Nadzor nad informatičkim servisima u bolničkom informacijskom sustavu

Dražen Pomper[1], Mario Hogge[2], Goran Delić[3], Sara Pomper[4]

[1]*Opća bolnica Varaždin, Odjel za informatiku, Varaždin*
[2]*Opća bolnica Varaždin, Odjel za informatiku, Odsjek za medicinsku administraciju, Varaždin*
[3]*Opća bolnica Varaždin, Odjel za informatiku, Varaždin*
[4]*FOI Varaždin, studentica IV godine, Varaždin*

E-pošta: drazen.pomper@obv.hr

Informacijska i komunikacijska tehnologija u zdravstvenom prostoru imaju svoju upotrebnu vrijednost jer unapređuju poslovne procese i dodana su vrijednost medicinskoj struci. Cjelovitost rješenja čini tehnologija, programska rješenja i ljudski potencijal. Osigurati dostupnost informacija zdravstvenom osoblju i korisnicima zdravstvene usluge jedna je od osnovnih zadaća informatike u zdravstvu. Podatke se ne smije izgubiti, ne smije ih se izložiti neautoriziranom pristupu i mora ih se uvijek učiniti dostupnim ovlaštenim osobama. Zato je potrebno načiniti sigurnosnu strategiju u domeni posla informatičke struke. Aktivirani procesi autentifikacije i autorizacije garantiraju sigurnost i povjerenje u sustav, jer se temelje na činjenici zaštite ugleda i reputacije zdravstvene ustanove. Administrator aplikacije postaje važan dispečer stalnih promjena u raspodjeli ljudskog potencijala koji radi prema sistemu 24x7. I sam sustav može svojim protokolima provoditi automatiziranu funkciju delegiranja prava dozvoljavajući ulaz u proces liječenja jedne epizode liječenja putem elektroničkih radnih naloga. Jedna od nužnih opcija je da kontrolira opravdan pristup zdravstvenim podacima osobama koje nisu aktivne u procesu liječenja, odnosno onima koji trenutno ne sudjeluju u epizodi liječenja. Primjena Uredbe za zaštitu osobnih podataka, GDPR (General Data Protection Regulation) osim što deklarativno promovira odgovornost kao poslovnu, moralnu i ljudsku kategoriju, prvenstveno otvara područje zaštite poslovnih sustava koji se temelje na novim informatičko-telekomunikacijskim tehnologijama s temom dostupnosti. Takav stav osigurava povjerenje u uslugu i zdravstveni sustav što moraju osigurati kompetentni, sposobni i dobro educirani i ekipirani informatičari koji danas upravljaju informatičkim sustavom u zdravstvenom prostoru RH.

Ključne riječi: bolnički informacijski sustav; nadzor nad servisima

Uvod

Informatička i komunikacijska tehnologija u zdravstvenom prostoru imaju svoju upotrebnu vrijednost jer unapređuju poslovne procese i dodana su vrijednost medicinskoj struci. Cjelovitost rješenja čini tehnologija, programska rješenja i ljudski potencijal. Informatičari imaju osnovnu zadaću osigurati dostupnost informacija zdravstvenom osoblju i korisnicima zdravstvene usluge. Podaci se ne smiju izgubiti u digitalnom svijetu, ne smiju se izložiti neautoriziranom pristupu i moraju uvijek biti dostupni u zdravstvenom poslovnom sustavu. Zato se postavlja čitava sigurnosna strategija u domeni posla informatičke struke. Osim povijesne važnosti praćenja stanja bolesnika, danas je informatički sustav u potpunosti integriran, odnosno pojam interoperabilnosti je u potpunosti aktiviran. Imamo informatičke sustave na različitim platformama i tehnologijama i svi međusobno komuniciraju. Osnovni modul BIS (Bolnički informatički sustav) integriran je sa LIS-om (Laboratorijski sustav), RIS-om (Radiološki sustav), Delphyn-om (Transfuzijski sustav), Mikrobiološkim sustavom, PIS-om (Poslovni informatički sustav), Kuhinjom što čini jednu kompaktnu i složenu strukturu, gdje je pristup podacima baziran na autoriziranom sustava prava, i moraju biti dostupni u svim segmentima poslovnog procesa Kontrolira se pristup podacima, jer

sistematizirani i obrađeni medicinski podaci čine medicinsku poslovnu informaciju, najvažniji resurs u poslovnom procesu. Aktivirani procesi autentifikacije i autorizacije garantiraju sigurnost i povjerenje u sustav, jer se baziraju na činjenici zaštite ugleda i reputacije zdravstvene ustanove. Administrator aplikacije postaje važan dispečer stalnih promjena u raspodjeli ljudskog potencijala koji rade u sistemu 24x7. I sam sustav može svojim protokolima raditi automatiziranu funkciju delegiranja prava, jer dozvoljava ulaz u proces liječenja jedne epizode liječenja putem elektroničkih radnih naloga. Jedna od nužnih opcija sustava je da kontrolira opravdan pristup zdravstvenim podacima za osobe koje nisu aktivne u procesu liječenja, odnosno da da im nije trenutno otvorena epizoda liječenja.

No i primjena Uredbe za zaštitu osobnih podataka, GDPR (General Data Protection Regulation) osim što deklarativno promovira odgovornost kao poslovnu, moralnu i ljudsku kategoriju, prvenstveno otvara područje zaštite poslovnih sustava baziranim na novim informatičko telekomunikacijskim tehnologijama sa temom dostupnost. Dostupnost informacijama je neupitna i konstanta kategorija i prvenstveno se odnosi na besprijekoran tehnološki rad informatičkog sustava.

Takav stav osigurava povjerenje u uslugu i zdravstveni sustav. A to moraju osigurati kompetentni, sposobni i dobro educirani i ekipirani informatičari koji danas upravljaju informatičkim sustavom u zdravstvenom prostoru RH (1).

Nadziranje i kontrola postupaka u poslovnom sustavu

Kao i kod obrade zdravstvenih podataka za sve ostale tehnološke podržane aktivnosti u svim djelatnostima postoje mehanizmi praćenja aktivnosti svih korisnika u sustavu. Svako računalo ima svoj jedinstveni broj u informatičkom svijetu, pored MAC adrese tu je i IP adresa koja u virtualnom svijetu jednoznačno identificira korisnika usluge. Tu su korisničko ime i zaporka, vjerodajnice koje omogućuju korisniku upotrebu svih raspoloživih resursa u informatičkom okruženju. Strategija upotrebe korisničkog imena i zaporke u digitalnom svijetu izazvala je potrebu „multi-factor authentication“, jer snaga i kvaliteta zaporke ovisi i o korisniku i nadzornom sustavu. Potvrditi da se korisnik stvarno prijavljuje u sustav još jednom kolateralnom identifikacijom je nužnost. Zato je dobra ideja prijava u sustav putem mobitela, RFID kartice i digitalnog certifikata. Postoje resursi operativnog sustava i korisnički programi dedicirani za obavljanje svakodnevnih poslova. Dobro izbalansirane vjerodajnice štite korisnika od zloupotreba, jer se danas u digitalnoj transformaciji svih poslovnih procesa kolateralno pojavljuju i razne maliciozne aktivnosti. Zbog toga djelatnici računskog centra u dijapazonu svojih poslovnih aktivnosti primjenjuju tehnike digitalne forenzike i nadzora informacijskog sustava da bi informacijska sigurnost omogućila nesmetan i kontinuiran rad poslovnog sustava koji se temelji na informatičko komunikacijskim tehnologijama (2).

