PRISLUŠKIVANJE - STVARNA PRIJETNJA INFORMACIJSKOJ SIGURNOSTI

„Zatvaranje vrata staje nakon što je konj pobjegao“ nije učinkovito rješenje

Kada se pojavi sumnja da su informacije procurile, mnoge će organizacije angažirati specijalizirane tvrtke kako bi otkrile ilegalno postavljene uređaje za prisluškivanje

Alen Gojak, prokurist u Signal Intelligence d.o.o. sigint.hr

PRISLUŠKIVANJE - ili prikriveno slušanje razgovora - nije ništa novo. Tijekom svoje evolucije napredovalo je od jednostavnog čina virenja kroz grmlje do točke u kojoj su se razgovori pratili izvan zgrade, blizu vrata ili prozora, ili sa skrivenih mjesta unutar objekta. Tajno prikupljanje podataka tehničkim sredstvima ili elektroničko prisluškivanje je ista stvar - osim što uključuje korištenje elektroničkih uređaja kao što su kamere, mikrofoni, RF odašiljači, i snimači. Razvoj tehnologije iznjedrio je novu prijetnju - kibernetičku špijunažu - koja se odvija putem interneta, računalnih mreža, mobilnih uređaja ili osobnih računala korištenjem tehnika hakiranja, i infiltracije sustava zloćudnim programima.

Kibernetička sigurnost je ključan preduvjet poslovanja, ali ne štiti izgovorene riječi

Iako kibernetička prijetnja opravdava čvrste sigurnosne mjere, staromodno prisluškivanje RF “bubicama”, zbog tehnološkog napretka i dostupnosti, prijeti korporativnom i financijskom sektoru u svijetu više nego ikada. Dobro skriven uređaj za prisluškivanje u sobi za sastanke banke, tijekom donošenja strateških odluka, je sve što je potrebno za ugrožavanje integriteta te banke i njenih klijenata. Afera s prisluškivanjem tajnih strateških sjednica Volkswagena tijekom 2017. i 2018. godine može nam poslužiti kao ilustracija. Audio snimci - u trajanju od 50 sati - pružaju uvid u to kako su visokorangirani menadžeri isključili jednog dobavljača.

Kada se pojavi sumnja da su informacije procurile, mnoge će organizacije angažirati specijalizirane tvrtke kako bi otkrile ilegalno postavljene uređaje za prisluškivanje. Iako se ovo može činiti logičnom reakcijom, ovakav pristup “zatvaranja vrata staje nakon što je konj pobjegao” nije se pokazao učinkovitim rješenjem.

Da bi se učinkovito upravljalo rizikom u području korporativne špijunaže, važno je da organizacije razmotre kohezivnu strategiju koja podupire cjelokupnu poslovnu strategiju. U idealnim okolnostima bilo bi potrebno odrediti posebne

Sofisticirane prijetnje informacijskoj sigurnosti

Visokokvalitetni digitalni audio odašiljači nerijetko koriste tehniku proširenog spektra (engl. Spread Spectrum) kao zaštitu od otkrivanja. Prošireni spektar je tehnika prijenosa koja za modulaciju signala koji prenosi informaciju koristi pseudo slučajni niz (kod) neovisan od signala informacije. Prošireni spektar ima vrlo široki frekvencijski raspon što ga čini vrlo sličnim signalu šuma. To ima za posljedicu težu detekciju, demodulaciju, presretanje i interferenciju s drugim signalima.

Najpoznatija metoda koja se koristi u zaštiti od otkrivanja prisluškivanja je širenje spektra skakanjem po frekvencijama (eng. Frequency Hopping Spread Spectrum-FHSS). Primjenom navedene tehnike signal tijekom emitiranja mijenja frekvencije i “skače” po unaprijed određenom i dogovorenom slijedu do 1600 puta u sekundi.

U profesionalnim krugovima koriste se i “rafalni” odašiljači (eng. Burst Transmitters) koji snimaju i pohranjuju audio podatke u integriranoj memoriji, a zatim ih u podatkovnim paketima odašilju do prijamnika. Period “rafala” može varirati između 30 i 250 milisekundi, odnosno prema korisnički definiranim intervalima.

Posljednjih godina iznimno su popularni Wi-Fi i Bluetooth audio snimači koji koriste tehnologiju “pohrani i proslijedi”. Drugim riječima, snimač 99 posto vremena radi u pasivnom modu i pohranjuje podatke na memorijskoj kartici, šifrira ih i zatim prenosi u zadanim intervalima na FTP poslužitelj ili se bežično preuzimaju. Kada je „online“, snimač može mijenjati MAC adresu, raditi u skrivenom načinu i daljinski se uključiti/isključiti, što otežava njegovu detekciju na WLAN mreži. Visokokvalitetni algoritam kompresije omogućava da se na memoriju od 128 GB pohrani preko 30.000 sati audio snimki bez potrebe za fizičkim pristupom uređaju. Snimači se isporučuju i kao modul kako bi se omogućila instalacija u uređaje pod napajanjem. Napadač 24 satni audio zapis neprekidnog snimanja preuzme za otprilike 12 minuta što je jedini period kada je snimač aktivan.

