Agentúra na podporu výskumu a vývoja
Mýtna 23, P.O.BOX 839 04, 839 04 Bratislava 32

Formulár ZK

Záverečná karta projektu

Názov projektu

Elektronizácia v podnikaní s akcentom na právne a technické aspekty

Evidenčné číslo projektu **APVV-14-0598**

Zodpovedný riešiteľ **doc. JUDr. Regina Hučková , PhD.**

Príjemca **Univerzita Pavla Jozefa Šafárika v Košiciach**

Názov pracoviska, na ktorom bol projekt riešený

Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta

Názov a štát zahraničného pracoviska, ktoré spolupracovalo pri riešení

-

Udelené patenty/podané patentové prihlášky, vynálezy alebo úžitkové vzory, ktoré sú výsledkami projektu

-

Najvýznamnejšie publikácie (knihy, články, prednášky, správy a pod.) zhrňujúce výsledky projektu – uveďte aj publikácie prijaté do tlače

1. SOKOL, P., BAJTOŠ T., et al. - Network Intrusion Detection with Threat Agent Profiling. In: Security and Communication Networks. ISSN 1939-0114. (2018), art.no. 3614093, [17 s.]
2. HUČKOVÁ, R., SOKOL, P., RÓZENFELDOVÁ, L. – 4th Industrial Revolution and Challenges for European Law (with special attention to the concept of digital single market). In: EU and Comparative Law Issues Challenges Series (EU Law in context – adjustment to membership and challenges of the enlargement). ISSN 2459-9425, s. 201-215
3. RÓZENFELDOVÁ, L., SOKOL, P. – New Initiatives and Approaches in the Law of Cookies in the EU. In: IDIMt 2018 (Strategic modeling in management, economy and society). Linz, 2018, s. 303-310
4. BAJTOŠ, T., SOKOL, P., GAJDOŠ, A., LUČIVJANSKÁ, K., MÉZEŠOVÁ, T.: Analysis of the infection and the injection phases of the telnet botnets. In J.UCS Journal of Universal Computer Science. (IF: 0.910) (v tlači)
5. TREŠČÁKOVÁ, D. – On some aspects of protection of personal data in the European area. In: Topical issues problems of modern law and economics in Europe and Asia. Moskva, Justicinform, 2018, s. 144-163

Uplatnenie výsledkov projektu

Riešiteľský kolektív riešením projektu reagoval na nezvratný trend elektronizácie a digitalizácie podnikateľského prostredia v tuzemských i zahraničných podmienkach, ktorý však priniesol radu otvorených právnych a legislatívnych otázok prameniacich v technických riešenia a prístupoch. Interdisciplinárnym zložením riešiteľského kolektívu boli vytvorené optimálne podmienky pre skúmanie najexponovanejších otázok spojených v čase

podávania projektu s problematikou elektronizácie podnikania. V priebehu riešenia projektu vyvstali i ďalšie témy, ktoré boli iniciované najmä (no nielen) európskou legislatívou.
Výsledky riešenia projektu sú uplatniteľné vo viacerých smeroch:
1. v ďalšom vedeckom výskume: riešiteľský kolektív formuloval vo svojich vedeckých výstupoch viaceré poznatky a postoje, ktoré sú využiteľné pre ďalší vedecký diskurz v predmetnej oblasti - časovú neobmedzenosť skúmaných poznatkov potvrdzuje aj skutočnosť, že väčšina riešiteľov projektu pokračuje v riešení pokračujúcej témy.
2. v aplikačnej praxi: riešiteľský kolektív akcentoval viaceré témy s výrazným presahom do aplikačnej praxe, čo nenechali bez povšimnutia aj so zreteľom na formu transferu poznatkov smerom k aplikačnej praxi. Riešitelia zorganizovali viaceré semináre pre odbornú prax.
3. v pedagogickom procese: riešiteľský kolektív pretavil výsledky svojich vedeckých aktivít aj do pedagogického procesu - v rámci študijného programu na právnickej fakulte boli vytvorené viaceré nové predmety. Zároveň riešiteľský kolektív pripravil pre študentov Právnickej fakulty a Prírodovedeckej fakulty podujatie jedinečné svojho druhu na Slovensku - Letnú školu kyberkriminality založenú na kooperácií študentov práva a informatiky pri riešení technických a právnych problémov.
4. v popularizácií témy smerom k odbornej a laickej verejnosti: riešiteľský tím sa pravidelne zúčastnil popularizačných podujatí s cieľom transferu poznatkov aj smerom k laickej verejnosti - Noc výskumníkov, Deň otvorených dverí na univerzite, etc.

