Eudace

Nekdo je brskal po mojem računalniku

..Kako ravnati v situacijah, ko sumite, da vam je nekdo ukradel podatke, nepooblaščeno dostopal in prenašal podatke z vašega računalnika..

Avtor: Andrej Zupan in Maša Kralj, Eudace, d. o. o.

Združene države Amerike kraja podatkov s strani zaposlenih letno stane do 200 milijard dolarjev. Ste se že kdaj vprašali, kako učinkovito upravljate s svojimi podatki? Kakšen je vaš postopek za varovanje podatkov ob odhodu sodelavca? Ali spremljate dostope svojih kolegov do podatkov? Kako ravnati v primeru suma kraje oziroma nepooblaščenega kopiranja podatkov? Z današnjimi tehnologijami, ki lajšajo vsakdanje delo posameznikov, so podatki postali dostopni na vsakem koraku, v vsakem trenutku. To so lahko osebni podatki, slike, gesla ali podatki podjetja. Doseganje primerne agilnosti podjetja in s tem povezana optimizacija časa nas nezavedno vodi v uporabo programske opreme, ki omogoča vpogled v podatke iz praktično vseh naprav, ki se povezujejo s svetovnim spletom. Programska oprema, ki je na voljo brezplačno, omogoča dostop do podatkov vsem – tudi tistim, ki s področja IT nimajo širokega znanja.

Kako si zaposleni odprejo vrata do podatkov?

Najbolj pogost (in tudi preprost) način za nepooblaščen vstop v informacijski sistem, glede na naša opažanja v praksi, je uporaba enega od programov za oddaljeni dostop. Najbolj razširjen program te vrste je vsem dobro poznan TeamViewer. Ta je dandanes nameščen na kopico računalnikov, saj ga tehniki pogosto uporabljajo za dostop do računalnika stranke v primeru težav. TeamViewer med drugim omogoča tudi vzpostavitev tako imenovanega računa, ki omogoča dostop do računalnika brez potrditve oziroma omogočanja dostopa na oddaljenem računalniku. Podobne rešitve za oddaljeni dostop so tudi VNC, ISL Light, Windows remote desktop in druge.

Dostop do omrežja podjetja je velikokrat omogočen tudi prek kanala VPN . VPN je virtualni kanal, ki ga uporabnik vzpostavi iz oddaljene lokacije na spletu in se poveže v lokalno omrežje podjetja. S tem dobi vse dostope, kot če bi sedel v pisarni (dostop do intraneta, datotek v skupni rabi, tiskalnikov, računalnikov, nadzornih sistemov).

Pri uporabi platforme B2B ali druge spletne platforme za sodelovanje s svojimi kupci moramo biti še posebej previdni. Nenadzorovano dodeljevanje dostopov lahko omogoči zaposlenim, da si ustvarijo dostop za lažnega kupca, ki ga pozneje uporabljajo sami.

Na spletu so na voljo različne skripte, ki bodisi pošiljajo podatke na oddaljeno mesto bodisi omogočajo dostop do podatkov v določenem časovnem terminu.

Konkretni primer nepooblaščenega vstopa

V tem tednu smo bili svetovalci podjetja Eudace priča kraji podatkov iz računalnika ene od naših strank. Po preučitvi primera smo ugotovili, da je podatke iz računalnika pobrisal eden od bivših zaposlenih v podjetju (z izbrisom je bilo delo v podjetju za kratek čas močno oteženo), ki se je med vikendom povezal iz domačega računalnika (IP-ji so izsledljivi!). Do računalnika je dostopal v nočnih urah med vikendom, in sicer z uporabo prej omenjene rešitve TeamViewer. Če bi kdo onesposobil omenjeno aplikacijo, sta bila na računalniku nastavljena še dostop VPN in skripta, ki bi jo lahko aktiviral na daljavo in na ta način upravljal s podatki.

Kako ukrepati ob sumu kraje ali neupravičenega prenosa podatkov?

Najprej vam svetujemo, da nemudoma zavarujete svoje omrežje. Če nimate lastne službe IT, bo najboljši način, da izključite internetno povezavo dotičnega računalnika, najbolje pa kar celotne mreže podjetja. Preverite, kateri procesi tečejo na računalniku, in odstranite tiste, ki se vam zdijo sumljivi (če jih ne poznate, si pomagajte z Googlom). Ne brišite ali spreminjajte podatkov na disku.

Kaj o tem govori zakonodaja?

V primeru suma, da je nekdo neupravičeno vstopil ali vdrl v informacijski sistem ali neupravičeno prestregel podatke ob nejavnem prenosu v informacijski sistem ali iz njega, o tem obvestite policijo, kajti s tem je oseba izvršila zakonske znake napada na informacijski sistem. Za tako ravnanje lahko kršilec dobi zaporno kazen do enega leta. Če je podatke v informacijskem sistemu neupravičeno uporabil, spremenil, preslikal, prenašal, uničil ali v informacijski sistem neupravičeno vnesel kakšen podatek, oviral prenos podatkov ali delovanje informacijskega sistema, se kaznuje z zaporno kaznijo do dveh let. Če bi bila s takim dejanjem povzročena velika škoda, se kaznivo dejanje kaznuje z zaporno kaznijo od treh mesecev do petih let (221. člen Kazenskega zakonika, Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, v nadaljevanju KZ-1). Zloraba informacijskega sistema je podobno kaznivo dejanje, ki pa se ga izvrši ob gospodarskem poslovanju (237. člen KZ-1).

Z denarno kaznijo ali zaporom do enega leta se kaznuje oseba, ki vdre ali nepooblaščeno vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobila kakšen osebni podatek (143. člen KZ-1).

Če tako ravna zaposleni, stori kršitev pogodbenih obveznosti iz delovnega razmerja, ki imajo znake kaznivega dejanja, zaradi česar je podan razlog za izredno odpoved pogodbe o zaposlitvi (1. alineja 1. odstavka 110. člena Zakona o delovnih razmerjih, Uradni list RS, št. 21/13, 78/13 – popr. in 47/15 – ZZSDT).

Skladno s 306. členom KZ-1 pa se lahko z zaporno kaznijo do enega leta kaznuje tudi tistega, ki z namenom storitve kaznivega dejanja poseduje, izdeluje, prodaja, daje v uporabo, uvaža, izvaža ali kako drugače zagotavlja pripomočke za vdor ali neupravičen vstop v informacijski sistem.

Kako se lahko zavarujete?

Če želite trdno spati, vam svetujemo, da v podjetju vzpostavite sistem varovanja informacij ISO 27001. Pripravite politiko upravljanja s podatki, kjer specificirate potrebne posege v sistem IT ob prihodu novega zaposlenega in še bolj pomembno ob odhodu zaposlenega. Pripravite seznam potrebnih aktivnosti, da ne izpustite pomembnega dela pri zavarovanju svojih informacij ob tovrstnih dogodkih. Bolj konkretno in nekaj načinov za zagotavljanje osnovnega nivoja varnosti sistema IT si bomo pogledali v eni od naslednjih številk. (P. R.)