

Cyber rizici – Izazovi digitalnog doba

Zlatan Filipović
Arandjelovac, 29.11.2018.

Život ispred mašte

- Nekada se smatralo da je nadzor svih ljudskih aktivnosti mogao zamisliti samo George Orwell u svom romanu 1984. A tada svijet nije bio digitalan
- Nepunih 70 godina nakon objavljivanja tog romana, zahvaljujući digitalizaciji sami snimamo i objavljujemo svoje fotografije, video-zapise, navike i misli

Život ispred mašte

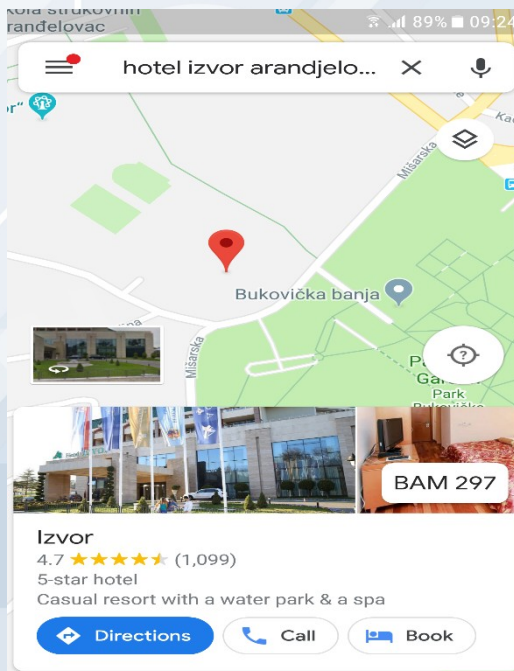
- I sve je to dostupno cijelom svijetu a digitalni zapisi će ostati i iza nas
- Zahvaljujući maloj kameri i WiFi-ju



shutterstock.com · 239509051

Život ispred mašte

- Cijeli svijet zna gdje sam, šta radim, šta jedem, šta sam kupio, s kim sam...



Znate li da

- Prosječan korisnik pametnog telefona pogleda u svoj telefon 150 puta dnevno
- Ne zna se postaje li korisnik zaista pametniji
- Isti taj prosječni korisnik dotakne telefon 2.617 puta dnevno
- će broj mobilnih aparata u svijetu preći 5 milijardi do 2019. godine

Prednosti

- Velika međusobna povezanost
- Lakša komunikacija
- Mogućnost on-line kupovine
- On-line bankarstvo
- Komunikacija sa državnim organima
- Digitalizacija razbija moć u rukama institucija i pojedinaca

Nedostaci

- Kupovina, uglavnom nepotrebnih stvari, još uvijek dominira
- Hakeri mogu pristupiti vašim kamerama i mikrofonima, kao i podacima
- Digitalizacija omogućava koncentraciju moći u rukama institucija, organizacija, država i pojedinaca

Ljudi su još analogni

- Digitalizacija je sveopšta
- Digitalizovani proizvodni procesi
- Digitalizovani liftovi
- Digitalizovani frižideri
- Samoupravljiva vozila
- Digitalizovana distribucija robe

Digitalni svijet i mi

- Ako možete neku uslugu uraditi preko internet bankarstva, procedure su zaćudo jednostavnije nego u banci
- Ali i vař raćun u tren oka moće biti poćišćen od strane neovlařtene osobe

Digitalni svijet i mi

- Digitalni svijet je omogućio i postojanje kriptovaluta
- Procjena je da ih postoji 1.110



Digitalni svijet i mi

- Imate li još uvijek klasični novčanik?



Digitalni svijet i mi

- Ili ste prešli na moderni, digitalni wallet?



Perspektive digitalnog svijeta

- Razvoj tzv. “pametnih gradova”
- Prvi je Singapur, drugi London
- Prag je krenuo tim putem
- Bezgotovinsko, beskontaktno plaćanje
- Pogodno za gradski prevoz
- Odvoz smeća, pronalaženje parkinga
- Mali grad Kolin u prednjači u Češkoj

Perspektive digitalnog svijeta



Opasnosti digitalnog svijeta

- Uz ogromne mogućnosti koje digitalni svijet otvara, pojavile su se i vrlo značajne opasnosti
- Prvi takav veliki slučaj bio je Millenium bug ili Y2K
- Uložen je ogroman novac da se problem riješi (ili „riješiti“), 483 milijarde USD
- Moguće je da je bilo više dima nego vatre

Opasnosti digitalnog svijeta

- Prekid lanca snabdijevanja može dovesti do nestašica, poslovnih gubitaka pa i propasti pojedinih poduzeća
- Dublin je u januaru ove godine ostao bez urednog snabdijevanja hranom, istina ne zbog cyber napada već snijega, ali efekat je isti – nije bilo hljeba, mlijeka, voća, povrća...

