**KRIMINAL NA BANKOMATIMA**

**SEMINARSKI RAD**

[www.maturski.org](http://www.maturski.org/)

SADRŽAJ:

1. UVOD.....................................................................................................................3

2. KRIMINAL NA BANKOMATIMA..................................................................5

2.1. Najćešči oblici zloupotrebe platnih kartica........................................6

2.2. Procedura i mjere sigurnosti koje se poduzimaju na prodajnom mjestu....7

2.3. Mjere sigurnosti koje se poduzimaju kod izdavaoca platnih kartica.....8

2.4. Procedure za slučaj zloupotrebe..........................................................8

3. MEĐUNARODNA REGULATIVA SAJBER KRIMINALA.........................10

3.1. Međunarodne konferencije............................................................11

3.2. EU osniva centar za borbu protiv sajber kriminala.............................11

3.3. Institucionalni oblik za borbu protiv sajberkriminala...........................12

3.3.1. Lažna tipkovnica direktno snima sve podatke za izradu lažnih kartica.........................................................................................................12

3.3.2. Primjer.............................................................................12

4. CJELOVITA RJEŠENJA ZAŠTITE FINANSIJSKIH INSTITUCIJA...............15

4.1.Osiguravatelji stimuliraju mjere zaštite............................................15

4.2. Ulaganja se isplate........................................................................16

4.3. Interakcija klijenta i bankara – uvjet bez kojeg se ne može....................16

4.4. Rješenja zaštite bazirana na novim tehnologijama omogućuju

otvorenost i sigurnost....................................................................................16

4.5.Iskustva iz svijeta – sve veći opseg digitalne integracije.....................17

5. BSA KONFERENCIJA 2010.................................................................................19

6. ZAKLJUČAK.........................................................................................................21

7. LITERATURA.......................................................................................................22

**[[1]](#footnote-2) 1. UVOD**

Ljudsko društvo je krajem prošlog i početkom novog milenijuma doživjelo najbrže promjene u svojoj historiji. U ovom periodu promijenjen je način obavljanja mnogih djelatnosti, nastupile su promjene u strukturi rada, na tržištu i u drugim oblastima. Time je industrijsko društvo evoluiralo u informatičko. Ovakve tehnologije omogućile su neuporedivo brži protok roba i usluga.

Moderne tehnologije su uticale na značajne promjene u oblasti platnog prometa. U strukturi sredstava plaćanja danas dominiraju plastični, elektronski, mobilni i virtualni novac. Trgovina i bankarstvo se u sve većem obimu odvijaju putem korištenja kompjuterskih i telekomunikacionih mreža i uređaja baziranih na visokim tehnologijama. Ove promene neminovno su dovele i do novih oblika kriminala. Povećana je frekvencija vršenja krivičnih djela kojima se iz koristoljubivih motiva zloupotrebljavaju visoke tehnologije.

Rizici kojima se bankarko poslovanje i platni promet izložilo zbog profita, zahtijevale su izmjene zakonske regulative na međunarodnom i nacionalnom nivou. Nesporno je da bi visina štete bila mnogo velika da se ne primjenjuje čitav niz bezbjednosnih procesa i zaštitnih mjera u cilju onemogućavanja i sprečavanja vršenja krivičnih djela kojima se zlouporebljavaju moderna sredstva bezbjednosnog plaćanja.

Iskustvo govori da se kriminalci vode idejom „najmanjeg rizika, a najvećeg profita“. Oni se paralelno sa razvojem novih tržišta u oblasti poslovanja platnim karticama, vrše migriranje procesa zloupotreba istih.

Sprečavanje vršenja i efikasno otkrivanje i dokazivanje krivičnih djela koja se vrše u ovoj oblasti, podrazumijeva da pripadnici pravosudnih organa, kriminalističke i poreske policije i drugih državnih organa raspolažu određenim znanjem o:

* savremenim sredstvima bezbjednosnog plaćanja i tehnologijama njihovog korištenja,
* tehnološkim, bezbjednosnim i preventivnim mjerama kojima se štiti funkcionisanje platnog prometa u ovoj oblasti,
* pojavnim oblicima kriminala u ovoj oblasti,
* načinu izvršenja krivičnih djela u ovoj oblasti,
* sredstvima za izvršenje ovih krivičnih djela,
* metodici otkrivanja i dokazivanja ovih krivičnih djela i
* profilu učinilaca krivičnih djela u ovoj oblasti.

