

USPEŠAN DIZAJN BANKOMATA – KLJUČ USPEHA U ZAŠTITI OD ZLOUPOTREBE

ZETA SYSTEM je dugogodišnji zastupnik poznatog proizvođača bankomata **BANQIT** iz Švedske. Intenzivno je prisutan na tržištu Srbije i Crne Gore, Makedonije i Bosne i Hercegovine. Nagrada za najbolji rast prodaje u sistemu Banqit-a u svakoj od poslednje 3 godine najbolje govori o rezultatima. Preko 130 ATM-ova isporučenih i instaliranih u SCG i regionu govori o iskustvu i potencijalima kompanije.

BANQIT je među ekspertima poznat kao proizvođač izuzetno kvalitetnih bankomata koji nikada ne pravi kompromise nauštrb sigurnosti i kvaliteta. Pored oklopa ATM-a od poznatog švedskog čelika koji ni u jednoj varijanti ne ustupa mesto plastici (uobičajeno kod Lobby modela ostalih proizvođača), **BANQIT** u sve svoje modele ugrađuje najbolji (i najskuplji) svetski model dispenserera - DeLaRue. Specifičan dizajn omogućava maksimalnu zaštitu i sigurnost korisnika.

Zbog istog porekla i sličnih projektantskih i proizvodnih ciljeva, u svetu se često čuje poređenje: «**BANQIT** je **VOLVO** među bankomatima», što izvanredno oslikava njegovu poziciju na tržištu.



Iako je još pre par godina izgledalo da ćemo se teško privići na kartice i korišćenje bankomata, stvari su se brzo i značajno promenile. Preko pet stotina instaliranih bankomata na teritoriji Srbije i veliki broj transakcija na njima, govore o tome da su bankomati konačno pronašli svoj put do korisnika kartica. Ako vam zatreba gotovina, možete je podići ne samo na prometnim ulicama velikih gradova, već i u malim mestima.

Kako to obično biva, bankomati privlače pažnju i nekih drugih «korisnika». Po svetskim statistikama Japanski lopovi godišnje opljačkaju oko 50 bankomata, u Velikoj Britaniji je gubitak zbog zloupotrebe platnih kartica prošle godine prešao cifru od 500 miliona funti. U našem okruženju je sve više «obučenih» kriminalaca koji se bave ovom vrstom posla. U Hrvatskoj i Sloveniji je zabeleženo nekoliko slučajeva nelegalnog korišćenja kartica na bankomatima, dok je kod nas zabeležen, zvanično, samo jedan slučaj.

Svi proizvođači bankomata, naravno, pri projektovanju svojih uređaja vode računa i o bezbednosnoj komponenti i pokušavaju da dizajnom, tehničkim rešenjima i softverom preduprede moguće zloupotrebe na ATM-ovima.

Ali kao i kod svakog projektovanja kompleksnog uređaja, projektant mora da zadovoljava razne oprečne zahteve. U tom smislu, finalni proizvod je rezultat kompromisa i svaki proizvođač bankomata je poznat po «akcentu» na pojedinom skupu karakteristika, često nauštrb nekih drugih kvaliteta.

Navedimo samo neke kombinacije:

- izuzetan i tehnološki avangardan izgled, nauštrb jednostavnog izgleda koji ne plaši prosečnog korisnika,
- velika, luksuzna i pristupačna tastatura, nasuprot maloj i uvučenoj tastaturi koja se teško može zloupotrebiti (akvizicija PIN-a),
- modularni i univerzalni dizajn, nasuprot kompaktnom uređaju koji zauzima malo prostora,
- itd.

Kao odlični poznavaoци BANQIT-ovih bankomata sa značajnim iskustvom u nadzoru i prevenciji od zloupotreba, želimo da to iskustvo iskoristimo da napravimo jedan osvrt na najčešće zloupotrebe i način kako se pre svega dobrim dizajnom bankomata, ali i monitorisanjem, nadzorom i izborom lokacije ATM-a, rizik može znatno umanjiti.