Neracionalno korištenje web prostora ima za direktnu posljedicu iznimno povećanu mogućnost aktivacije bilo koje vrste malicioznog koda. U konačnosti za informatički sustav sa kojim se upravlja optimalno, gdje je uspostavljen nadzor i kontrola, primjerena edukacija na temu informacijska sigurnost svih djelatnika, može se računati na stabilnost i pouzdanost informatičkog sustava. U protivnom bilo kakva nekontrolirana aktivnost uzrokuje u najmanjoj mjeri usporeni rad sustava, sa tendencijom potpunog zastoja rada poslovnog sustava.

Kontrolu prometa rade vrlo sofisticirani informatički uređaji sa programima posebne namjene. Za te namjene koristimo vatrozid (*eng. firewall*), antivirusni program i program za analizu prometa na mreži.

Antivirusni program je softver koji se koristi za zaštitu, identifikaciju i uklanjanje računalnih virusa, kao i drugih štetnih programa koji mogu uzrokovati probleme u korištenju računala ili oštetiti podatke. Dobar antivirusni program koji se može koristiti (Sophos, NOD32 ili Windows defender i drugi) instalira se na sva računala i poslužitelje, te se mora redovito dnevno ažurirati sa najnovijim antivirusnim definicijama. Ključna je pojava nove generacije antivirusnog programa koji se baziraju na tehnologijama umjetne inteligencije, nema antivirusnih definicija i svakodnevnog spuštanja datoteka preko interneta na lokalnu mašinu ili poslužitelj. Namjera je jasna, mada na sreću danas su u okviru antivirusnih programa prava više namjenska sigurnosna rješenja velike moći sigurnosne prevencije. Cilj je eliminirati vrijeme od pojave prijetnje u web prostoru pa do vremena kada službena antivirusna industrija odgovori adekvatno na pojavu prijetnje. Iskustvo nas uči da „0-day exploit“ i rješenja na „darkwebu“ nisu optimalna rješenja u ozbiljnom poslovnom svijetu. Zato su nužna rješenja nove generacije. Već danas.

Vatrozid (*engl. firewall*) je mrežni sigurnosni uređaj čija namjena je filtriranje mrežnog prometa tako da se stvori sigurnosna zona, a program koji želi pristupiti internetu mora imati dopuštenje vatrozida. Sustav služi da se zaštitimo od neautoriziranog pristupa u informatički sustav, da se netko izvan ustanove ne može spojiti na mrežu bolnice, osim onih koji imaju dopuštenje. Dobro je imati u konfiguraciji dva uređaja tipa Cisco ASA Firewall-a, zbog toga ako jedan prestane raditi da drugi odmah preuzima njegovu ulogu. Ista logika je i kod upravljanja poslužiteljima, preklopnicima, UPS-ima. Kontrolirana redundancija na nivou fizičke opreme informatičkog sektora ima svoju cijenu, ali i opravdanje.

Kontrola prometa na mreži ostvaruje se upravo preko dva Cisco ASA Firewalla na koje je instaliran FirePOWER modul, koji se licencira godišnje. Upravljački alat Cisco Firepower Management Center nam omogućuje cjelovito i jedinstveno upravljanje vatrozidima, kontrolu aplikacija, prevenciju upada, filtriranje URL-ova i naprednu zaštitu od zlonamjernog softvera kao i napredno izvještavanje o upotrebi interneta i različitim tipovima otkrivenih prijetnji za sigurnost računalnog sustava. [3]

Instaliran je na virtualnu mašinu (VMWare). Svi korisnici koje možemo nadzirati moraju biti prijavljeni na domenu, Microsoft AD. Za UNIX svijet sve je identično, ima i komparativnih prednosti.

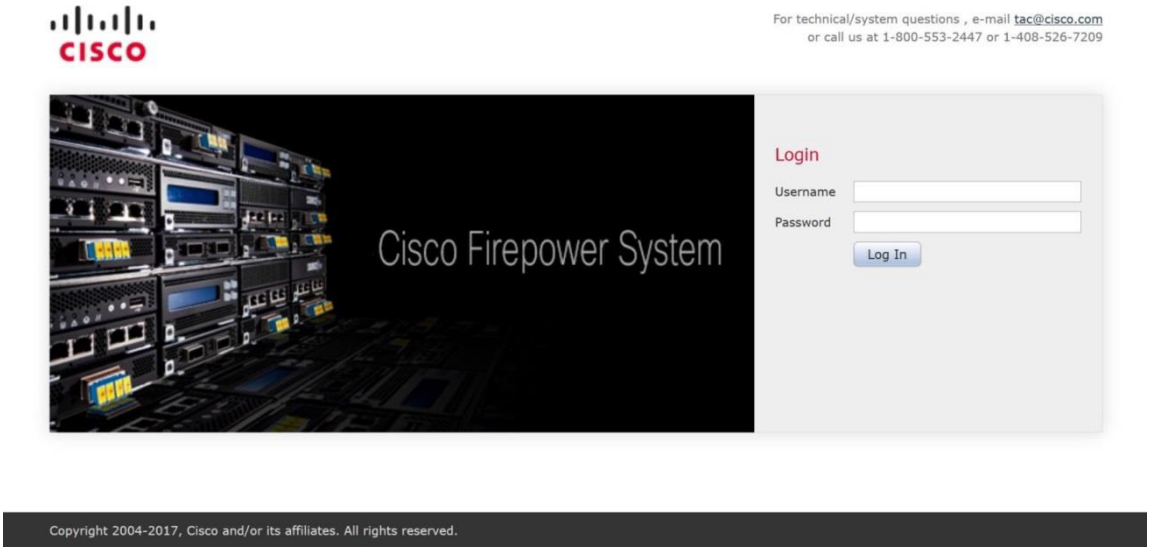
Osnovne značajke alata Cisco Firepower Management Center

Osnovne značajke alata Cisco Firepower Management Center su:

