

TEMA UP6: UVODNA PREDAVANJA

Paper No.UP6.1

01133

VISOKOTEHNOLOŠKA BEZBEDNOST SISTEMA ZA STICANJE ZNANJA

Milica D. Đekić¹

¹Nezavisni istraživač za bezbednost, Subotica, Srbija

¹milicadjekic82@gmail.com

Kratak sadržaj: Sa informatičkog stanovišta, sistemi za sticanje znanja se uglavnom oslanjaju na internet uslugu koja im omogućava da budu umreženi i da sa servera povuku podatke ili definišu rutu kojom se informacije kreću. Bilo da je sama aplikacija na uređaju ili u cloud okruženju, ono što je bitno uočiti je da su date tehnologije ranjive na visokotehnoške napade. Taj vid ranjivosti može da se odnosi na krajnjeg korisnika ili neki od mrežnih, kao i uređaja za pohranjivanje podataka. Jednom kada se hakeri dokopaju IP adrese računara, čitava mreža je u opasnosti da bude hakovana. Iz tog razloga, jako je važno da sistemi za onlajn učenje imaju neku vrstu zaštite od hakerskih napada. Drugim rečima, celokupna informaciona infrastruktura treba da poseduje sisteme za zaštitu kako bi svi u mreži bili sigurni. Osim toga, nije dovoljno odbiti neki visokotehnoški napad – potrebno je imati i odgovarajući mehanizam procesuiranja aktera visokotehnoškog kriminala. Konačno, na crnom tržištu podaci imaju svoju cenu i svaka tačna informacija može da se iskoristi za sticanje prednosti nad nekim, te, stoga, mnogi su spremni da plate hakersku uslugu kako bi se dokopali i suviše vrednih informacija iz akademske zajednice. Svrha ovog članka je da obezbedi sveobuhvatni uvid u nove trendove i tendencije kada je visokotehnoška bezbednost tehnologija za učenje u pitanju.

Ključne reči: visokotehnoška bezbednost, saznanje, hakovanje, informatika, podatak.

CYBER DEFENSE OF KNOWLEDGE SYSTEMS

Abstract: From an informatics point of view, the knowledge systems mainly rely on the internet service providing them an opportunity to be networked as well as pull data from the server and define the route of the information transit. Either the information is on device or in the cloud environment it's significant to see those technologies are vulnerable to the cyber attacks. That sort of vulnerability is correlated with the end user as well as some network or data storage device. Once the hackers obtain someone's IP address the entire network is under threat to be hacked. For such a reason it's important for online learning systems to deal with some kind of cyber security. In other words, the entire IT infrastructure should have a protection system as everyone will be assured. Beside so, it's not sufficient to just terminate the cyber attack – it's mostly necessary to cope with the adequate law enforcement prevention mechanism. Finally, on the black market any data has its price as any accurate information can be used in taking advantage over anyone else, so that's why many are ready to pay a lot for the hacker's service in order to get so valuable information from the academic community. The purpose of this article is to offer a comprehensive insight into new trends and tendencies regarding the cyber defense of the knowledge systems.

Key Words: cyber defense, intelligence, hacking, informatics, data.

1. UVOD

Kao što je poznato, računarske mreže koje se koriste u akademskoj zajednici mogu da sadrže vrlo kritične podatke o samoj ustanovi, ali i o njenom ljudstvu. Mnogo ilegalnih i protivničkih aktera bi volelo da dođu u posed tih informacija iz razloga što onaj ko vlada tačnom informacijom vlada i situacijom u nekoj oblasti. Zamislamo samo šta bi se desilo kada bi neko saznao sadržaj naučno-istraživačkog projekta i plasirao ga na tržište pre drugih. U savremenom svetu, **vreme znači novac** i mnogobrojna konkurencija i tek kako razume tu izreku. Dakle, da bismo bili konkurentni na tržištu ne treba da prepisujemo od drugih, nego bar da zaštitimo ono što je naše kako neko drugi ne bi ubirao plodove našega rada [1-17]. Mediji u razvijenom svetu izveštavaju da su mnoge obrazovne institucije hakovane i da su hakeri i po deceniju i više bili u vezi sa tom informacionom infrastrukturom svakoga dana skidajući nove i nove podatke i, naravno, niko to nije znao.

