Pametno konfigurisanje računara kao prevencija od hakovanja i cyber špijuniranja

MILICA D. ĐEKIĆ, Subotica

Stručni rad
UDC: 343.533:004.3´2
DOI: 10.5937/tehnika1605761D

U modernom poslovnom svetu, IT sistemi su često meta cyber napada, poslovnog špijuniranja i drugih informatičkih incidenata. Nemali broj današnjih softverskih alata ima i opciju za daljinski pristup drugom računaru i ta mogućnost se često koristi za izvlačenje poverljivih informacija iz sistema, kao i nadzor hakerskih napada. Kao jednu od najpouzdanijih preventivnih mera ovde, naveli bismo koncept pametnog konfigurisanja računara koji omogućava da se informacioni sistemi, u određenoj meri, zaštite od pretnji kao što su hakovanje i cyber špijuniranje. U ovom radu, planiramo da bolje objasnimo slučajeve koji se javljaju u praksi, ali i da kroz praktične savete sugerišemo kako bi realno moglo da se deluje u preventivnom smislu – kako kod kuće, tako i u poslovnom ambijantu.

Ključne reči: *cyber, hakovanje, špijuniranje, poslovanje, prevencija, itd.*

1. UVOD

Savremena informatička praksa je pokazala da su mnogi računari – bilo kod kuće, bilo u poslovnom okruženju – izloženi raznim vidovima cyber rizika i pretnji. Ono što je svakako od vitalnog značaja za ekonomiju jedne zemlje je rizik po poslovne računare. U današnje vreme nije redak slučaj da se preko cyber tehnologija izvlače poverljive i vredne informacije iz nekog preduzeća ili da se koriste najnovije verzije hakerskih alata za upade i nanošenje štete informacionoj infrsatrukturi organizacije.

Za svrhe hakovanja i cyber špijuniranja se obično koriste niskobudžetna rešenja i razni alati koji daju mogućnost daljinskog pristupa drugom računaru. Ovakvi programi su ili vrlo jeftini ili čak potpuno besplatni, pošto njihove open-source varijante mogu bez problema da se skinu sa interneta. Drugim rečima, čini se da nikada nije bilo lakše upasti nekome u računar, izvući informaciju od značaja ili čak naneti štetu u informatičkom smislu.

Ono što je potrebno da se dublje razume na ovom nivou je sam problem hakovanja, kao i izazovi koji su povezani sa tom cyber pretnjom današnjice, zatim posledice koje sa sobom nosi cyber špijuniranje, kao i potencijalni gubici koje ta vrsta aktivnosti može da nanese u poslovnom svetu i, na kraju, da za sve to postoje određene preventivne mere koje utiču na smanjenje stepena rizika i koje su u ovom slučaju predstavljene kao koncept pametnog konfigurisanja računara čiji je cilj da odbije svaki vid daljinskog pristupa IT sistemu.

2. HAKOVANJE KAO CYBER PRETNJA DANAŠNJICE

Hakerska zajednica je široko rasprostranjen skup ljudi, servisa i alata koji postoji na internetu. [2] Hakerske grupe funkcionišu na prilično ilegalan način i dobro su poznate po pružanju svojih proizvoda i usluga na crnom tržištu. Pre nekoliko decenija, hakovanje je podrazumevalo upad u nečiji računar, pravljenje izmena u istom i potom napuštanje datog sistema. Danas je većina hakerskih napada finansijski motivisana i inteligentno koordinisana.

Grupe koje se bave cyber kriminalom postaju visoko organizovane i vrlo sofisticirane. Hakovanje ne podrazumeva više motivisane pojedince koje vodi želja za ozloglašenošću i potreba da učine nešto spektakularno, već je pre reč o načinu zarađivanja novca pomoću kriminalnih aktivnosti. Cyber kriminalci koriste forume, diskusione grupe i neke Darknet komunikacione kanale za uspostavljanje kontakta i održavanje komunikacije između sebe i to sa ciljem da ponude svoje proizvode i usluge ili, pak, organizuju neku kriminalnu ili terorističku akciju. Današnji hakeri su vrlo vešti u svom poslu, što otežava posao bezbednosnim službama.

Adresa autora: Milica Đekić, Vase Pelagića 39a, Subotica

Rad primljen: 29.12.2015.
Rad prihvaćen: 23.02.2016.