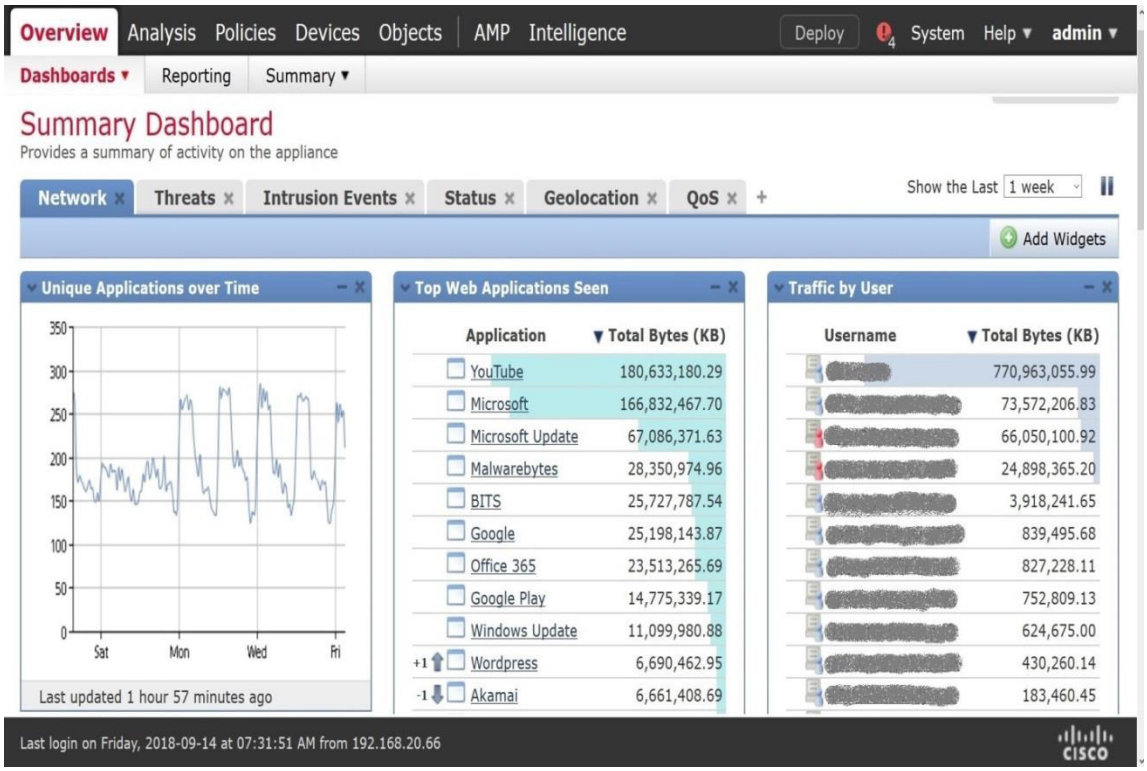
- Centralizirano upravljanje – olakšano upravljanje događajima i pravilima za mrežna sigurnosna rješenja
- Cjelovita vidljivost mreže – možemo vidjeti korisnike, „hostove“, aplikacije, datoteke, mobilne uređaje, virtualna okruženja, prijetnje i ranjivosti koje postoje u mreži koja se stalno mijenja „ne može se zaštititi ono što se ne može vidjeti“

- Upravljanje prijetnjama u realnom vremenu – kontroliranje pristupa mreži, kontroliranje aplikacije i obrana od napada
- Sigurnosna automatizacija – upravljački centar automatski povezuje sigurnosne događaje s ranjivostima u našem okruženju, to određuje prioritete napada tako da se mogu lako vidjeti događaji koji se trebaju istražiti, također preporučuje uspostavljanje sigurnosnih pravila
- „Threat Intelligence Director“ – korištenje sučelja industrijskih standarda, crpi inteligenciju iz više izvora i zatim olakšava odgovarajuće mjere praćenja i suzbijanja prijetnji

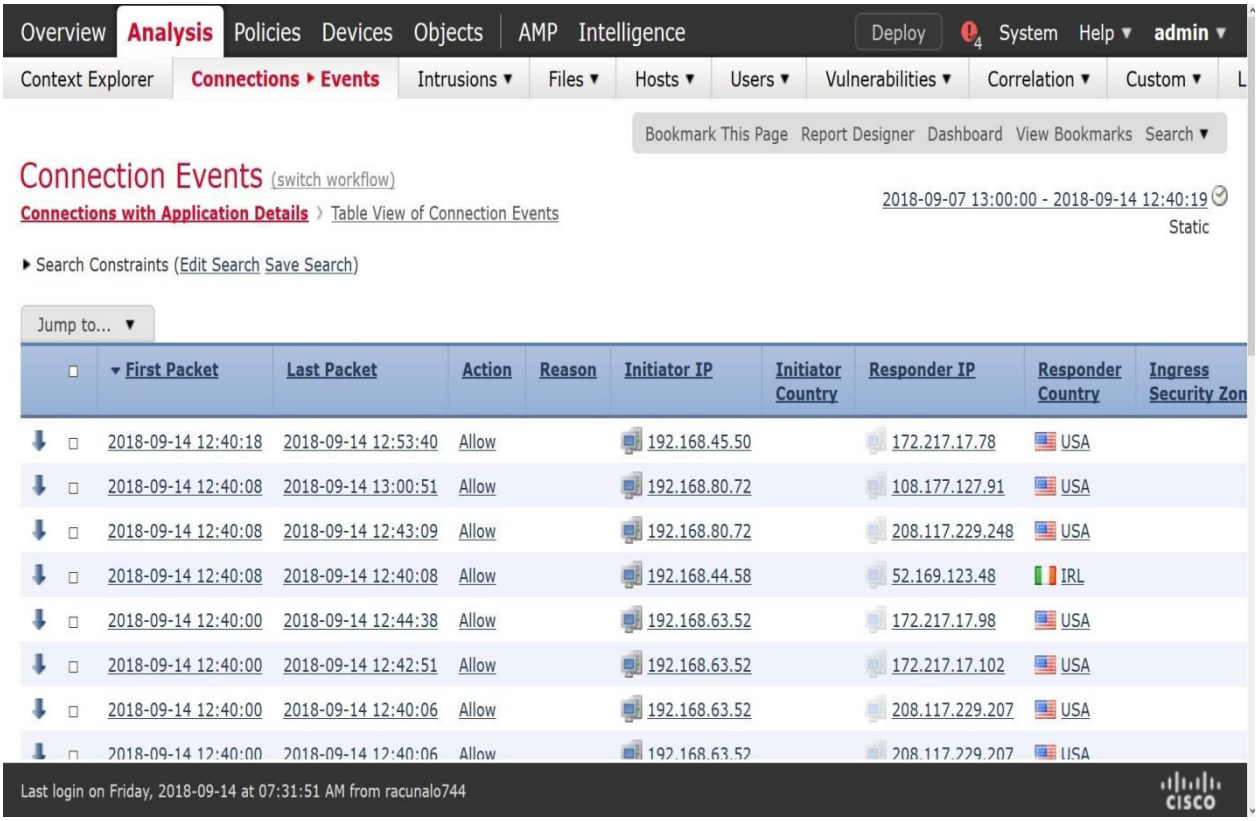
Kontrola prometa i rada na web prostoru je danas neophodna aktivnost jer, osim socijalnog inženjeringa, danas su u prometu i druge maliciozne aktivnosti, programi koji zaključavaju datoteke na računalu, uništavaju poslovne informacije, krađa intelektualnog vlasništva i važnih poslovno komercijalnih informacija, te mnoge druge aktivnosti sa tamne strane poslovanja u digitalnom svijetu. Uvodimo pojam preventivna digitalna forenzika, skup postupaka i alata koji informatičarima zaduženim za sigurnost informatičkog sustava daju mogućnost analize ponašanja korisnika kod upotrebe poslovnog sustava i na temelju analize preporučiti poslovodstvu kvalitetnu promjenu korporacijskih pravila ponašanja u internetskom prostoru. Informatička tehnologija daje egzaktne smjernice kako preventivno odraditi organizacijske aspekte s ciljem eliminacije sigurnosnih prijetnji koje se mogu pojaviti zbog nedovoljno kontroliranog ponašanja u internetskom prostoru korisnika poslovnog sustava. U daljnjem kontekstu prikazani su grafikoni i tablice iz kojih se mogu vidjeti aktualni procesi u mrežnom prometu. Na temelju njih jasno se mogu donositi sigurnosne smjernice koje osiguravaju stabilnost poslovnog sustava. Slijedi niz primjera nadziranja sustava u OB Varaždin.



