SIR IUS 5/19

Revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij

SLOVENSKI INŠTITUT za REVIZIJO

Dr. Boštjan Delak

Revizija neprekinjenega poslovanja

Business Continuity Audit

POVZETEK ● *Napadi z izsiljevalskim programjem od prve polovice 2017 v Sloveniji in svetu nas opozarjajo, kako zelo smo ranljivi na tem področju. Prav tako nas je žled v delu Slovenije leta 2014 opozoril, kako smo ranljivi pri naravnih nesrečah. Zato moramo poskrbeti, da pri kibernetskih napadih in naravnih nesrečah svoje poslovanje ponovno vzpostavimo na vnaprej dogovorjeno sprejemljivo raven za uporabnike in lastnike. Z upravljanjem neprekinjenega poslovanja lahko organizacije zmanjšajo tveganja na tem področju. Preverjanje oziroma analiziranje stanja neprekinjenega poslovanja v organizaciji izvedemo s presojami, revizijami in drugimi analizami. Prispevek predstavlja izvedbo revizije učinkovitosti upravljanja neprekinjenega poslovanja v javni organizaciji, ki ga je izvedlo Računsko sodišče Republike Slovenije.*

Ključne besede ● *neprekinjeno poslovanje, neprekinjeno delovanje, revizija neprekinjenega poslovanja, sistem upravljanja neprekinjenega poslovanja*

SUMMARY ● *Ransomware attacks since the first half of 2017 in Slovenia and the world remind us of our vulnerabilities. Additionally the glazed-frost natural disaster in 2014, that severely damaged our local infrastructure, exposed our vulnerabilities to natural disasters. For these reasons we have to ensure, that both in cases of cyber-attacks as well as in cases of natural disasters, our business can be recovered as soon as possible to the level, agreed with customers and owners. Organizations can mitigate the risk of disruptions with business continuity management. Checking or analyzing the level of business continuity management within the organization can be done either through an audit or as an assessment, as well as trough another type of analysis. The paper is a case study of the audit of business continuity management efficiency within a public organization, performed by the Court of Audit of the Republic of Slovenia.*

Key words ● *business continuity, operation continuity, business contiunuty audit, business continuity management system*

Mag. Maja Hmelak

Trendi v kibernetskem kriminalu 2019

Cybercrime Trends 2019

POVZETEK ● *Ali je izsiljevalske zlonamerne kode res čedalje manj? Ali je kraja procesorske moči res le nedolžna uporaba tujih procesnih virov? Kakšno grožnjo predstavljajo napadi na oskrbovalne verige? Kaj je ugrabitev form in zakaj nas mora skrbeti?*

Svet kibernetskega kriminala se zelo hitro spreminja. Paravojaške hekerske skupine nacionalnih držav zaposlujejo izjemno nadarjene ljudi, ti razvijajo nova, domiselna hekerska orodja, njihove načine pa hitro posvojijo tudi kibernetski kriminalci.

Spletne korporacije, izvajalci storitev informacijske varnosti, proizvajalci komunikacijske opreme, pa tudi različne državne in naddržavne institucije spremljajo in analizirajo raznolike trende na področju kibernetskega kriminala. Prispevek predstavlja sintezo trendov v spletnem kriminalu najpomembnejših ugotovitev za leti 2018 in 2019.

Ključne besede ● *NSA, kibernetsko vohunjenje, kibernetski napad, WannaCry, EternalBlue, Lazarus, izsiljevalsko programje*

SUMMARY ● *Is ransomware really in decline? Is crypto mining just a harmless borrowing of computing resources? How serious are supply chain attacks? What is form-jacking and why should we be concerned?*

Cybercrime is changing rapidly. Paramilitary hacker groups are employing their countries' finest minds and they are inventing ever new hacking tools and techniques. These soon find their way into the world of cybercrime.

Web giants, cybersecurity companies, telecommunication equipment experts and various national and international institutions issue periodical reports on the state of cybersecurity. We have decided to present some of their most interesting findings regarding cybercrime for 2018 and 2019.

