

IT-revyen

Mellvik-Rapporten er verken avis eller nyhetsmagasin, men vi er definitivt opp-tatt av det som skjer rundt oss. Under overskriften IT-revyen kommenterer vi aktuelle nyheter og temaer i markedet og bransjen forøvrig. Vi konsentrerer oss om emner og trender som faller inn under MRS naturlige fagfelt, og inviterer leserne til å komme med innspill.

Epost fra Larry Gates?

Nei, på ingen måte. Vi mener Larry Ellison, Oracles svar på Bill Gates og en fremtredende IT-visjonær – i egne øyne. Suksess har Ellison definitivt hatt, og suksess tar vi av oss hatten for. Samtidig lider han åpenbart av et utemmelig Gates-kompleks, som i tillegg til å virke på grensen til naivt, tydelig forstyrrer Ellisons gangsyn. Noen annen forklaring på hans siste ‘epostale krumspring’ finner vi ikke. Med brask og bram annonserer han at Oracle vil overta markedet for store epost-tjenere – med en bombesikker løsning som utover å være sikker, også skalerer hinsides hva Exchange kan levere.

Noen burde klype herr Ellison i armen og minne ham om hvilken virkelighet både han og vi andre lever i. Riktignok ønsker vi langt bedre sikkerhet og skalerbarhet enn Exchange kan skilte med. Ingen ved sine fulle fem tror imidlertid at programmer som overstiger 100 linjer, kan garanteres å være sikre – eller 100% pålitelige for den del. Med hensyn til skalerbarhet, trenger vi kun å skjele til løsninger basert på andre plattformer enn Windows for å kunne håndtere belastninger som ligger to størrelsesordener over Exchange.

Ellisons fantasiverden stopper imidlertid ikke der. Han vil ikke ‘flytte brukerne ut av deres Microsoft-omgivelser’. Tvert imot er Outlook det foretrukne og sågar anbefalte brukerverktøy. Har ikke Ellison oppfattet at det i langt større grad enn Exchange er Outlook som representerer den største sikkerhetsrisikoen i hverdagen?

Underholdning er både nyttig og nødvendig, men fungerer best når underholderen er klar over sin rolle. Ellison mener åpenbart alvor, men kan umulig tas alvorlig. Kan noen fortelle ham det?

Kontinuerlig Web-angrep

Apropos sikkerhet: I likhet med tallrike andre små selskaper driver vi vår egen Web-tjeneste. Langt fra alltid vår foretrukne aktivitet, men ofte lærerik. Derfor studerer vi loggfilene regelmessig, i perioder daglig. Det har vært lite lystelig lesing i det siste. Bortimot halvparten av trafikken de siste månedene har vært varianter av “last ned siden /scripts/..%255c../winnt/system32/cmd.exe?/-c+dir”. Hundrevis eller tusenvis av innslag hvert eneste døgn i uke etter uke, måned etter måned. Utilslørte forsøk på å utnytte mer eller mindre kjente hull i Microsofts webtjener (IIS, INTERNET INFORMATION SERVER). Og åpenbart ‘robot-drevet’: Det sitter ingen godtroende tenåring og taster disse uendelige linjene. De genereres av lett tilgjengelige programmer som lever sitt eget liv i bakgrunnen – og effektivt sørger for at ingen systemansvarlig sover godt om ikke hun eller han har lagt inn alle tilgjengelige oppdateringer. Eller er i den heldige situasjon – som vi – at webtjeneren er av en helt annen opprinnelse, og ikke er perfekt, men noen størrelsesordener sikrere enn IIS. Det har vi lært oss å sette pris på.

Ut med IIS? Ikke så brått ...

Angrepene på Microsofts Web-tjener IIS gir seg ikke, og Gartner Groups anbefaling om å se etter andre alternativer, har ikke unngått å sette spor etter seg: Truslene er reelle, utfordringene store og gresset definitivt grønnere på den andre siden. Samtidig er elven bred og strømmen stri: IIS er riktignok i stand til å levere websider i noenlunde standardisert format, men har ellers lite til felles med andre Web-tjenere på markedet. De har alle sine særegenheter og spesifikke formater – for ikke å snakke om programmeringsmuligheter og sikringsmekanismer. Å skifte fra ett produkt til et annet er med andre ord ingen triviell affære, uansett hvilken plattform vi kommer fra – eller skal til. I beste fall er det snakk om en tidkrevende og kostbar prosess. Riktignok har det i kjølvannet av den nevnte Gartner Group rapporten dukket opp tjenesteleverandører⁹ (Web-hoteller) som tar på seg konverteringsjobben til en avtalt pris. Forutsetningen er naturligvis at det samtidig avtales å overføre (OUTSOURCE) Web-tjenestene til samme leverandør, hvilket for noen er en god idé, for andre uaktuelt.

De fleste IIS-miljøer sitter kort og godt i saksa: De må enten leve med usikkerheten eller ta hånd i hanke med situasjonen og sørge for å holde produktene oppdatert. Det er kostbart, men på kort sikt mindre ressurskrevende enn å bytte plattform. Likeledes arbeides det med prosedyrer som kan automatisere prosessen, og som forhåpentlig i seg selv blir sikre nok til å ikke gjøre galt verre. Videre lover Microsoft at neste versjon av Internet Information Server, v6, skal bli mye bedre på alle måter. Den har vi riktignok hørt før, men her er det mye som står på spill for verdens største programvareselskap: I motsetning til hva tilfellet er for operativsystemer, har markedet reelle alternativer når plattform for Web-tjenester skal velges.