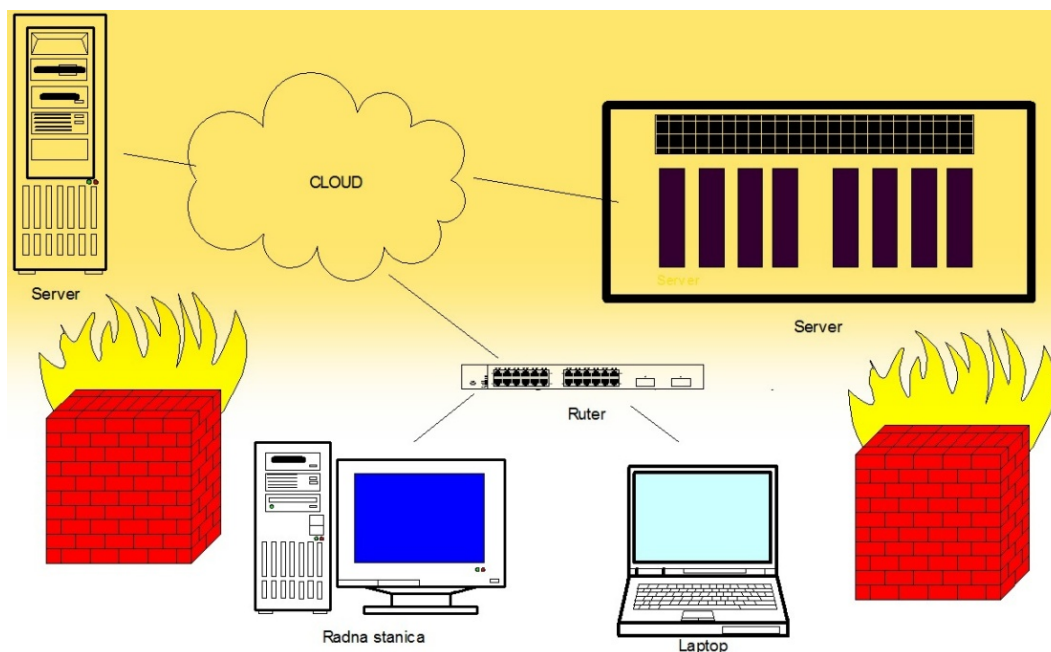
S druge strane, u današnje vreme je dostupna cloud tehnologija i, dakako, ti sistemi imaju svoje prednosti u smislu bolje obezbeđenosti datacentara i same komunikacione infrastrukture. Međutim, čak ni tako sofisticirana rešenja nisu otporna na hakerske napade iz razloga što niti jedan uređaj u toj mreži može da garantuje potpunu pouzdanost u radu. Drugim rečima, nije pitanje da li će se visokotehnoški upad desiti, nego je do nas da prihvatimo njegovu neminovnost. Dalje, uvek treba početi od pretpostavke da je nešto već hakovano i u tom smislu sprovesti mere provere i forenzičkog ispitivanja opreme koja je pod nadzorom. U datom smislu, reč je o dobro razvijenim bezbednosnim pretragama koje nam omogućavaju da detektujemo pretnju dok je još aktivna u našem delokrugu [18-25].