Najpoznatiji primeri hakovanja obuhvataju probleme vezane za izazivanje ekonomske i vojne štete određenim državama ili organizacijama. Hakovanje, samo po sebi, je pretnja u cyber smislu i kao takva podrazumeva nečiju nameru da prouzrokuje štetu nekome drugome. Ljudi današnjice su dobro upoznati sa hakerskim napadima kao što su ulaz u podatke, krađa identifikacionih i kreditnih kartica, sabotaža kritične infrastrukture, blokiranje satelitskih komunikacija, itd.

Na ovom nivou, potrebno je da se shvati postojanje malicioznih subjekta koji ne dozvoljavaju da se bezbrižno provodi vreme u cyber prostoru. S druge strane, pod pojmom kritične infrastrukture se podrazumeva nešto što je vitalno, odnosno strateški značajno za neku zemlju. To je praktično svaka infrastruktura koja koristi cyber tehnologije i može da obuhvati elektroenergetske sisteme, telekomunikacione mreže, vladine objekte i sve ostalo čiji kvar bi mogao da ima ozbiljne ili čak katastrofalne posledice po tu zemlju ili naciju.

Suštinski značajan detalj ovde je da se ta infrastruktura oslanja na cyber tehnologije, što je čini vrlo ranjivom na svaki vid hakerskog napada. Cyber napadi mogu da potiču od inteligentnih pojedinaca, hakerskih organizacija ili čak grupa finansiranih od strane neke države. Nije redak scenario da ponekad vlada jedne države ohrabruje svoje cyber kriminalce da napadnu neku drugu državu. Tipičan primer za to su hakovanja komunikacionih mreža, bankovnih sistema i zdravstvenih organizacija u SAD-u, koja dolaze iz Rusije ili Kine. [2, 10]

U realnom životu, hakeri nisu samo osobe koje provode mnogo vremena za računarom i koje koriste hakerske alate kako bi upali u nečiji računar. Oni su često vrlo talentovani pojedinci koji su u stanju da razviju maliciozni kod u smislu visoko-inteligentne malware aplikacije, koja može da izvede sabotažu ili špijuniranje nečijeg informacionog sistema koji sadrži poverljive podatke.

3. PROBLEMI CYBER ŠPIJUNIRANJA

Pod pojmom cyber špijuniranja se u praksi obično navodi scenario koji podrazumeva da se određena spyware aplikacija ubaci u ciljani računar i da se softverskim putem izvlače podaci iz cyber jedinice ili mreže. [5, 10] Međutim, ono što mi analiziramo u ovom radu je vid elektronske špijunaže koji omogućava da se putem daljinskog pristupa nekom IT sistemu vidi šta se dešava u njemu. Daljinski pristup računaru omogućavaju alati koji imaju tu opciju, a mogu da budu hakerskog tipa ili da služe za daljinsku administraciju.

U svakom slučaju, bilo koji alat koji ima mogućnost daljinskog pristupa je prikladan za ulaz u nečiji računar i praćenje situacije u istom. Najčešći problem u praksi je što većina savremenih hakerskih alata koji su besplatni i funkcionišu po principu otvorenog koda nudi i mogućnost daljinskog pristupa. [2] To znači da primenom jednog istog alata može da se izvrši i hakovanje i cyber špijuniranje željenog IT sistema.

Ono o čemu treba u ovom slučaju razmišljati su mogućnosti odbijanja daljinskog pristupa malicioznim subjektima kao mera prevencije od hakerskih napada i intruderskog delovanja. U ovom članku planiramo da navedemo primere iz prakse koji bi trebali da pojasne kako je moguće delovati preventivno u odnosu na navedene cyber pretnje, odnosno smanjiti rizik u cyber okruženju.

Ponekad je zbog prirode posla neizvodljivo isključiti opciju za daljinski pristup, jer je iz praktičnih razloga potrebno da neko može da vidi šta se dešava u nečijem računaru. U tom slučaju, ove preventivne mere ne mogu da se primene. Međutim, ako opcija daljinskog pristupa nije zahtevana za rad nekog računara ili mreže, tada je preporučljivo i da se ne koristi. U ovom radu, upravo dajemo mogući scenario delovanja vezan za konfigurisanje računara tako da opcija daljinskog pristupa bude isključena i time povećan stepen zaštite kada su hakerski napadi i daljinski nadzor IT sistema u pitanju.

4. KAKO PAMETNO KONFIGURISATI RAČUNAR?

Pametna konfiguracija računara je moguća zahvaljujući pametnom odabiru opcija podešavanja računara. U ovom članku, planiramo da predstavimo kako neka podešavanja mogu da se izvedu pod Windows XP operativnim sistemom, koji se prilično često primenjuje u tehničkoj praksi.

