

# Applikasjonsbrannmurer

*Brannmurene er på plass – sofistikerte høykapasitets-produkter som ikke bare kontrollerer sendere, mottakere, pakkehoder og hvorvidt forbindelser er etablert eller ikke, men dessuten titter på innholdet som passerer. I en verden hvor tillit synes å være forvist til ordlister og leksikon, kan vi ikke være forsiktige nok.*

Derfor er sikring ikke et mål, men en prosess. Vi kommer aldri i mål, kun til nye milepæler – som gir tilstrekkelig sikkerhet for den neste perioden, typisk 3 til 6 måneder. Kontinuerlige forandringer forlanger kontinuerlig oppfølging. Sikkerhetsansvarlige blir aldri arbeidsledige.

## 'Webifisering' til besvær

'Webifisering' av applikasjoner representerer et nytt utfordringsnivå i sikkerhetssammenheng. Nye mekanismer tas i bruk – gjerne uten å ha vært verken robusthets- eller sikkerhetstestet, og etter kort tid står nye trusler i kø. Mens vi blokkerer porter, sjekker adresser og kontrollerer pakkehoder og nye kontra etablerte forbindelser, passerer alle de nye applikasjonene gjennom ett eneste nåløye: TCP port 80, Web-tjenerens universelle kontaktpunkt, som dermed alltid står åpen.

Graden av åpenhet kommer an på en rekke forhold – ikke minst hvilken Web-tjener som benyttes, om den ligger bak en proxy og om den eksisterende brannmuren foretar ekstra kontroll på egen hånd. I parallell med at tjenestene som betjenes via denne 'åpningen' vokser i omfang, øker også eksponeringen – og interessen for å angripe nettopp her. Ferske tall viser at over 80% av alle ondsinnede angrep via Internettet er rettet direkte mot TCP port 80.

Veksten i bruk av ehandels-applikasjoner fungerer nærmest som fluepapir i den forbindelse: Der hvor det handles, finnes det informasjon som kan misbrukes i vinnings hensikt.

### Nye trusler

Den største trusselen er svak programvare – nå som tidligere, mens det nye i bildet er at eksponeringen tiltar og mengden programvare som utvikles for Web-relaterte anvendelser vokser eksponensielt. Kvaliteten på denne strømmen av nyutviklet programvare er kun unntaksvis på et nivå som står i forhold til oppgavens betydning og de trusler den eksponeres for.

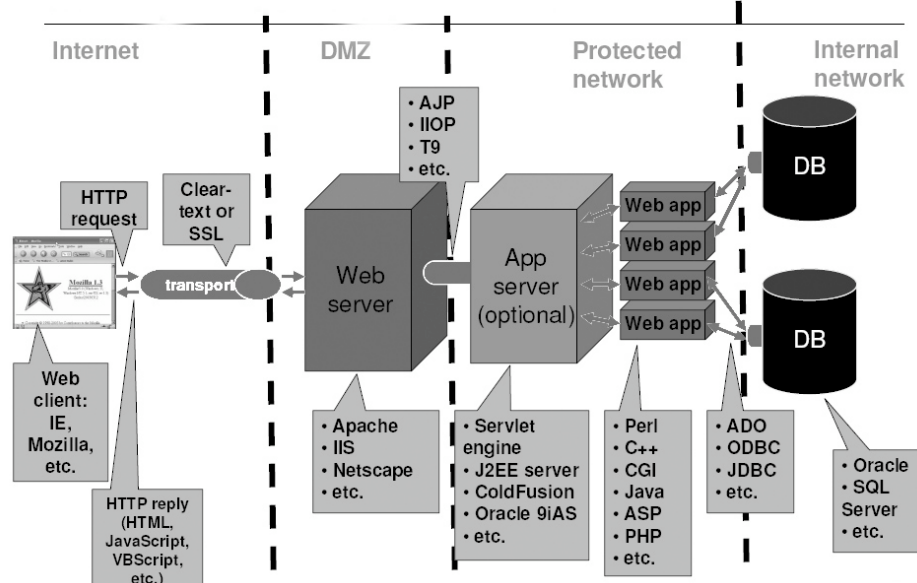
Dermed blir konsekvensene tilsvarende alvorlige. De viktigste 'mekanismene' som misbrukes i dag, er:

- ✓ **Manglende parameterkontroll:** Programmene sjekker ikke om verdier som mottas fra en klient er rimelige og akseptable. Behandling av parametre med urimelige verdier har gjerne uforutsigbare og utilsiktede konsekvenser i programmene. Parameterkontroll på klientsiden er vel og bra, men utilstrekkelig. Typiske konsekvenser er kapring av

