

Utfärdare

2230 Christer Jonsson/rml 031-669559

Datum

90-01-15

I330064

Sida 1

Ärende

INFORMATION

PU-uppdrag (slutrapport)

Aktivitet

Säkerhetsutredning avseende synkrona kopplade linjeingångar.

Förutsättningar/Bakgrund

Via nätstyrelsen har framförts behov av att skydda även synkrona uppringda datoringångar från obehörig åtkomst. En studie av säkerheten vid uppringd datoranslutning har påkallats vid säkerhetsrevision utförd av Volvo Datas revisorer. Även det tidigare genomförda PU-projektet avseende motringare i asynkrona nätet initierades av Volvo Datas revisorer. Resultatet av det projektet var att samtliga asynkrona uppringda ingångar till Volvo Datas nät nu är skyddade mot åtkomst med hjälp av s k motringare.

Mål/Inriktning

Endast behöriga användare skall ha åtkomst till Volvos nät.
Projektet är en förstudie (enl AU-modellen) avseende säkerhet och skydd av uppringda synkrona linjeingångar.

Resultat**Nulägesbeskrivning:**

Vi har för närvarande c a 500 användare av uppringd SDLC, d v s som emulerar 3270-protokoll. Dessutom har vi c a 450 användare som kör RJE via BSC eller SDLC. Dessa emulerar 3780 respektive 3770. Tjänsterna som används är antingen DATEL, DATEX eller X.25. Antalet ingångar fördelas enligt: DATEL c a 40st, DATEX c a 120st och X.25 1st (16 logiska kanaler som även används av DIALOUT). Dessutom finns ett antal leverantörer som kör ODETTE.

Användarna delas in enligt följande:

Alt	Tjäns	Prot	ID	PSW	XID	ACF2	Motring	Tvt	Övr
1	DATEL	3270	nej	nej	ja	ja	ja	nej	ja
2	DATEX	3270	ja	nej	nej	ja	nej,fast	CUG	ja
3	DATEX	3270	nej	nej	ja	ja	nej	CUG	ja
4	DATEX	3270	ja	nej	ja	ja	nej	CUG	ja
5	DATEL	37X0	ja	ja	nej	ja	ja	nej	ja
6	DATEL	37X0	ja	ja	nej	ja	ja	nej	ja
7	DATEL	37X0	ja	ja	nej	ja	ja	nej	ja
8	X.25	Odet	ja	ja	25kod	ja	nej	CUG	ja

Som synes är säkerhetsnivån skiftande. Lösningen är därför inte entydig utan ett flertal olika alternativ får tas under övervägande.

Av ovanstående framgår att det endast är DATEL som kan komma ifråga avseende motringning. Övriga kan, som jag ser det, få säkerhet genom att Televerkstjänsten CUG (closed user group=sluten anv grupp) används. Under kolumnen Övr finns andra typer av säkerhetslösningar enligt nedan. Tester med motringning har gjorts med bl a Informer och Minec vilka fungerat utmärkt.

Vi har goda erfarenheter av motringare i det asynkrona nätet. En motsvarande lösning i den synkrona världen skulle bli funktionellt jämförbar. Kostnaden för 2 st CEcure, c a 300 KSEK, skulle klara vårt behov.

Data-lock and key är en metod där användaren identifierar sig med en dosa (key) som kopplas in mellan modem och terminal. För att administrationen av denna lösning ska minimeras kan man lägga in den i ACF2-definitionen av en användare. Denna lösning kan användas där V24-interfacet är åtkomligt. På hostsidan sätts Data-lock mellan modem och 37X5.

Administrering från PC/DOS är också möjlig. Kostnad för 50 linjer och 500 användare blir c a 2200 KSEK plus tid för uppdatering av ACF2.

Denna lösning ger ytterligare en nivå av säkerhet genom dosan.

En annan lösning av liknande karaktär är Info-key och Traqnet. Det är också en dosa (Info-key) som sätts i telefonjacket, d v s närmare nätet än i Data-lock fallet. På hostsidan sätts den också i jacket, d v s innan modemmet, vilket ger den fördelen att användaren inte har åtkomst till modemmet förrän han slagit in sin kod. Den fungerar så att man ringer upp och anger sin kod varefter Traqnet verifierar det och skickar en 'challenge' som Info-key skickar tillbaka ett svar på. Varje Info-key är unik och kan knytas till en särskild användare.

Följande alternativ kan mixas efter behov:

- 1 Endast kod mot Traqnet
- 2 Info-key, kod och Traqnet
- 3 Mottringning mot Traqnet, statisk och dynamisk
- 4 Mottringning, Info-key och Traqnet

Administration sker via PC/DOS eller VT100-terminal av dagens typ med CEcure Loggning antingen på PC, i buffer eller på printer. Kostnaden blir 10 KSEK per linje och 1.5 KSEK per användare. 50 linjer med 500 användare skulle därför kosta $50 \times 10 + 500 \times 1.5 = 1250$ KSEK.

Det sista alternativet ger den bästa säkerhetsnivån samt mesta flexibiliteten och är en helt transparent lösning. Sammanfattningsvis kan sägas, att ju mer säkerhet man har desto mer kostar det.

Administrationen av ett säkerhetssystem är som vi märkt tung. Därför vore det bra om man kunde lägga detta på en redan fungerande funktion som t ex ACF2-administratören eller den redan fungerande för asynkron kommunikation. Lösningen med ACF2 andra nackdelar som krav på tillgång till V24-snittet, samt att endast en del av funktionerna i systemet finns tillgängliga i en synkron miljö.

Om man kan använda samma lösning i både asynkron som synkron miljö, vore det också en acceptabel lösning, då samma person skulle kunna administrera bägge. Lösningen med mottringning (CEcure) och Info-key skulle kunna klara detta. Ur kundens synpunkt måste man konstatera att det är svårhanterbart att öka säkerheten, d v s det blir besvärligare att logga på med flera nivåer av säkerhet. Info-key skulle kunna ge en hög säkerhet utan mottringning och därmed skulle användarnas problem minskas väsentligt.

Nästa steg

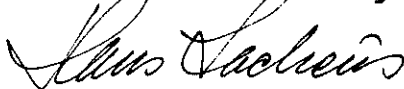
Jag föreslår att vi som nästa steg tittar vidare på Info-key och Traqnet. Leverantören har lovat att vi under en tid skulle kunna få testa utrustningen för att få erfarenhet för vidare beslut i frågan. Därför bör ett nytt projekt startas upp som tittar på denna produkt och hur den faller in i Volvo Datas säkerhetskoncept som helhet, d v s skyddet av våra datorer från obehörigt intrång såväl inifrån som utifrån. Införande av CUG bör också utredas då det ger ökad säkerhet till en ganska billig penning.

För ytterligare information kontakta:

Christer Jonsson, avd 2230, tfn 669559, MEMO-id VD.2230CJ.

Göteborg den 11 januari 1990

VOLVO DATA AB
Marknadsutveckling



Hans Lackéus

Distribution

35 Volvo Datas Affärsansvariga-
Marknadskontakt - Marknadsansvar
36 Produktansvariga
109 PU-rapport

FORSBERG INGE
02510
DA2