Ono što želimo da pokažamo kroz ove primere je da se u svega nekoliko koraka može konfigurisati ceo sistem i na taj način izbeći realni problemi u praksi. Moguća primena ovog pristupa bi mogla da se nađe pri prevenciji od hakerskih napada i cyber špijuniranja.

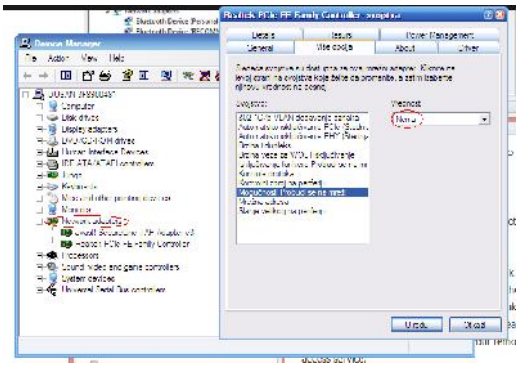
Ono što je svakako cilj u cyber okruženju – kako kod kuće, tako i na poslu – je da se spreči da neko neovlašćeno ostvari daljinski pristup IT jedinici i time ugrozi sigurnost tog računara, ali i čitave mreže. Većina današnjih alata koji omogućavaju daljinski pristup cyber sistemu su izuzetno pristupačni i normalno funkcionišu dok je korisnik online.

Znači, dok je ciljani računar na mreži, maliciozni subjekt i može da prati šta se dešava na njegovom računaru. U slučaju da korisnik nije na internetu, većina modernih hakerskih i sličnih alata postaje bespomoćna.

Međutim, ono što nas ovde zanima je da li postoji mogućnost da daljinski pristup nekom računaru bude

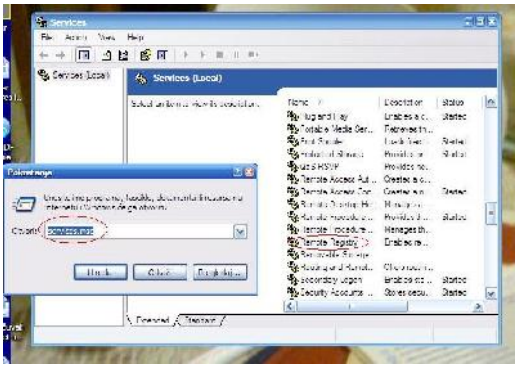
onemogućen, bio on na internetu ili ne. Ovo istraživanje pokazuje da je praktično moguće podesiti računar tako da njegove opcije za daljinski pristup budu onesposobljene. Treba napomenuti da ovi saveti ne mogu da se primene ako postoji realna potreba da neki računar bude dostupan i daljinskim putem. Dalje, navodimo neke primere iz prakse koji ukazuju kako se sprovode određene mere zaštite u tom smislu.

Prvi korak koji treba ovde učiniti je da se pristupi Device Manager podešavanjima, što se u slučaju Windows XP operativnog sistema postiže tako što se iz Start menija izabere opcija Run i tamo ukuca devmgmt.msc. Potom se dobija Device Manager prozor i tu se odabere odgovarajući kontroler u okviru opcije Network Adapters. Posle duplog klika na taj kontroler se pristupa njegovim podešavanjima i zatim se odavere funkcija Advanced. U okviru te funkcije se selektuje svojstvo Wake-on-LAN i ono se podesi na Disabled. Prikaz ove procedure je dat na slici 1.



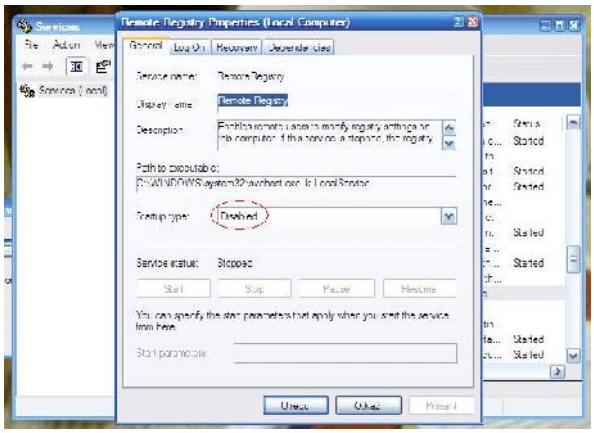
Slika 1 - Postupak isključivanja daljinskog pristupa preko Network Adapters opcije

Da bi se dalje nastavilo sa konfigurisanjem IT sistema, potrebno je u okviru Start menija opet odabrati opciju Run, ali ovaj put ukucati services.msc. Na taj način se dobija pristup prozoru Services. U okviru ovog prozora se odabere servis Remote Registry. Cilj ove procedure je da se odbije svaki vid daljnskog pristupa koji ide preko daljnskih registra. Prikaz ovog postupka je dat na slici 2.



