

Aktivt innhold, 'malware' og datafisking

Det var enklere før. Da var datavirus og 'ormer' noe vi kunne forstå og dermed beskytte oss mot. Nå er variantene blitt for mange og kompleksiteten så stor at kun ekspertene kan bruke tid på å forstå hvordan de fungerer. Men beskytte oss må vi fortsatt. Og selv om også beskyttelsestiltakene er utenfor vårt kompetansefelt, er det nødvendig med grunnleggende kunnskap om truslene vi står overfor.

Malware – fellesbetegnelse på programmer og mekanismer som misbruker, skader eller på annen måte tar seg til rette på IT-systemer på egen hånd: Virus, ormer, trojanske hester, spyware og så videre.

Først når vi har denne forståelsen, kan vi foreta en rimelig risikoanalyse. All verdens trusler kan virke uoverkommelige når de fremstilles i avisen, mens de i praksis kan være irrelevante for vårt miljø. Når influensaen herjer landet, kan vi etter en vaksine vandre ganske trygt blant snufsende, nysende og hostende medmennesker. Immunitet får vi neppe, men vi har sørget for å redusere sannsynligheten for smitte til et minimum.

Over til høy beredskap

Med mindre vårt IT-miljø er uten forbindelse med omverden eller kjemisk fritt for Windows-systemer,⁷ er tiden overmoden for en grundig gjennomgang av forsvarstiltakene. Den negative utviklingen i trusselbildet de siste 2 årene er mer enn nok til å gjøre selv den mest robuste sikkerhetsansvarlig søvnløs. Noen forhold som karakteriserer utviklingen, er:

- ✓ Mengden av virus – gamle og nye – som traverserer Internettet og lokale nettverk, har tiltatt voldsomt.
- ✓ Tidsluken fra en svakhet blir oppdaget i et system, en applikasjon eller en tjeneste, til den blir utnyttet (misbrukt), er blitt vesentlig mindre.
- ✓ Metoder og mekanismer er blitt mer avanserte, og *malware* benytter i voksende grad flere samtidige spredningsmekanismer. *Spyware* og *phishing* (datafisking) lurer intetanende brukere til å avgi fortrolig informasjon i god tro, og etterlater seg ingen spor. Smarte programmer er blindpassasjerer på infiserte web-sider, gjemmer seg på brukerens maskin og aktiveres 'i skjul'.
- ✓ Tilfanget av verktøy og web-steder som hjelper hvem som helst til å lage og spre ulike former for *malware*, har tiltatt og er blitt mer sofistikerte. De sørger for at praktisk talt hvem som helst med ondsinnede hensikter kan utvikle og sette i gang et angrep.

⁷ Ingen plattformer er immune mot MALWARE, men det er et faktum at reell risiko reduseres med over 90% der Windows ikke brukes eller eksponeres for trafikk som kan være bærer av MALWARE.

- ✓ Moderne datavirus (for eksempel MyDoom), angriper først antivirusverktøyene på offeret og setter oppdateringsmekanismene ut av spill. Metoden demonstrerer på en fortreffelig måte hvor lite egnet dagens typiske antivirus-produkter er til å gi reell sikkerhet.
- ✓ Hensikten med *malware* har forandret seg. Den typiske 'jeg skal vise at jeg kan'-hacker, som låste eller blokkerte systemer, slettet filer og gjorde annen ugagn, er erstattet av vinningsforbrytere: De er ute etter fortrolig person- eller virksomhets-informasjon – bankkonti, kredittkort-informasjon, passord, brukernavn, produkt-data og så videre.

Aktivt innhold

Drivkraft nummer én bak denne negative utviklingen er såkalt aktivt innhold – web-sider med små eller store 'program-snutter' ('applets') som utføres på klienten. Den potensielle trusselen i slikt innhold har vært åpenbar siden Netscape introduserte JavaScript midt på 90-tallet, og ble eskalert til et nytt nivå da Microsoft introduserte ActiveX i 1997.⁸

Både markedet og Microsoft valgte imidlertid å overse de potensielle trusselbildene, og dagens begredelige situasjon kan med stor rett karakteriseres som fortjent. Mens aktivt innhold forlengst er blitt en viktig del av utallige web-applikasjoner, og uten tvil har bidratt til å gjøre nettleseren til det universalverktøy den er i dag, er det også vår største sikkerhetsmessige utfordring i hverdagen.

