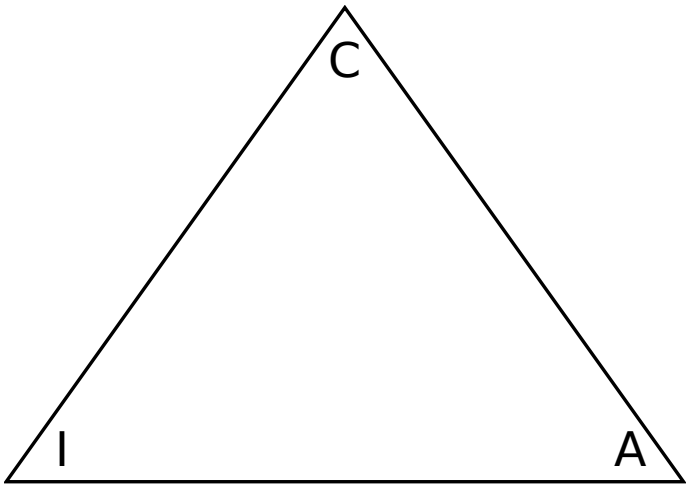
Kapitel 15

Säkerhet

15.1 CIA



CIA är en bra förkortning att tänka på när det gäller datorsäkerhet. Och då menar jag inte den amerikanska spionorganisationen utan triangeln med Confidentiality, Integrity och Availability. På svenska blir det ungefär hemlighet (eller sekretess), dataintegritet och tillgänglighet (men HDT är inte lika lätt att minnas).

Jag beskriver dessa tre faktorer mer ingående.

- Confidentiality är att ingen obehörig ska kunna läsa informationen. Till exempel kryptering på disk och nät, åtkomstkontroll via lösenord och filrättigheter.
- Integrity betyder att informationen går att lita på. Att ingen har ändrat den. Alltså inte samma som personlig integritet på svenska. Dataintegritet gäller både avsiktlig och oavsiktlig förändring, och kan tillgodoses via kontrollsummor och redundant (t.ex. dubbel) lagring.
- Availability är tillgänglighet, går inte informationen att komma åt när den behövs har den inte stort värde. Att ha informationen på flera ställen ökar tillgängligheten, som backup.

Det går inte att maximera alla tre faktorerna samtidigt. Kompromissen blir alltid en punkt någonstans inuti triangeln. Till exempel ökar en backup A och I, men sänker C (det blir ett ställe till att skydda). Och avancerad kryptering minskar tillgängligheten.

Säkerhet är viktigt, men svårt. Den som vill göra intrång behöver bara hitta ett hål, men den som skyddar måste hitta alla. Det gäller att försvåra så mycket att det inte blir värt mödan att attackera, men att hitta alla attackytor kan vara ett heltidsjobb. Jag försöker ge några tips i detta kapitel, och säkerhetsrelaterad information finns även i andra kapitel i boken (t.ex. kapitel 7 om brandväggar). Lite paranoia är bra, men det får inte gå till överdrift. Jag är inte säker på att min dator är säker, men jag har inte upptäckt intrång på några egna system. Däremot på några andra ställen.

15.2 Uppdaterad

Uppdateringar kommer till alla operativsystem. Inget system är felfritt. För produktionsservrar bör du köra ett system som enbart, eller främst, släpper säkerhetsrelaterade uppdateringar. Till exempel Red Hat, CentOS eller Debian. Inte Fedora eller Gentoo. Kör du någon av dem jag rekommenderar eller någon liknande kan du gärna ha automatiska uppdateringar påslagna. Till exempel genom `yum install yum-cron` på Red Hat och CentOS. Vissa rekommenderar att

ha en testmaskin där du manuellt lägger in uppdateringar och inte lägger in dem direkt på servrar i skarp drift, eftersom det kan bli problem. Men ett intrång skulle medföra större problem, och tillverkaren testar sina patchar innan de släpps. Vilket man väljer är en smaksak, men hur du än gör bör du inte vänta länge med att uppdatera. Kör du det manuellt är kommandona `sudo yum update` på RH och `sudo apt-get update` följt av `sudo apt-get upgrade` på Debian-baserade system. På Debian bör du ibland även köra `sudo apt-get dist-upgrade` för att få senaste kärnorna. Och du bör följa mejlinglistor för vilka nya paket som kommer, så du är förvarnad.

15.3 AAA

En annan förkortning som är bra att ha i minnet är AAA. Den betyder autentisering, auktorisation och accounting. Jag nämnde skillnaden mellan de två första A:na i kapitlet om Apache på sidan 79 men upprepar här. Autentisering är att bevisa vem man är. Både användare, system och datas ursprung kan autentiseras, jag beskriver här hur det kan fungera för en person. När du loggar in på en dator anger du ofta användarnamn och lösenord. Användarnamnet anger vem du är, och lösenordet ska det enbart vara du som vet. Kombinationen av dessa uppgifter bekräftar för systemet att du verkligen är du.

Nästa A, auktorisation, är en annan sak, det är en lista på vad den inloggade användaren för göra. Till exempel får inte en vanlig användare skriva i andra kataloger än sin hemkatalog och ett fåtal ställen till. Men root får göra allt.

Det tredje A:et skriver jag på engelska för att akronymen ska bli rätt. Man kan kalla accounting för loggning eller spårbarhet på svenska, det är alltså att man in efterhand ska veta vem som har gjort vad.

För autentisering brukar man skilja mellan tre sätt:

- Något du vet. T.ex. lösenord, PIN-kod eller personlig uppgift.
- Något du har. T.ex. bankdosa, ID-kort, data i en fil.
- Något du är. T.ex. foto, fingeravtryck, näthinna. Det kallas även för biometrisk autentisering.

Det är vanligt med kombinationer av ”vet” och ”har”. ”Är” används inte lika mycket i automatiska system än, men att inte släppa in okända på jobbet eller ringa upp kollegor vid lösenordsbyte är på sätt och vis en biometrisk autentisering.

15.4 Kryptering

Kryptering är att göra något oläsbart för andra. Man skiljer på symmetriska och asymmetriska krypton.

Vid symmetrisk kryptering har båda parter samma nyckel. Den måste hållas hemlig för alla andra.

Vid asymmetrisk kryptering använder man nyckelpar. En publik och en privat nyckel, den ena kan inte räknas ut från den andra. Den privata nyckeln måste hållas hemlig, däremot kan man sprida den publika nyckeln hur mycket man vill. Ett system som använder asymmetriskt krypto är PGP, med GNU-varianten GPG. Den som vill skicka krypterad e-post till dig letar reda på din publika nyckel (eller har den sen tidigare) och krypterar mejlet med den publika nyckeln. Ingen annan än innehavaren av den privata nyckeln (du) kan då dekryptera meddelandet.

Det finns flera olika algoritmer för asymmetriskt krypto. En vanlig är RSA, den bygger på svårigheten att hitta faktorer till stora tal. Vanliga nyckellängder är 1024 och 2048 bits. Ofta används asymmetrisk kryptering för att överföra en symmetrisk sessionsnyckel.

En annan användning av nyckelpar är att signera meddelanden. