa je predstavljen z nekaj praktičnimi navodili za izvedbo.*

Ključne besede | *CRM-Customer relationship management, tveganja, upravljanje odnosov s strankami, vsebinska tveganja, infrastrukturna tveganja, revizijski načrt.*

SUMMARY | *In the last few years, several companies have implemented CRM solutions and there are many implementations of Microsoft Dynamics CRM version 4.0 or 2011. After some period of usage there comes a time when we need to audit the implemented solution. Given the facts that this is a solution in which data is stored and processed, is subject to different legislation and a solution in itself is quite complex, the audit plan is essential for effective and efficient audit. The audit plan is based, like a well-known association ISACA audit plans and deals with all aspects and areas of security, effectivness and successful implementation of the CRM system. The audit plan is available for use in carrying out such audits. Following article presents some practical recommendations for implementation.*

Key Words | *CRM, Customer Relationship Management, Risk, Downside Risk, Upside Risk, Audit Plan.*

Milan Gabor[9]*

REVIZIJA NA HEKERSKI NAČIN

Audit – The Hacker Way

POVZETEK | *Na prvi pogled dva pojma, heker in revizor, nimata veliko skupnega. A če pogledamo iz drugega zornega kota, in sicer, da etični hekerji izvajajo revizije sistema, iščejo pomanjkljivosti in tudi velikokrat nepravilne ali pomanjkljive konfiguracije v informacijski infrastrukturi. Seveda to počno z eno samo majhno razliko! Rezultatov namreč ne sporočijo tistim, ki jih pregledujejo. Če imajo srečo nikoli ne zvejo, da so jih revidirali, če pa že zvejo, je v večini primerov prepozno.*

Ključne besede | *Revizija, etično hekanje, varnost, informacijski sistem, vdori, analiza.*

8 * Dipl. inž. elektrotehnike, CISA; svetovalec v službi notranje revizije; Pošta Slovenije d. o. o.
9 * Inštitut za varnost podatkov in informacijskih sistemov, ViRIS, d.o.o.

SUMMARY | *At first sight two words Hacker and Auditor doesn't have too much in common. But if we look from different angle we may find some similarities. Both are conduction auditing of information system, but hackers do little more than that. They try to find vulnerabilities, misconfigurations and other failures that system administrators or developers do. The only difference is that real hackers normally don't report to owners of the systems. If owners are lucky they never find out, that they have been audited by hackers. But if they do get informed, they might be already too late.*

Key Words | *Revision, ethical hacking, security, information system, break in, analysis.*

Mag. Andrej Zimšek[10*]

VIRTUALIZACIJA IN VARNOST

Virtualization and Security

POVZETEK | *Nove tehnologije prinašajo vrsto prednosti na področju optimizacije in zniževanju stroškov ter predvsem na področju preglednosti rešitev. S centralizacijo, ki jo ponuja virtualizacija, je potrebno posvetiti večjo pozornost elementom varovanja in nadzora novih tehnologij. Celotna infrastruktura postane navidezna in s tem za marsikoga tudi nevidna.*

Veliko implementacij virtualnih tehnologij je zaradi nepoznavanja novega okolja, orodij in procesov izdelano pomanjkljivo. Pomanjkljivosti so najbolj vidne na področju varnosti.

Pri uporabi virtualiziranih okolij je potrebno poleg vseh običajnih točk pregleda sistemov pregledati tudi virtualizacijsko infrastrukturo, ki lahko ob površni konfiguraciji dopušča zlorabe sistemov.

V prispevku so predstavljene tehnologije, ki se pojavljajo na področju virtualizacije delovnega okolja, strežnikov, diskovnih polij in omrežij. Podane so tudi osnovne smernice za revizijo virtualnih sistemov.

Ključne besede | *Virtualizacija, varnost, diskovna polja, strežniki, delovne postaje, omrežje, Cobit, PCI DSS.*

SUMMARY | *New technologies bring many advantages in the field of optimization and cost reduction, especially in the areas of transparency of the solutions. With the centralization offered by virtualization, it is necessary to pay greater attention to elements of protection and control of new technologies. The entire infrastructure becomes apparent and thus for many invisible.*

Many implementations of virtual technologies is due to unfamiliarity with the new environment, tools and processes designed and used incorectly. Deficiencies are most visible in the field of security.