Key words ● *NSA, cyber espionage, cyberattack, WannaCry, EternalBlue, Lazarus, ransomware*

Tina Kavčič

Analiza možnosti zavarovanj pred kibernetskimi napadi

Analysis of the possibilities of insurance against cyber attacks

POVZETEK ● *Zavarovalništvo se je v Evropi začelo razvijati v 19. in 20. stoletju, ko so nastala prva gospodarska zavarovanja. Sprva so bila to socialna zavarovanja, nato pa so počasi nastajala še druga. Danes poznamo že številna življenjska zavarovanja, avtomobilska zavarovanja, premoženjska zavarovanja itd. Z razvojem tehničnih naprav, računalnikov in brezžičnega omrežja smo izpostavljeni tudi kibernetskim tveganjem, predvsem kraji in šifriranju podatkov, izsiljevanju ter sabotaži zaposlenih, zato v ZDA in Evropi že ponujajo zavarovalne pakete za primere kibernetskega kriminala. Kljub temu da tudi v Sloveniji že prihaja do takih incidentov in škode, povezane z obnovo izgubljenih podatkov, stroški obveščanja strank ter pravnimi stroški, je zavedanje o prisotnosti kibernetskih tveganj še vedno majhno.*

V prispevku so predstavljeni rezultati ankete, ki smo jo opravili v slovenskem prostoru, kjer smo povprašali zavarovalnice, ali že ponujajo produkte kibernetskega zavarovanja. Namen prispevka je povečati ozaveščenost med zavarovalnicami, njihovimi regulatorji in potencialnimi strankami o produktih kibernetskega zavarovanja.

Ključne besede ● *kibernetsko zavarovanje, spletna varnost, varnostne naložbe, zavarovanja, zavarovanja za kibernetsko tveganje, nevarnost, tveganja*

SUMMARY ● *The insurance industry began to develop in Europe in the 19th and 20th centuries, when the first economic insurance, as we know it today, was created as social insurance, and then other insurances were slowly emerging.*

Today, we already know all kinds of life insurance, car insurance, property insurance, etc. With the development of technical devices, computers and wireless networks, we are now also exposed to cyber risks, especially theft and encryption of data, extortion and sabotage of employees. Consequently, insurance packages for cybercrime cases are already offered in the US and Europe. Despite the fact that such incidents also occur in Slovenia causing damage related to the restoration of lost data, and costs of informing clients and legal costs, awareness of the presence of cyber risks is still low.

The paper presents the results of a survey conducted in Slovenia where insurance companies were asked whether they already offer cyber insurance products. The purpose of the contribution is to raise awareness among insurance companies, their regulators and potential customers of the possibilities of cyber insurance products

Key words ● *cybersecurity, online security, security investment, insurance product, cyber risk insurance, risks*

Jaka Kosmač

Vpliv kazenskega prava na **preprečevanj**e kibernetske kriminalitete

Impact of Criminal Law on the Prevention of Cybercrimes

POVZETEK ● *V zadnjem desetletju uporaba sredstev informacijsko-komunikacijske tehnologije in povezanost omrežij hitro naraščata, digitalne tehnologije pa so temeljito spremenile naše okolje. Temu trendu je sledila tudi kibernetska kriminaliteta, katere obseg se iz leta v leto povečuje tudi zaradi vse številnejše uporabe in odvisnosti od informacijsko-komunikacijske tehnologije. Prispevek bo bralca seznanil o vplivu kazenskega prava na preprečevanje oziroma omejevanje kibernetske kriminalitete. To je posebna vrsta kriminalitete, ki se od klasične razlikuje v številnih pogledih, in sicer: ni ozemeljsko omejena in je pogosto čezmejna, zakonodaja zaostaja za novimi pojavnimi oblikami kibernetske kriminalitete, med storilcem in žrtvijo ni fizičnega stika, pogosto pa pride tudi do popolne anonimnosti vsaj z ene strani. Namen kazenskih sankcij je zatiranje in preprečevanje dejavnosti, ki kršijo ali ogrožajo pravne dobrine, zavarovane s kazensko zakonodajo. Kazenske sankcije imajo dve funkciji: represivno in preventivno. Kazensko pravo želi doseči s preventivno funkcijo cilje generalne in specialne prevencije. Cilj generalne prevencije je preprečevanje kriminalitete z zastraševanjem ljudi pred pretečo kaznijo, s čimer naj bi ljudi odvrnila od storitve kaznivega dejanja. Učinki generalne prevencije pa so lahko različni tudi glede na posamezne skupine kaznivih dejanj. Prispevek bo predstavil, ali in kakšen učinek ima generalna prevencija na področje kibernetske kriminalitete.*

