

# Zaposleni so najšibkejša točka varovanja informacij

**I**nformacijska varnost je že vrsto leto v vrhu prioritet direktorjev oddelkov IT, pri čemer se varnostne smernice in tveganja spreminjajo iz leta v leto. Katere so glavne smernice pri e-varnosti in kako se v družbi S & T Slovenija ukvarjajo s to tematiko, smo vprašali Mateja Saksida, svetovalca za varovanje informacij pri S & T Slovenija. »V praksi se velikokrat zatakne že pri samem pojmovanju informacijske varnosti, vendar mislim, da je najbolje, da jo razdelimo na dva dela – na zagotavljanje zaupnosti in na zagotavljanje razpoložljivosti in zanesljivost,« poudarja Saksida.

## Vzpostaviti celosten nadzorni sistem

Gibanja v svetu in tudi pri nas kažejo, da so vlaganja v opremo IT vedno manjša. »Oprema postaja zastarela in tudi izpadov pri strankah je bilo letos bistveno več kot v prejšnjih letih. Jedro problema je pogosto v tem, da podjetja ne merijo obremenitev strojne in programske opreme ter dejanskih izpadov. To pomeni, da direktor IT pogosto nima v rokah ustreznih argumentov, s katerimi bi lahko prepričal upravo, da poveča vlaganja v nakup opreme in informacijsko varnost. In to kljub temu, da so ta vlaganja ključna za uspeh poslovanja. Zato strankam priporočamo vzpostavitev celostnega nadzornega sistema, s katerim natančno merimo obremenjenost opreme in število izpadov, na podlagi teh podatkov pa je lažje načrtovati vlaganja v IT. Oprema je stara, to je dejstvo. In če ni denarja za novo, je treba vsaj

optimizirati staro, preveriti, kako jo je mogoče nadgraditi in dodati nove funkcionalnosti. V S & T Slovenija znamo poskrbeti tudi za te storitve,« pojasnjuje Saksida.

## Premalo vlaganj v izobraževanje

Na področju varovanja zaupnosti informacij v S & T Slovenija opažajo predvsem to, da organizacije premalo vlagajo v izobraževanje zaposlenih. Ti postajajo najšibkejša točka varovanja informacij v svetu in pri nas, kar v svojem poročilu o e-varnosti ugotavlja tudi Cisco. V prihodnjem letu naj bi se po napovedih Cisca povečal kriminal na področju socialnega inženiringa – torej neposrednega napada na ljudi. Njihove primarne tarče bodo predvsem tisti, ki uporabljajo socialna omrežja (denimo Facebook). Dejstvo je, da nihče več ne napada tehnologije, saj ta evidentira vsak korak. Bistveno lažje je priti do uporabnika, od njega pridobiti informacije in potem te informacije zlorabiti za vdor v sistem. »V letu 2011 bo izobraževanje uporabnikov ključnega pomena, če bomo hoteli zagotoviti ustrezno raven zaupnosti svojih ključnih informacij,« opozarja Saksida.

## Hekerje zanima le še denar

Varnostni strokovnjaki opažajo tudi vse večjo razširjenost škodljivih programskih kod, predvsem tistih, katerih delovanja ni mogoče zaznati s protivirusnimi rešitvami. Včasih sta hekerje zanimala predvsem slava in politično opredeljevanje, zdaj pa je pomemben samo denar. »Najhuje je, ker so ti škodljivi programi na voljo na internetu, dostopni so vsakomur, pa še

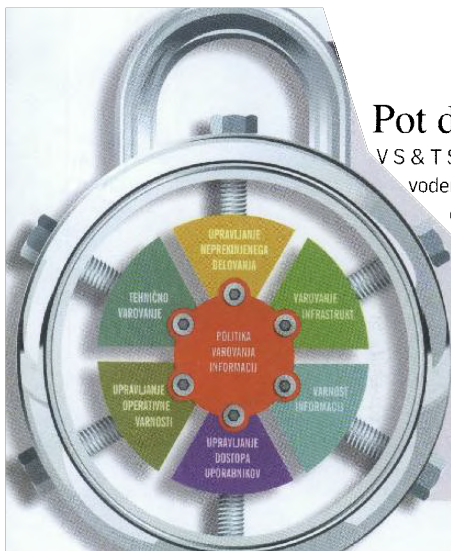
brezplačni so, tako da ni treba več imeti veliko znanja za vdiranje v informacijske sisteme,« razlaga Saksida.

## Ključavnica, ki varuje

Varovanje informacij je kompleksen sistem, zato so v S & T Slovenija oblikovali portfelj storitev za celostno varovanje informacij in mu dodali logotip ključavnice, ki nas že v izhodišču varuje. »V središču te ključavnice je sistem vodenja varovanja informacij. Če hočemo, da bo varnostna tehnologija ustrezno delovala, da bodo procesi ustrezno vodeni, vlaganja pa pravilno usmerjena, moramo najprej vzpostaviti sistem za vodenje varovanja informacij. Strankam svetujemo, da najprej vzpostavijo krovno politiko varovanja informacij in ustrezne organe za vodenje in upravljanje. Vodstvo se mora zavezati k temu, da bo zagotavljalo ustrezna sredstva in kadre za zagotavljanje ustrezne ravni informacijske varnosti; imeti moramo vodjo informacijske zaščite in odbor, ki se ukvarja z varnostjo in zna prepoznati tveganja,« poudarja Saksida.

## Najprej opredeliti, kje je potrebna višnja stopnja varnosti

Slabost v slovenskih podjetjih je, da se pravila in ravnanja na področju varovanja informacij oblikujejo le znotraj oddelka IT. V tujini ne poznajo več take prakse, saj je informatika tam v vlogi svetovalca in izvajalca. Informatiki v tujini ne odločajo o tem, kakšna naj bo dolžina gesel, katere podatke je treba šifrirati ali kako pogosto je treba izvesti varnostno kopiranje. Oni svetujejo, poslovni del pa postavlja varnostne zahteve. »Druga težava v Sloveniji je, da hočemo po navadi vse podatke zavarovati z najvišjo stopnjo varnosti. Bolj ko varujemo stvari, bolj so kompleksne za uporabo in več časa potrebujemo, da opravimo kakšno delo. Podatkov, ki bi jih morali v podjetjih varovati z najvišjo stopnjo, je največ pet do šest odstotkov (pogosto celo manj). V varovanje teh podatkov pa je smiselno vlagati denar in znanje. Varnostni sistemi stanejo, in če nimamo že v začetku jasno opredeljeno, katere informacije so tiste, ki potrebujejo višjo stopnjo varovanja, bomo zelo težko vzpostavili racionalen sistem,« še dodaja Saksida.



## Pot do dobre varnostne prakse

V S & T Slovenija pomagajo podjetjem vzpostaviti sistem vodenja varovanja informacij. Najprej pregledajo obstoječe stanje in jim svetujejo, kako naprej. Podjetje že v začetku ve, kaj ga čaka na tej poti do dobre prakse. V drugi fazi se opravi analiza tveganj, ki stranki razkrije, katere so prioritete. Po vzpostavitvi krovne varnostne politike ter opredelitvi vlog in odgovornosti postavijo še izvedbene politike. »Prednost družbe S & T Slovenija je v tem, da znamo teorijo prenesti v prakso. Temu je namenjen tudi portfelj storitev, ki smo ga poimenovali Varnostna ključavnica,« razlaga Matej Saksida, vodja informacijske zaščite pri S & T Slovenija.