Slika 1. Program za nadzor korištenja informatičkog sustava - web aktivnosti



Slika 2. Sadržaj ekrana komandne ploče: pregled i nadzor prometa u vremenu i prostoru



Slika 3. Kontrola kretanja paketa u mreži, izvor, količina, vrijeme

Izvještajni sustav Cisco Firepower Management Center

Tablica 1. Analiza vrsta i broja datoteka koje kruže našom mrežom. Najveći broj datoteka je tipa MSCAB, Microsoft-ove komprimirane datoteke (Windows update)

FILES SEEN MOVING AROUND THE NETWORK

TYPE	COUNT
MSCAB	110,498
RAR	33,655
PDF	8,983
MSEXE	3,050
NEW_OFFICE	2,189

Tablica 2. Rang lista aplikacija preko kojih dolaze prijetnje zlonamjernog koda te točan broj napada

APPLICATIONS ASSOCIATED WITH ATTACKS

APPS ASSOCIATED WITH LOWER IMPACT EVENTS	COUNT
Internet Explorer	1,204
Web browser	143
Chrome	15
Firefox	3
Skype Auth client	2

Tablica 3. Tipovi napada na mrežu odnosno njihovu klasifikaciju i broj - najveći broj odnosi se na detekciju nekih nestandardnih protokola i događaja

RELEVANT ATTACKS CARRY THE FOLLOWING RISKS

CLASSIFICATION	COUNT
Detection of a Non-Standard Protocol or Event	1,213
Web Application Attack	102
Misc Activity	37
Attempted Administrator Privilege Gain	4
Attempted Information Leak	3

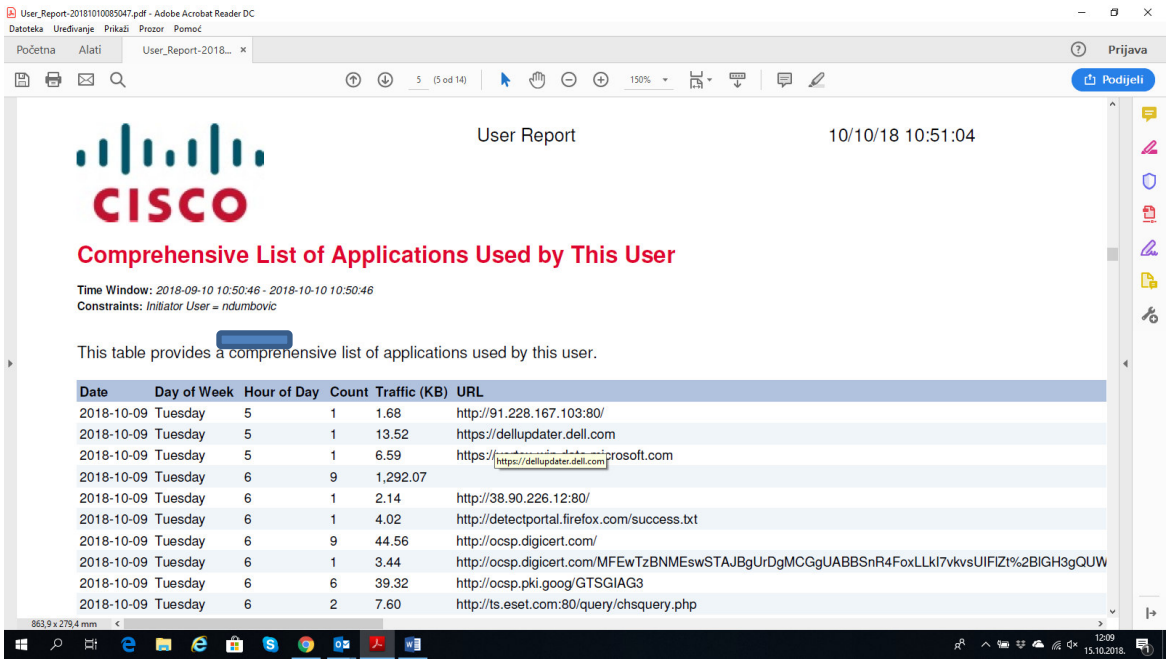
Tablica 4. Rang lista upotrebe aplikacija, broj pristupa, utjecaj rizika upotrebe, ocjena produktivnosti i količina podataka u transferu u vremenskom periodu

