SIR IUS 5/24
SLOVENSKI INŠTITUT za REVIZIJO
Revija za teorijo in prakso revizije, računovodstva, davkov, financ, ocenjevanja vrednosti in drugih sorodnih področij

Kazalo

Iz prakse za prakso

Ocenjevanje vrednosti pri določanju osnove za povečanje osnovnega kapitala družbe

Doseganje skladnosti pri izvajanju nekaterih določb iz novih Globalnih standardov notranjega revidiranja

Obveznost rabe slovenščine pri vodenju poslovnih knjig

mag. Maja Hmelak

Trendi v kibernetskem kriminalu v letih 2023 in 2024

Cybercrime Trends 2023 and 2024

Povzetek • *V prispevku so povzeti ključni trendi v kibernetskem kriminalu, ki so v letu 2023 in prvi polovici leta 2024 predstavljali resno grožnjo podjetjem in drugim organizacijam. Spletne korporacije, ponudniki storitev informacijske varnosti, razvijalci protivirusne programske opreme, proizvajalci komunikacijske opreme ter različne državne in nadnacionalne institucije skrbno spremljajo in analizirajo dogajanje na tem področju. Prispevek temelji na njihovih javno dostopnih analizah in poročilih. Poleg najpogostejših trendov v kibernetskem kriminalu so predstavljeni še nekateri izstopajoči primeri napadov na podjetja in organizacije v omenjenem obdobju.*

Izsiljevalska programska oprema ostaja najpomembnejša grožnja še posebej za ranljive sektorje, kot so zdravstvene ustanove. Poleg tega organizacije vse pogosteje doživljajo napade na hibridna in oblačna okolja, kar še dodatno otežuje zaščito njihovih informacijskih sistemov.

Prav tako pomembno vlogo pri organizaciji kibernetskih napadov imajo podporne storitve, ki kriminalcem olajšajo dostop do občutljivih podatkov in omogočajo izvajanje škodljivih aktivnosti tudi manj izkušenim napadalcem. V prispevku je poudarjeno, da bo imela umetna inteligenca v prihodnje ključno vlogo pri kibernetskih napadih, kar organizacijam nalaga okrepljene varnostne ukrepe in večjo pripravljenost za obrambo.

Ključne besede • *kibernetski kriminal, izsiljevalska koda, kraja podatkov, umetna inteligenca, podporne storitve, hibridna in oblačna okolja, tehnologije globokih ponaredkov*

Summary • *The article summarizes the key trends in cybercrime that posed significant threats to businesses and other organizations in 2023 and the first half of 2024. Online corporations, information security service providers, antivirus software developers, communication equipment manufacturers, as well as various national and supranational institutions closely monitor and analyse developments in this field. The article is based on their publicly available analyses and reports. In addition to the most common trends in cybercrime, several prominent examples of cyberattacks on companies and organizations during this period are also presented. Ransomware remains the most significant threat, especially to vulnerable sectors such as healthcare. Additionally, organizations are increasingly facing attacks on*

hybrid and cloud environments, further complicating the protection of their information systems.

Support services play a crucial role in organising cyberattacks, enabling criminals to gain easier access to sensitive data, which allows even less experienced attackers to carry out harmful activities. The article highlights that artificial intelligence will play a critical role in future cyberattacks, requiring organizations to adopt enhanced security measures and greater preparedness for defence.

Key words • *cybercrime, ransomware, data breach, artificial intelligence, support services, hybrid and cloud environments, deepfake technologies*

dr. Boštjan Kežmah

Kibernetska varnost v revizijskih družbah

Cybersecurity in Audit Firms

Povzetek • *Revizijske družbe morajo skladno s predpisi varovati zaupne podatke revidirancev. Pri tem se srečujejo s pomanjkanjem konkretnih smernic glede varovanja zaupnih podatkov v elektronski obliki, zato se soočajo z izzivi medsebojnih obveznosti pri zagotavljanju zadostne varnosti informacij. Tudi zaradi obvladovanja tveganj, povezanih z odgovornostjo revizijskih družb, je smiselno uporabljati okvire upravljanja informacijskih sistemov, standarde in dobre prakse, kot so COBIT 2019, CIS Controls in SIST EN ISO/IEC 27001. Zaradi pomanjkljivega zakonskega urejanja je doseganje in dokazovanje kibernetske varnosti trenutno prepuščeno trgu, pri tem pa kljub navidezni avtoriteti, ki jo imajo revizijske družbe, tudi revidiranci ohranjajo nekatere pogajalske možnosti.*