Slika 2 - Prikaz odabira opcije Remote Registry

U okviru opcije Remote Registry se potom u okviru kartice General izabere funkcija Disabled u smislu karakteristike Startup Type. Prikaz ovog koraka je dat na slici 3.



Slika 3 - Finalni korak u okviru Remote Registry podešavanja

Kroz ovaj kratak pregled iz prakse su navedeni samo neki primeri pametnog konfigurisanja sistema u smislu odbijanja daljinskog pristupa računaru. Predstavljeni su ključni primeri koji i realno mogu da zaštite računar od eventualnih upada koji su mogući zahvaljujući savremenim softverskim rešenjima sa daljinskim pristupom.

5. DISKUSIJA

Nastojanja ovog rada su usmerena na doprinos oblasti cyber menadženta. U ovom članku analiziramo vrlo značajan problem iz prakse i sugerišemo rešenja koja bi mogla da dobiju i realnu primenu. Sa tačke gledišta menadženta cyber bezbednosti, ovde izloženi problem ima svoj stručni značaj, jer otvara mogućnosti preventivnog delovanja.

Preventivno delovanje u praksi je veoma važno zbog mogućnosti da se izbegne da se neka situacija uopšte dogodi. U ovom članku se konkretno diskutuje prevencija od hakerskih napada i cyber špijuniranja primenom postupka odbijanja daljinskog pristupa računaru.

Ova procedura je sprovodiva samo u slučaju da ne postoji realna potreba da opcija daljinskog pristupa bude aktivirana na datom IT sistemu. U suprotnom slučaju, navedene mere mogu da se pokažu kao korisne za rešavanje praktičnih problema.

6. ZAKLJUČAK

Cilj ovog rada je da doprinese podizanju svesti u našoj zemlji kada je oblast cyber bezbednosti u pitanju. U ovom slučaju su izloženi neki primeri iz prakse i date su smernice kako da se isti prevaziđu.

Na taj način se povelo računa o potrebama u cyber okruženju, ali i ukazalo na korisne savete koji mogu da pomognu prilkom rešavanja praktičnih situacija.

LITERATURA

[1] Lillian Ablon, Martin C. Libicki, Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data*, Sponsored by Juniper Networks, 2014.

[2] Kevin Beaver, Peter T. Davis, *Hacking Wireless Networks for Dummies*, Wiley Publishing, 2005.

[3] Michael K. Bergman, *The Deep Web: Surfacing Hidden Value*, White paper, 2000.

[4] Scott Charney, *Rethinking the Cyber Threat: A Framework and Path Forward*, Microsoft, 2009.

[5] Vincenzo Ciancaglini, Marco Balduzzi, Max Goncharov, Robert McArdle, *Deepweb and Cybercrime*, A Trend Micro Research Paper, 2013.

[6] Stephen Cobb, *Four basic and effective defensive measures against cybercrime*, Tech Brief, ESET Business Solutions, 2014.

[7] *Cyber Threats to National Security*, Symposium Five: Keeping the Nation's Industrial Base Safe From Cyber Threats, 2011 CACI International Inc, 2011.

[8] Xinwen Fu, Zhen Ling, Wei Yu, Junzhou Luo, *Cyber Crime Scene Investigations (C2SI) through Cloud Computing*, 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops, 2010.

[9] Matthew Gardiner, *The Critical Incident Response Maturity Journey*, White Paper, EMC, 2013

[10] Alex Roney Mathew, Aayad Al Hajj, Khalil Al Ruqeishi, *Cyber Crimes: Threats and Protection*, 201O International Conference on Networking and Information Technology, 2010.

SUMMARY

A SMART CONFIGURATION OF COMPUTER AS A PREVENTION FROM HACKING AND CYBER ESPIONAGE

In a modern business world, IT systems are frequently exposed to attacks, business espionage and the other cyber incidents. Many software tools of nowadays got a remote access option to another computer which is suitable for a cyber espionage as well as a hacker's attack monitoring. As one of the most reliable measures here, we would mention a smart configuration of computer which offers a protection from these cyber threats. In this article, we plan to explain the cases that exist in the practice and provide some useful tips which would suggest how to prevent cyber incidents at home as well as within a business environment.

Key words: *cyber, hacking, espionage, business, prevention, etc.*