

MYMAYDAY.COM

23. FEBRUAR 2009

KOMMENTAR

LEDERKOMMENTAR — HELGE SKRIVERVIK



Etter å ha konstatert at dagens løsning ikke strekker til, hva gjør vi? Ser oss om etter alternativer naturligvis. Alternativer finnes – også med hensyn til virus- og annen innholds-kontroll. Dessuten: Markedet er i bevegelse – høyst nødvendige, svært viktige forandringer.

What's in it for me?

Forenkling gir alltid bedre sikkerhet. Og forenkling på klientsiden er oppløst og vedtatt som nødvendig for å komme på offensiven i sikkerhetsmessig forstand. Da må beskyttelsestjenestene flyttes – hvilket er eksakt hva som skjer. Alle vinner – unntatt *the bad guys*. Det var på tide.

Kan nettskyen overta virusbeskyttelsen?

Hva er det AntiVirus-leverandørene ynder å fortelle oss? At deres treffprosent – hitrate på fagspråket – er 98% eller deromkring. Og dessuten at tiden fra nye varianter oppdages til deres signatur er på plass hos kundene er 'noen få' timer i gjennomsnitt. De har muligens belegg for sine påstander, men målestokkene stemmer ikke med virkeligheten.

Forskere observerer at den reelle *hitraten* for klient/host-baserte AV-produkter er rundt 80%, og fallende. Påstandene følges av både empiriske tall og observasjoner de fleste av oss lett kjenner igjen fra hverdagen. Én av dem er at dagens virus muterer vesentlig raskere enn distribusjonstiden for nye digitale signaturer. Konsekvensen er at selv de mest oppdaterte AV-systemer, de som ligger først i køen for signatur-oppdateringer fra leverandørens side, havner langt utenfor det vi kan kalle 'sanntids beskyttelse'.

Kombinert med det faktum at såkalte *Zero Day exploits* stiger raskt, blir konklusjonen åpenbar: Vi er på defensiven. Ingen nyhet i og for seg. Vi har ved en rekke anledninger diskutert *malware* og *spyware* i et

Analysar:

- ✓ Action Item -09: Senke kostnader uten investeringer
- ✓ Tid for NAC?
- ✓ Fra outsourcing til cloudsourcing
- ✓ Når nettleseren ikke strekker til...

Kommentarer:

- ✓ Du trenger et webOS
- ✓ Med blanke ark – og litt hukommelse
- ✓ Rude awakening
- ✓ Optimaliserer vi bort robustheten?

