



Case study

eSec og Saxo Bank indgår samarbejde om sikring mod hackere

Med kunder og partnere i mere end 120 lande og over 250 ansatte er Saxo Bank en markant spiller på markedet for investeringsbanker på Internettet. Kravet til bankens IT-sikkerhed er således en konstant udfordring, og den bliver nu løst i nært samarbejde med eSec Security Management.

Saxo Bank er en international investeringsbank med fokus på onlinehandel. Banken har sit hovedsæde i København og her arbejder ansatte fra mere end 30 lande med at servicere kunder over hele verden.

De mange daglige handler samt medarbejdernes netværkstrafik hos Saxo Bank betyder, at banken stiller meget store krav til sikkerhed på data-netværkene. Hackere udgør en stigende trussel, og et nedbrud på centrale dele af netværket kan få katastrofale følger – både direkte, i form af tabt omsætning, og på længere sigt i form af manglende troværdighed.

Den udfordring har Saxo Bank løst i samarbejde med den danske IT-sikkerhedsvirksomhed eSec Security Management .

Grundig analyse af trafik

Konceptet går ikke blot ud på at lukke af for visse typer trafik, men tillige at analysere den tilladte trafik grundigt.

”Problemet med traditionel firewall beskyttelse er, at systemerne kun lukker for visse typer adgang til og fra netværk. Andre typer står stadig åbne – for eksempel medarbejderes adgang til Internettet. Det betyder blot, at fjendtligt-sindede hackere kan koncentrere deres angreb direkte mod de åbne huller, som nødvendigvis må være åbne af hensyn til hele netværkets funktionalitet,” siger Ole Schmitto, der er stifter og adm. direktør i eSec.

Rapporter beskriver problemer

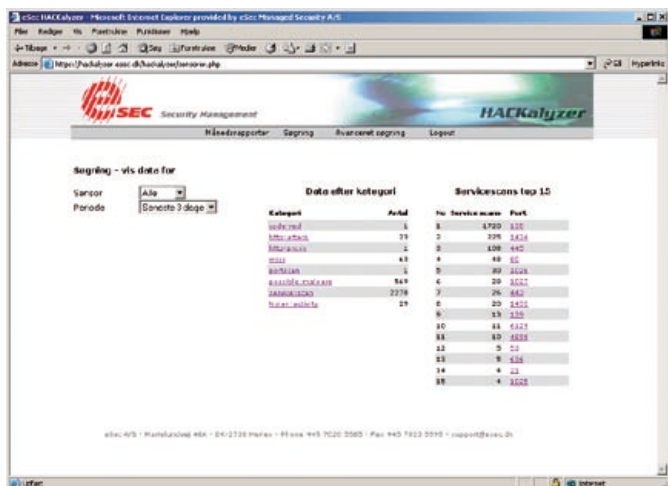
Ved at analysere og fortolke logfiler fra Firewall og IDS system, som beskriver hele netværks trafikken både ind- og udgående, kan eSec identificere mistænkelig, ikke tilladt og u hensigtsmæssig trafik.

Saxo Bank modtager ugentligt og månedligt en oversigt over de mest angrebekritiske punkter i netværket således, at IT-sikkerhedsafdelingen kan koncentrere indsatsen, der hvor der er mest brug for den. Skulle der opstå akutte problemer, modtager Saxo Bank en rapport med det samme.

... fortsættes på bagsiden.



SEC
ty Management



eSec's HACKalyzer gør det muligt for eSec's kunder løbende at følge med i de forsøg på angreb, som deres applikationer har været udsat for.

”Vi har med løsningen fra eSec valgt at outsource overvågningen af vores netværk. Markedet for den slags løsninger er forholdsvis lille og fordelt på en række små og et par store virksomheder. Vi valgte i første omgang at kigge nærmere på eSec, fordi de har et godt omdømme, og det er nu blevet til et langsigtet samarbejde,” siger David Boye, der er sikkerhedschef i Saxo Bank.

Beslutningen om at outsource opgaven var ifølge David Boye helt naturligt:

”Det ville have kostet os nogenlunde det samme at udføre opgaven selv. Ved at outsource opgaven slipper vi for bøvlet, og vi kan være sikre på, at opgaven får den nødvendige prioritet og ekspertise”

Angreb er hverdagskost

Al trafik fra både bankens handelsplatform og ansattes webbrug går gennem eSec's filter. En såkaldt ”sniffer” overvåger konstant og melder tilbage hver gang der opdages risikabel trafik. ”Vi har omkring 10.000 events om ugen, altså rapporteringer om trafik, der kan være farlig. Vi har haft en uge med over 90.000 events. Langt de fleste rapporteringer er brede og automatiske scanninger, som ikke er et problem for et system som vores, men vi fanger også deciderede angreb,” fortæller David Boye.

Succesfuld outsourcing

Fordelen ved at outsource overvågningen af firewall og logfiler er også, at Saxo Bank udelukkende modtager relevant data i form af en angrebs-

alarm fra eSec. Alarmen indeholder både en beskrivelse af problemet samt en gennemgang af, hvilke forholdsregler der bør tages. Opgaven varetages af en eSec-sikkerhedseksper. Det sparer Saxo Bank for mange timers arbejde med at analysere store mængder logfiler og vedligeholde den ekspertise, der kræves for at være på forkant med de seneste angrebsmønstre.

”Vi vedligeholder en omfattende database over hvordan hackeraktiviteten ser ud. I kraft af vores mange kunder udbygges denne database løbende, så vi hele tiden kan tilbyde en ydelse, der er up-to-date. eSec overvåger dagligt mange gigabyte data fra kunders netværk. Det betyder, at eSec har et godt overblik over hackermiljøernes seneste aktiviteter,” slutter direktør i eSec, Ole Schmitto.

Om eSec

eSec er 100% danskejdet og vore ydelser er direkte udviklet til virksomhedsstrukturen i denne del af verden.

eSec har både danske og internationale kunder, og vi arbejder dels direkte med slutbrugere og dels i samarbejde med danske leverandører af løsninger til Internet.