HIGH BANDWIDTH APPLICATIONS

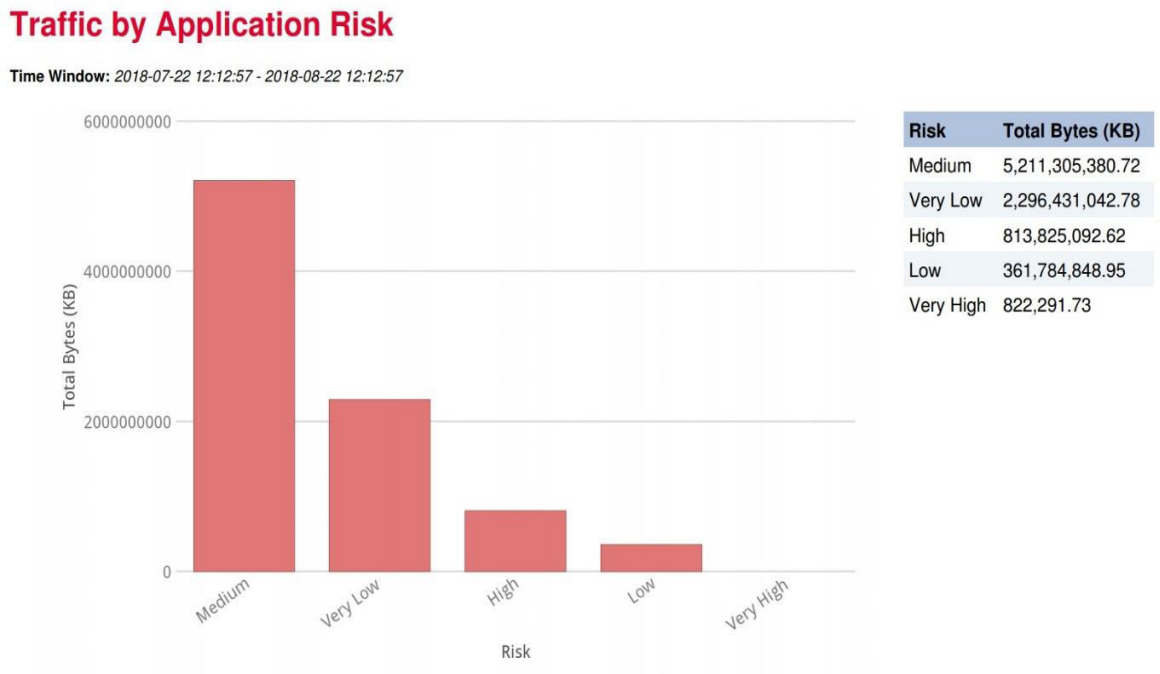
APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
YouTube	462,087	High	Very Low	764,791.67
Microsoft Update	172,095	Medium	Low	193,024.80
MPEG	3,679	Low	Medium	59,330.57
MP4	2,170	Very Low	Medium	10,686.27
Netflix stream	447	Very Low	Very Low	3,775.25

Tablica 5. Rang lista korisnika koji troše najviše podatkovnog prometa prema korisničkom imenu

Tablica 6. Izvještaj po korisniku: što koristi na webu: aplikacije, preglednike, koje stranice, ulazne sigurnosne prijetnje i konekcije

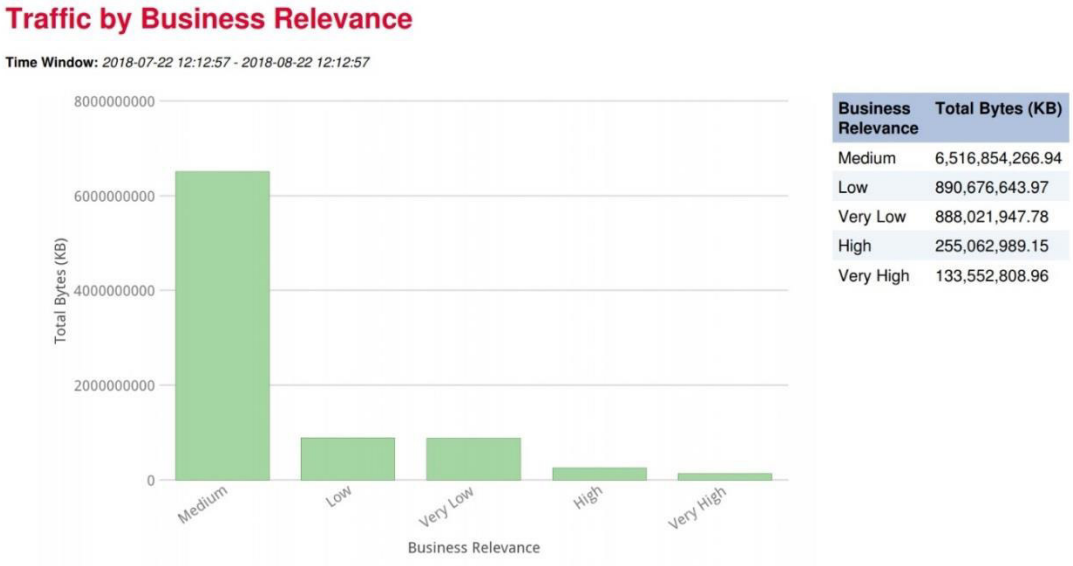


Tablica 7. Podatkovni promet prema riziku primjene



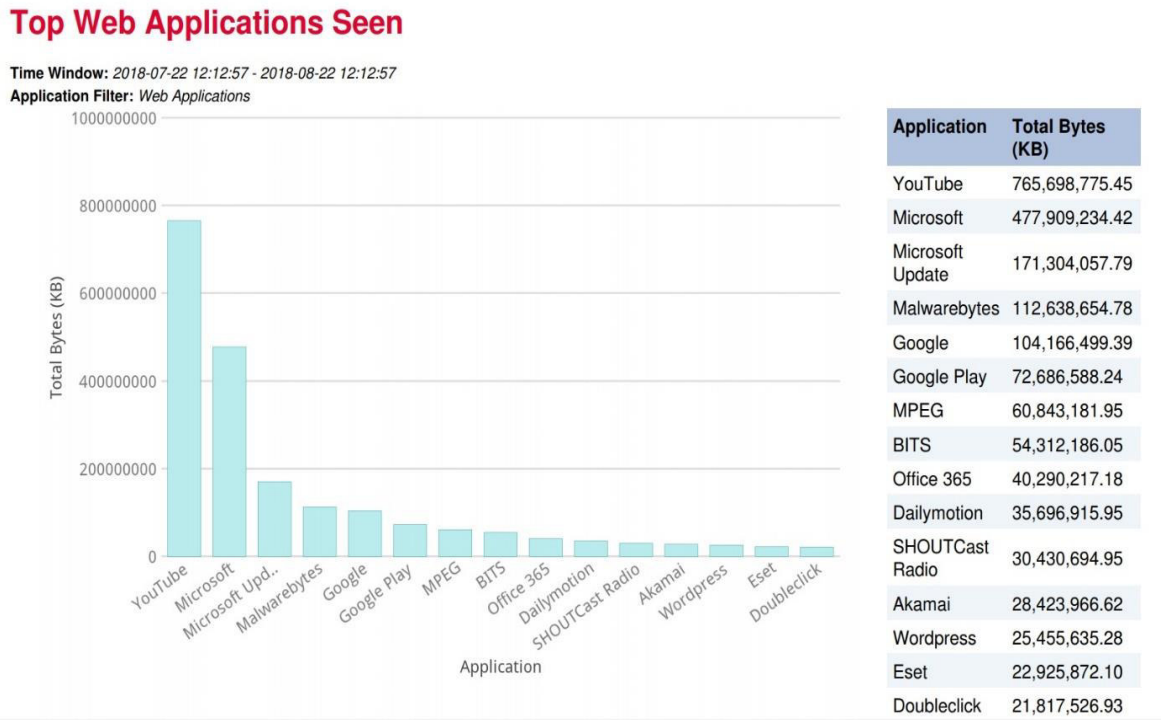
Risk	Total Bytes (KB)
Medium	5,211,305,380.72
Very Low	2,296,431,042.78
High	813,825,092.62
Low	361,784,848.95
Very High	822,291.73

Tablica 8. Podatkovni promet prema važnosti poslovanja - najveći ostvareni promet je od srednjeg značaja za poslovanje