When using virtual environments it is necessary to conduct, in addition to all usual audit points, special review of the virtualization infrastructure which likely allows abuse of the systems.

This paper presents the technologies that are emerging in the field of virtualization work environment, servers, disk and networks, with the basic guidelines for the revision of virtual systems.

Key Words | *Virtualization, security, servers, workstation, network, Cobit, PCI DSS.*

10 * Magister tehničnih znanosti; CISA, CGEIT, Brihteja, d. o. o.

Jernej Suhadolc[11*]

UPRAVLJANJE S PRAVICAMI POSAMEZNIKOV

Information Rights Management

POVZETEK | *V dobi WikiLeaks je skrb za zaupne podatke podjetja še posebej popularna. Če bi ameriška vlada uporabljala IRM, WikiLeaksa verjetno ne bi bilo. Vsaj ne v takem obsegu.*

Spoznali bomo orodje, ki Bradelyu sicer ne bi onemogočilo presneti dokumentov na znani DVD z oznako Lady Gaga, jih pa Julian ne bi mogel odpreti, ker ne bi imel ustreznih ključev.

IRM deluje torej tako, da vsak dokument na pomnilno enoto zapiše kodirano, za kodiranje pa uporabi javni del unikatnega ključa, ki mu ga izda IRM strežnik prav za ta dokument. Pred izdajo ključa, IRM strežnik v posebni bazi zabeleži, kdo, kdaj, od kod in kako dolgo lahko dostopa do dokumenta, pa tudi kaj lahko s tem dokumentom počne. Tako je mogoče denimo prepovedati posredovanje dokumenta, tiskanje, kopiranje in podobno...

Ključne besede | *IRM, ERM, E-DRM, Document Rights Management, Rights Management Server, AES, kriptografija, revizijska sled.*

SUMMARY | *In the WikiLeaks era, data protection has become one of the most wanted security technologies. We will see how it evolved from Xerox Parc laboratories into a technology that anyone can use.*

We'll also take a quick look into how the technology works behind a scene, how it encrypts data and how different certificates are generated and handed over.

Key Words | *IRM, ERM, E-DRM, Document Rights Management, Rights Management Server, AES, cryptology, Audit Trail.*

11 * Virtua d.o.o.

Peter Grasselli[12*]

AVTENTIKACIJA UPORABNIKOV V TRINIVOJSKIH REŠITVAH

Authentication in Three Tier Applications

POVZETEK | *Pri pregledovanju novejših aplikacij, ki so večinoma zasnovane trinivojsko, srečujemo različne načine izvedbe prijave in preverjanja pooblastil uporabnikov. V vlogi revizorja moramo oceniti poslovna tveganja, povezana s tehnično zasnovo in izvedbo sistema, namenjenega preverjanju istovetnosti in pooblaščanju uporabnikov pregledovane aplikacije, ter tveganja, povezana s postopki dodeljevanja pravic in nadzora nad njimi. Pri izvedbi prijave aplikacijskega strežnika na bazo se srečujemo z zelo različnimi prijemi, od uporabe avtentikacijskih strežnikov do prijave prek enega uporabnika in uvedbe (implementacije) lastnih algoritmov varovanja njegovega gesla. Glede na izkušnje so s tem delom arhitekture in izvedbe povezana pomembna inherentna tveganja, ki se jih mora revizor zavedati ter jih med pregledom zaznati in ovrednotiti.*

V prispevku je predstavljen postopek identifikacije ranljivosti in groženj, nanašajočih se na način izvedbe prijave med različnimi sloji večnivojskih aplikacij, s pripadajočim katalogom.

Ključne besede | *Avtentikacija, geslo, grožnja, odjemalec, ranljivost, strežnik, trinivojska arhitektura, tveganje.*

SUMMARY | *During audit of newer three tier applications different implementations of user login and user credentials verification could be seen. Auditor should asses bussines risks arising from technical design and implementation of authentication and authorisation subsistem of application under review as well as users' access rights grantig proces risks.*

One could see different implementations how application server autehnticate to database from specialised authentication servers to login through single user and appropriate password obfuscation algorithms. Experience shows that important inherent risks are connected with this part of application architecture. Auditor should be aware of those risks and identify and asses them during an audit engagement.

Mehod for assesment of vulenrabilities and threats originated from implementation of autentication between different application layers with resulting catalog is presented.