Sličan slučaj je i sa informacionim sistemima za sticanje znanja, jer oni mogu da budu kompromitovani u slučaju slabe kontrole pristupa. Na primer, kontrola pristupa putem verifikacionog koda ima svoje prednosti i nedostatke i čak i ona može da bude ranjiva na visokotehnološke napade. Takođe, u praksi se koristi i vremenski kontrolisana bezbednost, ali kako je sa manje ili više truda i vremena moguće upasti u neki informacioni sistem jasno je zbog toga da je i takva bezbednost sa ograničenjima. Konačno, treba razmišljati i o kriptografiji kao meri zaštite iz razloga što određeno vreme mnogi međunarodni stručnjaci apeluju da sve što se čuva u cloud-u treba da bude šifrovano. Izazov koji se tu nameće je menadžment kriptografskog ključa, ali u svakom slučaju svaka zaštita je dobrodošla i bolja nego bilo kakav vid nedostaka odbrane.

2. VISOKOTEHNOLOŠKA ZAŠTITA INTERNET MREŽE

Prema mnogobrojnim istraživanjima i anketama, došlo se do saznanja da izuzetno veliki broj korisnika računarskih uređaja i interneta ne zna kako izgleda hakerski napad. Prema tim studijama, većina ispitanika veruje da nikada nije bila izložena visokotehnološkim napadima, dok drugi deo njih odgovara da nije sigurno o čemu se uopšte radi. Da stvar bude još više zabrinjavajuća ovi rezultati dolaze iz razvijenog sveta i moguće je samo pretpostaviti šta imaju da kažu korisnici iz zemalja u razvoju. Dakle, kako izgleda hakerski napad? Za te potrebe se koriste alati kojima je potrebno dati IP adresu i, eventualno, port ciljanog uređaja i kada se to dostavi haker ima pristup tom uređaju. To znači da na udaljenoj lokaciji visokotehnološki kriminalac na jednom od svojih ekrana može da vidi nečiju radnu površinu i da ima odobrene opcije poput transfera podataka ili daljinske kontrole korisničkog uređaja. Takođe, moguće je ubacivati malware aplikacije u taj prozor ili, pak, blokirati i usporavati internet promet. Današnja tehnološka rešenja idu tako daleko da je moguće isključiti ili ponovo pokrenuti nečiji sistem, ako neko to već hoće. Drugim rečima, ako Vaš anti-malware sistem izveštava da postoje virusi u Vašem računaru ili ste primetili da Vam je internet sporiji nego inače, jasno je da ste se inficirali ili preko nekog linka ili Vas sam haker koji je onlajn sa Vašim uređajem zasipa tim virusima i u mnogim slučajevima u realnom vremenu prati Vaše aktivnosti. Zbog toga se i kaže da nije pitanje da li će i kada da dođe do hakerskog napada, već je neophodno prihvatiti njegovu neminovnost. To je nešto što je stalno dešava i čak bezazleni transfer informacija sa jednog uređaja na drugi bez znanja korisnika je oblik visokotehnološkog kriminala, jer se dešava u tajnosti i može skupo da košta onoga ko je podvrgnut tom obliku špijunaže.

Kao što je poznato, aplikacije za onlajn učenje mogu da budu snimljene na neki uređaj ili ubačene u cloud okruženje. U svakom slučaju, nepohodno je korišćenje internet usluge kako bi se razmena podataka odvijala. Tamo gde je internet, tamo su i hakeri i u tom smislu je jasno zbog čega je bitno sprečiti ili makar detektovati visokotehnološki upad u sistem. U praksi, postoji čitav spektar razvijenih metoda kako može da se dođe do nečije IP adrese koja je ključna za hakerski napad. Jedan od zgodnih primera u tom smislu je i phishing ili slanje phishing linka putem e-pošte, društvenih mreža ili na neki drugi način. Kada se klikne na dati link ostavljaju se podaci o tom uređaju i tada haker i te kako može da zloupotrebi nečiju nepažnju. Na Slici 1 je data ilustracija tipične korisničke mreže koja sadrži korisničke uređaje, zaštitu, servere, mrežne uređaje i samo cloud okruženje koje se oslanja na tu informacionu infrastrukturu [26-31].



