poročilo

NT KONFERENCA 2016

Microsoftova NT konferenca, na kateri se srečujejo strokovnjaki s področij informacijskih tehnologij in poslovnega sveta, velja za enega od osrednjih IT-dogodkov v Sloveniji. Letošnja, že enaindvajseta konferenca je potekala od 16. do 18. maja 2016 v Portorožu. V nadaljevanju predstavljamo vsebino dveh prispevkov.

DAVID MODIC: NE, PA NE BOM! ZAKAJ UPORABNIKI NE SLEDIJO VARNOSTNIM NAVODILOM?

Dr. David Modic je raziskovalec v računalniškem laboratoriju Univerze v Cambridgeu. Zadnjih petnajst let se ukvarja s psihologijo virtualnih skupnosti, zadnja leta pa predvsem s kiberkriminalom in psihologijo prepričevanja na internetu. V predavanju se je osredotočil na digitalno varnost in spletne prevare. Najprej je govoril o teoretičnih osnovah, nato pa je pojasnil razloge, zakaj se posamezniki upirajo prehodu na nove tehnologije. Vse je podprl z rezultati raziskav. Na koncu se je osredotočil na študije konkretnih primerov in predlagal izboljšave procesa.

Kratek eksperiment

Izhodiščno vprašanje je: Ali ljudje upoštevajo varnostne napotke? Nato se ponuja še cela vrsta drugih vprašanj. Če ljudje varnostnih napotkov ne upoštevajo, zakaj jih ne? Kaj lahko naredimo, da jih bodo? In, ali to sploh hočemo? V ospredju so ljudje, in ne tehnologija.

Dr. Modic je predstavil primer o varnosti v organizaciji, v kateri je bilo na to temo organizirano predavanje za vse zaposlene. Predavatelj je najprej predstavil in orisal strukturo podjetja ter zadnje napade in varnostno politiko. Koliko zaposlenih je poznalo varnostno politiko v svoji ustanovi? Koliko jih je poznalo odgovore na vsa vprašanja o tem, kako pogosto naj bi menjali geslo, koliko gesel je treba imeti, kako naj bodo sestavljena, komu prijaviti vdor, kako zaznati vdor, kakšno je nevarno obnašanje? Najustrezneje je, da imajo zaposleni za vsak sistem posebno geslo, ki je sestavljeno iz črk, številk in posebnih znakov, gesla pa je treba tudi pogosto spremeniti. Vsem, ki imajo šibka gesla, se svetuje, da jih spremenijo. Koliko ljudi ob tem pomisli, da bi morali spremeniti svoje geslo, in koliko jih nato to dejansko naredi? Varnostna služba v podjetju preverja, katera gesla so pogosta in šibka. Različne raziskave kažejo, da so problematična točno določena gesla. Kako vemo, katera gesla so to? V ta namen se za analizo uporabljata posebna specializirana oprema in groba sila (angl. *brute-force*) ali pa podjetje izvaja socialni inženiring. Kot se velikokrat izkaže, uporabniki ne vedo, da je njihovo geslo šibko. Mislijo, da je dovolj v geslu npr. zamenjati "e" in "3" ali na konec besede dodati številko, npr. "Janez123".

Ključno vprašanje je: Zakaj uporabniki ignorirajo napotke o varnosti?

Odgovorov je lahko več in se med sabo prepletajo:

- *Ljudje na splošno ne sledijo varnostnim navodilom.*
  Varnostnih navodil se običajno ne upošteva. Avtor je podal praktičen primer, ko je računalniška služba Univerze v Cambridgeu (University Information Service, UIS) vsem uporabnikom, ki v zadnjem letu niso spremenili gesla (n = 22.000), poslala sporočilo, da bodo preverili varnost njihovih uporabniških računov. Po enem tednu so zbrali podatke in jih poslali v obdelavo – izvedli so klasično slovarsko preverjanje. Rezultat je razkril 1.890 šibkih gesel, pri katerih je uspešna najdba gesla v povprečju trajala 12 sekund. Šibka gesla so bila prisotna na vseh nivojih – od receptorjev do profesorjev. Nobeno geslo se ni ponovilo. Večinoma so bila sestavljena iz besede in številk na koncu, npr. "Cambridge12" ipd. Med gesli sta bili tudi "1234567" in "abcdefg". Vsa odkrita gesla so bila v zbirki, namenjeni odkrivanju šibkih gesel (Openwall worldlists collection; 500 Mb – slovarske besede in kombinacije). Nivo izobrazbe pri tem ni igral vloge.