Key Words | *Authentication, password, threat, client, vulnerability, server, three tier arhitecture, risk.*

12 * Univ. dipl. inž. mat.; preizkušeni revizor informacijskih sistemov, CISA, CISSP. Zaposlen kot samostojni svetovalec v ITAD, Revizija in svetovanje d.o.o.

Mag. Janko Uratnik[13*]

OBVLADOVANJE REVIZIJSKIH SLEDI – UPRAVLJANJE, PROCESI, STANDARDI

Audit Trail Management

POVZETEK | *Prispevek podaja definicijo revizijske sledi (nastajanje, prenašanje, shranjevanje, analiziranje, odstranjevanje ter zagotavljanje zaupnosti, celovitosti in razpoložljivosti) ter opisuje zahteve zakonodaje, standardov in dobre prakse za vodenje revizijskih sledi. Našteva osnovne vrste revizijskih sledi in priporočila za njihovo uvajanje, pregledovanje, hrambo in varovanje revizijskih sledi.*

Ključne besede | *Revizijska sled, namen vzpostavitve, log - dnevnik, zahteve zakonodaje, pregledovanje, hramba, varovanje.*

SUMMARY | *The definitions of Audit Trails (generation, transmission, operational processes, storage, analysis, disposal, confidentiality, integrity, availability) are presented, actual legislation requirements, standards and good practice expectations for Audit Trail management are given. The basic typs of Audit Trails with implementation considerations, analysis, storage and security requirements are given.*

Key Words | *Audit Trail, implementation purpose and scope, activity logs, legislation requirements, analysis, storage, security.*

13 * Magister elektrotehnike; preizkušeni revizor informacijskih sistemov; CISA, CISM, CGEIT; sodni izvedenec in sodni cenilec za informatiko in računalništvo; Banka Sparkasse d.d., doma: j.uratnik@siol.net.

Matej Lamut Skok[14*]

PREDNOSTI ENOTNEGA OBRAVNAVANJA SISTEMSKIH REVIZIJSKIH SLEDI

Advantage of Systems Audit Trails Uniform Handling

POVZETEK | *Zagotavljanje sledljivosti je ena od temeljnih kontrol za preprečevanje neodgovornega ravnanja uporabnikov IS. Revizijske sledi aplikacij so navadno oblikovane tako, da omogočajo enostaven pregled, drugače pa je z dnevniki, ki jih beleži sistemska programska oprema. Ti dnevniki praviloma nastajajo in se hranijo za vsak strežnik (vsako napravo) posebej. Dobra varnostna praksa narekuje, da je treba sistemske dnevnike redno pregledovati. To je pri velikem številu strežnikov mogoče uspešno izvajati le ob podpori avtomatiziranih orodij, ki so sposobna dogodke s posameznih naprav povezovati v logično celoto. Prvi pogoj za učinkovito avtomatizirano obdelavo je, da se sistemski dnevniki nahajajo na enem mestu in so v standardizirani obliki. Prispevek bo predstavil izkušnje pri vzpostavitvi sistema SIEM v banki in njegovo mesto v procesih obvladovanja informacijske tehnologije.*

Ključne besede | *Beleženje dogodkov, privilegirani uporabniki, revizijska sled, SIEM, skladnost, varovanje informacij, uporabniški primer, zbiranje dnevnikov.*

SUMMARY | *Audit trail is one of the fundamental controls to prevent irresponsible behavior of information systems users. Application audit trails are usually designed in such a way that they are easy to review. This is not true for system logs. As a rule system logs are generated and archived on each server separately. According to best practices systems logs should be regularly reviewed. When we have many servers this can be done only with the help of the automated tools, which are capable of linking the events from separated devices into logical entity. The first prerequisite for efficient automated processing is having log located in one place and in the standardized format. This paper will present the experience with implementation of SIEM system in the bank and its place in the process of managing information technology.*

Key Words | *Event logging, privileged users, audit trail, SIEM, compliance, information security, use case, log collection.*

14 * Univ.dipl.ing.; CISA; preizkušeni revizor informacijskih sistemov; Nova Ljubljanska banka d.d., Ljubljana.