➤ **KRAĐA KARTICA ILI PODATAKA SA KARTICA**

Jedna od osnovnih zloupotreba u korišćenju platnih kartica se bazira na korišćenju bankomata kao sredstva za krađu kartica ili podataka sa kartica. Postoji više metoda, dobro poznatih proizvođačima ATM-ova i bankama, protiv kojih su manje više svi proizvođači bore dizajnom svojih modela ili naknadnim tehničkim intervencijama:

- **Libanska petlja** (Lebanese loop) je postavljanje mehaničke prepreke (elastične trake) u otvor čitača kartice koja dozvoljava korisniku ubacivanje kartice, ali sprečava put kartice do kraja. Uobičajeno, ATM ne uspeva da pročita karticu (ne detektuje je) i ostaje u statusu «čekanja».

Korisnik, posle izvesnog vremena gubi strpljenje i pretpostavljajući da je ATM pokvaren ili da mu je oduzeo karticu, odlazi do banke da reklamira oduzimanje kartice. Za to vreme, lopov izvlači «libansku petlju» zajedno sa karticom.

BANQIT ugrađuje SANKYO čitače kartica (magnetnih i čip) koji imaju standardno ugrađenu zaštitu od «libanske petlje». Iz jasnih razloga, nije zgodno objašnjavati detaljno tehnologiju ove zaštite.

- **«Skimming»** odnosno «snimanje» originalnih podataka sa magnetne trake platne kartice prilikom njihovog korišćenja na bankomatu. Ovo se postiže postavljanjem kompaktnih baterijskih čitača magnetnih kartica na samom ulazu standardnog čitača kartica ATM-a. Prilikom korišćenja ovako prepravljenog ATM-a korisnikova kartica prolazi kroz oba čitača kartica, bankomat normalno završava transakciju i korisnik kartice odlazi zadovoljan uslugom i ne znajući da je sadržaj njegove kartice kopiran.

Loš dizajn pojedinih bankomata sa širokim (i komplikovanim) otvorom čitača kartica dozvoljava neprimetno postavljanje ovakvih uređaja. Takođe, uređaj koji izgleda suviše «tehnički» sa mnogo elemenata i svetlećih signala u principu otežava uočavanje ovakvih naknadno ugrađenih elemenata.

BANQIT je svojim dizajnom koji se bazira na jednostavnom i «netehničkom» izgledu, bez suvišnih detalja koji neće «plašiti» svojom tehnologijom prosečnog korisnika, u velikoj meri otežao neprimetno postavljanje «skimming» uređaja. Takođe, uvučeni deo na kome



se nalazi čitač kartice i PIN tastatura, kao i uzan prostor otvora čitača kartica (veličine same kartice) ne dozvoljava postavljanje standardnih «skimming» čitača.

Pored takve pasivne odbrane bazirane na dobrom dizajnu, *BANQIT* sistemom elektronske zaštite i senzora (anti skimming), koja se standardno ugrađuje u sve modele, dodatno detektuje eventualno postavljanje «skimming» uređaja i blokira rad ATM-a. Do sada u svetu nije zabeležena ovakva zloupotreba na bankomatima ovog proizvođača.

- **Bugarski slučaj** zloupotrebe bankomata je najnoviji primer veštog korišćenja kombinovanih mana hardvera i aplikacije na bankomatima pojedinih proizvođača. Da bi zarobili i uzeli karticu, «obučeni» kriminalci su se koristili metodom lepljenja «enter» tipke na tastaturi za unos PIN-a da bi je blokirali.



Korisniku je sve izgledalo normalno. On je ubacivao karticu u čitač i unosio PIN na već blokiranoj tastaturi. Nakon toga, kako se ništa nije dešavalo i kartica se nije vraćala usled nekontrolisanog i suviše dugog time out-a, korisnik je, misleći da je kartica zadržana u bankomatu, odlazio. Po njegovom odlasku kriminalci su dolazili, čekali istek time-out-a i uzimali karticu.

Softverska aplikacija *BANQIT*-ovih bankomata sprečava ovakvu zloupotrebu. Nakon isteka prvog time-out-a od 10-tak sekundi, aplikacija postavlja pitanje korisniku (da li želi još vremena ili da prekine transakciju) i prihvata odgovor sa dirki pored ekrana (koje nisu blokirane). Ukoliko korisnik prekine transakciju, kartica mu se vraća bez problema.