**2. KRIMINAL NA BANKOMATIMA**

Sajber kriminal je jedan od najvećih izazova modernog društva. U 2007.g. 747 miliona ljudi koristilo je internet. Već oko pola miliona ljudi u Bosni i Hercegovini koristi internet. Elektronska trgovina napreduje velikom brzinom i milioni eura troše se svakodnevno preko interneta. Kupci se nalaze rasuti širom planete i udaljeni su od prodavaca samo za nekoliko klikova na tastaturi. Dosegnuta je potpuna globalizacija finansijskih tokova, međutim dosegnut je izuzetno visok nivo opasnosti koje prijete od strane sajber kriminala. Svakodnevno, gotovo u svakom trenutku, smo izloženi spam emailovima, virusima, hakingu, krađi identiteta, pornografiji, zloupotrebi djece, potencijalnoj opasnosti od sajber terorizma, odnosno rušenju vitalne informacione infrastrukture, korištenju kompjutera kao oružja za destabilizaciju vitalnih infrastrukturnih sistema. Opasnosti postoje da se informacione i komunikacione tehnologije koriste za vršenje klasičnih krivičnih djela na novi način, ali da se vrše novi oblici krivičnih dela koja do sada nisu bili poznati. Organizovani kriminal, odnosno terorističke grupe, prornografske i pedofilske mreže, ilegalni trafiking oružja, narkotika, ljudi, uznapredovali su u korištenju savremenih tehnologija. Šteta načinjenja od strane sajberkriminala u 2006 godini iznosila je oko 200 biliona eura.

Globalna rasprostranjenost platnih kartica, njihovog korištenja i laka dostupnost modernih tehnologija, učinile su ih izuzetno atraktivnim objektom napada kriminalaca. Na meti su nova i nedovoljno razvijena tržišta, bez dovoljno iskustva i u kojima ne postoji sistem za prepoznavanje i sprečavanje zloupotreba. Takvo tržište je potencijalni lak plijen za iskusne kriminalce i kriminalne grupe. Bankomati su kompaktan višenamjenski prostor. Specifičnost poslovnice smještene u malom prostoru je kompaktnost i multifunkcionalnost. Često je riječ o samo dvije prostorije (ponekad i jednoj) u kojima se obavlja i poslovanje usmjereno klijentu i tzv. pozadinsko poslovanje koje obuhvaća i pohranu novca. Osnovna svrha malih poslovnica je fizički biti što bliže klijentima i korisnicima kako bi se osigurala dostupnost usluga i povećao njihov broj. Zato se male poslovnice često nalaze na udaljenim i manje prometnim mjestima. U njima sve poslove obavlja jedna ili najviše dvije zaposlene osobe. Iz opisanih specifičnosti rada malih poslovnica proizlaze i specifični rizici kojima su takvi objekti i djelatnici u njima izloženi. Razbojništva su najčešća kaznena djela a posebno je opasno što su njihovi počinitelji doista spremni povrijediti pa i ubiti čovjeka kako bi se domogli novca. Poseban problem predstavlja što se napadači odlučuju na akciju i za veoma mali plijen.

**2.1. Najćešči oblici zloupotrebe platnih kartica**

Osnovni oblici falsifikovanja i zloupotreba platnih kartica su:[[2]](#footnote-3)

* zloupotreba ukradenih ili utajenih ( izgubljenih ) platnih kartica,
* zloupotreba neuručenih platnih kartica,
* neovlaštena upotreba tuđe platne kartice,
* pravljenje i korištenje lažnih platnih kartica,
* pribavljanje podataka za pravljenje lažne platne kartice,
* zloupotrebe i prevare od strane akceptanata ( trgovaca ),
* zloupotrebe od strane korisnika.

U slučaju nestanka ili gubitka kartice , korisnik je dužan da to odmah prijavi centru izdavaoca, a u slučaju krađe i policiji.

Svu materijalnu štetu nastalu zbog gubitka ili krađe kartice u periodu do prijave nestanka snosi korisnik.

Materijalnu štetu zbog gubitka ili krađe kartice od dana prijave se reguliše prema pravilima internacionalnog sistema platnih kartica.

Izdavaoc se obavezuje da će po prijemu informacije o gubitku ili krađi, karticu oglasiti nevažećom.

Ukoliko korisnik poslije prijave nestanka pronađe karticu, ne smije je koristiti već je mora poništiti i vratiti izdavaocu.

Imajući u vidu sve gore navedeno i pored mjera sigurnosti u svim fazama finansijske transakcije bezgotovinskog plaćanja platnim karticama, zloupotrebe su i dalje veoma česte i prijetnja sigurnosti ovoj vrsti bankarskog poslovanja.

**2.2. Procedura i mjere sigurnosti koje se poduzimaju na prodajnom mjestu**

Trgovac je obavezan da se prilikom prodaje robe i vršenja usluga korisnicima platnih kartica, pridržava sljedeće osnovne procedure i sigurnosnih mjera.

