

# Hemliga koder räddar affärsverksamheten

Mardrömmen för många är ett Al Qaida-angrepp som slår ut våra IT-system. Sanningen är att ett företag kan drabbas lika hårt om en leverantör går i konkurs!

TEXT TOMMY SVENSSON FOTO TOMMY SVENSSON, IMAGE LIBRARY

Det är många som är beroende av fungerande IT-system. Då måste man tänka framåt. Alla inser de närliggande problemen med hackerangrepp, datorvirus och elavbrott. En och annan oroar sig för Al Qaida. Det finns ett annat vardagligt problem som är enklare att lösa. De verksamhetskritiska datorprogrammen måste fungera. Därför måste man försäkra sig om att få tillgång till källkoderna om vissa saker inträffar. Företag kan gå i konkurs eller bli uppköpt och produkten nedlagd eller kompetensen kan försvinna om nyckelpersonerna lämnar företaget. Listan kan göras lång.

När företag och myndigheter gör kostsamma investeringar i IT-system hamnar de i ett dåligt läge om leverantören går i konkurs eller av någon annan anledning inte längre kan – eller vill – leverera det utlovade underhållet av programvaran. Ofta är det bara leverantören som har tillgång till källkoden. Utan källkod går det inte att underhålla och utveckla och rätta fel i programmet. Källkoden är i de flesta fall en viktig företagshemlighet som leverantören vill behålla för sig själv. När kunden tecknar en användarlicens får han en programversion som bara datorn förstår (objektкод). Det mest värdefulla – källkoden – vill de flesta leverantörer behålla. Källkoden är för en programmerare vad det hemliga receptet är för en stjärnkock. Det är vad programföretaget i framtiden ska tjäna pengar på genom underhållsavtal och vidareutveckling av nya programreleaser.

**KÄLLKODSDEPONERING HAR ÖKAT** under senare år och idag finns det etablerade rutiner tillgängliga på marknaden. Det gör det enkelt för kunderna. Sedan kunden undertecknat ett avtal tar depositionsföretaget över allt det praktiska. Kunden får därefter löpande rapportering om de olika åtgärder som vidtas för att bevaka kundens intresse. Men det finns många fallgropar och risker för både kund och leverantör.

Det är viktigt att bevaka kundens intressen för att säkerställa kontinuiteten i kundens verksamhet, men leverantörernas intressen är lika viktiga. Leverantörerna måste kunna lita på att källkoderna, som är en värdefull företagshemlighet, inte kommer på avvägar så därför är det en avancerad historia innan kunderna kan få tillgång till koderna. Avtalsregleringen måste vara tydlig så att både kund och leverantör vet vad som gäller. En leverantör måste vara mycket försiktig med valet av vem som ska få förtroendet att ta hand om de värdefulla källkoderna. Företagsgruppen *Escrow Europe* har enligt uppgift mer än 10 000 källkoder i förvar. Det är enkelt att förstå att detta är en veritabel guldgruva. Säkerhetsexperten oroas nu över att även denna bransch ska drabbas av lycksökare och bluffföretag. Men det finns också andra risker som lätt kan undanröjas om man inser problemet. Lösningen är verifiering, med

Ingel Rabenius är vd för företaget Deposit som har tusentals källkoder i förvar.



andra ord en seriös kontroll av vad som deponeras.

– När verksamheten startades för drygt tio år sedan bedömde vi att marknaden inte var mogen för mer än passiva förvaringstjänster, säger *Ingel Rabenius*, som är vd på företaget *Deposit AB – Escrow Europe Scandinavia*. Företaget började med att erbjuda en enkel förvaringstjänst, men siktet var inställt på att inom några år leverera en avancerad och aktiv depositionstjänst.

**VEM SOM HELST** kan förvara källkoder, exempelvis advokater och revisorer. En sådan passiv förvaring ger inte mycket säkerhet eftersom ingen har kontrollerat (verifierat) att materialet är komplett och användbart. En aktiv depositionstjänst med både verifiering och bevakning av att depositionen uppdateras varje gång leverantören släpper en ny programversion har stort värde för kunden. Naturligtvis måste också uppdateringarna verifieras.

