

Unix og sikkerhet:

Åpen som en sveitserost

– Unix-systemer er åpne som en sveitserost. Når man tetter hullene, dukker det opp stadig nye hull, hevder Anders Christensen. Han er datastudent på NTH og har bijobb med å holde oppsyn med studentmaskinene som kjører under Unix. Datasikkerhet er et viktig tema i oppsynet av over 100 maskiner.

KNUT STRØM

– Unix skulle i utgangspunktet ikke være noe spesielt sikkert system. Nå er dette bedret, og vanligvis kommer maskinene med sikkerhet innebygd, men du må «slå på» denne funksjonen selv, sier Christensen.

– De fleste sikkerhetsproblemer har ikke noe med konseptet å gjøre, men skyldes ofte dårlig programmering og idiotisk «innpakning» av systemene fra leverandørenes side.

Etter hvert som folk går over til Unix-maskiner, vil de oftest også koble seg inn på et nett. Da kan de få problemer med en gang når det gjelder sikkerhet. Når du er på et nett, kan andre også nå din maskin. Når du f.eks. skriver et passord, så kan dette gå over nettet. Det er det få som tenker på. Det sitter mange maskiner koblet til nett som ikke holder sikkerhetsmessig.

Godt sikkerhetsarbeid oppdager du ikke før du trenger det, og derfor gjelder det å ha en bevisst strategi. I alle operativsystemer er det svakheter. Det hjelper ikke med sikkerhetslåser på sidedøra når hoveddøra står åpen, sier Christensen lakonisk.

Tredelt sikkerhet

Sikkerheten ved Unix-maskiner kan deles i tre, mener han. – For det første har vi sikkerhet mot avbrudd. Her bør strategien være at man kan koble om på maskiner. Så kommer sikkerhet mot innbrudd. Man må sørge for at det ikke skjer noe ved «innbrudd» i maskinen. For det tredje må man følge opp maskinen, ved f.eks. overvåkning av loggene. Sikkerhetskopiering av data er det

enkleste og det første de fleste tenker på når det gjelder sikkerhet. Dermed tar mange sikkerhetskopier til «den store gullmedalje». Men det er dumt å legge mer arbeid ned i dette enn det er verdt.

Nå må man heller ikke se seg blind på sikkerhet. Maskinene skal tross alt fungere, det blir dermed ofte en avveining mellom sikkerhet og brukermiljø. For mange sikkerhetstiltak kan være til hinder for brukerne. Man bør også avveie faren for at noe går galt mot hvor mye arbeid det ligger i sikring. Hvis det ikke er følsomme ting, er det ingen vits med høy sikkerhet.

Ifølge Christensen har studentmaskinene på NTH 1000–2000 aktive brukere, og her har man en systematisk overvåkning av loggene. – Vi følger opp uregelmessigheter slik at brukerne vet at vi følger med dem, og vi oppdager mer enn det brukerne tror.

Ingen «hackerkultur»

– Heldigvis er det et aktivt og positivt miljø blant studentene. Vi har ikke noen hackerkultur. Vi har en studentforening for den datainteresserte student. Det er bedre å gjøre noe konstruktivt med datamaskiner enn å bruke dem til noe ulovlig.

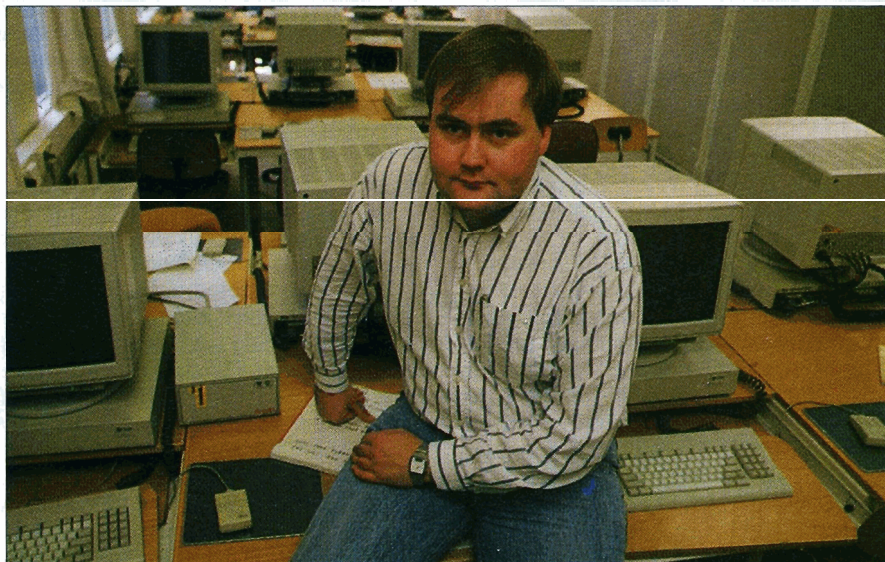
Det å skape en ansvarlig holdning blant studentene avhenger mye av hva institusjonen også legger opp til. Vi har klart å få et positivt miljø og et godt sam-

arbeid med studentene. Studentmaskinene får oftest stå i fred og er lite utsatt for destruktiv fikling. Det samme gjelder også programmene, sier Christensen.

– På Unix-maskinene har vi heller ikke noe virusproblem fordi virus ikke trives på slike maskiner. De har en arkitektur som ikke så lett lar seg påvirke av virus. Men vi har også en del PC-saler hvor vi har vært plaget med virus. Mesteparten utryddes raskt. Det kjøres virusjekk på alle PC-er. Det er viktig å ta slikt med en gang det kommer inn i maskinen. Hvis du ikke tar affære raskt og rensker ut, blir snart hele datasalen smittet.

Jeg tror at virus er en plage vi må fortsette å leve med så lenge PC-ene er så enkle. Hvis PC-ene hadde en annen arkitektur, ville vi ikke hatt virusproblemet. Nye operativsystemer vil kunne bedre dette.

Hvis man ønsker i å ha aktivt forhold til sikkerhet, er det viktig at man ser på systemet som en helhet. Problemet med Unix-maskiner er at de markedsføres som om de driver seg selv. Oftest har de fleste en person som driver med noe annet og har overoppsynet med maskinen ved siden av. Dermed får man en sikkerhet som er tilsvarende. Har du høye krav til sikkerhet, bør du ha egne folk til å ta seg av maskinen, påpeker Christensen. ●



Anders Christensen studerer data ved Institutt for datateknikk og telematikk. Siden 1988 har han hatt en bijobb med oppassing av studentmaskinene som kjører under Unix.