Slika 1. Internet mreža sa merama prevencije od visokotehnoloških napada

Iz ovoga proizilazi da da je onlajn nastava na Univerzitetima i tek kako ranjiva kada su hakerski napadi u pitanju. Osim toga, računari, mreža i serveri visokoškolskih ustanova čuvaju vrlo osetljive podatke i nije pametno

prepuštiti to blago visokotehnoškom kriminalu, jer kriminalci imaju načina da kompromituju neku instituciju u smislu objavljivanja kritičnih saznanja na web-u i obaveštavanja medija o tome, tako da vrlo brzo svi mogu da saznaju da je ta infrastruktura nepouzdana [32-36].

U svakom slučaju, mere zaštite moraju da budu preduzete, ali je neophodno i aktivno učešće bezbednosnih snaga koje kroz međunarodnu saradnju mogu da pronađu, istraže i kazne visokotehnoške kriminalce. Drugim rečima, ako je neki sistem hakovan to ne znači da je napad organizovan u toj zemlji, već može da dolazi iz inostranstva ili bilo kog drugog dela sveta.

Dakle, iz tog razloga je neophodna međunarodna saradnja službi koja bi pomogla da redukujemo stopu tog oblika kriminaliteta.

3. ZAKLJUČAK

Na kraju, bitno je naglasiti da se nastava na Univerzitetima obično izvodi uživo, ali da je iz razloga pandemijske krize prihvaćen i onlajn vid učenja.

Interesantno je spomenuti da je u SAD-u jedna srednja škola bila preko 10 godina onlajn sa hakerskim podzemljem i da je neko za to vreme izvlačio podatke iz date mreže i distribuirao ih dalje onima koji su bili voljni da plate za njih. Sve to je otkriveno u skorije vreme, ali je šteta bila nenadoknadiva.

Verujemo da u tom smislu i akademska zajednica Republike Srbije može da shvati koliko je dragoceno to što se čuva na računarima ili cloud serverima, te stoga treba i podići budnost o mogućim rizicima koji dolaze sa interneta. Konačno, internet je kritična infrastruktura koja nas čini zavisnim o novim tehnologijama i većina hakerskih napada se odvija upravo tim putem.

Očigledno, nivo budnosti u našoj zemlji bi trebao da bude na znatno višem nivou kako bi svi članovi društva uzeli aktivno učešće u borbi protiv visokotehnoškog kriminala. Nije reč samo o akademskoj zajednici, već o svima nama i Univerzitet je samo jedan od mogućih scenarija koji može da se desi u praksi.