* Trgovac će pregledati platnu karticu korisnika u cilju ustanovljavanja da li je kartica ispravna na prvi pogled ( odgovarajući materijal, boja, štampa, ime, datum važenja, potpis ).
* Trgovac će pregledati listu poništenih kartica koja mu je banka dostavila sa kojom ima zaključen Ugovor o prihvatanju kartica;
* Trgovac će obavijestiti banku u slučaju da ne primi listu poništenih kartica;
* Trgovac je jasno indentifikovan svojim registracionim brojem;
* Sistem mora uvek biti u mogućnosti da provjeri broj platne kartice, lični identifikacioni broj ( PIN ), broj transakcije, i da automatski primi sigurnosne mjere;
* Trgovac će poštovati proceduru sistema koji je prikazan na ekranu opreme sistema;
* U slučaju da je u skladu sa Uputstvom za upotrebu za trgovce, trgovac će zatražiti od korisnika da primeni svoj PIN na siguran način i obezbediće poseban dokaz izvršenja PIN kontrole;
* Trgovac je obavezan da traži autorizaciju od banke izdavaoca;
* Trgovac će obezbjediti potpis korisnika na slipu i takođe će se uvjeriti da je potpis identičan onome na korisnikovoj kartici;
* Trgovac će predati korisniku jednu kopiju slipa kao dokaz transakcije;
* Trgovac će oduzeti platnu karticu kada na to upućuje sistem ili kada i tome dobije obaveštenje prilikom zahtjeva za autorizaciju od banke ili ako je ta kartica na listi poništenih kartica i takođe će poništiti sva plaćanja koja su izvršena takvom karticom na istoj lokaciji i u istom danu;
* Trgovac će dostaviti slipove banci u vremenskim rokovima kako je to predviđeno Uputstvom za upotrebu za trgovca i čuvanje u arhivi informacija i dokumenata koja se zahtevaju Ugovorom zaključenim između trgovca i banke;
* Trgovac mora da se pridržava svih zahtjeva iz Ugovora za upotrebu za trgovce kao i drugih instrukcija koje primi od banke;

Sve navedene mjere sigurnosti se primenjuju na samom prodajnom mjestu kako bi se sprečila zloupotreba kartica, i sve mjere zaštite su od jednake važnosti.

**2.3. Mjere sigurnosti koje se poduzimaju kod izdavaoca platnih kartica**

Banka izdavaoc izdaje platnu karticu Klijentu koji kod Banke ima otvoren tekući račun. Kartica je neaktivna sve do momenta dok je klijent ne potpiše i ne preuzme.

Do momenta preuzimanja kartica je zaštićena i obezbeđena pick up codom koji se aktivira u momentu preuzimanja kartice od strane klijenta.

Zbog sigurnosti PIN ( Personal Identification Number ) se ni u jednom momentu ne nalazi zajedno sa karticom, niti zbog mera sigurnosti isti ljudi rade zajedno na poslovima izdavanja kartica i dodele PIN-a.

PIN se određuje kompjuterski, automatski se pakuje i niko ga ne yna osim samog korisnika kartice.

Sve navedene mere sigurnosti se koriste da bi se izbegle zloupotrebe kartica kod samod izdavaoca, ili da se iste svedu na minimum. U tom sistemu su svi sistemi bezgotovinskog plaćanja, VISA, MASTER CARD, DINERS, pripremili svoja stroga interna pravila, a sve iz razčoga sigurnosti i bezbednosti.

Zloupotreba se može javiti i u postupku slanja pošiljke tj. platnih kartica registrovanom poštom ili na neki drugi način, zatim kod samog proizvođača kartica ili kod procesora, bez obzira da li je isti identičan sa bankom izdavaocem, ili je odvojen fizički od njega.

**2.4. Procedure za slučaj zloupotrebe**

U slučaju da trgovac posjeduje karticu koja je zaboravljena od strane korisnika, trgovac će vratiti karticu korisniku, ali samo nakon utvrđenog udentitetakorisnika i nakon dobijanja dozvole banke da tako učinikroz proces autorizacije.

Kartica se može vratiti na ovaj način isključivo u roku od dva dana od dana kada je zaboravljena, nakon ta dva dana trgovac ima obavezu da poštuje proceduru za zaboravljene kartice koja je predviđena Ugovorom za upotrebu za trgovce, koji mu dostavlja banka sa kojom ima zaključen Ugovor o prihvatanju kartica.

U slučaju da je trgovcu ponuđena na prijem nepotpisana kartica, trgovac će, prije bilo kakve transakcije, zatražiti autorizaciju od banke i ustanoviće identitet držaoca kartice. Trgovac će takođe zahtijevati od držaoca kartice da potpiše karticu i ustanoviće da li je potpis identičan onome koji postojina dokumentu kojim se utvrđuje identitet.

U slučaju povratka novca od trgovca korisniku u pogledu prodate robe ili izvršenih usluga, takav povrat će biti izvršen isključivo preko metoda plaćanja predviđenih internim pravilima sistema kojim predmetna platna kartica pripada i neće biti izvršen na bilo koji drugi način.

