Informacijska sigurnost

ZAŠTITA mobilnog računalstva

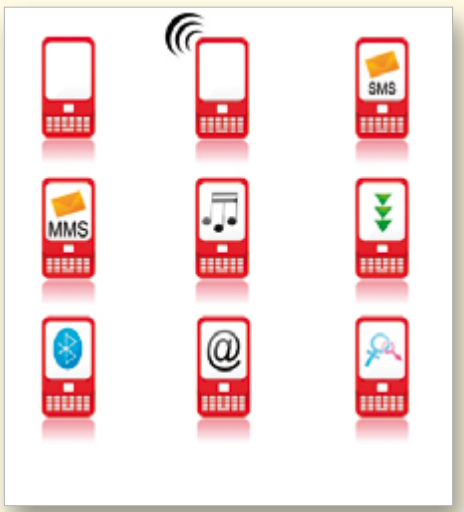
Informacijska se sigurnost već neko vrijeme ne promatra samo u okviru tvrtke i njenih lokacija na kojima je smještena ICT oprema. Novi koncepti, kao što su cloud ili BYOD, nezadrživo ruše ustaljene načine osiguranja povjerljivosti, cjelovitosti i raspoloživosti vaših poslovnih informacija. Kako se vi nosite s tim?

DALIBOR UREMOVIĆ

Sigurnost poslovnih informacija postaje noćna mora menadžerima sigurnosti; crni se scenariji vrte u glavi. Nerijetko se čuju prijedlozi uvođenja mjera zaštite kao u doba izvanrednog stanja i uvođenja policijskog sata. No nema smisla navlačiti teške oklope ili zabijati glavu u pijesak. Razmotrimo što sve možemo učiniti da bisni pokušali ovakvu situaciju staviti pod kontrolu.

Organizacijske i proceduralne mjere

Uvijek je dobro poći od *top-down* modela, ali pritom kontrolirati da se ono što je dogovoreno na vrhu praktično primjenjuje. Ako već imate politiku, pravilnik ili priručnik o informacijskoj sigurnosti, odnosno bilo koji drugi dokument koji propisuje načine zaštite koje će provoditi organizacija, samo ga dopunite i proširite s par članaka vezanih uz sigurnost mobilne komunikacije i računalstva. Unutar tih dokumenata svakako bi trebalo ubaciti odredbe koje se tiču instalacija dopuštenih i nedopuštenih aplikacija, korištenja web preglednika i SMS-a, geolokacijskih servisa, spajanja putem bežičnih veza odnosno Bluetootha, *tetheringa* (korištenja mobilnog uređaja kao WiFi pristupne točke), upotrebe kriptografije i zaporki, rada s *cloud* spremištima podataka i servisima, korištenja lokalnog spremišta podataka na uređaju te postupak u slučaju incidenta.



Mnoštvo vrsta komunikacija i servisa koje je moguće ostvariti putem mobilnih platformi

Naravno, ne zaboravite sve dokumente distribuirati do onih koji ih trebaju provoditi. Podrazumijeva se organizacijska jedinica za informacijsko-komunikacijske tehnologije, ali i svi djelatnici organizacije, pa i vanjski partneri, ako rade s vašim povjerljivim podacima. Osim distribucije i potvrde primitka i razumijevanja onog što u njima piše, periodična provjera mjera potrebna je da sve ne ostane samo mrtvo slovo na papiru. Provjere politike na tehničkoj je razini uobičajeno raditi putem MDM poslužitelja.

Sigurnost mobilnog komuniciranja svakako treba uvrstiti i u program podizanja razine svijesti o informacijskoj sigurnosti (*security awareness program*). Bez obzira na primjenjivost politika i procedura, uvijek će se dogoditi da se neki prijenosni uređaj izgubi ili bude ukraden. U tom je slučaju potrebno predvidjeti i postupke odgovora na takve incidente. Korisnici bi to trebali prijaviti sistemskoj podršci, koja će imati spremne aktivnosti jer će ih unaprijed isplanirati.

Krađa i gubitak samog uređaja nisu jedino što nas može zadesiti. S porastom funkcionalnosti i kapaciteta spremišta prijenosnih uređaja moramo ih početi tretirati jednako kao i bilo koji drugi IT resurs te se pripremiti i na mogućnost gubitka podataka koji su nam ključni i po pitanju raspoloživosti, a ne samo povjerljivosti. Za ovu ih je priliku zato potrebno uključiti u redovite procedure izrade pričuvne pohrane i brzog vraćanja uređaja u funkciju, ako je to potrebno.