- *Lahko gre za iluzorno superiornost.*
  Mislimo, da stvari bolj obvladamo, kot je res. Gre za Dunning-Krugerjev učinek (Manj ko posamezniki vedo o neki stvari, bolj so prepričani, da jo odlično poznajo, in več ko vedo o neki stvari, bolj so prepričani, da o njej ne vedo veliko.). Ljudje na splošno mislimo, da smo v nečem boljši, kot v resnici smo. Kot razkrivajo raziskave, velika večina voznikov npr. misli, da so boljši od povprečja. Prepričanje, da o varnosti vemo kar

precej oz. več kot večina drugih, je zmotno. Prav tako je zmotno prepričanje, da z geslom "Janez123" ni nič narobe, saj sledi vsem varnostnim navodilom, ker ima velike in male črke ter številke.

- *Pogoste so lažne predstave o lastni nepomembnosti.*
  Večina ljudi ignorira varnostne napotke na podlagi prepričanja, kako malo verjetno je, da bi kdo vdrl v njihov računalnik. Poleg tega mislijo, da nimajo kaj skrivati, tudi če bi se to zgodilo.

- *Zaznati je učinek lažnega konsenza* (angl. *false-consensus effect*).
  Na splošno verjamemo, da imajo drugi podobno mnenje kot mi. Izkaže pa se, da uporabniki ne vedo prav veliko o varnostni politiki, medtem ko tisti, ki jo je napisal, o njej ve veliko. Prav tako se izkaže, da delavci organizaciji običajno niso tako predani kot njihovo vodstvo ali ustanovni člani. To je avtor na šaljiv način ponazoril s citatom iz animiranega filma Chicken Run: "From now on, we work as a team. That means everyone does what I say!" (Od zdaj naprej delamo kot ekipa. To pomeni, da vsak sledi mojim zahtevam.)

- *Izobraževanje, ki je na voljo, ni najboljše.*
  Ne gre toliko za neinformiranost, ampak bolj za to, da uporabniki ignorirajo napotke. Zakaj jih ignorirajo? Nekaj razlogov je že bilo navedenih. Kaj pa pravi teorija?

- *Pogosto gre za "proračun ustreganja"* (angl. *compliance budget*).
  Ljudje imamo veliko dela. Čas je dobrina in posamezniki smo pripravljeni podariti le določen del te dobrine za posodabljanje računalnika. Če je teh zahtev preveč, jih ignoriramo.

- *Sledenje napotkom je iracionalno.*
  V večini primerov se namreč nič ne zgodi, tudi če ne upoštevamo varnostnih navodil.

- *Dosledno sledenje navodilom zmanjša varnost.*
  Zahteva po unikatnih geslih velikokrat pomeni, da si jih ljudje nekam zapišejo. Podan je bil resničen primer s poljske TV, ko se je v TV-prispevku v delu kadra pojavil izpis uporabniškega imena in gesla. Enako velja pri prisilnem posodabljanju in pri zelo kompleksnih geslih.

- *Uporabniki so neumni in ne vedo, kaj je dobro zanje.*
  To ne drži. Povprečen uporabnik je povprečno inteligenten. Vendar pa inteligenca ne igra vloge pri nasedanju spletnim prevaram.

Zakaj torej uporabniki ne sledijo navodilom?

Ali sploh hočemo, da bi sledili navodilom? Uporabnikom se večino časa ne zgodi nič. Včasih sledenje navodilom celo bolj škodi kot koristi. Poleg tega je navodil preveč in so preveč kompleksna.

Če imamo dobre razloge in želimo, da bi uporabniki sledili našim navodilom, se je dobro izogniti:

- prisili (ker prisila povzroči odpor – posreden ali neposreden),
- vzbujanju nezaupanja (ker nezaupanje rodi nezaupanje),
- etiketiranju,
- neposredni konfrontaciji.

Cilj je namreč večja varnost, ne pa izpostavljanje in sramočenje. Če nekoga izpostavimo, nam naslednjič, ko se bo pojavil vdor, tega preprosto ne bo povedal. Nekatere raziskave so pokazale, da samo približno 25 % spletnih prevar žrtve prijavijo. Ljudje se namreč bojijo sekundarne viktimizacije. Najpomembneje pa je, da so sistemski inženirji (angl. *security officers*) o napadu obveščeni čim prej; tako ga lahko zajezijo. Uporabniki pa morajo biti seznanjeni s tem, kakšen nivo varnosti se pričakuje in kako ga doseči.