**3. MEĐUNARODNA REGULATIVA SAJBER KRIMINALA**

Jedina međunarodna konvencija koja reguliše pitanje sajber kriminala je Konvencija o sajber kriminalu Savjeta Evrope donijeta 2001.g. u Budimpešti, koja je stupila na snagu jula 2004.g. Ona predstavlja vodič za države koje žele da razviju legislativu u borbi protiv sajber kriminala. Albanija je potpisala 2001.g. i ratifikovala 2002.g. Bosna i Hercegovina, potpisla 2005.g. i ratifikovala 2006.g. Bugarska potpisala 2001.g. i ratifikovala 2005.g. Hrvatska potpisala 2001.g. i ratifikovala 2005.g. Mađarska pospisala 2001. i ratifikovala 2003.g. Rumunija je potpisala 2001, a ratifikovala 2004.g., Slovenija je potpisala 2002, a ratifikovala 2004.g. Crna Gora potpisala 2005, ali je još nije ratifikovala, kao i Srbija koja je potpisala 2005.g. i nije je još ratifikovala. Do sada je Konvenciju potpisalo 46 zemalja, a ratifikovalo je 23 zemlje. U prvom dijelu konvencije dato je objašnjenje osnovnih pojmova. U drugom dijelu konvencije definisane su mjere koje treba da se preduzmu na nacionalnom nivou. To su krivična djela protiv tajnosti, cjelovitosti i dostupnosti računarskih podataka i mreža (neovlašten pristup, oštećenje podataka, mreža, itd.), kompjuterska krivična djela (neovlašteno unošenje, brisanje podataka, računarska

prevara, krivična djela vezana za diječju pornografiju, krivična djela protiv povrede

autorskih i srodnih prava sporedne odgovornosti i sankcije (pokušaj, pomaganje,

podstrekavanje), odgovornost pravnih lica, sankcijama, procesnom pravou, zaštiti

ljudskih prava, oduzimanje sredstava izvršenja krivičnog djela, prikupljanje računarskih podataka u realnom vremenu, itd.). U trećem dijelu definisana je međunarodna saradnja u okviru sprovođenja konvencije: opšta načela, izručenje, uzajamna pomoć, informacije, postupci, tajnost i ograničenja korištenja, hitno otkrivanje zaštićenih podataka, uzajamna pomoć u pogledu pristupanju podacima, prekogranično pristupanje podacima, itd. Četvrto poglavlje obuhvata završne odredbe u vezi potpisavanja i stupanja na snagu (pristupanje, teritorijalna primena, itd.).[[3]](#footnote-4)

**3.1. Međunarodne konferencije**

Konferencija Savjeta Evrope protiv sajber kriminala

Konferencija odžana u aprilu 2008. u Strazburu. Bilo je prisutno 210 eksperata za sajber kriminal iz 65 zemalja, a u zaključcima konferencije naglašen je značaj primjene konferencije i usvojen je vodič za saradnju između onih koji primjenjuju pravo i internet provajdera u istraživanju sajber kriminala. U okviru vodiča definisane su mjere koje treba da poduzmu posebno oni koji sprovode zakonsku regulativu, a posebno internet servis provajderi.

Treći Forum o upravljanju internetom Savjeta Evrope održan, 3-6 decembra 2006, u Indiji. Jedan od radionica na akonferenciji bila je posvećena zaštiti ličnih

podataka i privatnosti u informacionom društvu.

**3.2. EU osniva centar za borbu protiv sajber kriminala**

Ministri vanjskih poslova Europske unije složili su se na sastanku 26. aprila 2010. godine oko uspostave europskoga središta za borbu protiv sajber kriminala kao dijela dugoročne strategije EU u borbi protiv prevara na internetu, pronevjera i dječje pornografije. Ministri su pozvali Europsku komisiju da sačini studiju izvodljivosti povodom kreiranja ovoga specifičnog tijela koje bi trebalo stati u kraj cyber kriminalu u EU, ali i olakšati prekograničnu razmjenu informacija između nacionalnih istražitelja u ovim oblastima.

Iako su prekogranične istrage sve češče i djelotvornije, veliki broj prestupnika i dalje uspijeva da izbjegne ruku zakona uslijed nesavršene harmonizacije pravnih sustava država članica EU. I dalje postoje slučajevi prevara na internetu u kojima sudjeluju osobe koje su osnovale “fantomsko” poduzeće u jednoj, a klijente varaju u drugim državama članicama.

Novo središte trebalo bi se boriti protiv ovakvih problema koristeći se preventivnim i analitičkim mjerama širom država članica, kao i treninzima policije, sudija i tužilaca sa iskustvima u ovoj oblasti.

Središte bi moglo imati sjedište unutar Europske policijske agencije EUROPOL-a u Hagu koja je već razvila svoju “platformu za europski cyber kriminal”. Sa pravnoga gledišta, države članice trebaju još uvijek ratificirati Konvenciju Vijeća Europe o cyber kriminalu iz 2001.godine i usvojiti zajednički stav o praktičnim pitanjima kao što su blokiranje IP adresa ili ukidanje imena domena.

**3.3. Institucionalni oblik za borbu protiv sajberkriminala**

Sajberkriminal je stvorio potrebu za angažovanjem posebno tehnički obučenih stručnjaka, ali i reorganizacijom državnih organa. Zakona o organizaciji i nadležnosti

državnih organa za borbu protiv visokotehničkog kriminala, predviđa organizovanje i opremanje posebnih državnih organa koji će se baviti ovom oblasti.