Kontrola pristupa

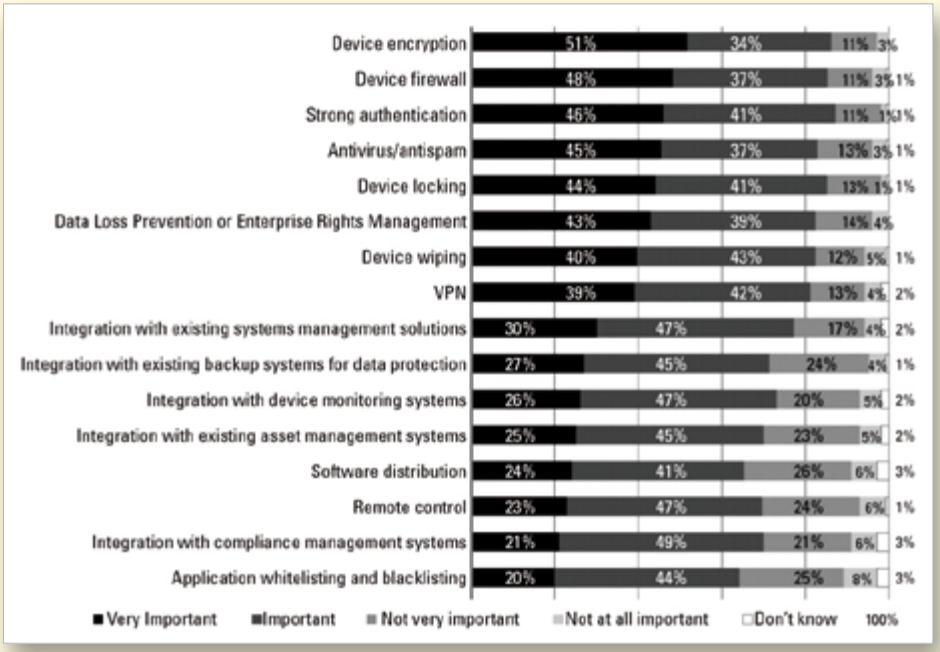
Teorijska pravila i postupke iz upravljačkih dokumenata treba praktično i provesti. Jedan od glavnih aspekata zaštite mobilnih uređaja i informacija vezanih uz njih jest kontrola pristupa tih uređaja na kor-

porativnu mrežu. Pretpostavka je da za vanjske veze koristite VPN (IPSec ili SSL, primjerice) pa je potrebno ispitati kako se trenutno korištena tehnologija može upotrijebiti i za pristup mobilnih uređaja. Danas je situacija puno bolja nego prije par godina pa je većinu mobilnih uređaja (laptopi, tableti, smartfoni) relativno lako uključiti u postojeću VPN proceduru. Spajanje na korporativnu mrežu jednostavno je postalo nužnost - što zbog pristupa *e-mail* poslužiteljima, što zbog sve većeg broja web aplikacija koje imaju i svoje mobilno klijentsko sučelje za rad. Naravno, tu su i razna RDP ili VNC spajanja sistemskih administratora radi obavljanja standardnih sistemskih poslova.

Nažalost, kontrola veza (WiFi, 4G, GPRS, EDGE, Bluetooth, IR...) prema vanjskoj okolini kudikamo je problematičnija. Riječ više nije samo o jednoj žici koju je moguće lako kontrolirati na granici sustava (korporativna mreža) te je potrebno poduzeti druge mjere kako bi se rizici sveli na najmanju moguću mjeru. U ovom slučaju možemo poći od politike zaporki (i PIN-ova) koja mora slijediti jednaka pravila kao i za ostale uređaje unutar korporativne mreže. Osim toga, moguće je i propisati koje je veze sve dopušteno ostvarivati te što je sve dozvoljeno unutar koje veze. Na djelu tada imamo kontrolu pristupa prema definiranim zonama koju inače već koristimo na raznim već poznatim mjestima (primjerice Public, Home ili Work zone, zone u web preglednicima i sl.).

Konfiguriranje samih uređaja

Osim kontrole pristupa, potrebno je propisati konfiguracijske postavke i konfigurirati uređaje te time zaštititi ostale veze kojima uređaj komunicira s okolinom (v. sliku). Jedno od područja jest zaštita od zlođudnog koda te je zato potrebno izabrati i primijeniti neko od antivirusnih rješenja. Neka od ovih rješenja sadržavaju i osobni vatrozid te još mnoge druge funkcionalnosti poput lociranja uređaja putem geolokacijskih servisa, zaključavanje odnosno brisanje povjerljivih podataka u slučaju gubitka ili krađe i sl. Ovakav softver možete propisati korisnicima za obavezno korištenje ili, još bolje, koristiti neku od centraliziranih *end-point security* platformi te tako imati puno bolju kontrolu nad instalacijom i korištenjem.