Ključne besede • *kibernetska varnost, revizijske družbe, zaupni podatki*

Summary • *Audit firms are required by regulations to protect the confidential data of their clients. However, they face challenges due to a lack of specific guidelines on protecting electronic confidential data, leading to issues regarding mutual obligations in ensuring adequate information security. To manage the risks associated with the responsibility of audit firms, it is advisable to use information system management frameworks, standards, and best practices such as COBIT 2019, CIS Controls, and ISO/IEC 27001. Due to insufficient legal regulation, achieving and demonstrating cybersecurity is currently left to the market. Despite the apparent authority of audit firms, clients still retain some negotiating power.*

Key words • *cybersecurity, audit firms, confidential data*

Dr. Tal Pavel

Cybersecurity in Slovenia: Threats and Countermeasures

Kibernetska varnost v Sloveniji: grožnje in protiukrepi

Povzetek • *Slovenia, a small but highly digitalised nation in Central Europe, faces unique cybersecurity challenges shaped by its geopolitical position, advanced digital infrastructure, and integration within the European Union. Slovenia faces several key cybersecurity challenges, primarily stemming from the rapid digitalisation of its economy. As a hub for technological innovation and a member of the EU, Slovenia is particularly vulnerable to cyber threats ranging from state-sponsored espionage targeting its critical infrastructure to sophisticated cybercrime aimed at its growing digital economy.*

The article delves into Slovenia's major cyber threats, including ransomware attacks, phishing schemes, and cyberbullying, which have emerged as a prevalent issue, particularly among schoolchildren. Then, the article analyses the countermeasures taken by Slovenia, such as developing a national cybersecurity strategy, efforts to bolster public-private partnerships, and regional multi-national initiatives. By analysing these factors, the article provides a comprehensive understanding of how Slovenia addresses its cybersecurity challenges and what further steps are needed to enhance its resilience against evolving cyber threats. The article concludes that while Slovenia is advancing in its digital economy, it must address the pressing cybersecurity threats through comprehensive countermeasures and community engagement.

Ključne besede • *Cybersecurity, Policy, Slovenia, Threats, Mitigation*

Summary • *Slovenija, majhna, a visokodigitalizirana država v Srednji Evropi, se sooča s posebnimi izzivi kibernetske varnosti zaradi svojega geopolitičnega položaja, sodobne digitalne infrastrukture in vključenosti v Evropsko unijo. Več ključnih izzivov kibernetske varnosti v Sloveniji izvira predvsem iz hitre digitalizacije slovenskega gospodarstva. Kot tehnološko inovacijsko središče in članica Evropske unije je Slovenija zlasti ranljiva za kibernetske grožnje vse od državno sponzoriranega gospodarskega vohunjenja, usmerjenega v njeno kritično infrastrukturo, do visokorazvitega kibernetskega kriminala, usmerjenega v njeno razvijajoče se digitalno gospodarstvo.*

V članku obravnavamo večje kibernetske grožnje v Sloveniji, kot so napadi z izsiljevalskim programjem, sheme lažnega predstavljanja in kibernetsko nadlegovanje, ki se je pojavilo predvsem med šolsko mladino. V nadaljevanju v članku analiziramo protiukrepe Slovenije, kot so razvoj nacionalne strategije za kibernetsko varnost,

prizadevanja za krepitev javno-zasebnih partnerstev in regionalne večnacionalne pobude. Z analiziranjem teh dejavnikov daje članek celosten vpogled v to, kako Slovenija rešuje izzive kibernetske varnosti in kateri nadaljnji ukrepi so potrebni za boljšo odpornost na vse večje kibernetske grožnje. Članek sklenemo z mislijo, da mora Slovenija vzporedno z razvijanjem digitalnega gospodarstva posvečati pozornost tudi perečim kibernetskim grožnjam ter jih obvladovati s celovitimi protiukrepi in dejavnim vključevanjem skupnosti.