3.3.1. Lažna tipkovnica direktno snima sve podatke za izradu lažnih kartica

Pojavljivanjem lažne tipkovnice u pitanje je dovedena prevencija kartičnog kriminala na bankomatima, u vidu koje je policija u saradnji s banakama upozoravala građane da zaklanjaju unos svog PIN broja prilikom korištenja bankomata. Uz lažnu tipkovnicu kriminalcima više nije potrebna mikrokamera, jer se ona postavlja na originalnu tipkovnicu bankomata, teško je uočljiva, te direktno snima unos PIN broja i sve podatke za izradu lažnih kartica. Nova kriminalna tehnologija je uveliko rasprostranjena na području jugoistočne Europe. Uhapšeni kartični kriminalci su uglavnom stranci koji u dobroj organizaciji podatke za izradu lažnih kartica sakupljaju u jednoj zemlji, šalju na obradu i proizvodnju u drugu zemlju, te su po saznanjima policije, novac podzali na bankomatima u trećim zemljama. U pet najvećih slučajeva kartičnih prijevara, policija je uz pomoć Interpola uhitila na desetke stranaca među kojima je najviše bilo Rumuna.

3.3.2. Primjer[[4]](#footnote-5)

Sajberkriminalci lakovjernim građanima kradu novac sa platnih kartica, šire viruse po kompjuterskim sistemima, prave neovlaštene kopije muzike i filmova, pljačkaju banke. Sajberkriminal obuhvata široku lepezu od širenja virusa, neovlaštenog pristupa računarskoj mreži, preko piraterije, do pornografije i pljački banaka, zloupotrebe platnih kartica najčešće ali i svih ostalih krivičnih djela u kojima se koriste kompjuteri. Naši sajberkriminalci pljačkaju lakovjerne građane uzimajući im na prevaru pin kod ili kopirajući magnetne trake sa „dina“ „juba“ „viza“ „master“

kartica. Među domaćim sajberkriminalcima veoma su popularne takozvane libanske

klopke. To su štipaljke, žabice koje su iste boje kao automat i koje se gurnu u otvor

na bakomatu u koji ulazi kreditna kartica. Kada građanin gurne karticu da podigne

novac, ona u stvari ne uđe u automat već upada u žabicu. Pošto automat ne registruje karticu, korisnik ne uspijeva da podigne novac, ali ni da izvadi karticu. U tom trenutku mu prilazi „brižni“ građanin koji mu kaže: „Jao, to se i meni jučer desilo. Možda mogu da vam pomognem. Koji je vaš pin kod?“ Ako mu građanin da broj, on ga, kao, ukuca, ali se, naravno, ništa ne desi. On onda građaninu predloži da ode do centrale banke i tamo zatraži pomoć. Čim čovek zamakne za ugao, prevarant se vraća, vadi karticu, ubacuje je u automat i uzima novac. Naši kriminalci su se prilično izvještili i u kopiranju brojeva kreditnih kartica i njihovom prenošenju na magnetne trake, koje se zatim prebacuju na bijelu plastiku identičnog oblika kao platna kartica. Kopiranje podataka sa originalne kartice obavlja se pomoću sprava ručno napravljenih od kompjuterskih dijelova. Ova prevara se sprovodi u buticima, prodavnicama, restoranima i prevarant mora da ima saučesnika iznutra. Zadatak

saučesnika je da karticu koju uzme od gosta, odnosno mušterije prilikom naplate provuče kroz taj mali uređaj i iskopira podatke sa kartice. Onda se ti podaci prenesu

na magnetnu traku koja se zalijepi na bijelu plastiku i to se onda koristi kao prava kartica. Zbog velikog obima krivičnih djela koje obuhvata sajberkriminal, širok je i dijapazon njihovih izvršilaca. Ovom vrstom kriminala se bave pripadnici svih starosnih grupa - od maloljetnih lica, studenata, pa sve do penzionera koji su dovoljno priučeni da uključe kompjuter, aktiviraju program za narezivanje diskova, iskopiraju filmove, muziku, računarske programe i te kopije prodaju na ulici ili na veliko. Skoro 99 odsto njih su obični kriminalci koji umjesto kalauza ili pištolja koriste kompjutere. Samo jedan odsto su vrsni stručnjaci za kompjutere.

**4. CJELOVITA RJEŠENJA ZAŠTITE FINANSIJSKIH INSTITUCIJA[[5]](#footnote-6)**

Broj napada se značajno povećao dok se prosječna šteta uzrokovana pojedinim napadom smanjuje čemu su sigurno pridonijele i mjere zaštite koje se sve više primjenjuju i postaju standardni dio poslovanja.

Provedenom zaštitom, štete se mogu smanjiti od 2 do 20 puta. Djelovanje zaštitnih mjera je višestruko. Najznačajnije je odvraćanje koje napadača tjera da odustane ili potraži slabiju žrtvu. Rana detekcija i usporavanje skraćuju trajanje napada a time

smanjuju njegov učinak. Identifikacija omogućuje naknadno hvatanje napadača i djelomični povrat izgubljenog.