Psihologija vedenjske spremembe

Splošno zaželeno je, da bi na čim bolj optimalen način dosegli drugačno obnašanje uporabnikov. S tem vprašanjem se ukvarja psihologija vedenjskih sprememb v različnih kontekstih (angl. *behavioural modification*). Različne raziskave kažejo, da vsi lažemo (predvsem pogoste so majhne laži), da se zlažemo približno dvakrat na dan, da je zlaganih 27 % neposrednih pogovorov (npr. Ne, nisi se zredila …), 37 % telefonske komunikacije (npr. Sem že na poti ...) in 14 % komunikacij po elektronski pošti (npr. Poročilo je že napisano, samo pošljem ga še …).

Večina ljudi goljufa malo oz. pogosto nekoliko priredi resnico (angl. *fibbing*). Kako se s tem spoprijeti? Avtor je v ponazoritev uporabil primer iz zavarovalništva. Zavarovalnice v Združenem kraljestvu in ZDA uporabljajo dva pristopa pri prepoznavanju goljufivih zahtevkov: preko umetne inteligence, znakov goljufije in uporabe socialnih omrežij ali z zmanjšanjem tveganja za zavarovalnice z nižjimi izplačili, manj možnostmi za izplačilo, več izjemami v drobnem tisku ipd.

Spoprijemanje z goljufijami je problematično. Rešitev je, da se zmanjša število goljufivih vlog. Tako se zmanjša količina dela, ki ga imajo zavarovalnice, in dolgoročno omogoči boljša storitev za stranke. Odkriti je treba, ali sta nivo in način goljufanja primerljiva z drugimi, že raziskanimi konteksti in kateri so mehanizmi, ki preprečujejo oddajo goljufivih vlog. V osnovi gre torej za spremembo vedenja posameznikov, kar je uporabno tudi na področju varnosti.

Avtor, ki se sam ukvarja s področjem zavarovalniških prevar, je z ekipo s serijo eksperimentov vpeljal nekaj mehanizmov. Pri tem so želeli ugotoviti, ali ti mehanizmi vplivajo na odločitev o vložitvi zahtevka in njegovi višini.

Uporabili so dva različna pristopa. To sta:

- mehanski in
- psihološki pristop.

Mehanski pristop je pristop, pri katerem ljudje sledijo normam, če so opazovani (učinek opazovalca). Naredili so dvoje stvari. V spletni obrazec so dodali sliko oči in sporočilo, da se ljudem sledi.

Pri psihološkem pristopu vpeljemo zgodbe, da je bil predmet uničen pod vplivom alkohola ali v afektu ali pa vpeljemo socialni vpliv – uvedemo dva tipa spletnih zavarovalniških formularjev (družinski in korporativni).

Izsledki so pokazali, da skoraj nihče ne goljufa veliko, večina pa jih nekoliko priredi zneske. Ljudje, ki so nekaj uničili v afektu, na splošno manjkrat zahtevajo zavarovalnino. Tisti, ki so bili pod vplivom alkohola, manjkrat zahtevajo odškodnine v družinskih zavarovalnicah. In zakaj je tako? Ljudje, ki so nekaj uničili iz jeze, krivijo sebe. Tisti, ki so bili pod vplivom alkohola, pa krivijo pijačo.

Zaključki

V zavarovalniškem kontekstu je šlo za doseganje vedenjske spremembe. Če pristop deluje na področju zavarovalništva, ni razloga, zakaj ne bi deloval tudi na področju varnosti. Vedenjska sprememba je bolj verjetna, če uporabimo psihološki pristop. Ljudi je mogoče mehansko siliti, da sledijo varnostnim navodilom, vendar je uspeh večji, če se jih zmanipulira. Bolje je, da se jih ne sili, ampak prepričuje (angl. *harsh vs. soft authority*). Verjeti je treba, da so ljudje dovolj pametni za racionalno odločanje.

DUŠAN ZUPANČIČ: RAZVOJ VEČPLATFORMSKIH APLIKACIJ APACHE CORDOVA

Dušan Zupančič je predavatelj z dolgim predavateljskim stažem na področju razvoja. Zadnjih 10 let se ukvarja predvsem z iskanjem rešitev na področju informacijske tehnologije pri večjih mednarodnih projektih. Trenutno se v podjetju Gorenje, d. d., ukvarja z aplikacijo za mobilne naprave za Gorenjeve povezljive gospodinjske aparate, ki bo temeljila na ogrodjih Cordova in Ionic.