Trusselen fra aktivt innhold er dessuten ikke begrenset til nettleseren. Epost-klienter, IM-klienter (øyeblikks-meldinger) og kontor-applikasjoner er også utsatt. Årsakssammenhengen er alltid den samme: Tankeløshet og manglende fremsynthet fra leverandørenes side, eller kanskje i like stor grad opportunisme under motto "fang markedet først, fiks problemene etterpå". Og markedet har latt seg lure – i mange tilfeller med åpne øyne.

Aktivt innholds duale natur gjør trusselen spesielt vanskelig å få under kontroll. Situasjonen er sammenlignbar med kombinasjonen motorveier og biler. Motorveiene sørger for effektiv trafikkavvikling, men frister samtidig til høy hastighet – som i sin tur skaper ulykker. Overvåking er mulig, men vanskelig, krevende og kostbart. Å fjerne de dårligste kjøretøyene kan være en måte å bedre statistikkene på, og tilsvarende gjelder for aktivt innhold. Å blokkere ActiveX fjerner ikke bare en stor trussel, men gir også større grad av plattformuavhengighet. Samtidig blir et betydelig antall web-tjenester utilgjengelige eller uanvendelige, en pris som stadig flere finner akseptabel i forhold til gevinsten.

Aktivt innhold forekommer i 3 hovedkategorier:

- ✓ Web-sider med ActiveX, JavaScript, Java eller Visual Basic kode.⁹

⁸ Se artikkelen "Active-X: Ukjent – nei, trussel – tja?" i Mellvik-Rapporten nr. 42.

- ✓ Makroer, regneark-formler og annen applikasjonsspesifikk kode som utføres under åpning eller bruk av dokumenter.
- ✓ Tradisjonelle eksekverbare filer som dukker opp via vedlegg, lastes ned eller finnes i filsystemet. Her er den egentlige trusselen en kombinasjon av brukernes naivitet og systemenes 'brukervennlighet': Eksekverbare filer utføres automatisk i stedet for på brukerens kommando.

Mens vi kan sette i verk mange slags tiltak for å redusere både eksponering og graden av 'disponerthet' for disse truslene (vi har diskutert en rekke slike tiltak ved tidligere anledninger), er det viktigere enn noen gang å ha optimale filtreringsmekanismer på plass i infrastrukturen. Erkjennelsen av at tradisjonelle antivirusløsninger aldri kan gjøre en tilfredsstillende jobb, sitter ofte langt inne, men er desto viktigere å få på bordet. Falsk trygghet er verre enn ingen trygghet fordi den fjerner motivasjonen for handling. Antivirus-verktøy er ikke dermed verdiløse. De er nødvendige, men ikke tilstrekkelige på egen hånd.

Malware

Mens *malware* er en fellesbetegnelse på alle tenkelige varianter av 'infeksjonssykdommer' for datamaskiner, betegner *spyware* og datafisking mer spesifikke varianter av elendigheten. De to er dessuten av relativt ny opprinnelse, og derfor både minst forstått og krevende å

beskytte seg mot. Dessuten har terskelen for beskyttelse mot tradisjonelle virus – som vi var inne på ovenfor – blitt vesentlig høyere. Virusene er mer sofistikerte på alle måter, inklusive metodene de benytter for å holde seg skjult. Dessuten baserer de seg gjerne på opptil et halvt dusin ulike spredningsmekanismer i stedet for én enkelt, som tidligere var regelen.

Spyware

Spyware er en fellesbetegnelse på programmer som installeres uten brukerens viten eller samtykke, og deretter samler og viderefremidler personlig eller virksomhets-relatert informasjon i det skjulte. Slike programmer kommer som regel inn

Ubudne gjester på 20 minutter

En rapport fra IT-sikkerhets-organisasjonen SANS kunne for en tid siden fortelle at 'overlevelses-tiden' for en ny Windows-PC som kobles til Internettet, er nede i 20 minutter. Tallet understreker to hovedpoenger: For det første at sikkerhetsnivået en alminnelig PC leveres med, er lite verdt på egen hånd, og for det andre at hyppigheten av såkalte 'prober' som søker etter nye objekter å angripe, fortsetter å stige.

