Data Center

Optimering af dine kunders virtuelle miljøer

Hos Arrow ECS bruger vi mange ressourcer på, at du som security-partner kan tilbyde dine kunder størst mulig beskyttelse af deres virtuelle miljøer.

Der er kræfter, der konstant arbejder på at få adgang til ubeskyttede IT-miljøer. Virtualisering af datacentre har enorme fordele, men rejser også vigtige sikkerheds-spørgsmål, som burde få alarmklokkerne til at ringe hos dine kunder. Vi kan pege på to store udfordringer, som kræver dine kunders opmærksomhed og fokus:

- 60%. Så mange virksomheder vil ende op med et virtualiseret IT-miljø, der er mindre sikkert end før virtualiseringen. Mange af dem er tilmed ikke klar over deres selvskabte sikkerhedsbrister.

- Virtuel patching udfordrer et stort antal virksomheder, der er underlagt myndigheders tidsfrister for identificering og udbedring af IT-sårbarheder. Problemet er, at en fysisk maskine indeholder så mange virtuelle maskiner med hver deres software, at en sikkerheds-patch kun kan installeres, hvis maskinen tages ud af drift. Det er ikke realistisk i en travl hverdag.

HJÆLP KUNDERNE OG SKAB MERSALG

Til trods for risikoen for katastrofale følger, har mange virksomheder ikke en handlingsplan for at gennemføre de sikkerhedsforbedringer, der skal til. Der er tale om et uudnyttet, betydeligt forretningspotentiale, som du kan hente sammen med Arrow ECS.

Arrow ECS arbejder til daglig med både at levere virtualisering med integrerede sikkerhedsløsninger. Vi har solide og gode erfaringer med rådgivning, salg, tilpasning og implementering af komplette sikkerhedsløsninger. Vores løsninger skaber værdi for dine kunder ved at være modulært opbygget – og ved at være udviklet specifikt til virtuelle miljøer. Dine kunder opnår dermed en paraplyløsning, de kan bruge til at overvåge alt ét sted – fra sikker mail over firewall og kryptering til VPN og anti-spyware. Det gør det lettere at opdage om ondsindet software fra én virtuel server spreder sig i det øvrige virtuelle miljø.

TAG OS MED PÅ DINE KUNDEMØDER

Fra sidelinjen kan vi hjælpe dig med at tage skridtet fra "blot" at forny licensaftaler, til at du kan skabe mersalg via salg af forskellige funktioner. Læg dertil nye muligheder for at gå i dialog med kundens sikkerhedsansvarlige om behovet for 360 graders sikkerhedsoptimering af deres virtuelle miljø – og effekten af det.

DET BLIVER IKKE VED SNAKKEN

Dine kunder kan ved selvsyn konstatere, hvor nemt det er at hacke et virtuelt miljø, der ikke er sikkerhedsoptimeret. Det kan vi konkret vise dem i en testinstallation. Desuden kan vi også vise dine kunder, hvor tilsvarende nemt de opnår fuld kontrol med datasikkerheden igen. Træk på Arrow ECS´ gennemprøvede metodesæt og erfaringer med at drive processen logisk fremad, hvis du vil sikre dine kunder det fulde sikkerhedspotentiale – og styrke din forretning.

5 tegn på

at din kunder har brug for security optimering

- Kunden kan ikke overvåge unormale hændelser i det virtuelle IT-miljøet
- Kunden benytter ikke produkter, der er udviklet til virtuelle miljøer
- Medarbejderne bruger mobile enheder, men har ikke tænkt på truslerne
- Kunden har ikke en sikkerhedsløsning, der kan adskille virtuelle maskiner fra hinanden
- Kunden har ikke beskyttet sig mod at ondsindet kode kan sprede sig fra virtuel maskine til virtuel maskine

Kontakt

Kim Due Andersen
Product Manager
Mobil +45 3016 1336
kim.due.andersen@arrow.com