Slika 1: Utrinek s predavanja Dušana Zupančiča

Nenehno ponovno izumljanje spleta

Skozi leta so se naše potrebe povečevale in spreminjal se je tudi razvoj. V nadaljevanju si poglejmo časovnico sprememb:

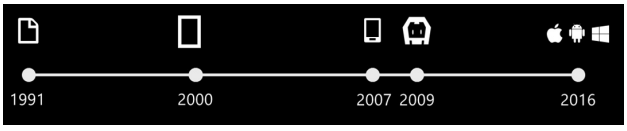
1991 – začetek HTTP, enostavni HTML-dokumenti itd.;

2000 – DHTML in Web 2.0 – dokumenti → aplikacije;

2007 – Apple je precej povečal priljubljenost mobilnega brskanja po spletu (dogovori s ponudniki podatkovnega prenosa …), aplikacije so se začele seliti z namiznega računalnika na telefone, kjer se izkušnja z uporabo senzorjev in drugih dodatkov mobilne naprave (fotoaparat …) še izboljša;

2009 – na iPhoneDevCamp v San Franciscu je bil predstavljen PhoneGap podjetja Nitobi; uspešno je zapolnil nišo med omejitvami brskalnika in zmožnostmi telefona (leta 2011 je Adobe prevzel podjetje in ime PhoneGap, vendar je produkt še vedno na voljo v odprtokodni različici pod imenom Cordova);

2016 – spremenilo se je dojemanje uporabnikov in mnenje o tem, kakšna mora biti uporabniška izkušnja, pomemben je design; čaka nas torej še eno ponovno izumljanje spleta



Slika 2: Razvoj spleta skozi čas (NTK, 2016)

Kaj je Apache Cordova?

To je odprtokodno ogrodje za razvoj mobilnih aplikacij na osnovi HTML5, CSS3 in javascripta. Ista rešitev se lahko prevede za izvajanje na različnih platformah. To pomeni, da zadošča ena skupna koda. Kljub aplikaciji, napisani v HTML5, CSS3 in javascriptu, je končni rezultat izvedljiva binarna datoteka za posamezno platformo (IPA – iOS, APK – Android, XAP – Windows Phone …).

Hramba podatkov pri razvoju z ogrodjem Apache Cordova

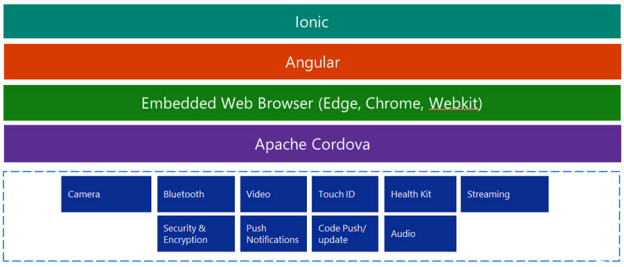
Podatke lahko hranimo na tri različne načine:

- v pomnilniku (začasna hramba);
- lokalno (localStorage, WebSQL; možnost trajne hrambe na napravi, možnost hrambe v predpomnilniku (angl. *cache*) za offline dostop do oddaljenih podatkov);
- na osnovi oddaljenih storitev (storitve REST/JSON; možnost uporabe poljubne storitve JSON, možnost uporabe Azure App Service, ki ponuja enostaven dostop do baze v oblaku preko JSON).

Kaj je Ionic?

To je odprtokodno ogrodje, ki na osnovi komponent HTML, CSS in JS olajša razvoj mobilnih aplikacij; zgrajeno je na ogrodju Angular, ki upošteva oblikovna določila platforme, na kateri teče (statusna vrstica je npr. pri Androidu zgoraj, pri iOS-u pa spodaj …). Ima zmogljiv CLI (Command Line Interface) za izgradnjo predloge aplikacij itd. ter tržnico za predloge aplikacij, vtičnikov in tem.

Arhitektura rešitve z ogrodjem Ionic



Slika 3: Grafični prikaz arhitekture programske rešitve, razvite z ogrodjem Ionic (NTK, 2016)

Ionic 2

Nekaj malenkosti je bilo predstavljenih tudi o beta različici Ionic 2. Novo ogrodje ima prenovljen CLI, posodobljeno strukturo datotek in še mnogo drugega. Pomembno je poudariti, da je celotno ogrodje po novem grajeno na ogrodju Angular 2.

Zaključek

Po predavanjih in razpravi smo zaključili, da sta tako Cordova kot Ionic v fazi, ko že veljata za dozoreli tehnologiji, da imata dovolj bogat ekosistem in da zanju argument o slabšem delovanju ne velja več.

Reference

NTK, 2016. [online] Dostopno na: http://www.ntk.si [14. 11. 2016].

Miran Lešič in Luka Juršnik