informaciju ili provjerava informaciju na Internetu, veća je vjerojatnost da će korisnik izgraditi povjerenje, nego kada svaki put dobije drugačiju informaciju. Uz sve navedeno, tu i je najveća snaga mobilnih rješenja.

Uspjeh počinje na – početku

Dobri poslovni rezultati kao rezultat uvođenja mobilnih rješenja, obično nisu posljedica slučajnosti. Uvođenje mobilnog rješenja nije trivijalan posao i zahtjeva stručnjake specijalizirane na tom području, posebno u području planiranja, pripreme i vođenja takvog projekta. Planiranje i detaljna analiza poslovanja i potencijalnih područja gdje će mobilno rješenje dovesti do najviše koristi, daje veću vjerojatnost uspjeha projekta i stvarnog benefita.

Podrška i aktivna uključenost menadžmenta u projekt je jedna od ključnih stvari u uvođenju. Jasno definiranje očekivanja, ciljeva i rokova, pridržavanje istih, pravovremena nabavka opreme, korištenje projektne metodologije – sve su to bitni faktori uspjeha. Problemi i nedosljednost u bilo kojem segmentu dovode u opasnost cijeli projekt. Obzirom na brojnost različitih timova u izvođenju projekta, vođenje projekta je izuzetno bitno i trebalo bi biti obavljeno od stručnih ljudi osposobljenih i iskusnih na tom području. Stručnost u samim mobilnim rješenjima je korisna ali ne i presudna kod odabira voditelja projekta.

Mjerenje poslovnih rezultata prije i poslije uvođenja mobilnog rješenja, dat će stvarnu sliku o uspješnosti i učinkovitosti u usporedbi sa očekivanim rezultatima. Ukoliko tvrtka nema potrebne kompetencije unutar kuće, korištenje usluga partnerskih i vanjskih firmi sa iskustvom u uvođenju mobilnih projekata povećat će šanse za uspješno provođenje i stvarnu korist.

Andrej Radinger

Plan sigurnosti

Osnovne smijernice za izradu plana sigurnosti osobnih podataka

Prema nekim procjenama preko 90% svih informacija danas se stvara i pohranjuje u računarskim sistemima. S obzirom da se u njima sve više prikupljaju, obrađuju, pohranjuju i razmijenjuju podaci i informacije od vitalnog interesa za organizaciju čiji su dio, a nerijetko i od šireg društvenog interesa, njihov nesmetan rad postaje preduvjetom ne samo njihovog funkcioniranja već sve više i cijelog društva koje se na njih sve više oslanja. Budući da je to moguće postići samo ako postoji zadovoljavajući stupanj njihove sigurnosti, načelo sigurnosti je jedan od temelja njihovog rada.

Zakonsko reguliranje pitanja informacijske sigurnosti

Upadi u računarske sisteme su realnost. Zloupotrebe informacijsko-komunikacijskih sistema treba prihvatiti kao neminovne prateće negativnosti društvenog razvoja, no treba im se svim sredstvima suprostavljati.

Zakonsko reguliranje pitanja informacijske sigurnosti započelo je pravnim reformama sedamdesetih godina zašitom baza podataka s osobnim podacima građana.

Kaznenopravna odgovornost za zaštitu privatnosti (osobnih podataka građana, odnosno baza podataka u kojima su pohranjeni) proširila se na područje kompjuterskog privrednog kriminaliteta (neovlaštenog pristupa drugim kompjuterskim sistemima – tzv. *hacking*, kompjutersku sabotažu, kompjutersku špijunažu i prisluškivanje, te razne druge manipulacije podacima na kompjuteru ili uz njegovu pomoć). Uskoro se širi i na područje pravne zašite intelektulanog vlasništva (kompjuterskih programa, topografije mikroelektroničkih poluvodičkih proizvoda i baza podataka i njihovog sadržaja), a od nedavno, posebno kao posljedica sve većeg korištenja telekomunikacija i širenja Interneta, i na zaštitu od prezentacije i distribucije raznih štetnih i nezakonitih sadržaja (pornografija, pedofilija, pranje novca, organizovani kriminal) koji se komunikacijskim kanalima putem Interneta brzo i jednostavno prenose između kompjutera, odnosno njihovih korisnika. Zakon uzima u biti dvosmjerni pristup u rješavanju izazova uzrokovanih opsežnim korištenjem informacija u elektroničkom obliku, kao i potencijalne štete koje mogu nastati kada se desi proboj sigurnosti i informacije budu ugrožene:

- Zakon definira nelegalnim određene vrste ponašanja koja krše sigurnost nečijih podataka, te određuje kazne za one koji se upuštaju u takva ponašanja;
- Zakon nameće na one poslovne subjekte koji posjeduju osjetljive podatke obavezu štićenja tih podatka i odgovarajućih informacijskih sistema u cilju zaštite različitih zainteresiranih stranaka.

Izrada plana sigurnosti osobnih podataka

Cilj zakona o zaštiti osobnih podataka je da se na teritoriji određene države svim licima, bez obzira na njihovo državljanstvo ili prebivalište, osigura zaštita ljudskih prava i osnovnih sloboda, a naročito pravo na tajnost u pogledu obrade osobnih podataka koji se na njih odnose. Europska direktiva o zaštiti osobnih podataka, zahtijeva od kontrolora i, u okviru svoje nadležnosti, obrađivača osobnih podataka izradu plana sigurnosti podataka kojim se određuju tehničke i organizacione mjere za sigurnost osobnih podataka.

Razvoj zakonski usklađenog programa informacijske sigurnosti uključuje iterativan proces koji zahtijeva da organizacija učini sljedeće:

- **Identificirati organizacijsku informacijsku imovinu;**
- **Provesti periodične procjene rizika:**
- Identificirati specifične prijetnje informacijskoj imovini,
- Identificirati ranjivosti informacijske imovine,
- procijeniti moguće štete ukoliko se prijetnje ostvare i iskoriste ranjivosti.
- **Utvrditi i implementirati sigurnosne kontrole:**
- S obzirom na kategorije sigurnosnih kontrola utvrđenih u važećim zakonima,
- U svjetlu rezultata procjene rizika i drugih relevantnih čimbenika.
- **Pratiti i testirati program informacijske sigurnosti kako bi se osiguralo da je učinkovit.**
- **Kontinuirano pregledati i prilagođavati program u svjetlu tekućih promjena.**
- **Nadgledati treće strane pružatelje usluga.**

Procjena utjecaja na privatnost *(Privacy impact assessment - PIA)* je također važan alat za identificiranje i ublažavanje mogućih problema povezanih sa pitanjima zaštite privatnosti klijenta u okruženjima automatake obrade podataka i umreženih informacijskh sistema.

Haris Hamidović,
IRCA ISMS auditor

Knjiga „Priručnik za izradu i reviziju plana sigurnosti osobnih podataka u automatskoj obradi“, autora Harisa Hamidovića, dostupna je za pregled čitateljima preko najveće svjetske digitalne knjižnice Google books.