INFORMACIJSKA VARNOST

Pravni vidiki preiskovanja in dokazovanja kaznivih dejanj s pomočjo informacijskih in komunikacijskih tehnologij

Nathan Klasinc

Namen prispevka
Namen prispevka je prikazati preiskovanje kibernetskega kriminala iz vidika organov pregona s poudarkom na pravnem vidiku. V prispevku sem se osredotočil na problematiko s katero se morajo spopadati organi pregona in tožilstvo.

Metode
Uporabljena metoda za prispevek je bila analiza slovenskih zakonodajnih aktov, strokovnih člankov in prispevkov konference.

Ugotovitve
Glede na hiter razvoj informacijskih in komunikacijskih tehnologih se Slovenija dokaj uspešno prilagaja temu razvoju vendar ne bo smela razvoja zakonodaje in tehnik preiskovanja opustiti.

Izvirnost/pomembnost
V prispevku je na kratek in razumljiv način predstavljena problematika s katero se srečujejo organi pregona in zakonodajna veja oblasti.

Ključne besede: Kibernetična kriminaliteta, Zakon o kazenskem postopku, Kazenski zakonik, informacijsko komunikacijska tehnologija, računalniška kriminaliteta

Kibernetsko ustrahovanje

Nejc Pantič

Namen
Namen prispevka je predstaviti problem kibernetskega ustrahovanja, kot mladostniškega nasilja, ki se zaradi hitrega razvoja informacijske tehnologije, začne že pri samem definiranju pojma. Prispevek se osredotoča na razlike med klasičnim in kibernetskim ustrahovanjem, opredeljuje metode izvajanja kibernetskega ustrahovanja, značilnosti storilcev in žrtev, pojasnjuje posledice za žrtve in poskuša opredeliti ustrezne ukrepe za preprečevanje oziroma omejevanje pojava.

Metode
Prispevek temelji na pregledu obstoječe literature s področja kibernetskega ustrahovanja.

Ugotovitve
Tehnološki razvoj omogoča obilo različnih načinov izvajanja kibernetskega ustrahovanja hkrati pa so uporabniki mobilnih telefonov in računalnikov vedno mlajši. Starši morajo zato v sodelovanju z učitelji nadzorovati mladostnikovo udejstvovanje na spletu. Tako bodo lažje sankcionirali neprimerno vedenje, hkrati pa tudi prej ugotovili ali je mladostnik viktimiziran. Glavni problem kibernetskega ustrahovanja je pojav neprestanega ustrahovanja, kar pomeni, da sedaj ustrahovanje ne poteka le v šolah pač pa se nadaljuje tudi skozi popoldneve, vikende in počitnice.

Omejitve/uporabnost raziskave
Glavna pomanjkljivost prispevka predstavlja odsotnost empiričnega dela.

Izvirnost/pomembnost prispevka
Za tiste, ki s tovrstno problematiko še niso seznanjeni, bo prispevek najbolj uporaben, sicer pa je lahko koristen tudi za starše, učitelje in ostale, ki se z mladoletniki, njihovimi problemi in ne nazadnje mladoletniško kriminaliteto, srečujejo bodisi v okviru svoje zaposlitve ali pa znotraj domačega okolja.

Ključne besede: ustrahovanje, kibernetsko ustrahovanje, tehnologija, "bully", žrtev

Lastnosti bodočih kibernetskih napadov

Blaž Ivanc

Namen prispevka
V zadnjih nekaj letih se je veliko prostora namenjenega informacijski varnosti posvečalo nekaterim znanim kibernetskim napadom. Hkrati so se na podlagi analiz preteklih kibernetskih napadov in odmevnosti le teh, v ozadju konstantno razvijale nove ofenzivne informacijske tehnike, taktike in procedure. Namen prispevka je zato prikazati lastnosti kibernetskih napadov, ki jih pričakujemo v prihodnjih letih.

Metode
Članek temelji na pregledu novih znanstveno raziskovalnih prispevkov z dodatnim komentarjem ter primerjavo analiz dovršenih kibernetskih napadov.