Key words • *kibernetska varnost, politika, Slovenija, grožnje, ublažitev*

Anže Novak

Postopki Informacijskega pooblaščenca na področju varstva osebnih podatkov

Procedures of the Information Commissioner in the Field of Personal Data Protection

Povzetek • *Varstvo osebnih podatkov v Republiki Sloveniji zagotavlja Informacijski pooblaščenec v okviru dveh temeljnih nadzornih postopkov – na zahtevo posameznika, na katerega se osebni podatki nanašajo (postopek na zahtevo prijavitelja s posebnim položajem), in po uradni dolžnosti (inšpekcijski postopek). V prvem postopku Informacijski pooblaščenec ščiti posameznika, ki je vložil zahtevo, v drugem pa odpravlja sistemske kršitve. V prvem postopku se lahko posameznik bodisi pritoži zoper odločitev upravljavca o njegovi pravici (npr. dostopa, izbrisa, popravka, ugovora), ki jo je predhodno uveljavljal pri upravljavcu, bodisi neposredno zahteva nadzor v zvezi s kršitvijo, ki jo zatrjuje. Posameznik v tem postopku lahko pridobi ugotovitev kršitve, ki jo lahko uporabi v morebitnem odškodninskem postopku. Postopek po uradni dolžnosti Informacijski pooblaščenec vodi kot inšpekcijski postopek. V prvem postopku sta stranki posameznik in nadzorovani upravljavec ali obdelovalec, v drugem pa le inšpekcijski zavezanec. Če Informacijski pooblaščenec ugotovi kršitev, po uradni dolžnosti ravna v skladu s pooblastili prekrškovnega organa.*

Ključne besede • *varstvo osebnih podatkov, prijavitelj, zavezanec, inšpekcijski postopek, prijavitelj s posebnim položajem, uveljavljanje pravic, nadzorovani upravljavec*

Summary • *The protection of personal data in the Republic of Slovenia is ensured by the Information Commissioner (hereinafter referred to as the IC) within the framework of two basic supervisory procedures - at the request of the data subject (complaint procedure or 'procedure at the request of the complainant with special status') and ex officio (inspection procedure). In the first procedure, the IC protects the individual who made the request, and in the second, he corrects system violations. In the first procedure, an individual can either 'complain' against the controller's decision on his or her right (e.g. access, deletion, rectification, objection) that he or she previously exercised with the controller, or directly request supervision in relation to the breach he or she alleges. An individual in this proceeding may obtain a finding of infringement that can be used in a potential damages claim. The ex officio IP procedure is conducted by the information commissioner as an inspection procedure. In the first procedure, the parties are the individual and the supervised*

controller or processor, and in the second, only the entity subject to inspection. If the IC finds a violation, he acts ex officio in accordance with the powers of the misdemeanour authority.

Key words • *personal data protection, complainant, obligated entity, inspection procedure, complainant with special status, exercise of rights, supervised controller*

Alenka Blas in Ruti Rous

Premiki na evropskem podatkovnem področju

Progress in the European Data Sector

Povzetek • *Evropski uniji je v razmeroma kratkem času uspelo sprejeti predviden regulativni okvir za uresničevanje Evropske strategije za podatke. Začelo se je vzpostavljanje enotnega evropskega podatkovnega trga, ki želi zagotoviti izkoriščanje moči podatkov in umetne inteligence ob zagotavljanju pravičnosti, preglednosti in konkurenčnosti v digitalnem gospodarstvu. Za najodmevnejšega izmed evropskih podatkovnih predpisov se je izkazal Akt o umetni inteligenci, ki se je osredotočil na zagotavljanje odgovorne rabe umetne inteligence ter iskanje ravnovesja med inovacijami in etičnimi vidiki. Velik vpliv na področje upravljanja in varnosti podatkov pa gre pripisati Aktu o podatkih, ki poudarja pravično porazdelitev vrednosti podatkov, ter digitalnemu dvojčku – Aktu o digitalnih storitvah in Aktu o digitalnih trgih, ki postavljata nove standarde odgovornega ravnanja akterjev na digitalnem trgu. Z vzpostavitvijo regulativnega okvira je EU prevzel globalno vodstvo na področju digitalne podatkovne regulacije. Uspeh tega v praksi kljub temu ostaja odvisen od implementacije aktov in njihovega izvrševanja v državah članicah, pa tudi od sposobnosti nadaljnjega prilaganja regulativnega okvira hitremu tehnološkemu napredku.*

Ključne besede • *podatki, umetna inteligenca, visokotvegani sistemi, digitalne storitve, varnost*

Summary • *The EU has successfully adopted the anticipated regulatory framework for the implementation of the European Data Strategy in a relatively short time. The establishment of a single European data market began, aiming to harness the power of data and artificial intelligence while ensuring fairness, transparency, and competitiveness in the digital economy. The most notable among the European data regulations has proven to be the Artificial Intelligence Act, which focuses on ensuring the responsible use of artificial intelligence and finding a balance between innovation and ethical aspects. In addition, the Data Act, emphasizing the fair distribution of data value, also had a significant impact on data governance and security, as did the Digital Services Act and the Digital Markets Act, which set new standards for responsible behaviour of the actors in the digital market. With the establishment of the regulatory framework, the EU has taken a global leadership role in digital data regulation. However, the success of this framework in practice remains dependent on the implementation and enforcement of the*

adopted Acts in the Member States, as well as on the ability of continuous adaptation of the regulatory framework to rapid technological advancements.