Boris Oblak[15*]

VODENJE REVIZIJSKIH SLEDI BREZ POSEGOV V APLIKACIJE

Audit Trail Management Without Any Changes to Applications

POVZETEK | *Poslovni informacijski sistemi (IS) so vedno bolj kompleksni, v njih podjetja zbirajo vse več podatkov, obenem pa vse večje število zaposlenih potrebuje dostop do teh podatkov. Zakonodaja in dobra poslovna praksa v zadnjem času zahtevata vedno večji nadzor nad delovanjem IS. Vedno pogosteje se postavlja vprašanje: Ali lahko zagotovite, da vaš IS deluje v skladu s pričakovanji?*

Uporabniki storitev javne uprave, komitenti bank in zavarovalnic ter drugih podjetij se vse pogosteje sprašujejo ali so njihovi osebni podatki varni. Ali administrator v banki vidi, kakšna posojila imam najeta? Kdo vse prebira moja elektronska sporočila? Kaj vse so razvojniki spremenili ali videli med zadnjimi popravki produkcijske zbirke podatkov? Ali poslovna programska oprema deluje tako kot pričakujemo? Vsa ta vprašanja terjajo odgovor.

Včasih te odgovore želimo zaradi sebe ali svojih strank, včasih pa moramo z njim postreči revizorjem, ki pričakujejo, da znamo dokazati transparentnost in točnost poslovanja. V zadnjem času je vsaka revizija povezana z revidiranjem informacijskega sistema oziroma revidiranjem računalniškega obravnavanja podatkov.

Ključne besede | *Revizijska sled, podatkovne zbirke, arbiter, ZVOP, osebni podatki, varovanje osebnih podatkov.*

SUMMARY | *Business IS are getting more and more comlex. Companies are collecting more data than ever while increasing the number of people having access to it. Best practice guidelines aswell as legislation demand more control over running IS. Questions such as „Are you able to ensure that your IS works as expected?“ keep on comming.*

Users of the public sector services, bank or ensurance agency customers or any other business want to know if their personal data is kept safe. Can the bank administrator see what loans I took out? Who else is reading my e-mail messages? What have the developers changed or seen during the last maintenance procedure of the production database? Does the business application work as expected? All these questions demand answers.

We sometime want answers to previous questions for ourselves or our customers yet we often need to produce them to auditors. Auditors expect the proof of business transparency and validity of the data. Within the last year most every audit is done with special attention towards the IS and especially the audit of the computer data processing.

Key Words | *Audit trail, database, arbiter, personal data, safeguarding personal data, PDPA.*

15 * Abakus plus d.o.o.

Dr. Borut Jereb[16*]

STANDARDA ZA UPRAVLJANE TVEGANJ: ISO 31000:2009 IN ISO/IEC 31010:2009

Risk Management Standards: ISO 31000:2009 and ISO/IEC 31010:2009

POVZETEK | *ISO 31000:2009 določa načela in splošne smernice za upravljanje s tveganji. Uporablja za vse vrste tveganj, ne glede na njihovo naravo, in predvideva tako pozitivne kakor tudi negativne posledice. Namenjen je organizacijam vseh vrst, ne glede na njihovo specifičnost. Čeprav določa splošne smernice, pri tem ne zahteva enotnosti pri upravljanju tveganj. Pri vzpostavitvi in implementaciji načrtov in okvirjev za upravljanja s tveganji upošteva različnost potreb v organizacijah, posebnosti njihovih ciljev, konteksta, strukture, načina delovanja, procesov, funkcij, projektov, izdelkov, storitev in sredstev ter specifičnosti obstoječih praks.*

Namen standarda je, da se v prihodnje z njim uskladijo procesi upravljanja tveganj v obstoječih standardih, kot sta ISO/IEC 27005 in ISO 28000, in v prihodnjih. Tako zagotavlja skupni pristop in podporo standardom, ki se ukvarjajo s specifičnimi tveganji, in jih pri tem ne skuša nadomestiti.

ISO/IEC 31010:2009 podpira standard ISO 31000 in daje napotke o izbiri in uporabi sistematičnih metod za oceno tveganja, postopek ocenjevanja tveganja in izbiro metode za oceno tveganja.