Microsoft i sikkerhetskrangel

Mens markedet vurderer alternativer og diskuterer utfordringer i den forbindelse, er Microsoft kommet på kant med sikkerhets-ekspertisen: MS mener det er uansvarlig å løpende publisere feil som oppdages, og at denne praksisen forverrer problemet ved å tiltrekke hackere til hullene som fluer til en hestelort. Sikkerhetseksperter på sin side påpeker at Microsoft er notorisk sene med å tette hullene som oppdages, og praktiserer 'SECURITY BY OBSCURITY', en forlengst avleggs praksis. Som så ofte er tilfelle når to parter havner i tottene på hverandre på denne måten, har begge delvis rett. Det kan føres gode 'prosedyrer' for partene, hvilket også ble gjort på et møte i California i første halvdel av november.

Møtet markerte en milepæl i den forstand at partene møttes med et ønske om å komme frem til en form for konsensus. Noen våpenhvile ble det riktignok ikke, men fremskritt likevel: Microsoft lovet på sin side å ta problemene på alvor, vise større åpenhet med hensyn til egne svakheter og hva som gjøres for å rette på dem. Likeledes skal selskapet gi høyere prioritet til tetting av påviste hull og sørge for at oppdateringer (PATCHER) kommer raskere ut til kundemiljøene.

⁹ Amerikanske Hostex er et eksempel på en slik leverandør (www.hostex.com).

Sikkerhetseksperter vil på sin side avstå fra å demonstrere hvordan hullene er funnet og hvordan de kan utnyttes, og skal begrense seg til å beskrive dem, deres tilhørighet og konsekvenser. De lærde strides om hvorvidt et slik tiltak er positivt eller negativt for sikkerheten. SECURITY BY OBSCURITY er en metode som forlengst har gått ut på dato, og som etter de fleste eksperters oppfatning gir falsk sikkerhet. Kompromisset synes imidlertid akseptabelt – og rimelig. Så vil tiden vise om effektene er målbare og i så fall, hvilken vei de peker.

Hvor ble det av sikker epost?

Sikring av epost har vært en gjenganger her i Mellvik-Rapporten de siste to årene, og gjenstand for detaljert diskusjon i vår ferskeste spesialrapport. Interessen viser at temaet er kommet på dagsorden – hvor det definitivt hører hjemme. Samtidig viser undersøkelser i markedet, innenlands og i andre vestlige land, at praksis fortsatt best kan karakteriseres som 'la det skure'. Kun et fåtall store organisasjoner med spesielle behov har for alvor tatt hånd i hanke med situasjonen, og brakt eposten under kontroll – teknisk, organisasjonsmessig, bevissthetsmessig og juridisk. Vi står overfor den bisarre situasjonen at alle ønsker tjenesten, men ingen bruker den, hvilket ikke kan lede til andre konklusjoner enn at kvaliteten er for dårlig. Standardene er mangelfulle, med den følge at produktene blir kompliserte og samspill vanskelig.

Det er imidlertid for lett å stoppe der: Det største problemet i dag som for ett eller fire år, siden er at 999 av 1.000 brukere ikke anser sikring av epost som viktig. De betrakter epost-meldinger som sikre på linje med telefonsamtaler, hvilket teknisk sett kan være riktig, mens det i praksis er ren fantasi.

I tillegg til at brukerne vegrer seg for å ta i bruk ekstrafunksjoner som gir bedre sikkerhet, har sikringen også en administrativ side: Med en blanding av kryptert og ukryptert post i brukernes postkasser, blir brukerstøtte, administrasjon av konti og arkivering langt mer komplisert. Selv i miljøer der smartkort eller andre former for pålitelig autentisering er på plass, finner vi kun unntaksvis kryptering av epost. Med digitale signaturer er pålitelighet og etterrettelighet blitt vesentlig bedre, hvilket ofte blir betraktet som viktigere enn konfidensialitet. Videre fører den voksende bruken av VPN-baserte forbindelser til at datatransporten er sikret en betydelig del av transportveien i alle fall.

Dermed er det galt å hevde at vi står på stedet hvil. Sikkerheten er blitt bedre, også for eposten, og kan lett bedres ytterligere gjennom å sørge for at brukerne får et realistisk forhold til verktøyets reelle karakteristika. Mens vi venter på standarder og mekanismer som kan gi skikkelig meldingssikkerhet på en transparent og enkel måte, er det slike tiltak som vil dominere.¹⁰

Der kravene er spesielle, finnes det produkter som kan hjelpe et stykke på vei. Ett av dem er ZixIT [www.zixit.com], som vi diskuterer i neste utgave, mens andre er HushMail [www.hushmail.com], Sigaba [www.sigaba.com] og TumbleWeed [www.tumbleweed.com]. Videre er det en overkommelig investering –

¹⁰ Nettopp slike tiltak får bred omtale i spesialrapporten "Effektiv sikring av Epost".

med hensyn til såvel penger som administrasjon – å etablere VPN-forbindelser mellom partnere som fordrer konfidensialitet og brukermessig transparens.

Hovedpoenget er fortsatt at sikker epost er mulig, tilgjengelig – og så krevende som behovene tilsier. I likhet med all annen sikkerhet må det en risikoanalyse til for å etablere riktig grad av sikkerhet i forhold til kostnadene. En slik analyse bør gjøres uansett, fordi kunnskapen den bringer er av uvurderlig verdi – for såvel IT-ledere som toppledere. ■

Kopiering forbudt