4. LITERATURA

- [1] Gyula Mester, 18-21.02.2013, *Univerziteti regiona na Šangajskoj rang listi univerziteta u svetu 2012*, Proceedings of the XIX Skup Trendovi Razvoja, paper No. T1.1-1, pp. 1-5, ISBN: 978-86-78924-95-9, Maribor, Slovenija.
- [2] Gyula Mester, 07-10.03.2011, *The Evaluation of the Impact Factor of the Journal Acta Polytechnica Hungarica*, Proceedings of the TREND 2011, 15th Conference: Doctoral studies in Serbia, region and EU, pp. 70-73, ISBN 978-86-7892-323-4, Kopaonik, Serbia.
- [3] Attila Albini, Gyula Mester, László B. Iantovics, *Unified Aspect Search Algorithm*, Interdisciplinary Description of Complex Systems, Indecs, Zagreb, Croatia Interdisciplinary Society, ISSN 1334-4684, Vol. 17, No. 1-A, pp. 20-25, DOI: 10.7906/indecs.17.1.4, 2019.
- [4] Gyula Mester, 2015, *Merenje rezultata naučnog rada*, Tehnika-Mašinstvo, Belgrade, Serbia, Vol. 64, No. 3, ISSN 0040-2176, pp. 445-454.
- [5] Gyula Mester, 2011, *Academic Ranking of World Universities 2009/2010*, Ipsi Journal, Transactions on Internet Research, TIR, Belgrade, ISSN 1820 - 4503, Vol. 7, No. 1, pp. 44-47.
- [6] Gyula Mester, 23 - 26. 02. 2015, *Novi trendovi naučne metrike*, Proceedings of the XXI Skup Trendovi Razvoja: "Univerzitet u Promenama...", TREND 2015, Zlatibor, Serbia, ISBN 978-86-7892-680-8, DOI: 10.13140/RG.2.1.1754.2486, paper No. UP 1-3, pp. 23-30.
- [7] Aleksandar Rodic, Gyula Mester, 03-06.03.2013, *Control of a Quadrotor Flight*, Conference: ICIST Conference, Kopaonik, Serbia, ISBN: 978-86-85525-12-4, pp. 61-66.
- [8] Gyula Mester, May 14-16, 2015, *Modeling of Autonomous Hexa-Rotor Microcopter*, Proceedings of the IIIrd International Conference and Workshop Mechatronics in Practice and Education, MechEdu 2015, Subotica, Serbia, ISBN 978-86-918815-0-4, pp. 88-91.
- [9] Gyula Mester, Aleksandar Rodic, 01-03.03.2012, *Navigation of an Autonomous Outdoor Quadrotor Helicopter*, Proceedings of the 2nd International Conference on Internet Society Technologie and Management ICIST, Kopaonik, Serbia, ISBN: 978-86-85525-10-0, pp. 259-262.
- [10] Gyula Mester, April 16-18, 2009, *Obstacle - Slope Avoidance and Velocity Control of Wheeled Mobile Robots Using Fuzzy Reasoning*, Proceedings of the IEEE 13th International Conference on Intelligent Engineering Systems, INES 2009, Barbados, ISBN: 978-1-4244-4113-6, DOI: 10.1109/INES.2009.4924770, pp. 245-249.
- [11] Gyula Mester, July - September 2015, *Backstepping Control for Hexa-Rotor Microcopter*, Acta Technica Corviniensis - Bulletin of Engineering, Tome VIII, Fascicule 3, ISSN 2067-3809, pp. 121-125.
- [12] Gyula Mester, 07-08.05.2015, *New Trends in Scientometrics*, Proceedings of the SIP 2015, 33rd International Conference Science in Practice, Schweinfurt, Germany, pp. 22-27.
- [13] Josip Kasac, Vladimir Milic, Josip Stepanic, Gyula Mester, 9-12 December 2014, *A Computational Approach to Parameter Identification of Spatially Distributed Nonlinear Systems with Unknown Initial Conditions*, Proceedings of the IEEE Symposium on Robotic Intelligence in Informationally Structured Space RiSS