Ukoliko se objedine sve četiri funkcije, maksimizira se djelotvornost sustava a štete se značajno smanjuju.

Dok su neposredne štete – gubitak novčanih i drugih vrijednosti, odnosno materijalne štete na opremi - jasno prepoznatljive i mjerive, posredne štete – izgubljeni radni dani, izgubljene veze s klijentima, psihološki problemi zaposlenika i posljedične parnice, gubitak poslovnog ugleda, itd. – dosižu razinu približno jednaku onoj neposrednih šteta.

**4.1.Osiguravatelji stimuliraju mjere zaštite**

Osiguravatelji sve više prepoznaju utjecaj primijenjene razine zaštite na redukciju rizika od navedenih šteta. Stoga sve više u opće uvjete osiguranja ugrađuju minimalne standarde zaštite koje osiguranici moraju primijeniti, kao i mehanizme vrednovanja dodatnih zaštitnih mjera. Ti uvjeti proizlaze iz iskustva i višegodišnjeg praćenja i analize statističkih pokazatelja koji se redovito prikupljaju i ona su, na neki način, suština dobrog gospodarenja osiguravajućih društava. Primijenjene mjere zaštite stimuliraju bonusima na premije pa tako i novčarske institucije ulaganjem u mjere zaštite mogu uštedjeti na policama osiguranja svojih djelatnika, poslovanja

i imovine.

**4.2. Ulaganja se isplate**

Ulaganje u sustav zaštite je razmjerno maleno u odnosu na ostale infrastrukturne sustave pa tim više opravdano zbog niza pogodnosti koje jamči. Uz već navedene značajno manje rizike i štete, tu je i smanjenje troškova održavanja štićenih objekata, dulji životni ciklus, kvalitetnija

analiza i izvještavanje, bolje upravljanje procesima, brža reakcija na promjene, lakše učenje i unaprjeđivanje. Sve ovo svakako osigurava znatno veće zadovoljstvo i osjećaj sigurnosti zaposlenika i klijenata, što konačno vodi boljem poslovnom ugledu.

**4.3. Interakcija klijenta i bankara – uvjet bez kojeg se ne može**

Primjena novih tehnologija u zadnjem je desetljeću potaknula strukturne promjene u bankarskom poslovanju. Šaltersko poslovanje (podizanje gotovine, plaćanje računa, izdavanje čekova, isplata plaća, upis kamata) naprosto je preseljeno iz poslovnica banaka u dom ili na radno mjesto klijenata koji putem Interneta mogu zadovoljiti većinu vlastitih potreba, odnosno na bankomate koji nisu ograničeni radnim vremenom te su uvijek i svuda dostupni. Time su resursi banaka oslobođeni za sasvim nove usluge a glavni posao bankara sada je informirati klijenta o uslugama i programima u ponudi, prikupiti od klijenta informacije o njegovoj konkretnoj potrebi i financijskim mogućnostima te konkretnoj osobi ponuditi konkretno rješenje problema. S druge pak strane otvorenost prostora u kojem se nalaze vrijednosti za koje su mnogi spremni riskirati kako bi ih se brzo domogli dovodi u pitanje realizaciju novih trendova u poslovanju banaka. Otvorenost znači i pristupačnost svima - pa i onima koji nemaju poštene namjere - čime može biti dovedena u pitanje osobna sigurnost i djelatnika i klijenata.

**4.4. Rješenja zaštite bazirana na novim tehnologijama omogućuju**

**otvorenost i sigurnost**

Novi smjer poslovnog razvoja diktira otvoren i udoban kontakt s klijentom. Klijent želi sve usluge, na jednom mjestu, sad i odmah. Takav koncept isključuje klasični šalterski prostor i prostornu odvojenost koja pogoduje sigurnosnim aspektima. Nove tehnologije omogućavaju razvoj integralnih rješenja utkanih u poslovne procese.

Digitalni sustavi zaštite ugrađeni u TCP/IP poslovnu mrežu temelj su koji se jednostavno implementira i jednostavno nadograđuje. TCP/IP integriran i centraliziran sustav nadzora i dojave prenosi trenutni uvid u situaciju na proizvoljne udaljenosti i mjesta. Digitalne kamere ultra-visoke rezolucije i napredni inteligentni algoritmi čine rješenje koje je uvijek korak isprednapadača. To je samodjelujući sustav koji prepoznaje neuobičajene situacije i automatski aktivira obrambene mehanizme čime se izbjegava namjerna i nenamjerna greška čovjeka. Biometrija postaje jednostavna i pouzdana tehnologija, prvi alat u prepoznavanju i blokiranju

slučajnih i namjernih pogrešaka. Beskontaktna kontrola pristupa ne usporava poslovne procese, ali značajno usporava napadača.