Ugotovitve
Kibernetski napadi katere bomo srečali v prihodnjih letih, so navdih dobili v analizi delovanja preteklih znanih in visoko dovršenih napadih. Kibernetski napadi bodo po večini že v osnovi združevali več zlonamernih metod, skladno s tem bodo pogosto prikazali izvirno napadalno tehniko in avtonomno ustvarjanje zlonamerne aktivnosti na strani tarče.

Izvirnost
Čeprav razprave o znanih kibernetskih napadih v obdobju zadnjih treh let še vedno trajajo, se že zelo kmalu pričakuje nove kibernetske napade z razširjenimi lastnostmi. Obravnavani napadi bodo s svojo izvirno modularno zasnovo in tudi avtonomnim delovanjem poskušali izkoriščati šibkosti v varnostnih protiukrepih in postopkih, ki so se širše integrirali ravno v zadnjem obdobju. Prispevek je namenjen strokovnjakom in akademikom, ki se ukvarjajo s problematiko povezano s kibernetskimi napadi.

Ključne besede: informacijska varnost, bodoči kibernetski napadi, metode delovanja, zlonamerna aktivnost

Kompromisi pri zagotavljanju informacijske varnosti v organizacijah

Kaja Prislan, Igor Bernik

Namen prispevka
Zagotavljanje informacijske varnosti je v organizacijskem okolju zahtevna naloga, saj pogoji ki jih postavlja zunanje okolje vodijo v sprejemanje varnostno-poslovnih kompromisov. Prispevek se nanaša na idejo, da morajo organizacije za pridobitev določene kvalitete informacijskega sistema žrtvovati ali zmanjšati drugo kvaliteto istega ali drugega poslovnega procesa. Namen je prikazati vpliv sprememb informacijske varnosti na povezane procese in predlagati priporočila, kako zagotoviti čim manjši vpliv ukrepov na obstoječe funkcionalnosti. Prav tako predstavljamo mite, etične in psihološke vidike informacijske varnosti, ki vodijo v sprejemanje slabih kompromisov.

Metode
V prispevku je uporabljena metoda deskriptivne analize znanstvenih in strokovnih virov, sinteza in interpretacija ugotovitev. Obstoječa spoznanja podpiramo s pregledom raziskav o trenutnem stanju informacijske varnosti.

Ugotovitve
Ugotavljamo, da ukrepi s katerimi povečujemo informacijsko varnost vplivajo na dostopnost storitev, neprekinjeno poslovanje, zasebnost zaposlenih, njihove pravice in obveznosti ter uporabnost sistemov. Raziskave in strokovnjaki navajajo, da organizacije zaradi precenjevanja tveganj, psiholoških pritiskov in nepravilnega razporejanja varnostnih ter upravljavskih funkcij, pogosto sprejemajo napačne odločitve. Če želijo sprejemati dobre kompromise morajo prepoznati varnostne potrebe, neetično ravnanje varnostne stroke in zagotoviti konstruktivni konflikt med odgovornimi.

Praktična uporabnost
Spoznanja prispevajo k boljšemu razumevanju sodobne varnostne dileme s katero se srečujejo organizacije. Uporabnost prispevka se kaže v pojasnjevanju razlogov nepravilnih odločitev, kar v kombinaciji s podanimi priporočili ponuja rešitve za sprejemanje dobrih kompromisov.

Izvirnost
Izvirnost prispevka se kaže v njegovi aktualnosti. Prispevek je inovativen zato, ker obravnava problem, ki je v tujih virih parcialno obdelan, v Sloveniji pa se ga namensko še ni obravnavalo.

Ključne besede: informacijska varnost, varnostni kompromisi, organizacije, učinkovitost

Informacijsko varnostna kultura v Policiji

Blanka Strmšek, Blaž Ivanc

Namen prispevka
Prispevek prikazuje problematiko zaščite in varovanja zaupnih podatkov pred nepooblaščenimi dostopi, s katero se sooča Generalna policijska uprava (GPU). Ta se nanaša na evidence informacijskega in telekomunikacijskega sistema policije (ITSP), pri kateri lahko pride do njihove izdaje, razkritja ali zlorab. Tovrstna ravnanja vplivajo na delovanje Policije, saj lahko ogrozijo izvajanje nalog Policije in škodijo njenemu ugledu. S pomočjo prispevka želimo strokovni javnosti predstaviti stanje na področju informacijsko varnostne kulture v Policiji. Glavni cilj prispevka je na podlagi rezultatov analize podati priporočila in predloge za zavarovanje podatkov ter izboljšanje informacijsko varnostne kulture.