➤ **KRAĐA PIN-a**

Karticu ili sadržaj magnetne piste, ukraden na jedan od gore pomenutih načina, moguće je zloupotrebiti na bankomatu samo uz odgovarajući PIN. Zato uz neku od navedenih “tehnologija” uvek u paru ide i “tehnologija” za krađu PIN-a:

- **Lažna PIN tastatura** koja se postavlja na postojeću PIN tastaturu bankomata i pamti PIN-ove koje korisnik unosi pokušavajući da završi započetu transakciju. Uz ranije ukradenu sadržinu sa magnetne piste (skimming uređajem) lako je napraviti lažnu karticu i zloupotrebiti je a da korisnik toga dugo ne bude svesan.

Otvoreni dizajn tastatura pojedinih proizvođača bankomata, sa širokim i nezaštićenim prostorom za PIN tastaturu (koji je planiran za mogućnost dodavanja kompletne internet-like tastature), daje veliku šansu za postavljanje tanke i neprimetne lažne tastature. Takva nesmotrenost u projektovanju je naterala mnoge banke (na severu Evrope je to obaveza) da postave dodatne zaštite u obliku stubića oko PIN tastature koji ometaju postavljanje lažnog uređaja.



BANQIT je pri projektovanju svojih modela,

vodeći računa o ovom detalju, smestio PIN tastaturu u udubljenje (zajedno sa čitačem kartica) koje je dovoljno veliko samo za PIN tastaturu. Svako smeštanje lažnog uređaja bi zbog malog prostora bilo uočljivo, jer bi taj uređaj morao da ima znatnu debljinu (zbog baterije, elektronike,...). To se potvrdilo i u praksi.

- **Kamera** je takođe uređaj koji se često koristi za snimanje PIN tastature i PIN-a koji unosi korisnik. Minimalizacija ovih uređaja je omogućila da se zajedno sa radio-odašiljačem mogu montirati na ATM ili u okolnoj galanteriji.

Zloupotrebu ovde opet olakšava loš dizajn bankomata koji su projektovani sa mnogo tehničkih detalja koji otežavaju uočavanje ovakvih dodataka. Takođe "otvorene" tastature omogućavaju lako snimanje ugrađenim kamerama onoga što se na nju unosi.

Rešenje koje je upotrebio BANQIT je vrlo elegantno i bazira se na uočljivo "čistom", ravnom i jednostavnom rešenju frontalne površine bankomata. Lažna kamera jednostavno nema gde da se montira a da to odmah ne bude uočljivo. Čak ako se to i uradi i kamera montira na okolnoj galanteriji, korisnik vrši unos PIN-a na tastaturi koja je uvučena u telo bankomata i zaklonjeno je od pogleda i kamere.

Sve ono što može da uradi dodatna kamera, može da uradi i «neželjena» osoba koja se nalazi u okolini korisnika bankomata i narušava njegovu **privatnost** pokušavajući da vidi PIN koji se unosi. Bankomat koji ima PIN tastaturu zaštićenu od pogleda je sigurno u prednosti u odnosu na druge.

BANQIT preporučuje pored standardnog zaštitnog filtera na ekranu, koji onemogućava čitanje sadržaja ekrana osobama sa strane, i ugradnju ogledala koje pomaže korisniku da uoči prisustvo «neželjene» osobe.



Zloupotrebe koje smo ovde naveli spadaju u red najčešćih zloupotreba bankomata koje se danas dešavaju.

Banke se protiv njih mogu boriti **pažljivim izborom modela i proizvođača** opreme i pokloniti poverenje onima koji već u standardnoj konfiguraciji i samom dizajnu imaju implementirane sve (ili bar većinu) zaštitnih elemenata.

BANQIT se sa pravom reklamira kao proizvođač sa najvećim stepenom sigurnosnih elemenata implementiranih već u baznom dizajnu i konfiguraciji. Statistike potvrđuju da na njihovim tipovima bankomata, nema zabeleženih zloupotreba ovog tipa.

Banke mogu pored pravilnog izbora proizvođača ATM-a, da broj zloupotreba smanje i dodatnim elementima zaštite koji će omogućiti privatnost, nadzor i monitorisanje mreže bankomata. U tom delu želimo da sažeto iznesemo osnovne metode i konkretne proizvode koje ZETA SYSTEM i BANQIT nude za realizaciju tih metoda.