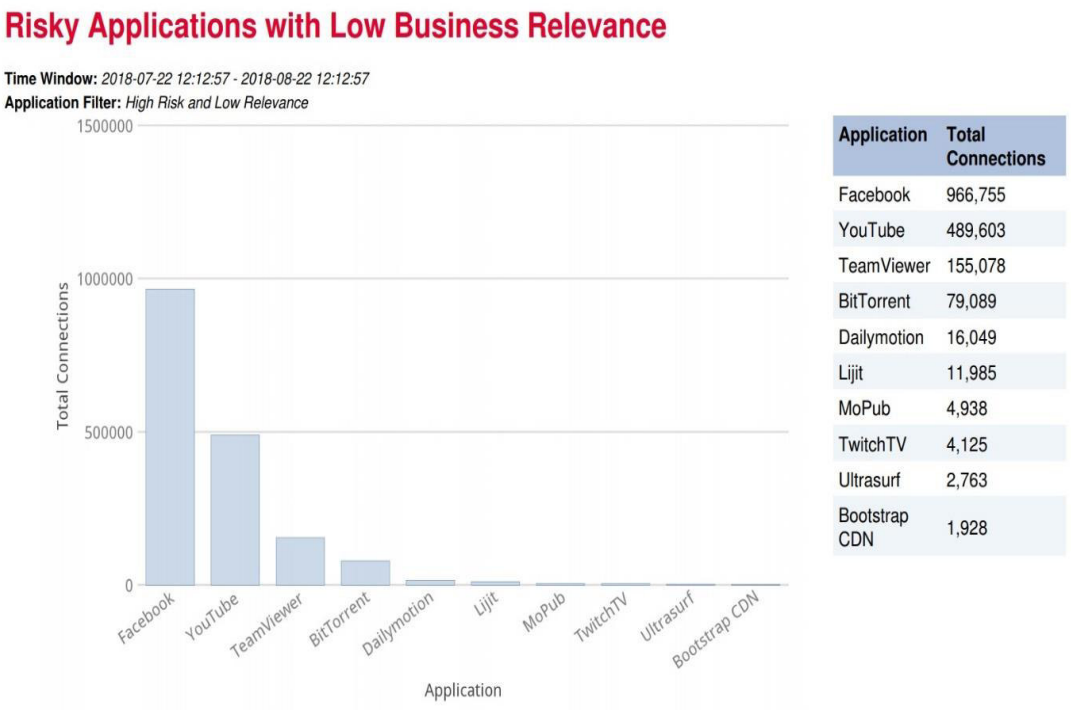
Business Relevance	Total Bytes (KB)
Medium	6,516,854,266.94
Low	890,676,643.97
Very Low	888,021,947.78
High	255,062,989.15
Very High	133,552,808.96

Tablica 9. Podatkovni promet korištenih web aplikacija kroz lokalnu mrežu



Application	Total Bytes (KB)
YouTube	765,698,775.45
Microsoft	477,909,234.42
Microsoft Update	171,304,057.79
Malwarebytes	112,638,654.78
Google	104,166,499.39
Google Play	72,686,588.24
MPEG	60,843,181.95
BITS	54,312,186.05
Office 365	40,290,217.18
Dailymotion	35,696,915.95
SHOUTCast Radio	30,430,694.95
Akamai	28,423,966.62
Wordpress	25,455,635.28
Eset	22,925,872.10
Doubleclick	21,817,526.93

Tablica 10. Naziv i broj pristupanja rizičnim aplikacijama s niskom važnosti za poslovanje

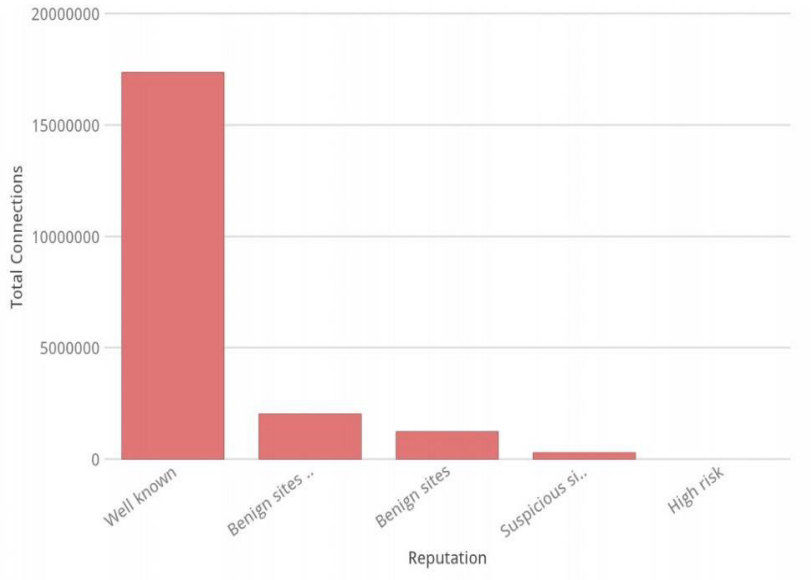


Application	Total Connections
Facebook	966,755
YouTube	489,603
TeamViewer	155,078
BitTorrent	79,089
Dailymotion	16,049
Lijit	11,985
MoPub	4,938
TwitchTV	4,125
Ultrasurf	2,763
Bootstrap CDN	1,928

Tablica 11. Broj povezivanja odnosno pristupanja prema URL reputaciji

Connections by URL Reputation

Time Window: *2018-07-22 12:12:57 - 2018-08-22 12:12:57*

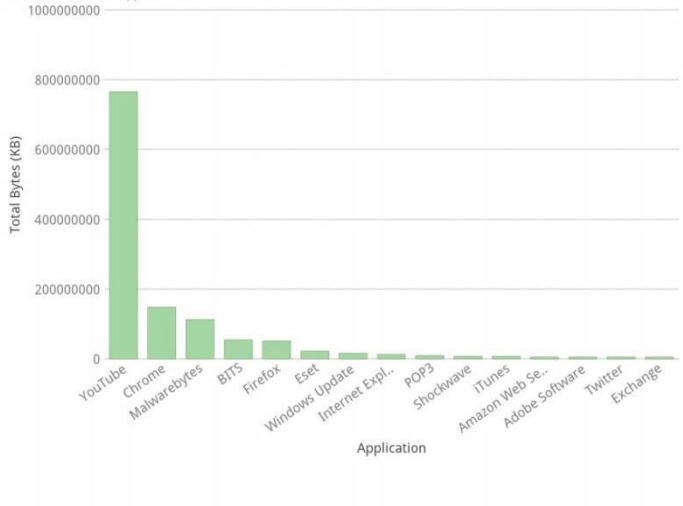


Reputation	Total Connections
Well known	17,381,612
Benign sites with security risks	2,032,714
Benign sites	1,250,606
Suspicious sites	290,870
High risk	4,276