Metodologija
Prispevek je rezultat analize virov s področja informacijsko varnostne kulture. Uporabljeni sta deskriptivna in analitična metoda. Izvedeno je bilo tudi anketiranje in statistična obdelava podatkov, v okviru katere smo preučili stanje informacijsko varnostne kulture v Policiji.

Ugotovitve
Policija poskuša s sodobnim varnostnim rešitvam in normativno ureditvijo zmanjšati škodljive posege in zagotoviti varno uporabo informacijskega okolja. Toda absolutne varnosti podatkov in delovanja informacijskega sistema ni, saj je vedno navzoč človeški dejavnik. Prav zaradi tega je pomembna visoka informacijsko varnostno kultura zaposlenih in dobra seznanjenost z varnostno politiko ter predpisi.

Izvirnost/pomembnost prispevka
Izvirnost se kaže v proučitvi trenutnega stanja v Policiji. Prispevek je namenjen GPU, da bo lahko prepoznala težave najšibkejšega člena informacijske varnosti, človeka. Z vsebino prispevka jih želimo opozoriti, da doseganje ciljev informacijsko varnostne kulture ni samo odgovornost posameznikov in skupin, potrebna je tudi močna podpora vodstva, ki mora ustvariti, upravljati in ohranjati informacijsko varnostno kulturo.

Ključne besede: Informacijsko varnostna kultura, Policija, zaupni podatki, kršitve, zlorabe, priporočila

Sigurnosna mjera - zabrana pristupa internetu

Dražen Škrtić

Namen prispevka
Prikaz pravnih okvira za izricanje sigurnosne mjere zabrane pristupa internetu i načina provođenja sigurnosne mjere

Metodologija
Deskriptivnom metodom obuhvaćene su odredbe Kaznenog zakona kojima su definirani okviri za izricanje sigurnosne mjere i provedbeni propis za izvršavanje sigurnosne mjere.

Ugotovitve
Sigurnosna mjera zabrane pristupa Internetu uvedena je u Kazneni zakon prema uzoru na poredbeno pravo i izriće se počiniteljima koji kriminalnu aktivnost ostvaruju uporabom Interneta. Neubrojivoj osobi, koja je kazneno djelo počinila putem Interneta ako postoji opasnost da će zlouporabom Interneta ponovno počiniti kazneno djelo, može se izreći sigurnosna mjera zabrane pristupa Internetu u trajanju od šest mjeseci do dvije godine računajući od izvršnosti sudske odluke. O pravomoćno izrečenoj mjeri sud obaviještava Hrvatsku agenciju za poštu i elektroničke komunikacije na čiji zahtjev operatori elektroničkih komunikacijskih usluga koji pružaju uslugu pristupa Internetu ili putem koje je moguć pristup Internetu obustavljaju pružanje usluge pristupa Internetu, raskidaju postojeći i provode zabranu sklapanja novog ugovora uključujući i unaprijed plaćene usluge s osobom kojoj je izrečena sigurnosna mjera za vrijeme trajanja izrečene sigurnosne mjere.

Omejitve/uporabnost raziskave
Ograničenje predstavlja nedostatak izrećenih sigurnosnih mjera zabrane pristupa internetu i praktičnog izvršenja te sigurnosne mjere.

Praktična uporabnost
U preglednom članku daje se prikaz odredbi Kaznenog zakona, poredbenog prava i provedbenog propisa za izvršavanje izrečene sigurnosne mjere zabrane pristupa Internetu.

Izvirnost/pomembnost prispevka
Predstavljene su odredbe Kaznenog zakona kojima su definirani pravni okviri za izricanje sigurnosne mjere zabrane pristupa Internetu

Ključne besede: kazneni zakon, internet, sigurnosne mjere