PRIVATNOST

Postavljanjem bankomat na mestima koja su zaštićena i omogućavaju privatnost klijentima je jedan od bezbednosnih faktora na koji banka može da utiče.

Takva mesta mogu da budu posebni prostori u okviru ekspozitura banke koja su otvorena i čuvana 24h (Lobby) i omogućavaju selektivan pristup samo vlasnicima kartica.

Jedna od interesantnih mogućnosti za zaštitu out-door bankomata su i specijalno dizajnirani kiosci, koji omogućavaju siguran pristup korisnicima i privatnost prostora oko samog uređaja.

Ovi kiosci nisu jeftini, ali osim toga što proširuju broj potencijalnih lokacija za postavljanje ATM-a, kiosci, takođe pružaju i reklamni prostor koji se može koristiti u raznim bankarskim marketinškim kampanjama ili se mogu iznajmljivati drugim marketinškim agencijama.

BANQIT i ZETA SYSTEM imaju u svojoj ponudi kompletnu lepezu Kiosk-a poznatih svetskih proizvođača.



VIDEO NADZOR

Video nadzor je primarni metod koji omogućava bolje praćenje bankomata i sprečavanje pokušaja zloupotrebe na njima. Kamere se mogu na jednostavan način ugraditi, ukoliko već nisu ugrađene od strane samog proizvođača bankomata.

Fotografije se snimaju tokom obavljanja transakcije, najčešće prilikom unosa kartice, u trenutku kada bankomat dobije odgovor od hosta i prilikom isplate novca.

Optimizacija nadzora se može vršiti i instaliranjem dodatnih kamera koje pokrivaju prostor oko samog bankomata, naročito ako se bankomat nalazi na udaljenoj lokaciji.

ZETA SYSTEM i *BANQIT* u svojoj ponudi imaju mogućnost isporuke kamera za video nadzor koje se povezuju u klasičan sistem video nadzora banke, kao i kamera koje su kontrolisane od lokalne aplikacije ATM-a i beleže na disku fotografije odabranih trenutaka svake transakcije na bankomatu.

MONITORISANJE

Monitoring treba da obezbedi konstantni nadzor i upravljanje bankomatima, poboljšavajući raspoloživost samih bankomata i sprečavajući rizik. Većina bankomata ima ugrađene senzore koji detektuju pokušaj «napada». U slučaju da neko neovlašćeno pokušava da pristupi određenim delovima npr. sefu, automatski se aktiviraju poruke koje se šalju službi nadzora, koja na osnovu same statusne poruke može da dijagnosticira koji slučaj se desio na bankomatu.

Osnovni koncept softverskog rešenja za monitorisanje bankomata firme *ZETA SYSTEM* je u tome što osim konstantnog nadzora i informisanja o statusu mreže bankomata, takođe objedinjuje prenos snimljenih fotografija, prenos podataka iz elektronskih žurnala, udaljeni

restart u slučajevima kada je to neophodno, kao i udaljeni update konfiguracionih datoteka i upgrade aplikacije.

ZAKLJUČAK

Bez pretenzija da smo pomenuli sve elemente koji poboljšavaju bezbednost i smanjuju broj zloupotreba u oblasti platnih kartica na mreži bankomata, mislim da smo ipak uspeali da ilustrujemo svu kompleksnost ove problematike i da smo dali neke osnovne elemente o kojima treba voditi računa.

Možda je osnovni zaključak da se ovde bezbednost ne može postići ukoliko se na rešenje ove problematike ne gleda kao na kompleksan skup akcija pri izboru opreme (hardver, softver), lokacije, organizacije rada (monitorisanje, nadzor), servisa i servisnih partnera (održavanje, nadzor)

Naše i Banqit-ovo rešenje za povećanje sigurnosti transakcija na bankomatu je zasnovano na kombinaciji dizajna, sigurnosnih hardverskih komponenti, aplikativnog softvera i procedura za rukovanje bankomatom u skladu sa najvišim sigurnosnim standardima, koji su propisani. Primenjena tehnologija vodi računa o korisnicima, štiteći njihov identitet, integritet i smanjujući mogućnost zloupotrebe, kao i o samim vlasnicima bankomata, minimizirajući rizik zloupotrebe.