Tablica 12. Podatkovni promet korištenih klijentskih aplikacija

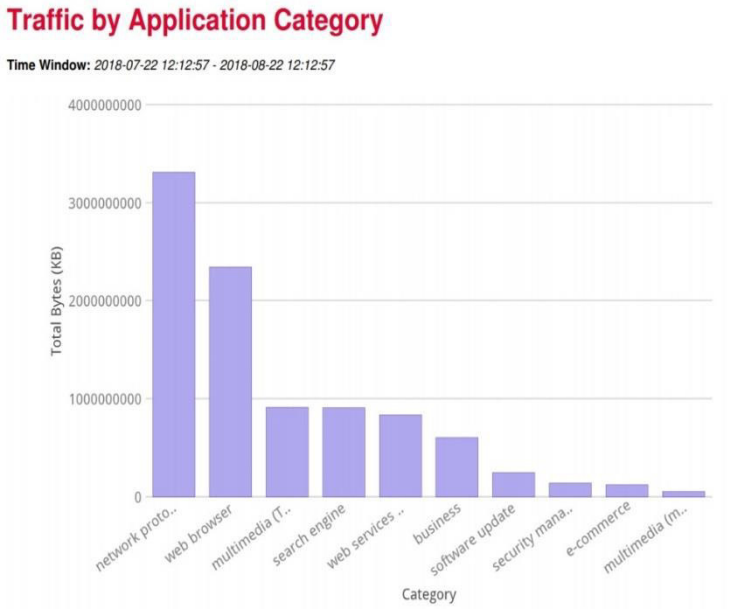
Top Client Applications Seen

Time Window: *2018-07-22 12:12:57 - 2018-08-22 12:12:57*
Application Filter: *Client Applications*



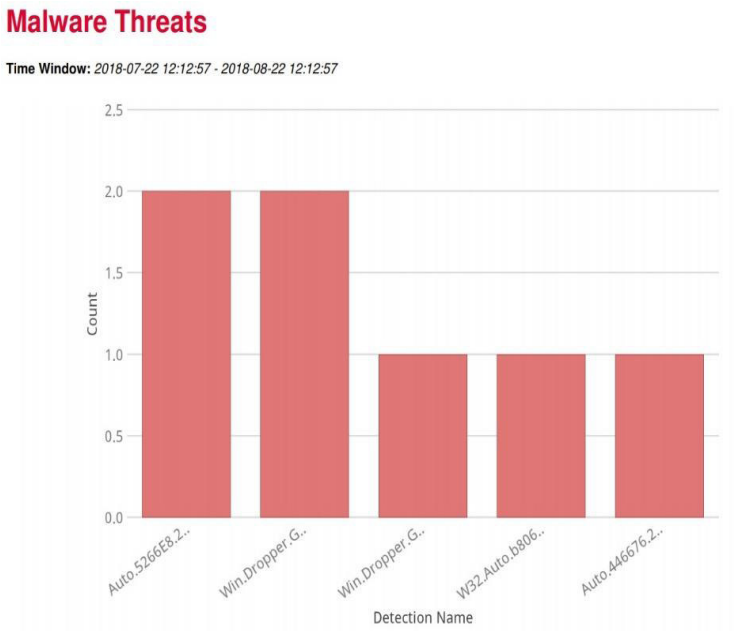
Application	Total Bytes (KB)
YouTube	765,698,775.45
Chrome	148,048,013.14
Malwarebytes	112,638,654.78
BITS	54,312,186.05
Firefox	51,598,504.35
Eset	22,925,872.10
Windows Update	16,620,046.43
Internet Explorer	12,962,987.69
POP3	9,885,018.22
Shockwave	7,625,669.76
iTunes	7,273,366.94
Amazon Web Services	5,038,172.22
Adobe Software	4,960,032.95
Twitter	4,941,839.74
Exchange	4,929,687.09

Tablica 13. Promet prema kategoriji aplikacija - analizira se podatkovni promet prema kategoriji u koju spadaju aplikacije - najveći promet odlazi na kategoriju mrežni protokoli i servisi, a zatim na kategoriju web preglednici



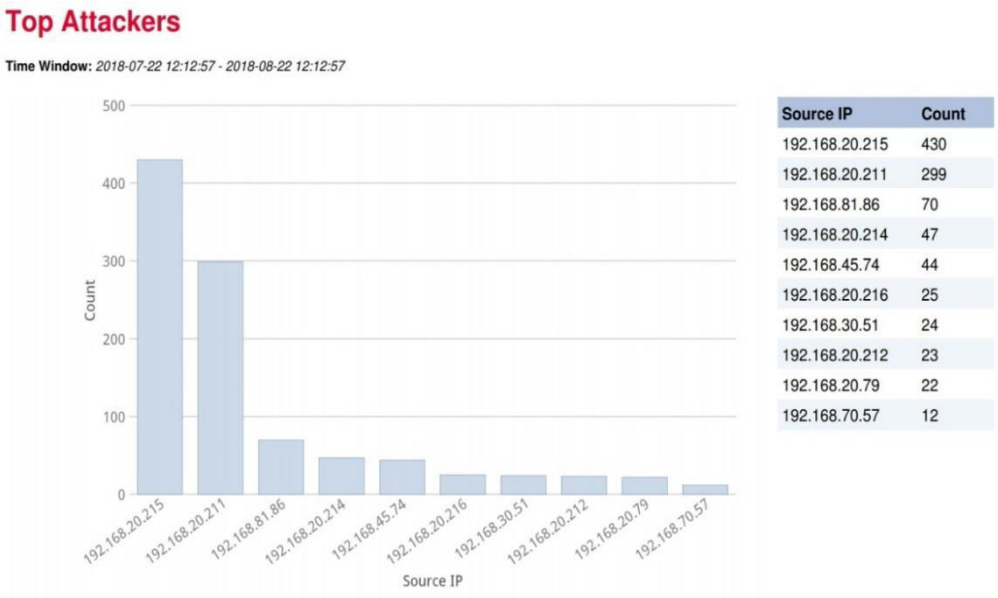
Category	Total Bytes (KB)
network protocols/services	3,313,119,503.27
web browser	2,347,621,916.89
multimedia (TV/video)	913,200,101.34
search engine	912,644,441.96
web services provider	837,787,534.81
business	604,543,242.95
software update	249,381,620.24
security management	142,125,152.56
e-commerce	123,134,612.31
multimedia (music/audio)	56,133,379.29

Tablica 14. Broj i ime otkrivene prijetnje u lokalnoj mreži



Detection Name	Count
Auto.5266E8.212138.in02	2
Win.Dropper.Generic::in07.talos	2
Win.Dropper.Generic::in03.talos	1
W32.Auto.b8060d.MASH.RT.SBX.VIOC	1
Auto.446676.212143.in02	1

Tablica 15. Izvorne IP adrese „hostova“ koji su pokrenuli neki događaj - najveći broj odnosi se na BIS-terminal-servere