Opasnosti digitalnog svijeta

- Potencijalna šteta može nastati bilo kada i bilo gdje
- Ugroženi su vlade, vojske, proizvodni pogoni, transport, zdravstvo, edukacija, finansijski sektor, razni drugi poslovi

Opasnosti digitalnog svijeta

- Posebno ugrožen segment su baze podataka
- Identity Theft Resource Center kaže da je u 2017. bilo oko 1.300 proboja u podatke, sa ukupno izloženim brojem podataka od 174 miliona
- U 2016. 1.093 proboja

Opasnosti digitalnog svijeta



Opasnosti digitalnog svijeta

- Cyber rizici su još 2014. ušli među 10 najvećih globalnih poslovnih rizika, u UK su na prvom mjestu
- U zadnje vrijeme se porede sa iznosima šteta nastalih od prirodnih katastrofa (330 milijardi USD u 2017.)
- Svjetska ekonomija gubi zbog cyber kriminala 445 milijardi USD godišnje

Opasnosti digitalnog svijeta

- Poslovni sektor je pretrpio 50,5% napada
- Zdravstveni sektor 28,3%
- Edukacioni sektor 8,8%
- Bankarski i finansijski sektor 8,8%
- Vlada/vojni sektor 5,3%

Razvoj cyber osiguranja

- U Evropi je razvoj počeo 1995. donošenjem Direktive EU o zaštiti podataka
- Povećana zavisnost od IT i hakerski napadi doveli do povećane tražnje sredinom 2000.
- 2013. EU Direktiva o cyber sigurnosti
- 2013./2014. ponuda na širem tržištu

Razvoj cyber osiguranja

- Propis European Global Data Protection Regulation (GDPR) u EU stupio na snagu u maju 2018. (odredba donijeta 2016.)
- Kazna za propust 2% do 4% globalnog prihoda, uz maksimum od 20 miliona EUR
- Ovaj propis može dodatno ojačati potražnju za cyber osiguranjem

Razvoj cyber osiguranja

- Strožiji zakoni o zaštiti ličnih podataka
- Trošak rješavanja cyber upada povećan
- Trošak obavještanja unutar 72 sata, obavještavaju se vlasti, klijenti
- Trošak odnosa sa javnošću, pravni troškovi

Šansa za osiguranje

- Za 2018. procjena premije cyber tržišta u Evropi 800,000,000 EUR
- U periodu od 2012. do 2015. premija u svijetu porasla sa 1 milijarde USD na 2 milijarde USD
- Do 2020. predviđeno utrostručenje premije
- Procjene za 2025. skok premije na 20 milijardi USD

Šansa za osiguranje

- Informacionu aktivu osigurava negdje 15% privrednih društava
- Stopa osiguranih društava je puno veća kod imovinskih osiguranja – npr. požar 59%
- Pri tome, vjerovatnoća ostvarenja događaja požara je manja

Prosječni troškovi napada

- Uzorak: „nekoliko stotina“ kompanija
- 7% društava u SAD izgubila preko 1 mio USD (3% na nivou svijeta)
- Narednih 19% društava u SAD su izgubile između 0,5 i 1 miliona USD (svijet: 8%)

Prosječni troškovi napada

- Trošak prouzrokuju krađa informacija te
- Troškovi vezani uz poremećeno poslovanje ili izgubljenu produktivnost
- Uključuju kazne, sudske postupke, utrživost ukradene intelektualne imovine itd.

Prosječni troškovi napada

- Neblagovremeno rješavanje problema povećava troškove
- Prosječno vrijeme rješavanja cyber napada je bilo 32 dana
- Šanse za ponovni napad 27,7% u naredne dvije godine

Veliki cyber napadi

- 2000. – Hunter Water
- 2006. - Los Angeles City hall
- 2006., 2007. – TJX (maloprodaja), 90 miliona USD troškova
- 2008., 2009. – Heartland (fin. usluge) 110 m \$
- 2010. – Lodz City Tram system

Veliki cyber napadi

- 2010. – napadnut razvojni nuklearni program Irana
- 2012. – Saudi Aramico
- 2012. – Zappos (internet prodaja) 500 m \$
- 2013. – Adobe
- 2014. – JP Morgan Chase

Veliki cyber napadi

- 2014. – Ebay (internet trgovina), smanjenje prihoda za 200 m \$
- 2014. – Target (maloprodaja) 162 m \$
- 2015. – LOT
- 2015. – Anthem (zdravstvo) 100 m \$
- 2017. – Equifax (kreditni registar) tuženi za milijarde \$

