It-sikkerhed

Børsen Ledelseshåndbøger er Danmarks største og stærkeste videns- og udviklingsklub. Uanset hvilket område eller emne du beskæftiger dig med, får du her et komplet opslagsværk på print, cd-rom og internet, der giver dig overblik og indsigt.

Ledelseshåndbogen er et praktisk og overskueligt værktøj til dig, der vil være 100% opdateret inden for et bestemt område – selvom du har en travl hverdag.

Børsen Forum A/S
Møntergade 19, DK – 1140 København K
Telefon 33 32 01 02, www.blh.dk

Børsen Ledelseshåndbøger

9.7.

Netværkssikkerhed i en mobil Web 2.0-verden

af teknisk direktør Kent Madsen, kentmads@cisco.com,
Cisco Danmark

Udbuddet og anvendelsen af webservices og sociale online-netværk er eksploderet de senere år, og internettet står i dag som den stærkeste serviceplatform nogensinde – kendt af mange som "Web 2.0".

Det har for alvor åbnet danske erhvervslederes øjne for netværkets muligheder, og mange virksomheder er allerede i fuld gang med at udvikle mere eller mindre åbne webservices, som skal gøre det muligt at udveksle data med hidtil isolerede it-systemer via internettet – uanset om man sidder på sit kontor foran en desktop eller i en lufthavn med en trådløs mobil enhed.

Men med mulighederne følger også væsentlige udfordringer – særligt på sikkerhedsområdet. Derfor skal vi i det følgende se lidt nærmere på, hvordan man nu og i fremtiden kan sikre sit datacenter bedst muligt imod de mange trusler, der følger med, når man rykker det ind i en mobil Web 2.0-verden.

1. De nye trusler

Nye potentielle sikkerhedsrisici

De attraktive webservices skaber en række nye kontaktpunkter mellem virksomhedens netværk og omverden, og derfor er det vigtigt, at virksomheden er opmærksom på alle de potentielle sikkerhedsrisici, der ligger i at føje webservices og mobile adgangsmuligheder til it-infrastrukturen.

Blandt de potentielle sikkerhedsproblemer/risici kan nævnes:

Vanskeligere at kontrollere brugernes identitet

- **Brugerne bliver flere og mere forskellige.** For at styrke kontaktfladerne med stadig flere interessentgrupper åbnes systemerne for nye typer af brugere. Ikke blot medarbejdere, men også partnere, kunder og myndighederne får adgang, og det gør det vanskeligere at kontrollere brugernes individuelle identitet og rettigheder på netværket.

Sikkerhedshuller i programmeringen

- **Brugerne får hele tiden adgang til nye tjenester,** der mætter nye behov. Presset på den enkelte virksomhed for konstant at differentiere sig i markedet med nye webservices er voldsomt, og hastigheden, hvormed nye applikationer udvikles, skaber ofte kritiske sikkerhedshuller i programmeringen, som kan udnyttes.

Vanskeligere at adgangskontrollere trafik af følsomme data

- **Brugerne benytter et voksende antal kanaler.** Virksomhedernes indbyrdes kamp om at tilbyde webservices på så mange platforme som muligt (fx mobiltelefoner, bil-GPS'er, tv, iPods osv.) er hård, og den hurtige spredning til nye platforme gør det stadig vanskeligere at adgangskontrollere trafikken af følsomme data.

Øgede beføjelser skaber nye risici

- **Brugerne interagerer i stigende grad aktivt med systemerne** frem for blot at hente information. Interaktionsmuligheder højner typisk brugeroplevelsen af den enkelte webservice, hvorfor mange virksomheder giver brugerne stadig videre beføjelser på netværket. Det er god service, men det gør det samtidig nemmere at forgifte systemerne med skadelig kode.

Sårbare forbindelser

- **Brugerne bliver mere mobile.** Til de fleste webservices tilføjes før eller siden en mobilservice, som gør det muligt at udveksle data trådløst med virksomhedens netværk via en mobil enhed som fx en PDA eller en smartphone. Men de mobile muligheder betyder også, at virksomheden udveksler data via forbindelser og med enheder, der som udgangspunkt er langt mere sårbare end de computere, der står inden for virksomhedens mure.

Risiko for tyveri af kodeord m.v.

- **Professionalisering af internetkriminalitet.** Der er mange penge i at stjæle og videresælge værdifulde oplysninger, og derfor findes der i dag et stort antal professionelle internetforbrydere, som går systematisk efter at udnytte websites og -services, som ikke er tilstrækkeligt sikkert

opbygget, eller som ikke bliver vedligeholdt sikkerhedsmæssigt. Det betyder, at en virksomhed nemt kan risikere at få stjålet kodeord til virksomhedens netværk eller at få manipuleret sit website.

2. Netværket som platform for sikkerhed

Spørgsmålet er, hvordan man som virksomhed kan udnytte de mange muligheder og platforme maksimalt og samtidig imødekomme de ovenstående sikkerhedsudfordringer.

Ledelsen skal tænke sikkerhed ind fra starten

Aktiv deltagelse i it-strategien

Sikkerhed i en mobil Web 2.0-verden handler ikke om, at it-afdelingen skal huske at installere antivirusprogrammer på samtlige pc'er. Sikkerhed er blevet en ledelsesbeslutning – og en beslutning, der skal ses som en grundlæggende forudsætning for enhver webservice eller mobil løsning.

Det er nemlig ledelsen, som i sidste ende bliver stillet til ansvar, hvis virksomhedens netværk bliver hacket, og der lækkes fortrolige oplysninger til offentligheden, der efterfølgende får aktiekursen til at falde eller betyder, at virksomheden ryger ud i en retssag. Det er derfor afgørende for sikkerheden i en virksomhed, som vil udbygge sine systemer med mobile webservices, at ledelsen indledningsvis deltager aktivt i planlægningen af virksomhedens it-sikkerhedsstrategi. Dels fordi det kun er ledelsen, der er i stand til at udpege de dele af forretningen, som er kritiske og derfor skal gives sikkerhedsmæssig topprioritet, og dels fordi det kun er ledelsen, der kan sørge for, at sikkerheden bliver tænkt ind fra begyndelsen.