Súhrn výsledkov riešenia projektu a naplnenia cieľov projektu v slovenskom jazyku (max. 20 riadkov)

Riešiteľský kolektív analyzoval široké penzum tém súvisiacich s problematikou elektronizácie podnikania. Digitalizácia spojenú s markantným rozmachom informačných a komunikačných technológií možno v súčasnosti považovať za jeden z rozhodujúcich aspektov determinujúci spoločnosť a rôznorodé vzťahy.
V rámci elektronizácie procesov podnikateľských subjektov sa v projekte venovala pozornosť elektronickým právnym úkonom, dynamickým biometrickým podpisom a formám oznamovania protispoločenskej činnosti.
V rámci projektu sme sa zamerali na podvodné systémy (deception systems) využívané aj podnikateľskými subjektami na zabezpečenie svojich aktív voči bezpečnostným hrozbám a útokom. Cieľom týchto systémov je podvrhnúť útočníkovi informačný systém, prihlasovacie údaje, citlivé dokumenty a pod., ktoré pre organizáciu nemajú hodnotu, ale dokážu detegovať prienik do informačného systému, resp. zneužitie týchto údajov a dokumentov. V rámci projektu sme sa venovali problematike implementácie a použitia týchto systémov v rámci podnikateľských subjektov, najmä z pohľadu súkromnoprávnej zodpovednosti a ochrany súkromia a osobných údajov.
Členovia riešiteľského kolektívu reagovali súčasne na aktuálne zmeny v legislatíve EU v oblasti zodpovednosti a ochrany súkromia. Venovali sa dopadom nového regulačného rámca na ochranu autorských diel zdieľaných online platformami a používaniu online identifikátorov - cookies.
V oblasti ochrany osobných údajov a riešenia bezpečnostných incidentov je výsledkom projektu analýza správania používateľov organizácie (zamestnancov podnikateľských subjektov) pri používaní emailovej komunikácie a reakcie na rôzne formy sociálneho inžinierstva. Pracovné vzťahy v rámci podnikateľských subjektov riešiteľský kolektív bližšie analyzoval najmä v súvislosti s otázkami ochrany osobných údajov (napr. rodným číslam v pracovných zmluvách), používania sociálnych sietí, elektronického doručovania a pod.
Výsledkom projektu je aj predikcia bezpečnostných udalostí pomocou časových radov (time series). S predikciou bezpečnostných udalostí úzko súvisí aj profilovanie útočníkov. Podľa správania sa útočníkov je možné ich zatriediť do určitých skupín (clustrov) a podľa tohto triedenia predikovať ich nasledujúce správania. To môže výrazne zvýšiť pravdepodobnosť rýchleho odhalenia bezpečnostného incidentu, resp. jeho cieľa a znížiť náklady podnikateľských subjektov na riešenie bezpečnostných incidentov a odstraňovaní ich následkov.

Súhrn výsledkov riešenia projektu a naplnenia cieľov projektu v anglickom jazyku (max. 20 riadkov)

The research team analyzed a wide range of topics related to the issue of e-business. Digitization associated with a marked boom in information and communication technologies

can now be considered as one of the crucial determinant aspects of society and diverse relationships.
As regards the computerization of business subjects, the project focused on electronic legal acts, in particular on contractual penalties in the contract for the trip reservation, dynamic biometric signatures and on forms of anti-social activities' notification.
Within the project, we considered the deception systems used by business subjects to secure their assets against security threats and attacks. The purpose of these deception systems is to provide the attacker with an information system, login data, sensitive documents etc., that have no value for the organization, but can lead to the detection of an attack on the information system, or of the abuse of this data and documents. As a part of the project we analysed the issue of the implementation and use od these systems by the business subjects, particularly as regards the issues of private liability, privacy and personal data protection.
The members of the research team have also responded to the latest legislative changes in the EU law in the area of liability and privacy protection. They analysed the impacts of the new regulatory framework on the protection of works shared by online platforms, as well as on the use of online identifiers.
As regards the personal data protection and the security incidents solution, the project resulted in the analysis of the organisation users' behaviour (employees of the business subjects) during their use of email communication and their reactions on different forms of social engineering.
The project has also resulted in the prediction of security incidents through the use of time series. The profiling of attackers is closely connected with the security incidents' prediction. According to the attackers' behaviour, it is possible to differentiate attackers to specific groups (clusters) and use this to predict their further behaviour. This can significantly increase the possibility to quickly detect the security incident or its purpose, and decrease the business subjects' expenses invested to handle security incident and to eliminate their consequences.