Činitelji koji najviše utječu na smanjenje rizika:

(prema rezultatima istraživanja J. P. Freeman Co., Inc.)

1. Uniformirani čuvar

2. Digitalni video-nadzor s daljinskim pristupom

3. Integrirani sustavi

4. Kontrola pristupa

5. Zaštita podataka

6. Protuprovalni i protuprepadni sustav

**4.5.Iskustva iz svijeta – sve veći opseg digitalne integracije**

Na temelju istraživanja časopisa Focus on Magazine provedenog među 1500 novčarskih institucija u SAD-u ustanovljeno je da voditelji zaštite financijskih ustanova rizike kojima su izloženi rangiraju sljedećim redoslijedom: računarska zaštita, prepad, pronevjera od strane djelatnika, neovlašteni ulaz i izlaz te provala.

Kako bi prevenirali prepoznate rizike sudionici istog istraživanja navode digitalni umreženi video i integraciju raznih podsustava tehničke zaštite kao rješenje koje ima najviše utjecaja na smanjivanje svih vrsta rizika kojima su izloženi. Ispitanici su istaknuli da je odvraćanje počinitelja najvažniji segment sprječavanja počinjenja kaznenih djela. Temeljni trend koji traje već godinama se i dalje potvrđuje: rješenja zaštite idu u smjeru manje upotrebe ljudi. Već dulje vrijeme sve novčarske institucije raspolažu temeljnim mehanizmima zaštite – protuprovalnim i protuprepadnim sustavom, odnosno trezorima s vremenskom odgodom. U posljednje vrijeme ovim se sustavima pridružuje i video-nadzor. U specifičnim okolnostima i potrebama (trideset do pedeset posto primjena) koriste se posebne mehaničke zapreke kombinirane sa sustavima kontrole pristupa.

Međutim, najvažnija i još uvijek najbrže rastuća je upravo poveznica među tim sustavima – digitalna integracija – kojoj ne samo da raste udio primjene, već i opseg.

**5. BSA KONFERENCIJA 2010**

|  |  |
| --- | --- |
|  | *Na današnjoj press konferenciji, održanoj u prostorijama sarajevskog hotela Holiday Inn, međunarodna asocijacija ispred globalne industrije softvera, Business Software Alliance (BSA), objavila je svoju sedmu godišnju studiju o softverskom piratstvu. [[6]](#footnote-7)* |

|  |  |  |  |
| --- | --- | --- | --- |
| U kratkom obraćanju, prisutnim novinarima su se obratili Mirna Milanović-Lalić iz BSA, Lejla Hadžiabdić ispred Microsofta BiH, predstavnici državnih institucija, Boris Grubešić iz Tužilaštva BiH i Jasmin Gogić iz Državne agencije za istrage i zaštitu, te Aladar Urbanke iz kompanije HSM Informatika, regionalnog distributera Adobe proizvoda.   |  | | --- | |  |   BSA/IDC Global PC Software Piracy studija napravljena je u saradnji sa poznatom kompanijom za istraživanje tržišta, IDC,  a obuhvata više od stotinu zemalja. Konferenciju je otvorila Mirna Milanović-Lalić, glasnogovornica BSA u BiH, koja je istakla zadovoljstvo kontinuiranim padom stope piratstva na bosanskohercegovačkom tržištu. Prema objavljenim podacima, u periodu od 2008. do 2009. godine, procent nelicenciranog softvera u Bosni i Hercegovini smanjen je za 1%, te danas stopa softverskog piratstva 66%.  Što se zemalja u regiji, prema studiji iz 2009. godine,  Bosna i Hercegovina ima nešto bolji prosjek od istočnih susjeda, pa je u Srbiji stopa piratstva visokih 74%, a u Crnoj Gori čak 81%. Istovremeno značajno zaostajemo  za Hrvatskom u kojoj je 54% softvera ilegalno, i Slovenijom koja sa 46% ima najmanju stopu softverskog piratstva u regiji. Milanović-Lalić je ukazala i na jasnu povezanost između stepena ekonomske razvijenosti i uređenosti tržišta.   |  | | --- | |  |   Unatoč činjenici da je od ukupno 111 zemalja koje su obuhvaćene ovom studijom, u 54 zemlje stopa softverskog piratstva smanjena, na globalnom planu primijećen je rast stope piratstva sa 41% u 2008. godini na 43% u prošloj godini. Uzrok ovakvog rasta stope piratstva vidi se u eksploziji tržišta u velikim zemljama u razvoju, kakve su Indija, Brazil, Kina i druge. Kao pozitivni primjeri s najnižim stopama softverskog piratstva navedene su SAD sa 20%, Japan sa 21% i Luksemburg sa 21%, dok u regionalnom smislu očekivano najmanji prosjek imaju zemlje Sjeverne Amerike sa 21% i Zapadne Europe sa 34%.  Ispred kompanije Microsoft BiH, prisutnim novinarima se obratila Lejla Hadžiabdić, menadžer za antipiratske aktivnosti pri Microsoftu BiH. Hadžiabdić nas je upoznala sa aktivnostima ove kompanije u posljednjoj godini, a koje su za cilj imale povećanje svijesti korisnika o štetnosti korištenja nelicenciranog softvera. Microsoft BiH je do sada podnio više krivičnih prijava protiv osoba koje su putem oglasnih web portala u promet ilegalno stavljale Microsoft proizvode. Istaknuto je kako su prijave uglavnom podnošene na dojavu korisnika, te kako Microsoft BiH u budućnosti planira i još agresivnije akcije i kampanje na ovom planu.  Prvi put Bosna i Hercegovina je ovo istraživanje uključena 2004. godine, kada je stopa softverskog piratstva bila 70%. Detaljne podatke o stopi piratstva u našoj zemlji, kada se razdvoje privatni i javni sektor, nažalost nismo dobili, no prema podacima koje ima Microsoft BiH i koji se odnose na proizvode ove kompanije,  procent legalnog softvera u javnom sektoru je veći od 90%. Ovo u osnovi znači da na procent nelicenciranog softvera na državnom nivou u negativno najvećoj mjeri utječe privatni sektor, te ukazuje na nužnost edukacije prosječnog korisnika.   |  | | --- | |  |   Glasnogovornik Tužilaštva BiH, Boris Grubešić, upoznao nas je s radom ove državne institucije, kao i aktivnostima koje ova institucija sprovodi na suzbijanju softverskog piratstva. Tužilaštvo BiH u posljednjih nekoliko mjeseci pokrenulo je niz aktivnosti  u borbi protiv svih oblika cyber kriminala, te značajnije rezultate najavio za skoriju budućnost. Istaknut je i problem nedostatka zakonske regulative u pojedinim oblastima, što se zasigurno negativno odražava na borbu protiv ovog tipa kriminala. Stopa softverskog piratstva u Bosni i Hercegovini se u prosjeku smanjuje 1% godišnje, što naravno nije dovoljno, posebno imajući u vidu procent zastupljenosti ilegalnog softvera u ekonomski razvijenim zemljama Zapadne Europe.  Za značajniji napredak na ovom polju, potrebne su edukacijske kampanje, programi povoljne legalizacije, usvajanje zakonske regulative i promjene tehnologije kada je zaštita sadržaja u pitanju, rečeno je na današnjoj konferenciji. |

