VARNOST MOBILNIH NAPRAV KOT KLJUČNI ELEMENT ZAVAROVANJA INTEGRITETE (POSLOVNIH) PODATKOV

Igor Bernik, UM FVV in FIŠ

Uvod

- Sodobne tehnologije so porušile mejo med komunikacijo v informacijskem sistemu organizacije in zunanjim svetom.
- Dostop do pomembnih podatkov od kjerkoli je preprost. Kaj pa varen?
- Je komunikacija s kibernetskim prostorom varna pred zlorabami?
- Smo z razvoj informacijske tehnologije zagotovili varen dostop do informacij in varnost njihovega prenosa?
- Poznamo ustrezne varnostne mehanizme za zaščito?

Dinamičen razvoj tehnologije, ozaveščenost, zahteve uporabnikov, hitre spremembe na pravem področju in kompleksnost sistemov zahtevajo ustrezno znanje.

Mobilne naprave

Mobilne naprave so postale pomemben del vsakdanjega življenja:

- So majhne, lahko prenosne, imajo veliko računsko in spominsko zmogljivost.
- Zaradi majhnosti jih je lažje odtujiti ali izgubiti, predvsem na javnih mestih. Manjše in zmogljivejše ko so naprave, večje je število odtujitev.
- Zaradi računske zmogljivosti in različnih zmožnosti povezovanja je z vdori možno prevzeti nadzor nad uporabo.

Razumevanje pravilne in s tem varne uporabe razumemo kot konkurenčno prednost v tekmi za prevlado v gospodarskem in znanstvenem svetu.

Uporaba naprav

Poznavanje zmožnosti mobilne naprave nam omogoča:

•Največji izkoristek naprave in nameščene programske opreme; s tem si olajšamo opravila, pospešimo delovne procese in spreminjamo način dela;

•Ugotoviti, prek katerih funkcij oziroma programske opreme smo ranljivi in s tem izpostavljeni grožnjam; tako lahko razvijemo oz. poiščemo primerne rešitve za zaščito.

Uporabniki, ki iste naprave sočasno uporabljajo za poslovne namene in zasebno, je večja verjetnost, da bodo tarča napada.

Varnost podatkov

- Podatki, ki jih prenašamo (na primer elektronska pošta, dokumenti ali podatki o prijavi v aplikacije v informacijskem sistemu organizacije – prenos podatkov med aplikacijami strežnika in odjemalca), so razmeroma lahko dostopni tistim, ki bi jih želeli zlorabiti.
- Le-ti ne potrebujejo niti posebnega znanja in priprav, saj je dostop in prenos podatkov slabo zaščiten.

Uporabnik se mora zavedati, da se ob vsaki vzpostavitvi dostopa vzpostavi povezava skozi zunanjo zaščito omrežja organizacije, s tem pa se pojavi informacijsko tveganje za celotno organizacijsko infrastrukturo.

Ko gre za vdore v sistem, sta trenutno najšibkejša člena uporabnik in njegova mobilna naprava, s katero vstopa v sistem organizacije.

Varnostna tveganja

Da zagotovimo varnost naprav, moramo poznati najmanj ključne varnostne grožnje, ki obstajajo na ravni:

- Dostopa do občutljivih podatkov, shranjenih na napravi,
- Dostopa do podatkov, shranjenih v poslovnem omrežju,
- Zlonamerne programske opreme,
- Sposobnosti nepooblaščenega izdajanja za pooblaščenega uporabnika – socialni inženiring.

Kriminaliteta in kibernetski prostor

Polega dela in podatkov se v kibernetski prostor prenašajo tudi različne oblike kriminalitete.

- Pojavljajo se nove oblike kriminalitete, povezane na primer s spletnimi socialnimi omrežji, saj količina osebnih podatkov, ki jih posamezniki izmenjujejo in objavljajo v internetu, hitro narašča, zlasti z vse večjo priljubljenostjo spletnih socialnih omrežij.
- "Koristno" se uporabljajo stare metode in tehnike, ki delujejo tudi v kibernetskem prostor; zaradi globalne dostopnosti pa so mnogo bolj donosne.

Kriminaliteta v kibernetskem prostoru

- Zaradi zapletenosti in kompleksnosti tehnologij in globalnosti je odkrivanje storilcev izjemno oteženo.
- Moč formalnega družbenega nadzorstva je v primeru zapletenih kaznivih dejanj manjša kot v primeru vsakodnevne kriminalitete, kar se še posebno kaže pri odkrivanju storilcev kibernetske kriminalitete.
- Odzivanje na kibernetsko kriminaliteto zahteva specializacijo in sposobnost zbiranja dokazov, da bi se storilce kibernetskih kaznivih dejanj ustrezno nadzorovalo in kaznovalo.

Ogroženost

Za zmanjšanje ogroženosti pred zlorabo mobilnih naprav in dvig zavedanja o varnem delu se morajo uporabniki zavedati nevarnosti:

- nepooblaščenega dostopa do omrežja,
- internetnih goljufij,
- kraj identitete,
- prestrezanje e-pošte,
- kraja gesel,
- kibernetskega nadlegovanja in izsiljevanja ...

Omenjene pojavne oblike se še dodatno krepijo pri stalnem dostopu in povezanosti v kibernetski prostor z mobilnimi napravami.

Sklep

- Stalen dostop v kibernetski prostor je odprl mnogo priložnosti za napadalce in izpostavljenost uporabnikov pred (kibernetsko) kriminaliteto.
- Če se zavedamo, da sodobne naprave niso varne, in sprejmemo vsaj osnovne ukrepe za varnejše delo, se izpostavljenost kriminaliteti zmanjša.
- Izobraževanje in usposabljanje o nevarnosti kibernetske kriminalitete mora na vseh ravneh družbenega življenja postati nekaj vsakdanjega.

Posameznik mora premišljeno in odgovorno uporabljati kibernetski prostor brez strahu pred zlorabo.

Diskusija