Ključne besede | *Upravljanje tveganj, ISO/IEC 31000:2008, ISO/IEC 31010:2009, ISO/IEC 27001:2005.*

SUMMARY | *ISO 31000:2009 provides principles and generic guidelines on risk management. It can be used by any public, private or community enterprise, association, group or individual. Therefore, it is not specific to any industry or sector and it can be applied to any type of risk, whatever its nature, whether having positive or negative consequences. Although it provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed. It is intended that ISO 31000:2009 be utilized to harmonize risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace those standards. IEC 31010:2009 is supporting standard for ISO 31000 and provides guidance on selection and application of systematic techniques for risk assessment.*

Key Words | *Risk Management, ISO/IEC 31000:2008, ISO/IEC 31010:2009, ISO/IEC 27001:2005.*

16 *Doktor računalniških znanosti; CISA, CISM, CGEIT.

Primož Simončič[17*]

MODEL COSO IN REGISTER TVEGANJ

COSO Model and Risk Register

POVZETEK | *Registri tveganj postajajo vse pogostejši način evidentiranja tveganj v organizacijah. Model COSO predstavlja okvir za celovito obvladovanje tveganj in ga lahko uporabimo kot orodje pri vzpostavitvi registra tveganj.*

V organizaciji nastajajo različni dogodki. Tveganja so tisti dogodki, ki negativno vplivajo na poslovanje. Model COSO tveganje opredeljuje kot možnost izgube, ki nastane kot posledica dogodka uresničitve tveganja in lahko slabo vpliva na doseganje cilja. V praksi pa se tveganje velikokrat razume kot nekaj, kar je treba izločiti/odstraniti.

Ključne besede | *COSO, Register tveganj, notranje okolje, postavljanje ciljev, identifikacija dogodkov, ocena tveganj, odziv na tveganje, kontrolne aktivnosti, informacije in komuniciranje, nadzorovanje.*

SUMMARY | *Risk registers are becomming a more frequent approach that organisations use to record risks. COSO model represents a framework for a holistic risk management and can be used as a tool for setting up a risk register.*

Key Words | *COSO, Risk register, internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, monitoring.*

17 * specialist za management; univ. diol. ekon.; Državni notranji revizor; notranji revizor, Banka Slovenije.

Mag. Aleš Košir[18*], mag. Andrej Orel[19], Jernej Potočnik**

OCENA TVEGANJ

Risk Assessment

POVZETEK | *Področje obvladovanja tveganj se v zadnji dekadi izjemno intenzivno razvija. Metode ocenjevanja tveganj so razvite. Strokovna literatura priporoča, da se za oceno tveganj pripravi popis virov, zanje ugotovi ranljivosti in za ranljivosti pripravi popis groženj, ki izkoristijo te ranljivosti.*

V praksi se izkaže, da je tako pripravljeni seznam groženj lahko obsežen. Ker vsaka ranljivost zahteva pozornost, je analiza časovno in strokovno zahtevna, saj je treba upoštevati številne podrobnosti z različnih področij.

Avtorji so pri preučevanju tega področja uporabili dognanja, ki prihajajo iz raziskav kompleksnih (ekonomskih) napovedi. Znana je ugotovitev, da so pri napovedovanju prihodnje vrednosti delnic uspešnejši tisti s kognitivnim slogom lisic*, ki vedo malo o veliko stvareh, kot pa* ježi, *ki kopičijo vednost na enem ozkem področju.*

Avtorji tvegajo trditev,da je lahko ocena tveganj časovno veliko bolj učinkovita, a vsebinsko ne slabša, če namesto preiskovanja prostora vseh ranljivosti, ki so povezane z virom, upoštevamo le najpomembnejše. Trditev podkrepimo s primerjavami z drugimi področji človekovega delovanja. Prepričani smo, da so za koristno obvladovanje tveganj bistveni element ukrepi, ki sledijo iz analiz.

Ključne besede | T*veganja, obvladovanje tveganj, orodja za obvladovanje tveganj, metode obvladovanja tveganj, viri, ranljivosti, grožnje, verjetnost tveganja, vpliv tveganja, izpostavljenost, matrika izpostavljenosti.*

SUMMARY | *Risk management has been in the last decade in extremely intense development. Risk assessment methods are already developed. Methodologies recommend that a risk assessment is drawn up on the inventory of assets, leading to analysis of inherent vulnerabilities and threats which can exploit them.*

In practice the comprehensive list of threats turns out to be very long. As each vulnerability requires attention, the analysis is time demanding and technically difficult, considering the high number of various technical details.