Veliki cyber napadi

- 2017. – WannaCry ransomware
- 2017., 2018. – NonPetya “izgleda kao ransomware”
- 2018. – Coincheck, gubitak 534 m \$ u bitcoinima
- 2018. - Under Armour, sportska odjeća i prehrana

Veliki cyber napadi



Pristup osiguranju

- Industrija osiguranja sve je manje podložna standardizovanju
- Osiguranje cyber rizika bi bila oblast gdje bi standardizacija bila dobrodošla
- Iako su ponude “po mjeri” dobre, puno privrednih društava će biti zbunjeno različitom ponudom

Rizici po društva i institucije

- Zakonska odgovornost
- Proboj kompjuterske sigurnosti
- Narušavanje privatnosti
- Cyber krađa
- Cyber špijunaža i industrijska špijunaža
- Cyber ucjene
- Cyber terorizam

Rizici po društva i institucije

- Gubitak prihoda
- Namirenje troškova
- Narušeni ugled
- Kontinuitet poslovanja/prekidi u lancu snabdijevanja
- Cyber prijetnje infrastrukturi
- Osiguranje „prvog lica“ prema osiguranju „trećeg lica“

Rizici po društva i institucije

- Vjeruje se da su stariji informacijski uređaji ranjiviji
- Namjerno ažuriranje starijih softwera na način da usporavaju rad
- Nepodržavanje softwera
- Prisiljavanje na kupovinu novih uređaja i novih softwera

Šta se može osigurati

Jedan od vodećih osiguravača pokriva:

- Pokriće za proboj privatnosti i podataka
- Pokriće prekida poslovanja i troškova obnove
- Pokriće za odštetne zahtjeve na osnovu sigurnosti mreže
- Pokriće odgovornosti po odštetnim zahtjevima zbog medija

Šta se može osigurati

- Pokriće troškova nametnutih od strane regulatora
- Pokriće kazni i penala od strane regulatora
- Troškovi obavještanja
- Troškovi odgovora
- Pokriće hakerske krađe
- Pokriće cyber ucjena

Šta se može osigurati

- E-plaćanja
- Pokriće za krizno komuniciranje
- Pokriće konsultantskih usluga
- Dodatno pokriće kao što je prošireni prekid poslovanja
- Pokriće zasnovano prema zahtjevima specifičnog posla

Šta se može osigurati

- Uobičajeno fizičko oštećenje nije pokriveno
- Često je fizička šteta iz cyber napada isključena i po imovinskom osiguranju
- Kumuliranje rizika je opasnost
- Zbog razvoja teško je napraviti model primjenjiv na cyber rizike kao mjerilo izloženosti

Kako se može osigurati

- Cyber rizici se preuzimaju kao zasebno pokriće ali i kao dodatak postojećoj polisi

„Razumijevanje“ cyber rizika

- Nedostatak shvatanja izloženosti je jedna od najvećih prepreka za prodaju cyber pokrića
- Stav da IT sistemi ne mogu biti kompromitovani
- Nisam izložen, nikad mi se to nije desilo
- Nemogućnost dostavljanja dokumentacije za preuzimanje rizika

Reosiguranje i cyber

- Uloga reosiguranja je u ranom stadiju razvoja
- Kapacitet osiguranja je nedovoljan
- Dileme u reosiguranju su identične onima u direktnom osiguranju
- Često su cyber rizici u ugovorima o reosiguranju isključeni

Reosiguranje i cyber

- Učešće koje se nudi je od 20-30%, uglavnom na kvotnoj osnovi
- Reosiguranje je konzervativno u pogledu ukupne izloženosti
- Zahtijevaju se ograničenja po štetnom događaju za prekid poslovanja
- Značajan dio reosiguranja plasiran van SAD, u Londonu i na Bermudama

Reosiguranje i cyber

- Na konkretnom primjeru zaključenog pokrića, vidjeli smo da se traži franšiza koja je iskazana i monetarno i vremenski
- Limit je dat agregatno
- Pokriće isključuje SAD i Kanadu
- Prenosni uređaji poput diskova, traka, USB ili flash memorija su isključeni iz pokrića, ukoliko nisu enkriptirani

Zaključak

- Cyber rizici pružaju velike mogućnosti za razvoj osiguranja i reosiguranja
- Takođe donose mnoštvo nepoznanica
- Potrebna je velika opreznost kod procjene rizika i preuzimanja
- Potrebno je poznavanje problematike

Hvala na pažnji



Ilustracije: Pixabay.com, vlastite fotografije, Google maps, portal Jutarnjeg lista