**6. ZAKLJUČAK**

U svijetu se odavno koriste smart ili chip kartice, a kod nas još uvijek traju rasprave o karticama sa magnetnom trakom, i još uvijek čekamo na normativno regulisanje osnovnih pojmova iz ove oblasti, kao što su: vlasništva nad karticom, položaj izdavaoca i korisnika kartice, njihovih međusobnih prava i obaveza, sankcije za nepoštovanje tih obaveza, kao pojam i vrste zloupotreba kartica, sankcija za slučaj zloupotreba uključujući krivična djela i prekršaje, kao i postupak i proceduru za obeštećenje u tom slučaju. Kako navedena materija nije uopšte, ili djelimično regulisana, to su banke primorane da, poštujući okvire koje daje postojeća regulativa, kao i interna pravila diktirana od strane internacionalnih kompanija čije platne kartice izdaju, definišu i kreiraju cjelokupnu materiju.

Sa stanovišta zloupotreba platnih kartica, da bi se broj istih sveo na minimum, potrebno je djelovati, kako preventivno, tako i naknadno, sankcionisanjem navedenih slučajeva, pri čemu bi bila od velike koristi reforma pratećeg zakonskog okvira i veća angažovanje i bolja saradnja sa policijom.

**7. LITERATURA**

Prlja, D. ¨Sajberkriminal“, Pravni fakultet Beograd, 08. decembar 2008.godine.

www.alarmautomatika.com/ebrochure/bankalog.../bankalog\_cro.pdf

www.phy.hr/~dandroic/nastava/rm/racunalni\_virusi.pdf

www.pravo.hr/KP/uvod\_u\_kriminologiju

Ćano, J. BSA Konferencija 2010, Kategorija: Reportaže, 19.05.2010. godine

[www.maturski.org](http://www.maturski.org/)

1. Prlja, D. ¨Sajberkriminal“, Pravni fakultet Beograd, 08. decembar 2008.godine. [↑](#footnote-ref-2)
2. www.phy.hr/~dandroic/nastava/rm/racunalni\_virusi.pdf  [↑](#footnote-ref-3)
3. Prlja, D. ¨Sajberkriminal“, Pravni fakultet Beograd, 08. decembar 2008.godine. [↑](#footnote-ref-4)
4. www.pravo.hr/KP/uvod\_u\_kriminologiju  [↑](#footnote-ref-5)
5. www.alarmautomatika.com/ebrochure/bankalog.../bankalog\_cro.pdf [↑](#footnote-ref-6)
6. Konferencija 2010, Kategorija: Reportaže, 19.05.2010. godine [↑](#footnote-ref-7)