Source IP	Count
192.168.20.215	430
192.168.20.211	299
192.168.81.86	70
192.168.20.214	47
192.168.45.74	44
192.168.20.216	25
192.168.30.51	24
192.168.20.212	23
192.168.20.79	22
192.168.70.57	12

Nadzor nad elektroničkom poštom na domeni obv.hr

Uz popularni klijentski pristup elektroničkoj pošti preko Microsoft Outlook-a, Mozilla Thunderbird-a, Windows Live Mail-a, kao jednih od popularnih klijentskih instalacija programa za upravljanje elektroničkom poštom može se paralelno ili samostalno koristiti i web klijent. Za pristup elektroničkoj pošti preko web sučelja koristi se Internet preglednik na primarne „host“ adrese, npr, webmail.obv.hr. Web pristup korisnicima omogućuju potpunu mobilnost, ali i preporuku vođenja brige o vjerodajnicama kod upotrebe pristupa sa tuđih računala. Osobni mobilni telefon i aplikacija je apsolutno komparativna i kompetitivna prednost. Nadzor i upravljanje radi se preko VIP-ovog cPanela. Spam filter je konfiguriran od strane VIP-a, ali isto tako svaki korisnik lokalno može postaviti filter na svojem korisničkom računu. Svaki korisnik može koristiti složen alias (npr. marko.maric@obv.hr, alias je mmaric@obv.hr), a preporuka je korištenje nepersonalizirane elektroničke adrese (npr. informatika.voditelj@obv.hr).

Kontrolira se popunjenost elektroničkog sandučića s obzirom na broj i količinu pristigle pošte. S obzirom na potrebe veličine sandučića svakom korisniku se dodjeljuje potrebna veličina izvan dogovorenog standarda zbog potrebe službe. Uvijek provjeravajte adresu pošiljatelja ePošte. Bitna je tema poruke. Mora imati smisleni sadržaj. Nikada nemojte kliknuti na link unutar elektroničke pošte. Potražite savjet informatičara u trenucima kada ste neodlučni. Dovoljan je jedan krivi klik i računalo može pokrenuti lavinu neželjenih događaja. SPAM filter koji je konfiguriran na poslužitelju može eliminirati i dobru poštu. Složite si filtere i kategorizirajte si tematiku dolazne pošte. Smanjite si pritisak velike količine dolazne pošte na početku radnog dana a koja u Spam verziji troši bespotrebno vaše dragocjene radne resurse.

Upute za postupanje s elektroničkom poštom:

- Otvoriti poštu na klik
- Provjera pošiljatelja

- Kontrola privitka, .jpg .exe, .bat
- Analiza sadržaja u Predmetu
- Link u tijelu poruke – visok rizik

Nadzor nad fiksnom i mobilnom telefonijom

Davatelj telefonskih usluga prati individualni promet po brojevima i obavještava nadležne osobe o dosezanju dozvoljenog limita u aktivnom razdoblju. Praćenje troškova je u domeni nadzora financijske službe koja analizira količinu stvarne potrošnje po mjesecima pristiglih računima od telekomunikacijskih operatera.

Kontrola vanjskih medija

Kontrola vanjskih medija za pohranu podataka (memory stick, CD, DVD, …) podržana je na svakom klijentskom računalu pomoću antivirusnog programa s uključenom zaštitom u realnom vremenu. Za preventivno kontrolni proces sigurnosne provjere „čistoće“ vanjskih medija i uređaja, potrebno je u odjelu za informatiku imati posebno računalo koje ima ažurnu zadnju verziju antivirusnog programa i nije spojeno na računalnu mrežu bolnice. Ono služi da se prekontroliraju vanjski mediji za pohranu podataka prije same upotrebe u produkcijskoj okolini. Ako je medij čist od malicioznog koda podaci se prebacuju na mrežni disk za daljnju internu upotrebu. Korisna je i opcija isključivanja samopokretanja (engl. „Autorun“) koja automatski pokreće program naveden u autorun.inf, datoteci vanjskog medija.

Zaključak

Preventivni pristup koji uključuje nadzor informatičkog sustava je optimalan način za upravljanje informatičkom imovinom i osiguranje besprijekornog rada poslovnog sustava. Nužan je nadzor sofisticiranim i pouzdanim programskim rješenjima djelatnika i sadržaja koji se koristi u zdravstvenom prostoru. Dedicirana je kontrola prava i obveza na polju pristupa medicinskoj dokumentaciji i pristupu internetskom prostoru. Cyber space, prostor koji je kontaminiran malicioznim sadržajem zahtjeva specijalistu informatičara, usmjerenja informatička sigurnost. To je toliko propulzivno i brzo rastuće područje interesa koja zahtjeva stručno i dedicirano, te konstantno dodatno obrazovano osoblje. „0-day exploit“ je termin koji definira vrijeme kada službena informatička industrija još nije odgovorila na probleme koji su se pojavili u informatičkom prostoru. Zato je preventivna briga od ključne važnosti, zastoj informatičkog sustava je sigurnosno poslovni problem najviše kategorije. Dobro educirani informatičari koji rade u sustavu zdravstva osnovna su karika koja garantira stabilnost i dostupnost poslovnog sustava. Zato jer znaju što se mora poduzeti u prevenciji, da potreba za digitalnom forenzikom nikada neće biti ni potreba, a informacijska sigurnost neupitno optimalna. O njihovom znanju, planiranju pravovremenih i korisnih aktivnosti na polju zaštite sustava, konstantnog rada na preventivnoj strategiji obnove opreme, ažuriranja pogonskih programa, o iznimnoj tehnologiji zaštite podataka danas ovisi opstojnog bolničkog sustava. A prijetnji je više nego ikada, maliciozni kodovi i aktivnosti prijete sa svih strana, ali informatičari u zdravstvu imaju znanje i strategiju kako se obračunati sa svim vrstama prijetnji u njihovom poslovnom okruženju.

Pristup podacima određuje se pravilnicima i normama ponašanja upotrebe poslovne imovine u poslovnom okruženju. Stvari moraju biti popraćene informatičkim rješenjima. Prava i zabrane

moraju biti programski upravljane, i pravno utemeljene te protokolima podržane. Zato imamo poziciju administrator aplikacije, osobe koja se sa profesionalnim alatima za nadzor i upravljanje brine da procesi autentifikacije i autorizacije budu jasno i nedvojbeno sprovedeni i permanentno nadzirani. Cilj je preventivno eliminirati svaku prijetnju koja ugrožava stabilnost i dostupnost poslovnog informatičkog sustava upotrebom informatičkih alata iz područja informacijska sigurnost.

Literatura

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal oft he European Union 2016, L 119/1. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

2. McClure S, Scambray J, Kurtz G. Hacking Exposed, Network Security Secets & Solutions. Fifth Edition. New York: MacGraw-Hill/Osborne 2005.Available at: http://media.techtarget.com/searchSecurity/downloads/Hacking_Exposed.pdf

3. Cisco Firepower Management Center on-line education point. Available at: https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html