Key words • *data, artificial intelligence, high-risk systems, digital services, security*

Zala Miklič

Vpliv evropskega zelenega dogovora na vrednost nepremičnin v prihodnosti

The Impact of the European Green Deal on the Value of Real Estate in the Future

Povzetek • *Že nekaj let je treba pri prodaji, najemu oziroma nakupu nepremičnin upoštevati nova merila, ki jih je za skupno dobro leta 2019 oblikovala Evropska komisija. Evropski zeleni dogovor je oblikovan s ciljem izničenja emisij CO2 do leta 2050. Kljub temu da smo si ljudje edini, da so smernice evropskega zelenega dogovora ustrezne in jih je nujno upoštevati za dostojno življenje prihodnjih generacij, je bilo skladno s pričakovanji mogoče ugotoviti, da je ozaveščenost o takojšnjem in nujnem ukrepanju še vedno premajhna. Ljudje, ki se ukvarjajo s prodajo, oddajo, najemom in nakupom nepremičnin, dajejo prednost nižji ceni, dostopnejši lokaciji in boljšim logističnim povezavam. Evropski zeleni dogovor za zdaj še ni sprožil revolucionarnih sprememb, kot bi bilo potrebno. Vlagatelji v poslovne nepremičnine preusmerjajo svoje investicije v projekte, ki spodbujajo trajnostni razvoj, zaradi svojih podjetniških vrednot glede varovanja okolja. Velik korak v pravo smer za nepremičninski sektor je upoštevanje smernic ESG-ja. Kljub temu da so poslovne stavbe že nekako prisiljene upoštevati evropski zeleni dogovor, pa je pri zasebnih nepremičninah drugače. Ne samo da so zasebni investitorji o ciljih in načelih evropskega zelenega dogovora slabo ozaveščeni, večinoma niti niso finančno sposobni povečati izdatkov za energijsko učinkovitejšo in pasivnejšo nepremičnino. Zaradi prevelike potrošnje in onesnaževanja smo ljudje izrabili in uničili prevelik del neobnovljivih virov. Evropski zeleni dogovor bi pomagal naš planet vrniti v prave tirnice in rešiti, kar se še da.*

Ključne besede • *evropski zeleni dogovor, smernice ESG-ja, energijska učinkovitost, biotska raznovrstnost, klimatske spremembe, krožno gospodarstvo, nepremičninski sektor, sveženj »pripravljeni na 55«, zelena premija, rjavi diskont, trajnostne nepremičnine, energetske izkaznice*

Summary • *In the recent years, it has become necessary to take into consideration the new criteria in the process of selling, renting or buying real estate that Europe created for the common good in 2019. The European Green Deal is designed with the aim of eliminating CO2 emissions by 2050. People agree that the guidelines of the European Green Deal are appropriate and they have to be followed to enable decent life to future generations. Nevertheless, as expected, it has been established that the level of awareness to take immediate and urgent actions is still insufficient. People engaged in selling, leasing, renting and buying real estate prefer a*

lower price, more accessible location and better logistics connections. Currently, the European Green Deal does not cause revolutionary changes which are needed. Investors in business real estate redirect their investments into projects that promote sustainable development because of their corporate values, oriented to environment protection. A big step in the right direction for the real estate sector is made by following the ESG guidelines. Commercial buildings are to some extent already forced to comply with the European Green Agreement. However, private real estate is a story of its own. Not only are private investors poorly aware of the goals and principles of the European Green Agreement, they are also largely unable to increase their budget for a more energy efficient and passive real estate. Due to excessive consumption and polluting, people have used up and destroyed too many non-renewable resources. The European Green Deal is something that would help put our planet back on the right track and save what still can be saved.

Key words • *European Green Deal, ESG guidelines, energy efficiency, biodiversity, climate change, circular economy, real estate sector, "Fit for 55", green premium, brown discount, sustainable real estate, energy efficiency certificates*