- (2014), Orlando, Florida, USA. DOI:10.1109/ IISS.2014.7009170, ISBN: 9781479944637, p. 154, Vol. 1, pp. 55-61.
- [14] Gyula Mester, *Metode naučne metrike i rangiranja naučnih rezultata*, 3-6. June 2013, Proceedings of 57th ETRAN Conference, Zlatibor, Serbia, pp. RO3.5.1-3
- [15] Aleksandar Rodic, Gyula Mester, June 6-9, 2011, *Ambientally Aware Bi-Functional Ground-Aerial Robot-Sensor Networked System for Remote Environmental Surveillance and Monitoring Tasks*, Proceedings of the 55th ETRAN Conference, Section Robotics, Society for Electronics, Telecommunications, Computers, Automatic Control and Nuclear Engineering, Banja Vrućica, Bosnia and Herzegovina, Vol. RO2.5, ISBN 978-86-80509-66-2, pp 1-4.
- [16] Gyula Mester, 2011.08.24-26, *Felsőoktatási világranglisták 2011*, Proceedings of the Informatika a felsőoktatásban 2011, Konferencia, pp. 269-277, ISBN 978-963-473-461-1, Debrecen, Hungary.
- [17] Gyula Mester, Aleksandar Rodic, *Modeling and Navigation of an Autonomous Quad-Rotor Helicopter*, e-Society Journal Research and Applications, Vol. 3, No. 1, pp. 45-53, ISSN 2217-3269, University of Novi Sad, Serbia, July 2012.
- [18] Milica D. Đekić, *Kako sačuvati kontinuitet u poslovanju uprkos cyber incidentima*, Tehnika, Vol. 70, No. 2, pp. 346-349, 2015.
- [19] Milica D. Đekić, *Cyber procedure za poslovno okruženje u Srbiji*, Tehnika, Vol. 71, pp. 471-474, 2016.
- [20] Milica D. Đekić, *The Cloud's Computing Security*, Tehnika Vol. 73, No. 2, pp. 300-304, 2018.
- [21] Milica D. Đekić, *The Internet of Things Security*, Tehnika, Vol. 72, No. 2, pp. 309-312, 2017.
- [22] Milica D. Đekić, *The Commerce Crime and Ways of Conducting a Financial Security*, Tehnika, Vol. 71, No. 5, pp. 782-786, 2016.
- [23] Milica D. Đekić, *Cyber Procedures for a Business Environment in Serbia*, Tehnika, Vol. 71, No. 3, pp. 471-474, 2016.
- [24] Milica D. Đekić, *The Internet of Things Cybersecurity Standardization*, Tehnika, Vol. 74, No. 4, pp. 603-607, 2019.
- [25] Milica D. Đekić, *The Application of Marketing for Small and Medium-sized Enterprises Competiveness Rise in the Republic of Serbia*, Tehnika, Vol. 72, No. 4, pp. 587-590, 2017.
- [26] Milica D. Đekić, *A Smart Configuration of Computer as a Prevention from Hacking and Cyber Espionage*, Tehnika, Vol. 71, No. 5, pp. 761-764, 2016
- [27] Milica D. Đekić, *How to Create Training for the IT Industry's Staffs?* Tehnika, Vol. 71, No. 4, pp. 644-647, 2016.
- [28] Milica D. Đekić, *How to Maintain a Business Continuity Despite Cyber Incidents?* Tehnika Vol. 70, No. 2, pp. 346-349, 2015.
- [29] Milica D. Đekić, *The Use of Video Detection as a Function of Traffic Safety*, Tehnika, Vol. 66, No. 3, pp.471-475, 2011.
- [30] Milica D. Đekić, *How a modern business could respond to the Phishing Attack Challenges*, Tehnika, Vol. 72, No.3, pp. 455-459, 2017.
- [31] Milica D. Djekic, Gyula Mester, *The Technological Aspects of Tor's Project*, Transactions on Advanced Research, IPSI, Belgrade, Vol. 17, No. 1, pp. 49-54, ISSN 1820-4511, January 2021.
- [32] Jelena Pisarov, Gyula Mester, *The Future of Autonomous Vehicles*, FME Transactions, Vol. 49, No. 1, pp. 29-35, ISSN: 1451-2092, UDC: 621, DOI: 10.5937/fme2101029P, 2021.
- [33] Jelena Pisarov, Gyula Mester, *The Impact of 5G Technology on Life in the 21st Century*, Transactions on Advanced Research, IPSI, Vol. 16, No. 2, I pp. 11-14, ISSN 1820-4511, July 2020.
- [34] Jelena Pisarov, Gyula Mester, 16-19.02.2020, *Rang lista fizičara Srbije*, Trend 2020, XXVI Skup Trendovi Razvoja: "Inovacije u Modernom Obrazovanju", Zbornik radova, paper No. T4.2-3, pp. 559-562, ISBN 978-86-6022-241-3, Kopaonik, Serbia.
- [35] Jelena Pisarov, Gyula Mester, December 12, 2019, *Programming the mBot Robot in School*, MechEdu Conference & Workshop 2019 (MechEdu 2019), ISBN 978-86-918815-5-9, pp. 45-48, Subotica Tech, Subotica, Serbia.
- [36] Jelena Pisarov, February 16-19, 2020, *5G i samovozeći automobili*, XXVI Skup Trendovi razvoja: „Inovacije u modernom obrazovanju”, TREND 2020, ISBN 978-86-6022-241-3, pp. 391-394, Kopaonik, Serbia.