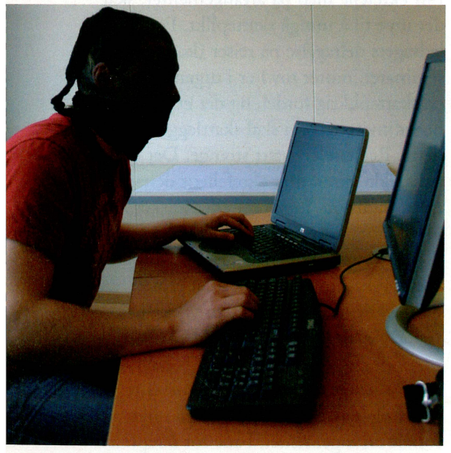
Sikkerhetsanalyse:

Egne ansatte, en trussel mot sikkerheten?

Vi har hørt det før og vil høre det igjen: IT-sikkerhet er viktig, koster penger og blir i mange tilfeller ikke vurdert på alvor. At dette budskapet er klart og lett å huske betyr ikke at det er lett å håndtere for den som skal lede. For å oppnå et tilfredsstillende sikkerhetsnivå, er det avgjørende å prioritere rett og å skille det viktige fra det mindre viktige. Det betyr i praksis at man må gjennomføre en sikkerhetsanalyse.

Av Folker den Braber og Ketil Stølen, SINTEF IKT

Som leder er det altfor lett å fokusere på de tekniske aspektene ved it-sikkerhet. Brannmur, kryptering, virusskanner, spamfilter og intrusion detection kan kjøpes of-the-shelf og gir god gjenklang hos nettverk- og system-administratorer. Men som vi alle vet: At dører har låser og korridorene har video-kameraer, betyr ikke nødvendigvis at verdisakene er trygge. Retningslinjene hvordan nøklene oppbevares og kameraene brukes og hvem som får hvilke nøkler er vel så viktig.



Utfordringen er å oppdage hendelser eller mulige hendelser før det er for sent. Dette krever at ledelsen har god oversikt over de respektive systemenes aktiva og hvordan de blir tatt vare på. Foto: Einar Ravndal.

INTERNE DEN STØRSTE TRUSSELEN

Flere undersøkelser viser at brudd på interne retningslinjer og instrukser er blant de største truslene mot bedriftenes sikkerhet. I en nylig publisert undersøkelse fra U.S. Secret Service og CERT Coordination Center/SEI hevdes bare hackere utgjør en større trussel mot sikkerheten enn ansatte, tidligere ansatte og innleide konsulenter.

Typiske eksempler:

- En ansatt med tilgang til nøkkeldata er misfornøyd med sin arbeidssituasjon og ødelegger forretningskritiske data.
- En ansatt får beskjed om å omgå sikkerhetsretningslinjer og rutiner fordi det haster med en leveranse.
- En tidligere ansatt har blitt fratatt administratorrettigheter, men har fortsatt tilgang til bedriftens IT-systemer via remote aksess.
- En ansatt bruker jobb pc-en til å laste ned musikk, film eller porno¬grafisk materiale og lagrer dette på et felles område i intranettet.

Som leder må man ta stilling til følgende spørsmål:

- Kan dette skje i min bedrift?
- Hva er sjansen for at det skjer, og hva kan gjøres for å minske den?
- Hvordan oppdager jeg det om det skjer?
- Hva skjer med den som forårsaket skaden?

Kan dette skje i din bedrift? For de fleste virksomheter er it-systemer tett integrert i den daglige driften. De ansatte sitter på nøkkelkompetanse rundt disse systemene. Alle bedrifter som kjører kritiske applikasjoner og lagrer kritiske data digitalt er derfor i utgangspunktet sårbare for denne type trusler, uavhengig om disse handlingene er gjort med hensikt eller ikke.

VIRKEMIDLER

Hva er sjansen for at det skjer, og hva kan gjøres for å minske den? Langt fra alle sikkerhetshendelser blir rapportert, og det er nok mer enn vanlig å rapportere hendelsen med ekstern årsak enn de som har intern opprinnelse. En undersøkelse gjort av E-Crime Watch Survey antyder at 70 prosent av hendelsene rapportert fra 500 bedrifter kunne sies å ha enten ekstern eller intern årsak. 29 prosent av disse tilhørte siste kategori. Det viser seg at sabotasje som oftest utføres av en person som er misfornøyd med sin arbeidssituasjon og som har forutsetninger for å kunne skade bedriften, enten som ansatt eller som tidligere ansatt. Dette betyr at det er viktig for ledelsen å følge opp sine ansatte, og ikke minst være klar over hvem som sitter på hvilken kompetanse.

Hvordan kan du oppdage slike sikkerhetsbrudd? Når konsekvensen er alvorlig nok, er ikke oppdagelsen det største problemet. Utfordringen er å oppdage hendelser eller mulige hendelser før det er for sent. Dette krever at ledelsen har god oversikt over de respektive systemenes aktiva og hvordan de blir tatt vare på. En slik oversikt kan man kun få ved å utføre en risikoanalyse med fokus på hele virksomheten, altså ikke bare brannmurer, spamfiltere og viruskontroll-verktøy. En leder som har kontroll over uvanlig nettverktrafikk, endring av konfigurasjonsfiler og hvem som har administrasjonsrettigheter, har gode forutsetninger for å oppdage hendelsene før det er for sent.

KONSEKVENSER FOR ANSATTE

Hva skjer med den som forårsaket skaden? En amerikansk rapport om konsekvenser fra 49 sabotasjesaker utført av insidere i perioden 1996-2002 viser at 90 prosent ble domfelt. Lengden på dommen var mellom 12 til 180 måneder, med et snitt på 36 måneder. Erstatningsbeløpene var mellom $100 og $2 million.

> "At dører har låser og korridorene har videokameraer, betyr ikke nødvendigvis at verdisakene er trygge"

> "Fristelsen blir mindre når en potensielt utro tjener er klar over at ledelsen har tilgang og evne til å tolke for eksempel logger"

De ansatte utgjør en stor del av bedriftens verdi og i kombinasjon med elektroniske data og IT-tjenester har de stor innflytelse. Foruten å motivere de ansatte er det viktig å følge opp med kurs og trening for å bevisstgjøre de ansatte med hensyn til eksisterende sikkerhetsretningslinjer og instrukser. Fristelsen blir mindre når en potensielt utro tjener er klar over at ledelsen har tilgang og evne til å tolke for eksempel logger.

It-sikkerhet handler om å beskytte it-systemenes aktiva. Illojale ansatte eller tidligere ansatte med kompetanse og motivasjon for å skade bedriften, kan utgjøre en stor trussel dersom ikke ledelsen

- formidler klare retningslinjer og instrukser for IT-sikkerhet,
- vedlikeholder en god sikkerhetskultur, og
- klarer å utnytte de tekniske muligheter for å oppdage mulige hendelser i tide.