- klient-konti, tapping av data og tilgang til personlig informasjon. Løsning: Korrekt parameterkontroll på tjenersiden.
- ✓ **'Buffer overflow':** Egentlig en variant av manglende parameterkontroll, og en typisk svakhet som kan utnyttes til å krasje vertssystemet, sette tjener-programmene ut av drift eller i verste fall skaffe seg kontroll over vertssystemet. De kjente Code Red- og Nimda-angrepene hadde sistnevnte som målsetting – og lykkes faretruende ofte. Løsning: Skikkelig kontroll av innkommende data.
  - ✓ **Injeksjon av kommandoer:** Klient-programmer sender ofte serier av kommandoer som blir viderefremmet fra Web-tjeneren til bakenforliggende applikasjoner (se figur 2 nedenfor). Med mindre hver enkelt av disse kommandoene kontrolleres både med hensyn til innhold og sammenheng, kan det være mulig å 'injisere' ekstra-kommandoer som for eksempel ber databasesystemet om å returnere all klientinformasjon (SQL-kommandoer). Følgeskadene er innlysende. Løsning: Kontroll av inn-data, sikker programmeringsmetodikk.
  - ✓ **Usynlige krysskoblinger:** Web-sider kan inneholde usynlige koblinger til vilkårlige steder på nettet. Intetanende brukere kan dermed uten å være klar over det både motta data fra og sende data til helt andre steder enn hva skjermbildet indikerer. Tilsvarende kan svake kontrollmekanismer på en Web-tjener gjøre det mulig for en klient å lure den til å sende svarene til et helt annet sted enn den egentlige klienten. I begge tilfeller kan den som introduserer krysskoblingene, skaffe seg adgang til privilegert informasjon. Løsning: Kontroll av innkommende data.
  - ✓ **Tvangs-surfing:** Programmer som automatisk og meget raskt forsøker å aksessere tilfeldige adresser og tilfeldige URLer, kan få tilgang til nettstedet og ressurser som var antatt å være skjulte fordi de ikke annonseres eller refereres til noe sted. Til tross for at *security by obscurity* gikk ut på dato for mange år siden, både lages og brukes metoden fortsatt av utviklere som ikke kan sitt håndverk.
  - ✓ **Svake mekanismer for autentisering og aksesskontroll:** Innlysende problemområder som like fullt blir stemoderlig behandlet av utviklere som haster mot avslutning av prosjekter og ofrer sikkerheten underveis. Mekanismene og metodene finnes, sammen med retningslinjer for hvordan de bør brukes. Løsningen er å ta dem i bruk i stedet for å reparere skadene når katastrofen er et faktum.

Denne listen får nye elementer eller nyanser hver eneste uke, og aksentuerer behovet for å introdusere et ekstra kontrollnivå når bruken av Web-applikasjoner fra Internettet passerer det mest elementære nivå. Applikasjonenes sammensatte natur bidrar til oversikt og modularitet, mens det også er et faktum at mange av komponentene er ferske og dermed mindre robuste enn vi kunne ønske. Figur 2 gir et

bilde av hvordan komponenter, standarder og mekanismer forholder seg til hverandre.



**Figur 2** En Web-applikasjon involverer typisk en lang rekke komponenter og funksjoner. Hver enkelt av disse kan inneholde feil og svakheter som i sin tur kan misbrukes av kompetente inntrengere. (Figur fra Steve Acheson, Cisco.)

## Behov avfører løsninger og produkter

Helt i tråd med dette behovet har en ny produkt-kategori dukket opp på radarskjermen i løpet av det siste året. Applikasjons-brannmurer retter seg direkte mot slike trusler, og plasseres mellom den eksisterende brannmur og første Web-tjener eller proxy. I mange tilfeller kan den nye brannmuren overta proxy-funksjonen og dermed erstatte en eksisterende 'boks' i stedet for å introdusere ytterligere kompleksitet.

Disse produktene – fra nykommere som Sanctum, Teros og KaVaDo, og kjente navn som Internet Security Systems og Network Associates, er allerede modne nok til å representere en nødvendighet i tilknytning til Internett-baserte ehandels-løsninger og et voksende antall Web-applikasjoner som håndterer følsomme, personrelaterte data. Offentlige informasjonsportaler er et godt eksempel, der brukerne både kan slå opp og kontrollere registrert informasjon om seg selv, samt registrere søknader og forespørsler av konfidensiell natur.

Produktene kan grovt deles i to hovedkategorier: Programvare og komplette 'bokser' (*appliances*). Hvilken kategori som passer, kommer an på omstendighetene. Bokser koster mer og har høyere kapasitet og enklere administrasjon, mens programvareløsningene kan integreres med en eksisterende Web-tjener eller proxy. En variant av hardware-alternativet er tilleggsmoduler til eksisterende sikringsutstyr fra for eksempel Cisco og CyberGuard.<sup>7</sup>

<sup>7</sup> En oversikt over leverandører som er aktive i dette segmentet er å finne på siden med tilleggsinformasjon til denne utgaven på vår Web-tjeneste, se side 35.

## Konklusjon

De viktigste observasjonene å ta med seg fra denne gjennomgangen er:

- ✓ Web-applikasjoner med tilgang fra Internettet er risikable – på grunn av sin store eksponering og programvarens generelle beskaffenhet.
- ✓ Applikasjons-brannmurer er en nødvendig komponent i slike systemer, og kan i tillegg til å heve sikkerheten dramatisk, også avsløre svakheter i applikasjonene.
- ✓ Applikasjons-brannmurer kan inndeles i tre grupper: Programvare (som er rimeligst), spesialiserte bokser (som koster mest og gir størst fleksibilitet og ytelse), og kombinerte produkter (for eksempel brannmurer med ekstra funksjonalitet).
- ✓ Produkt-kostnader ligger typisk i området NOK 25.000 til over 200.000.

På mellomlang sikt – 2 til 3 år frem i tiden – vil de fleste av dagens nykommere i segmentet bli spist av sine eldre og langt større konkurrenter, og deres funksjonalitet vil finne veien inn i rimelige standardprodukter. En slik utvikling er helt analog med hva vi har sett på alminnelige brannmurer de siste 3 årene. Å sitte på gjerdet og vente på at prisene skal falle, er imidlertid en høyst risikabel og lite anbefalesverdig angrepsvinkel. ■