For egen del foretok vi for et par måneder siden et eksperiment som viser en annen side av samme problemstilling – som ligger enda tettere opp til dagens tema. En tenåring fikk til disposisjon en nyinstallert Windows 2000 PC som ble brukt mot Internettet en hel weekend. Han lastet ned et chatte-program, et par spill og brukte (etter instruks) Firefox når det lot seg gjøre – til Java-baserte spill og HotMail. Også MSN var hyppig i bruk. Maskinen var forøvrig godt beskyttet bak brannmur og NAT.

Etter helgen gjorde vi opp status, og fant et dusin programmer som hadde havnet på auto-opstart-listen i Windows Registry. De fleste av dem var harmløse i den forstand at de fungerte som kanaler for annonser og pop-ups, mens de resterende var av mer alvorlig karakter, og dukket opp igjen automatisk etter å ha blitt fjernet. Mer enn en halv dag gikk med for å få fjernet sporene etter 'festen'.

Erfaringen illustrerer for det første hvor utsatt alminnelige brukere er for *spyware* og andre former for *malware*. Alminnelige antivirus-programmer har beskjeden effekt mot slike 'inntrengere' – som uansett formål representerer en krenkelse av brukerens private sone, og dessuten spiser ressurser av utstyret. De fleste 'gutteroms-pcer' har mellom 15 og 50 slike programmer aktive til enhver tid, med innlysende konsekvenser for ytelsen. Er det rart PC-bransjen gnir seg i hendene?

⁹ Listen av typer aktivt innhold som potensielt kan misbrukes, har vokst over tid og inkluderer også Adobe pdf og Macromedia Flash. Trusselgraden knyttet til de ulike innholdstypene spriker imidlertid voldsomt, med ActiveX som den suverene ener.

sammen med web-sider eller som blindpassasjerer til andre programmer. Spill, fildelingsprogrammer og andre gratis programmer av ukjent opprinnelse er typiske bærere av *spyware*. Eksempler finnes også på at gratisprogrammer fra anerkjente leverandører er blitt kompromittert av blindpassasjerer.

Utover å benytte plattformer som ikke kan kjøre brorparten av disse *spyware*-programmene, skal det langt mer enn tradisjonell virusbeskyttelse til for å holde sin sti ren. De mest effektive beskyttelsesproduktene benytter en kombinasjon av trafikk-inspeksjon (grenseskontroll) og overvåking av og på klientsystemene. Ved å registrere og etablere et erfaringsbilde av nettverkstrafikken på klienten, kan slike produkter detektere og blokkere mistenkelige avvik. Videre kan de overvåke opprettelse av nye filer og programmer, samt endringer i Windows Registry, hvilket gir muligheter til å stoppe ubudne gjester før de får slått seg til ro.

Å drive overvåking og kontroll på dette nivå er imidlertid både ressurskrevende og komplisert, og har lett for å komme i veien for vanlig bruk. Derfor kan vi trygt observere at det fortsatt er et betydelig lerret som skal blekes før *spyware*-trusselen kan sies å være under tilfredsstillende kontroll.

Datafisking (PHISHING)

... er for tiden den raskest voksende metode for svindel via Internettet. PHISHING er en smart variant av dokumentforfalsking, der brukeren mottar en tilsynelatende autentisk epost fra for eksempel en bank, en kreditt-institusjon eller en offentlig etat. Hun eller han blir bedt om å oppdatere personlig informasjon, med passord, konti etc. Dataene som registreres går naturligvis direkte til svindlerne, mens brukere flest ikke aner at noe galt er på ferde.

Metoden dukket først opp i 2003, og har siden vokst med ca. 50% per måned! Den kolossale veksten til tross har vi først det siste halve året sett filtreringsprodukter som tar trusselen på alvor. I mellomtiden har flere nettlesere blitt oppjustert til på egen hånd å oppdage og hindre i alle fall de mest overlagte forsøk på datafisking. Heldigvis har denne type svindel karakteristika som gjør det om ikke lett, så i alle fall overkommelig å detektere forfalskningene. En del av dem stoppes av vanlige antivirus- og antispam-programmer, mens de mer sofistikerte variantene krever spesialfiltrering – enten i nettverket eller i nettleseren.

