Več varovanja, manj varnosti?

Tomaž Bratuša dipl.var.,CCE
Maldin d.o.o.
tomaz.bratusa@teamintell.com

The Inside Job

Analitiki skupine Cyber-Ark so z nedavno izvedeno anketo ugotovili, da:

- 60% pisarniških delavcev odkrito prizna, da si redno izdelujejo kopije pomembnih podatkov, ki jih bodo uporabili v primeru izgube službe.
- Zanimiva je ena izmed izjav anketiranca: **"Če bi nadrejeni in lastniki vedeli v kakšni količini in kolikokrat ključni podatki zapuščajo podjetje vam garantiram, da nikoli več ne bi mirno spali."**
- Kar 62% vprašanih je zatrdilo, da je prenos podatkov iz podjetja zelo enostavno početje.
- **40% zaposlenih, ki so priznali da si shranjujejo kopije pomembnih podatkov je povedalo, da bodo trenutno dostopne podatke uporabili v pogajanjih pri bodočih delodajalcih.**

V februarju je Dennis Blair, direktor nacionalne varnosti ZDA, pričal pred senatom glede ugotovitev dokumenta z naslovom "Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence“.

Glavna ugotovitev analize groženj je, da trenutno predstavljajo glavno grožnjo varnosti ZDA ravno kibernetske nevarnosti.

Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication. While both the threats and technologies associated with cyberspace are dynamic, the existing balance in network technology favors malicious actors, and is likely to continue to do so for the foreseeable future. Sensitive information is stolen daily from both government and private sector networks, undermining confidence in our information systems, and in the very information these systems were intended to convey. We often find persistent, unauthorized, and at times, unattributable presences on exploited networks, the hallmark of an unknown adversary intending to do far more than merely demonstrate skill or mock a vulnerability.

Energizer Trojanizer ;)

Energizer DUO USB je klasični polnilec baterij, ki deluje preko USB priključka. Polnilcu je priložena programska oprema preko katere lahko spremljate napolnjenost baterij.

Programska oprema, ki prihaja s polnilcem na vaš računalnik namesti trojansko datoteko *Arucer.dll*, ki se namesti v sistemski direktorij windows/System32 in napadalcu omogoča dostop do vašega računalnika preko komunikacijskih vrat 7777 TCP.

Nekaj podobnega se je pred dnevi zgodilo s HTC mobilnimi telefoni, ki so od ponudnika Vodafone prišli okuženi z zlonamerno kodo.

Informacijska tehnologija danes skrbi za nadzor in usmerjanje:

- dobave elektrike,
- zemeljskega plina,
- krimiljenja letališč in usmerjanja letal,
- delovanja železniškega prometa
- računalniško podprtih nevrokirurških operacij
- delovanja zavor vašega avtomobila
- ...

Sodobno industrijsko vohunstvo in kibernetski terorizem se širita tudi na področje avtomobilske industrije, kjer lahko prve znake vidimo v nedavnih dogodkih, ko se je izkazalo, da so zavore na vozilih Toyota Prius odpovedovale zaradi napake v programski opremi (CNN, 2010). Kako pravilno usmeriti varnostne službe, da bodo sposobne pravočasno odkrivati tovrstne grožnje se v letu 2010 sprašujejo tudi v senatu ZDA?

Časi, ko je vgradnja varnostnih ključavnic, namestitev varnostne razsvetljave, protivlomnih vrat, kontrole pristopa in alarmnih sistemov zadostovala za občutek večje fizične varnosti so že davno minili.

Informacijska varnost nikakor ni samo varnost informacij, temveč lahko kot smo videli njeno neustrezno zagotavljanje hitro privede do izgube življenj s tem, ko prične digitalna tehnologija zaradi zlorab napačno delovati.

Prihajamo v čas strateškega zbiranja informacij iz kibernetskega okolja?

Poglejmo si samo na primer rentgenski aparat ali linearni pospeševalec delcev, ki lahko v primeru napake privedeta do smrti pacienta, kar se je v preteklosti že dogajalo.

S trenutnimi orodji (antivirus, IDS, IPS...) je pravočasna identifikacija virov ogrožanja praktično nemogoča v kolikor v preiskavo incidenta ni vključen kvaliteten incidentni odgovor, digitalna forenzika in temeljita analitika dogajanja pred, med in po incidentu.

V Sloveniji imamo situacijo, ko večino podatkovnih strežnikov in računalniške infrastrukture teče na opremi ameriških proizvajalcev kot so Cisco, IBM, Oracle, Adobe, Microsoft ipd.

Tovrstna oprema je nato nameščena na najbolj kritične lokacije v državi kot so računalniški centri ministrstev, davčne uprave, letališč, elektrarn in ostalih ključnih podjetij. Ker so nameščeni izdelki in programska koda zaprtega tipa in podpisane pogodbe prepovedujejo vsakršen obratni inženiring (Angl. Reverse Engineering) država in uporabniki pravzaprav ne morejo vedeti kaj v bistvu sploh imajo nameščeno v svojih računalniških centrih in kdo vse ima dostop do njihovih sistemov.

Vpogled v tehnično dokumentacijo in 1. nivo skrivnosti izdelovanja in delovanja strojne opreme smo izgubili s težavami podjetja Iskra Delta okrog leta 1987, ko so ZDA ugotovile, da podjetje tehnologijo na skrivaj prodaja Rusiji in Kitajski.

Varnostna služba, ranljiv video nadzor in vdor v VNC

- Primer iz prakse

Več varovanja, manj varnosti!

To sta pred kratkim okusila ameriška velikana Google in Adobe v katera naj bi po poročanju medijev vdrli Kitajski internetni napadalci (Wired, 2010). Dogodek je v medijih bolj znan kot operacija Aurora v kateri so napadalci zlorabili varnostno vrzel internetnega brskalnika Internet Explorer in preko nje pridobili dostop do operacijskega sistema in datotek napadenih računalnikov.

Kitajska naj bi si s podobnimi napadi omogočila dostop do znanja s področij kot so

- termo-nuklearno orožje,
- pogonski sistemi podmornic,
- vesoljske tehnologije Space Shutle
- ...

Podobni usodi se lahko Slovenska podjetja in državne ustanove izognejo samo s kvalitetnimi preiskavami incidentov (digitalna forenzika), strateško analitiko, striktnim pregonom storilcev in pravočasnim odpravljanjem varnostnih vrzeli (varnostna testiranja)!