Izvor: Enterprise Strategy Group 2010.

Kako biste ocijenili važnost mjera zaštite mobilnog računalstva?

Neke od sigurnosnih postavki uređaja korisnici sami isključuju, poput opcija zaključavanja i otključavanja uređaja, jačine zaporki, pamćenja zaporki prilikom prijave na razne sustave i sl. U slučaju gubitka ili krađe uređaja time ste izloženi automatskom otkrivanju povjerljivih podataka. Kako je rečeno ranije, ovo je potrebno propisati proceduralno, ali i primijeniti one tehničke mjere koje će onemogućiti korisnika da mijenja ove osjetljive postavke. Također je dobro postaviti i preventivno neke od mogućnosti koje ćemo daljinski pokrenuti u slučaju krađe ili gubitka. Tu su svakako zanimljive opcije udaljenog zaključavanja, upotrebe geolokacijskog servisa za lociranje uređaja ili udaljeno brisanje povjerljivih podataka.

Ako korisnici rade s povjerljivim podacima organizacije, potrebno je razmotriti i neko od rješenja za kriptiranje mobilnog uređaja, odnosno dijela spremišta na kojem će se takvi podaci držati. Uobičajeno je da se kriptiranje koristi, osim na spremištima podataka, i na svim onim mjestima koja predstavljaju točku komunikacije. Tako je mehanizme kriptiranja potrebno primijeniti i za elektroničku poštu, SMS poruke, kontakte ili primjerice kalendar. Ako mobilni uređaj ne podržava neku vrstu hardverske enkripcije, u tu svrhu poslužit će i neka od danas raspoloživih aplikacija, često unutar kompletnih antivirusnih rješenja.

Otkuda početi

Kako bi se primijenila neka od mjera zaštite koje su dosad spomenute, opseg primjene mora se jasno dogovoriti i definirati. Pritom treba jasno razlučiti službene od privatnih mobilnih uređaja. I dok kod službenih lako možemo propisati sve što smo naumili, privatne nećemo moći tako lako kontrolirati te će manje-više sve ostati na organizacijskim i proceduralnim mjerama.

BYOD teško možemo ignorirati, osim ako radimo u nekoj organizaciji koja barata s vrlo tajnim podacima. U tom su slučaju program edukacije te jasno propisana i distribuirana pravila prva i najvažnija točka.

Istraživanje koje je provela analitička kuća Enterprise Strategy Group još u 2010. na uzorku od 174 ispitanika (uglavnom direktori informatičkih organizacijskih jedinica) može poslužiti kao polazna točka za plan implementacije mjera zaštite. Mjere mogu proizići i kao rezultat procjene rizika koja će nam ukazati na mjesta na kojima smo najranjiviji. Naravno, koristeći strukturni pristup svakako ćemo prvo propisati politiku odnosno pravilnik koji ćemo potom implementirati i na tehničkoj razini te se nadati da smo dovoljno dobro zaštitili informacije koje obrađujemo tehnologijama mobilnog računalstva. @

JAILBREAKANJE I SIGURNOST

Izdvojit ćemo ovaj segment rada s mobilnim uređajima koji neki korisnici vole kako bi izbjegli ograničenja koja su im postavili proizvođači uređaja i operacijskih sustava. Ovdje prvenstveno mislimo na smartfone i tablete koji prilikom *jailbreakanja* otvaraju korisnicima još jedan čitav novi svijet. Jedno od osnovnih ograničenja jest pristup trgovinama aplikacijama, pri čemu su posebno poznati AppStore ili Google Play. I dok je softver na ovim tržnicama standardnih verzija operacijskih sustava koji dolaze na uređajima kontroliran i testiran na zlođudni kôd, postupkom *jailbreakanja* dolazimo do mnoštva softvera koji nije prošao razne faze testiranja, odnosno razbijenih i "besplatnih" verzija komercijalnog softvera. Ne moramo napominjati koliki rizik ovo unosi u rad, pogotovo imajući u vidu trendove proizvodnje zlođudnog koda za mobilne platforme koji ima strahovitu uzlaznu putanju. Među raznim zlođudnim aktivnostima koje čine standardni set pisaca ove vrste koda jesu prikupljanje podataka o kontaktima, bilježenja lokacije uređaja, korištenje uređaja za slanje spam poruka, brisanje podataka ili slanje povjerljivih podataka na udaljena računala pod nadzorom napadača.