Ključne besede ● *kazensko pravo, kibernetska kriminaliteta, kibernetska varnost, kibernetske grožnje*

SUMMARY ● *Over the past decade, the use of information and communication technology resources and network connectivity have been rapidly increasing, and digital technologies have fundamentally changed our lives and our environment. This trend was followed by cybercrime, the volume of which has been increasing every year due to our increasing use and dependence on information and communication technology. This article will inform the reader about the impact of criminal law on the prevention of cybercrimes. Cybercrime is a particular type of crime, since it differs from traditional crimes in many aspects, namely: it is not territorially limited and is often cross-border, legislation lags behind its new forms, there is no physical contact between the perpetrator and the victim, and it often occurs in complete anonymity for at least one of the parties involved. The purpose of criminal sanctions is to suppress and prevent activities that violate or threaten legal goods protected by criminal law. Criminal sanctions have two functions: repressive and preventive. Criminal law with the preventive function pursues the aims of general and special prevention. The goal of general prevention is to prevent*

crime by intimidating people with criminal sanctions in order to deter them from committing a crime. However, the effects of general prevention may also vary with individual crime groups. The article will present whether and what effect general prevention has on cybercrimes.

Key words ● *criminal law, cybercrime, cybersecurity, cyber threats*

Mag. Anton Ujčič, Damir Savanović

Okvir medsebojnega priznavanja EU-SEC

EU-SEC Multiparty Recognition Framework

POVZETEK ● *Projekt EU-SEC (European Security Certification Framework) je razvil model arhitekture, katere namen je odpraviti stranske učinke, ki jih povzroča uporaba velikega števila certifikacijskih shem na področju storitev v oblaku, ter s tem prispevati koristi za vse deležnike v oblaku. Metoda, ki smo jo razvili za dosego tega cilja v okviru projekta EU-SEC, se imenuje medsebojno priznavanje, realizirana pa je kot natančno opredeljena večplastna arhitektura, imenovana Okvir medsebojnega priznavanja (angl. Multiparty Recognition Framework – MPRF).*

Ključne besede ● *certificiranje, oblačne storitve, projekt EU-SEC, okvir*

SUMMARY ● *The EU-SEC project has developed a model architecture, which aims to tackle the side effects of certification schemes' proliferation as a means to benefit all cloud-based stakeholders. The method we developed to achieve this goal is called multiparty recognition, and it is realized as a well-defined layered architecture called: the multiparty recognition framework (MPRF).*

Key words ● *certification, cloud service, project EU-SEC, framework*

Katarina Sitar Šuštar

Aktualno dogajanje na področju revidiranja in nadzora v Veliki Britaniji in ZDA

Current developments in the area of auditing and regulation in Great Britain and USA

POVZETEK ● *V članku povzemam rezultate treh raziskav, ki so jih izvedli v Veliki Britaniji po izbruhu štirih večjih finančnih škandalov: Kingmanove neodvisne preiskave o delu britanskega regulatorja, CMA-jeve raziskave o trgu revizijskih storitev v Veliki Britaniji ter Brydonove raziskave o kakovosti in učinkovitosti revizij. Ker je tudi regulator ameriškega trga PCAOB najavil določene spremembe pri izvedbi nadzora, povzemam tudi te ter v sklepnem delu članka primerjam (možne) smeri sprememb pri nadzoru, ukrepih na trgu revizijskih storitev, na področju komunikacije z različnimi deležniki ter morebitnih vplivih na širše korporativno upravljanje.*

Ključne besede ● *nadzor, revizijski trg, revizorjevo poročanje, Kingman, CMA, Brydon, FRC, PCAOB*

SUMMARY ● *The article summarizes the results of three reviews that were conducted in Great Britain after four recent financial scandals that have been discovered: Kingman's Independent Review of the Financial Reporting Council (FRC), Competition & Markets Authority's (CMA) Statutory Audit Service Market Study and Brydon's Independent Review into the Quality and Effectiveness of Audit. As the US regulator, PCAOB also announced certain changes in the approach to the regulation and the article summarizes those as well. The concluding part of the article gives a summary of (potential) changes to the regulation, measures related to the audit market, communication with different stakeholders. and possible impacts on corporate governance.*

Key words ● *regulation, audit market, auditor reporting, Kingman, CMA, Brydon, FRC, PCAOB*