prostore ili sobe za sastanke u kojima se vode osjetljivi razgovori, a zatim provesti dovoljno primjerenih i proporcionalnih mjera kako bi se ti prostori zaštitili. Proaktivne posebne mjere tehničke zaštite su vrlo učinkovite ne samo u otkrivanju i uklanjanju prijetnji, već i u odvraćanju potencijalnih napadača jer su svjesni da su uspostavljeni sigurnosni postupci i protumjere. Cjelovitiji i strateški pristup prevenirat će potencijalne financijske gubitke i reputacijsku štetu koju bi elektroničko prisluškivanje moglo prouzročiti

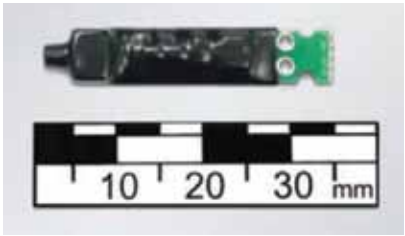
Postoji mnogo tehnika i tehnologija za provođenje tajnog nadzora i prikupljanja podataka tehničkim sredstvima, te nekoliko tehnika za zaštitu od elektroničkog prisluškivanja.

Posebne mjere tehničke zaštite (eng. Technical Surveillance Countermeasures), poznatije kao protuprislušni pregled, visokospecijalizirana je usluga koja otkriva tehnička sredstva za tajno prikupljanje podataka, te utvrđuje druge opasnosti i sigurnosne slabosti po informacijsku sigurnost. Procjena razine sofisticiranosti potencijalne ugroze prvi je važan korak pri izradi operativno-tehničkog plana, koji u konačnici određuje izbor adekvatne opreme i metodologiju postupanja. Na primjer, ako nam analiza ugroze pokaže da je ulazak neovlaštenog osoblja u ciljni prostor sveden na minimum, onda je za pretpostaviti da će napadač koristiti uređaj za prisluškivanje na stalnom napajanju, najvjerojatnije adaptiranom u električnom uređaju koji se nalazi u okruženju. Drugi mogući scenarij je penetracija iz susjednih prostorija što iziskuje temeljitu pretragu zidova, stropa i poda.

Poznavanje prijetnji, iskustvo, te širok izbor specijalizirane tehničke opreme nove generacije preduvjet su za uspješnu neutralizaciju rizika

Sigint kao partner privatnim detektivima

Privatni detektivi i članovi Hrvatskog Reda Privatnih Detektiva (HRPD) nerijetko u svojim istragama koriste usluge eksperata iz različitih područja, a sve kako bi klijentima pružili najbolju moguću uslugu. Jedan od partnera kada govorimo o kompleksnim protunadzornim pregledima privatnim detektivima je nerijetko i Sigint.



Žično ozvučenje

Osnovna karakteristika tzv. "žičnog ozvučenja" je da se tajno prikupljeni podaci, od njihovog izvora (ciljnog prostora) do mjesta prijema (prislušna baza) prenose putem provodnika različitih funkcionalnih i nefunkcionalnih instalacija. Najčešće su to telefonske instalacije ili instalacije električne mreže, dok se u izuzetnim slučajevima za prisluškivanje mogu koristiti nefunkcionalne, odnosno ilegalno ugrađene instalacije. Kod ovoga tipa prisluškivanja koriste se subminijaturni visoko-osjetljivi mikrofoni s analognom i digitalnom modulacijom, koji se ugrađuju u standardne električne uređaje, ili pak ukopavaju u zidove, strop ili pod. Kod žičnog ozvučenja ne postoji elektromagnetsko zračenje u slobodnom prostoru pa detekcija standardnim uređajima kao što je analizator spektra i širokopojasni detektor nije moguća, već istražitelji koriste posebna protuprislušna pojačala i analizatore ožičenja. Za otkrivanje ove vrste ugroze, od presudne je važnosti znanje i iskustvo istražitelja.

Sofisticirana i komercijalno nedostupna tehnička sredstva za tajno prikupljanje podataka koriste složene modulacijske tehnike i sisteme prijenosa podataka, te ih je moguće otkriti samo dugotrajnim i višeslojnim postupcima korištenjem različitih metoda i specijalizirane opreme. Poznavanje prijetnji, iskustvo, te širok izbor specijalizirane tehničke opreme nove generacije preduvjet su za uspješnu neutralizaciju rizika.

Signal Intelligence d.o.o. jedina je tvrtka u Hrvatskoj usko specijalizirana za posebne mjere tehničke zaštite. Korištenjem vrhunske tehnologije uspješno prepoznajemo napade iz širokog spektra prijetnji, te pomažemo klijentima u upravljanju rizikom i zaštiti njihove reputacije. Naši se projekti kreću od: Posebnih mjera tehničke zaštite (TSCM), zaštite od kibernetičke špijunaže (Cyber TSCM), analize mogućih prijetnji, te ranjivosti kompanije (OPSEC), forenzičkih istraga temeljenih na prikupljanju javno dostupnih podataka (OSINT) i digitalne forenzike. ■