Netscapes nye nettleser, som ble annonsert og presentert tidlig i mars og blir 'klar til bruk' i løpet av sommeren, har nye, avanserte funksjoner mot både *phishing* og *spyware*. Ved siden av filtrering i nettverket, er nettleseren et naturlig 'hjem' for forsvar mot denne type angrep. Derfor er det rimelig å forvente at også andre populære nettlesere får tilsvarende funksjoner i tiden fremover.

Oppsummering

Kunnskap er makt – også når det gjelder virus og beslektede trusler. Om vi er sikkerhets-ansvarlig, drifts-ansvarlig, IT-sjef eller bruker, er viten om hvilke trusler som finnes og hvordan de fungerer, første forutsetning for å kunne gjøre noe med dem. Samtidig er det urimelig å forvente at brukere flest skal ha slik kunnskap – eller interesse for å forstå noe annet enn verktøyene vedkommende bruker. Derfor er det et krav at systemene og infrastrukturen er i stand til å beskytte brukerne, informasjonen og virksomhetene som er avhengige av IT-verktøy mot slike trusler.¹⁰ Vi vet at dette kravet ikke er tilfredsstillende i dag, og gjennomgangen ovenfor indikerer at utfordringen er større enn noen gang.

Bildet er imidlertid langt fra helsvart. Riktignok er det innlysende at tradisjonelle brannmurer og antivirusprogrammer ikke lenger utgjør et tilfredsstillende forsvarsverk. Dessuten forteller kunnskapen om hvordan de ulike truslene fungerer, mye om hva som skal til for å få bukt med elendigheten.

Vi kan avslutningsvis gjøre følgende observasjoner om 'rikets tilstand' og våre muligheter til å håndtere utfordringene:

- ✓ Mekanismen bak datafisking er å sende informasjon fra brukeren til et helt annet sted enn hun eller han tror. Slike omrutinger er alltid detekterbare – i nettleseren og i intelligente filtre. Derfor er problemet løsbart med riktige verktøy. Organisasjoner som ikke har full kontroll på hvilke nettlesere og versjoner som benyttes, må stole på filtrering.
- ✓ *Spyware* er malignante programmer som 'lures inn' på brukernes systemer. Dette er en hardere nøtt å knekke, blant annet fordi en rekke klient-plattformer ikke lar seg beskytte (for eksempel Windows 95 og 98). På plattformer som kan beskyttes, er det i mange tilfeller lett å sette beskyttelsen ut av funksjon. Derfor må vi igjen ty til intelligent filtrering i infrastrukturen kombinert med klient-baserte verktøy, eller gjøre noe med klient-plattformen (oppgradere til ferskere OS, gå over til tynne klienter, bytte plattform etc.).
- ✓ Nettverket er selve surstoffet for all *malware*. Uten nettverk, ingen trusler (av denne typen). Derfor er beskyttelsestiltak i infrastrukturen alltid mest effektive. *Malware* sprer seg i hovedsak via Web-sider og epost, og innsats på nettopp disse to områdene har størst nytteverdi. Vi er med andre ord tilbake til problemstillinger og løsninger som vi har diskutert en rekke ganger tidligere: Valg av nettleser og epost-filtrering som tar vare på sikkerheten i stedet for en ensidig fokusering på hva som er mest lettvinnt i øyeblikket. Verktøy som ikke gir god sikkerhet, bør være uaktuelle uansett hvilken funksjonalitet de måtte ha eller hvilken leverandør de kommer fra. ■

¹⁰ Vi har registrert (se side 30) at enkelte leverandører forsøker å velte ansvaret for sikkerheten over på brukerne. Dette blir som å forlange at passasjerene tar overlevelseskurs og bringer sin egen fallsjerm når de skal reise med fly. Tankegangen signaliserer en foruroligende useriøsitet og mangel på kontakt med virkeligheten.