Examining the subject, the authors took into account the findings of economic predictions research. The predictions of the future value of shares are better of those experts with cognitive style of foxes, who know little about many things, rather than hedgehogs, who accumulate information in one narrow area.

The authors assert that the risk assessment can be much more time efficient, but not worse in quality if instead of investigating the space of all vulnerabilities associated with the asset, only the most important vulnerabilities are considered. The allegation is substantiated through comparisons with other areas of human activity. Additionally, we believe that for useful risk management the essential element are the actions that follow from the analysis.

Key Words | *Risks, risk management, risk management tools, risk management methods, assets, vulnerabilities, threats, risk probability, risk impact, risk exposure, risk exposure matrix.*

18 [*] magister; univ. dipl. inž. Fizike; SAP.
19 [**] magister elec. zn.; vodja izobraževanja in kakovosti, Marand d.o.o..

Alen Mitrovič[20*]

ZAZNAVANJE VLOGE IN POMENA INFORMATIKE V LETNIH POROČILIH DRUŽB

Perception of the Role and Importance of IT in the Annual Reports of Companies

POVZETEK | *Vloga poslovne informatike v podjetju se je v zadnjih letih bistveno spremenila. Spremembe vloge informatike in spoznanje njenega vpliva na konkurenčnost, produktivnost in dodano vrednost ter na celostno obvladovanje tveganj v družbah, se odraža tudi v potrebi po opredelitvi, katere informacije je potrebno pripraviti različnim deležnikom in kako jih predstaviti tej širši javnosti. Glede na pogoste trditve v praksi in izvedene raziskave, da strateško načrtovanje informatike in njeno upravljanje vpliva na konkurenčnost, dodano vrednost in uspešnost poslovanja, se poraja vprašanje, kako in v kakšni meri so o vlogi in stanju informatike za potrebe strateškega odločanja obveščeni in informirani delničarji in druge interesne skupine. Prispevek povzema, kakšno je trenutno stanje poročanja o informatiki v letnih poslovnih poročilih slovenskih družb.*

Ključne besede | *Poslovna informatika, korporativno upravljanje, poslovno obveščanje, letno poročilo, upravljanje informatike, revizija IT.*

SUMMARY | *The role of business informatics in companies has changed substantially over the recent years. Alongside concern about the operative support for business operations, the proper and - above all - stategically planned use of information technology proved itself a possibility for gaining and retaining competitive edges in business operations. The changes of the role of informatics and the awareness of its influence on competitiveness, productivity and added value as well as on the integral risk management in corporations reflect also in the need to define what information has to be prepared for different stakeholders and how it has to be presented to them.*

Regarding the frequent claims in practice and the performed surveys that strategic planning of informatics and its management influence the competitiveness, added value and successfulness of the operations, the question arises as to how and to what extent shareholders and other interested groups are informed about the role and the status of informatics for strategic decision-making. What is therefore the current status of reporting about informatics in annual reports of the Slovene corporations, intended for the wider circle of stakeholders?

Key Words | *Information technology, business informatics, corporate governance, business intelligence, annual report, IT governace, IT audit.*

20 * univ.dipl.inž. elektrotehnike; CISA; pomočnik direktorja, Banka Slovenije. Članek izraža stališča avtorja in ne pomeni hkrati tudi uradnih stališč organizacije, kjer je zaposlen.

Mag. Borut Žnidar[21*]

VARNOST IN PSIHOLOGIJA

Security and Psychology

POVZETEK | *Na varnost lahko gledamo iz dveh strani. Na eni je to realnost varnosti, ki jo lahko opišemo z matematiko, z verjetnostjo tveganja in učinkovitostjo protiukrepov. Varnost pa je na drugi strani tudi občutek, ko gre za naš psihološki odziv na varnostna tveganja in protiukrepe. Ne glede na statistiko se lahko zelo bojite leteti z letalom ali pa vas tega sploh ni strah. In če primerjamo občutek in realnost varnosti lahko opazimo obe skrajnosti: lahko smo varni, čeprav se ne počutimo tako in lahko se počutimo varne pa v resnici sploh nismo.*

Varnost pa je tudi kompromis. Ker absolutna varnost ne obstaja smo prisiljeni sklepati kompromise. Varnostne odločitve od nas zahtevajo iskanje kompromisov med vloženimi sredstvi, energijo, časom, svobodo na eni strani in ter pridobljeno varnostjo na drugi strani. Iskanje primernega ravnotežja oz. kompromisa predstavlja naše varnostne odločitve. In izkušnje kažejo, da smo pri mnogih varnostnih odločitvah ljudje slabi.

