



SECUREDEVICE

SÅDAN BESKYTTER DANSKE SPIL 250.000 ONLINE-SPILLERE



Hvordan sikrer man, at en kvart million online-spillere altid kan få adgang til webbaserede spil, uden at man samtidigt giver orme og hackere frit spil på netværket? Danske Spil valgte at løse problemet med en IDS/IPS-løsning fra SecureDevice.

Da Danske Spil i slutningen af 2004 begyndte at se sig om efter en intelligent netværkssikkerhedsløsning, skete det ud fra et klart formuleret krav: Det skulle være en løsning, der gjorde Tipstjenesten i stand til at standse angreb på netværket, før de fandt sted. Tidligere erfaringer med et andet sikkerhedssystem baseret på loganalyse viste, at det ikke var nok at vide, at et angreb havde fundet sted. Danske Spil havde brug for en mere proaktiv beskyttelse af sin webserverpark.

Vores dilemma var, at vi ikke måtte gøre vores netværksbeskyttelse så restriktiv,

at almindelig netværkstrafik fra kunderne kunne blive misforstået som angreb og blokeret. På den anden side skulle beskyttelsen være så effektiv, at alle angreb kunne afværges før de gjorde skade, siger Poul Richardt Jensen, it-teknikchef hos Danske Spil.

ØGET NETVÆRKSINTELLIGENS VAR SVARET

Løsningen på Danske Spils sikkerhedsproblem blev en løsning, der er en blanding af automatisk og manuel overvågning af netværkstrafikken. Den automatiske del

består af en IDS/IPS-løsning fra SecureDevice. Systemet er placeret bag firewall'en, hvor den inspicerer al trafik, der slipper igennem firewall'en. Ud fra en række kriterier kan systemet enten komme med en advarsel (IDS - Intrusion Detection System) og eventuelt blokere for mistænkelig trafik, hvis truslen er alvorlig nok (IPS - Intrusion Protection System).

Systemet er også forbundet med programmet Internet Scanner, der hele tiden scanner Danske Spils infrastruktur for eventuelle sårbarheder. Ud fra sårbarhedsscanningen opbygger IDS/IPS-systemet en profil af,



“I FREMTIDEN SKAL SYSTEMET KUNNE STANDSE ENDNU FLERE TYPER AF ANGREB AUTOMATISK”

hvilke typer af angreb, der er farligst for netop Danske Spils infrastruktur. Profilen gør med andre ord systemet i stand til at træffe mere intelligente valg af, om der skal slås alarm og blokeres for særligt mistænkelig netværkstrafik.

Det er meget vigtigt for os, at vi ikke standser den almindelige kundetrafik på grund af falske positive. Hvis vi gør det, mister vi indtjening, fordi folk ikke kan få adgang til vores spil. På det punkt er vi meget tilfredse med løsningen fra SecureDevice. Der er så vidt jeg ved ingen spillere, der er blevet nægtet adgang, fordi deres almindelige trafik på netværket er blevet fejltolket som et angreb, siger Poul Richardt Jensen.

HØJRISIKOALARMER BEHANDLES MANUELT

Den manuelle del af sikkerhedssystemet består i at IDS/IPS-systemet sender advarsler til et døgnovervåget sikkerhedscenter hos Fort Consult. Her vurderer sikkerhedseksperter alarmerne og kontakter Danske Spil, hvis den vurderes at udgøre et reelt sikkerhedsproblem. Ser man på statistikkerne over angrebsforsøg er det dog de færreste angreb, der kræver vurdering fra Fort Consult's eksperter. De fleste standses automatisk af ISS Proventia-løsningen.

UGENTLIG SUPPORT

Foruden levering og implementering af systemet sørger SecureDevice også for løbende support. Hver uge kommer en af

SecureDevice's sikkerhedskonsulenter på besøg hos Danske Spil for at optimere, opdatere og tilpasse IDS/IPS-systemet til det aktuelle trusselsbillede, der skifter hele tiden.

Næsten hver dag kommer der nye sikkerhedsopdateringer, og systemet kan naturligvis godt sættes op til at modtage dem automatisk. Men på grund af Danske Spils høje krav til sikkerheden, bliver opdateringen udført af en af vores tekniske eksperter. Hver uge tilføjer vi alle relevante opdateringer, og sørger for at de også føjes til de policies, der sætter system i stand til at træffe de rigtige beslutninger. Vi gennemgår også indholdet af alle opdateringerne og aktiverer kun dem, der er relevante. Der er for eksempel ingen grund til at aktivere opdateringer, der beskytter servertyper, der slet ikke findes i Danske Spils infrastruktur, siger Michael Albek fra SecureDevice.

FREMTIDEN ER AUTOMATISK

På baggrund af de gode erfaringer med automatisering af netværkssikkerheden, har Danske Spil ambitioner om at skrue op for systemets IPS-funktionalitet. Der er nemlig store økonomiske fordele forbundet med at lade systemet håndtere så mange angreb som muligt - uden menneskelig indblanding.

I fremtiden skal systemet kunne standse endnu flere typer af angreb automatisk. Men det skal foregå i en glidende overgang, så vi hele tiden kan føle os sikre på, at sikkerhed og uhindret brugeradgang går

hånd i hånd. Jeg mener helt klart, at løsningen fra SecureDevice har potentiale til at indfri disse forventninger, siger Poul Richardt Jensen.