

Traditionelt har IT-sikkerhed bygget på konceptet om at sikre perimeteren med firewalls, antivirus osv. og dermed beskytte virksomheden mod eksterne trusler. Men det er også vigtigt at kende sine interne netværk og skabe synlighed i forhold til identificering og håndtering af uønsket indhold. Sikkerhedsspecialisterne i Ezenta arbejder tæt sammen med IBM omkring løsninger, der tager hånd om netop denne problemstilling.

Foto: Tommy Hvitefeldt



"Vores samarbejde med IBM udspringer af, at IBM ønskede en lokal dansk partner, der kan levere de spidskompetencer, som er nødvendige for at levere strategiske end-to-end sikkerhedsløsninger."

# NETVÆRKET KAN BLIVE SMUTVEJ FOR KRIMINELLE

► "Det er vigtigt at erkende, at interne netværk udgør en sikkerhedsrisiko," siger Jesper Sobol, som er Sales Director og partner i Ezenta.

"Virksomhederne bør have systemer og processer, der skaber synlighed omkring trafikken på netværket, som overvåger hændelser og giver mulighed for at gribe ind."

Det drejer sig grundlæggende om, at virksomheden igennem øget synlighed på netværket opnår bedre muligheder for håndtering af eventuelle hændelser. Virksomheden kan sikre sine aktiver og får lettere ved at overholde branchespecifikke lovkrav på området.

## MAL- OG SPYWARE SOM VÅBEN

Det er heldigvis sjældent, at virksomheder i Danmark bliver ramt direkte af målrettede eksterne hackerangreb, der går direkte efter forretningskritiske data og systemer.

Men det ændrer ikke ved, at de fortsat er udsat for angreb. Ofte

foregår disse angreb med såkaldt Spy- og Malware, der typisk infiltrerer klientcomputere igennem tilsyneladende ufarlige hjemmesider, e-mails og downloadede applikationer. Kendetegnet ved disse angreb er, at de sjældent er synlige for brugeren, men kan i værste tilfælde betyde at virksomhedens IT-infrastruktur anvendes som springbræt til mere alvorlige angreb eller udnyttes til illegal distribution af pirat-software, børneporno og lignende.

"Medarbejderne kan helt uforvarende kompromittere virksomhedens sikkerhed ved blot at besøge en given hjemmeside, eller åbne den forkerte e-mail," fortæller Jesper Sobol.

"Hvis ikke man har systemer og processer på plads, der løbende overvåger aktiviteter på netværket, kan man umuligt gardere sig mod disse, desværre, og efterhånden meget udbredte trusler."

Trusselsbilledet har ændret sig markant igennem de senere år, fra hackere der blot ønskede at

blive berømte, til i dag, hvor der findes en hel undergrundsøkonomi indenfor IT-kriminalitet.

Ezenta arbejder blandt andet med sådanne løsninger og leverer i dag til mange virksomheder, primært inden for finans- og medicinalvirksomheder.

"Især banker, forsikringselskaber og medicinalvirksomheder stiller meget høje krav til IT-sikkerhed og forlanger derfor at samarbejde med de bedste på markedet. Men selvsagt har alle typer af virksomhed behov for at sikre sig mod de trusler, der eksisterer," siger Jesper Sobol.

## FACEBOOK SOM POTENTIEL RISIKO

Effektiv overvågning og kontrol af netværksaktiviteter dæmper også op for en lang række andre problemstillinger, som f.eks. upassende hjemmesider, online spil, instant messaging, adgang til sociale netværk, illegal distribution af musik og film samt uautoriseret download af software.

Tilsvarende åbner det også mulighed for identificering af datalækager og beskyttelse af de hemmelige eller følsomme virksomhedsinformationer, der flyder i netværket.

En efterhånden meget populær hjemmeside som Facebook kan f.eks. være kilde til informationslækage, såkaldt "drive-by" installation af mal- og spyware,

men mange virksomheder har endnu ikke taget stilling til disse nye trusler.

"I takt med at Internet- og især webapplikationer bliver mere avancerede, er det nødvendigt med avancerede værktøjer til identificering og håndtering af potentielle trusler," understreger Jesper Sobol.

## FAKTA

• Overvågning af netværkstrafik er et komplekst område, der kræver specialiserede kompetencer og systemer for at kunne håndteres effektivt. Derfor har Ezenta og IBM

indgået et tæt samarbejde, så de kan tilbyde en komplet vifte af rådgivnings- og designydelser koblet til state-of-the-art hard- og software.



## LYST TIL AT HØRE MERE?

Kontakt Jesper Sobol, Sales Director & Partner, Ezenta A/S · Telefon 7020 1260  
jes@ezenta.com

## UDNYT EKSPERTISEN OG SPAR PENGE

Udgifter til IT-sikkerhed fylder en hel del på virksomhedernes driftsbudgetter. Men med IBM's vifte af outsourcete sikkerhedssystemer, Managed Security Systems (MSS), kan der ofte opnås et højere sikkerhedsniveau til en lavere omkostning sammenlignet med at håndtere opgaverne i eget regi. MSS-ydelserne omfatter

ekspertise, ressourcer, værktøjer og infrastruktur, så en kunde kan lade IBM håndtere sine sikkerhedsopgaver til en fast pris med et garanteret service- og sikkerhedsniveau. Via web-baserede interfaces kan kunden på et øjeblik se status på sine systemer, både dem IBM håndterer og dem, der måtte ligge uden

for aftalen. Udover den konkrete besparelse i personaleressourcer og penge opnår kunderne også, at deres sikkerhedssystemer løbende opdateres og dermed altid leverer op til den gældende lovgivning og de branchespecifikke krav. Kalkulationer viser, at virksomheder kan reducere deres omkostninger med op til 55 %.

MSS er en ydelse, der leveres af IBM Internet Security Systems.

## HÆDER FRA GARTNER GROUP

Det ansete, uafhængige analysefirma Gartner Group, har netop udnævnt IBM ISS som den eneste "leader" inden for Managed Security Systems (MSS).

De skriver i deres redegørelse, "at virksomheder, der kræver stærk sikkerhedsekspertise, multinational support og udstrakte konsulenttydelser, bør overveje IBM ISS". Desuden fremhæver de IBM ISS's globale leveranceapparat og forsknings- og udviklingsenheden X-Force.