V članku prikažem področje sprejemanja odločitev, posebej na področju varnosti. Pri tem pogledamo tipične napake, ki se pri teh odločitvah pohjavijo in razloge za to. Pomagajo nam nekatere psihološke raziskave in njihovi rezultati. Cilj predavanja ni podajanje receptov, temveč odpiranje novih pogledov in tem, ki lahko s časom pomagajo izboljšati komunikacijo in rezultate dela v informacijski varnosti.

Ključne besede | *Informacijska varnost, analiza tveganja, odločanje, psihologija, teorija obeta.*

SUMMARY | *Security has two aspects. One aspect presents rational expectations regarding security that can be described using mathematical methods, which are risk probability and the effectiveness of countermeasures. On the other hand, security is also a notion, our psychological response to security risks and countermeasures taken. Regardless of statistics, one can either be afraid of flying a plane or not be afraid at all. When comparing notions to the rational expectations regarding security, one can observe two extremes: we can be either safe although we do not feel that way, or we can feel safe while in reality we are not safe at all.*

Security is also a compromise. Since absolute security does not exist we are forced to compromise. Security decisions demand compromises that balance invested funds, energy, time and freedom on one side and achieved security on the other. The pursuit of suitable balance or compromise is in fact our security decision. The experience shows that humans are often weak at making security decisions.

The article addresses the area of decision making with special emphasis on security. I describe common mistakes and causes that lead to them. The presentation is supported by the results of some psychological research. The purpose of the article in not giving advice but rather opening new views which will, in time, help to improve communication and work results in information security.

Key Words | *Information security, risk assessment, decision making, psychology, prospect theory.*

21 * Magister znanosti; univ. dipl. inž. računalništva; CISSP, CISM; vodja oddelka, Astec, Stegne 31, Ljubljana.

Mag. Rado Ključevšek[22*]

POSLOVNI MODEL ZA INFORMACIJSKO VARNOST (BMIS)

The Business Model for Information Security – BMIS

POVZETEK | *Poslovni model za informacijsko varnost predstavlja celovit in poslovno usmerjen način upravljanja informacijske varnosti. Istočasno se umešča tudi kot skupni jezik na dveh sicer med seboj precej odmaknjenih področjih, to sta upravljanje informacijske varnosti in poslovno upravljanje. To pomeni, da se področji lahko med seboj pogovarjata in razumeta. Upravljavcem informacijske varnosti omogoča reševanje zapletenih varnostnih primerov, kjer se v okviru sodelovanja znotraj organizacije išče primerno ravnotežje med zaščito in poslovanjem. Poslovni model informacijske varnosti, ki ga je pripravila ISACA, temelji na sistemskem gledanju na varnost, kjer so posamezne sestavine sistema v dinamičnem ravnotežju z ostalimi sestavinami. Model se lahko uporabi ne glede na obstoječi okvir upravljanja varnosti, kot na primer ISO/IEC 27001, PCI DSS ali COBIT. Prispevek podrobno razloži sestavne dele modela in njegovo delovanje, na koncu pa še uporabo v praksi.*

Ključne besede | *Varnost informacij, informacijska varnost, poslovni model, element modela, dinamična povezava, uporaba modela, BMIS.*

SUMMARY | *Business model for information security represents a comprehensive and business-oriented way of managing information security. It also positions itself as a common language on two otherwise rather distant areas, these are information security and business management. This means that the areas are able to communicate and understand each other. The model enables managers of information security to solve complicated security matters where a suitable balance between security and business is sought by cooperation within the organization. Business model for information security which is promoted by ISACA is based on the systemic view on security, where individual parts of a system are in a dynamic balance with the other parts. The model can be used regardless of the existing framework for security management for example ISO/IEC 27001, PCI DSS or COBIT. This article explains in detail the components of the model and its functioning and at the end how to use it practically*.

Key Words | *Security of information, information security, business model, element of a model, dynamic interconnection, use of a model, BMIS.*

22 * Mag., univ. dipl. ing. rač CISM, CISSP, MBCP, CHFI, MBCI, direktor, K.Sec d.o.o.