Den som nöjer sig med att leverantören deponerar en sluten försändelse köper ”grisen i säcken”, för att citera *Tomas Djurling*, säkerhetsexpert på *Computer Sweden*.

Det händer att leverantörer erbjuder kunderna att vara närvarande när depositionen förpackas och försluts för att lämnas in för förvaring. Det kan verka vara ett alternativ till verifiering men det räcker inte att kunden är närvarande. Det krävs teknisk kompetens och en teknisk analys för att förvissa sig om att all kod och teknisk dokumentation finns med och att det är läsbart.

Utan att misstänka att leverantörer luras eller medvetet slarvar när materialet laddas ner kan man konstatera att alla som tagit en back-up vet hur lätt det blir fel. Det är vanligt med fel och brister i den första depositionen som då får rättas till och kompletteras, berättar *Richard Hoek* som ansvarar för den tekniska avdelningen på *Escrow Europe*.

**DET VORE EN MARDRÖM** för depositionsföretaget att lämna ut en förvarad källkod och upptäcka att den inte är användbar, det vill säga att kunden i flera år levt utan den säkerhet som han trott sig ha. Det är som att känna sig trygg med en tom brandsläckare.

Man kan tro att leverantörerna knorrar inför kundernas krav på källkodsdeponering, men så är inte fallet. Många leverantörer tar själva initiativet och deponerar källkod för att kunna använda det som ett säljargument. Kunderna sätter värde på den ökade tryggheten och föredrar ofta att teckna licensavtal med en leverantör som deponerat källkoden. Leverantörer inser också att administrationen blir minimal med deposition – och uppdatering – på ett enda ställe. Alla kunder – oavsett var i världen de befinner sig – kan sedan anslutas till den redan gjorda depositionen. En annan fördel är att leverantören då bestämmer vilken lagstiftning som ska gälla. Det förenklar för en svensk leverantör om svensk lag gäller genomgående. ●

## Se upp för fallgroparna!

Johan Kahn, advokat och säkerhetsjuridisk expert på S.O.S Skydd och Säkerhet varnar för de vanligaste fallgroparna vid källkodsdeponering.

- ✓ Man inser inte källkodernas och IT-systemens betydelse för verksamheten och missar frågan om källkodsdeponering
- ✓ Man accepterar obalanserade avtal som inte tar tillräcklig hänsyn till både kundens och leverantörens intressen. Leverantören måste försäkra sig om att affärshemligheterna är tillräckligt skyddade och kunden måste veta att det finns relevanta grunder för utlämnande av källkoden. (Källkoden är vanligtvis att betrakta som en företagshemlighet enligt lagen om skydd för företagshemligheter. Det innebär att angrepp på källkoden är både straff- och skadestandsgrundande.)
- ✓ Trots att det finns avtal om att leverantören ska deponera källkoder och teknisk dokumentation så glömmer man att bevaka att depositionen verkligen görs och att det sedan följs upp med uppdateringar. (Dokumentationen är central för användningen av källkod vilket innebär att koden i sig själv sällan räcker för framtida användning.)
- ✓ Ingen kontrollerar tillräckligt bra (verifierar) vad som deponeras och uppdateras
- ✓ Kunden får inget kontrakt eller annat skriftligt bevis på sina rättigheter utan nöjer sig med en uppgift om att leverantören har deponerat källkoden för kundernas räkning
- ✓ Koden lämnas i förvar hos någon som saknar tillräcklig kompetens eller rent av är ohederlig
- ✓ Det är kritiskt att depositionsavtalet och/eller det ursprungliga avtalet (om nyttjanderätt eller överlåtelse av rättigheterna) uttryckligen anger om kunden skall få göra ändringar i källkoden. Om sådant uttryckligt medgivande till ändringar inte finns avtalat får de inte göras. Samma sak gäller för kundens rätt till vidareöverlåtelse av källkoden. Rättighetsfrågorna måste således regleras utförligt för att kunden överhuvudtaget skall ha någon nytta av källkoden.

