Arvutid kontrollivad inimeste elusid

25 aastat tagasi - 09.11.2001 Autor: Lauri Levo

Tehnika juhtimist usaldatakse aina rohkem arvutite kätte, mõtlemata seejuures nende haavatavusele. Üks hoolikalt valmistatud viirus võib pea peale pöörata kogu maailma juhtimissüsteemid, jättes inimesed ilma kõigest elutähtsast. Ükski arvutit kaitsev vall ei saa kunagi olema nii turvaline, et sellest hoida eemale kurbade tagajärgedega rünnakud. Kõik inimese loodu saab varem või hiljem sama liigi poolt murtud.

Katastroof katastroofi otsa

Elekter, mida võib pidada üheks tähtsamaks inimese abiliseks, on täielikult arvutite kontrolli all. Eluks vajalike ressursside hulgas on energia 21. sajandil raudselt esiviisikus, selle puudumine halvaks praktiliselt kõiki toiminguid ja muudaks mitmed igapäevased tegemised eluohtlikuks.

Ilma elektrita ei suudaks suurlinna elanikud üle päeva elada - seisma jääks praktiliselt kõik. Raske on ette kujutada, mis juhtuks talvises New Yorgis, kui elekter kaoks jäädavalt. Arvatavasti oleks ohvrite arv suur. Kui õnnetus on ajastatud päevasele ja soojale ajale, võib kodutee ja abi mureta leida, kuid pimeda ja miinuskraadide puhul muutub stsenaarium mustemaks. Tehnikajastu vahenditega ei suudetaks minna avasüli vastu kiviajale, kus lõkketule, vee ja metsloomade olemasolul võiks terve elu ära elada.

Elektri kadumisele järgneks rida õnnetusi: haiglad, küttesüsteemid, telefonid, suur osa ühistranspordist ja lennujuhtimiskeskused oleksid rivist väljas, samuti valguse ja turvameetmete puudumisel hakkaks tänavatel kriminogeense elanikkonna seas kiirelt valitsema anarhia, vabaneksid vangid jne. Fantaasial pole sellise olukorra puhul piire. Kuigi taoliste sündmuste jaoks on varutud tagavarasüsteemid, mis kriisi korral toitega varustavad, ei saa ka neile abilistele väga kindel olla. Ja isegi kui nad töötaksid laitmatult, ei ole nende varud ammendamatud.

Kolmas maailmasõda arvutites

Sõdivad riigid varuvad enda ümber hulga häkkereid ning asuvad vastaste arvutisüsteemidesse tungima. Võitjaks saab see, kes suudab vastaspoolele oma sissemurdmisega piisavalt palju laastamistööd teha. Näiteks pöörab pea peale nii õhu- kui ka maaliikluse regulatsiooni, kommunikatsioonivahendid või aktiveerib

sõjaväebaasides tuumapead. Selline võiks vabalt olla kolmas, kõrvalt jälgides, salaja toimuv maailmasõda. Samuti võib USA planeeritav raketikaitsekilp kord saada saatuslikuks hoopis neile endile, juhul kui mõni kinnisideega Lähis-Ida häkker sinna sisse murrab.

Arvutitele ei kujuta endast ohtu vaid viirused, vaid ka erineva sagedusega signaalisegajad, mida iga lihtinimene võib kurjadel eesmärkidel kasutada. Mobiiliga rääkimine segab nii haiglate aparatuuri kui ka lennumasinate tööd, samuti on pea kõik näinud, kuidas telefon raadiolaineid moonutab.

Ärajäänud suurõnnetus

2000. aasta saabumisel ennustasid IT-spetsialistid globaalsete arvutirikete esinemist Y2K-ks kutsutud probleemi näol. Infotehnoloogia algkümnendeil oli arvutimälu kümneid kordi kallim, seega kasutati mälu kokkuhoiuks sellist tarkvara, mis luges aastaarvudest ainult kahte viimast numbrit. Uusaastaööl järgneks 99 aastale 00, mida arvuti tõlgendab 1900. aasta saabumisena. Sündmused, mis sellise aastaarvestamisega järgnevad, võiksid olla ettearvamatud. kulutusi taolise olukorra ärahoidmiseks ülemaailmselt hinnati 8,580 triljonile Eesti kroonile.

Y2K probleem hakkas endast märku andma juba paar aastat varem, kui rahaautomaadid keeldusid EuroCheque pangakaartide omanikele raha väljastamast. Nimelt pidas arvuti aastatuhandeni kehtivaid magnetkaarte 1900. aasta omadeks ning luges neid juba sada aastat kehtetuks.

Kõige suurema löögi saajaks peeti Aasia ja Euroopa firmasid, kes vahetavad arvuteid välja teistest maadest märksa harvemini. Õnneks probleem lahenes ning suurem jälg Y2K-st jäi maha ainult Inglismaale, kus pangasüsteemides esines ajutisi häireid. Milleeniumi probleemi tagajärjed olid suuresti ülepaisutatud ja kandsid ainult ühte eesmärki: täita tarkvaratootjate kukruid.

Õnnetuste ennetamine

Vigadest õpitu põhjal on hakatud hoolikalt valima juhtarvutite operatsioonisüsteeme ja neid ümbritsevaid turvamüüre. Mitmetes suurfirmades on palgal häkkerid, kelle ülesandeks on turvaaukude otsimine ja parandamine. Viimase puhul võidakse kergelt orki lennata, sest sageli on palgatud nn Interneti-huligaane, kes jätavad palju auke enda teada ning mätsivad kinni vaid kõige läbinähtavamad. Seega proovige ainult süsteemi administraator töölt lahti lasta või siis talle lihtsalt vähe palka maksta, tagajärjed arvutivõrgule saavad olema kurvad.

Inimeludega manipuleerivad arvutid nagu lennujuhtimiskeskuste süsteemid peavad töötama veatult. Iga väiksem valearvutus või masinate kokkujooks võib endaga kaasa tuua palju ohvreid nõudva sündmuse. Lendude juhtimiseks kasutatakse laialdaselt DOS operatsioonisüsteemil põhinevat softi, millesse pidavat olema väga raske sisse murda, ainukeseks ohuks sellele on elektrikatkestus.
USA-s kosmoselendudega tegelev NASA ei häbene jälle väita, et nende kõrgtehnoloogilised süstikud kasutavad igivanu 486 Mhz protsessoriga raale. Pigem muuseumieksponaatidena esitletavaid igivanu arvuteid ei tahaks kosmonaudina enda ümber küll näha, eriti kui oled osa saanud nende sagedastest kokkujooksmistest. Kuid eks ole NASA teadlastel kogemusi ning etteheited arvutite valikuks oleks siinkohal kohatud. Eriti veel, kui pole mõtet karta, et Microsofti loodud operatsioonisüsteemid kosmosesse jõuavad.

Lauri Levo

- Uudised
- Turvalisus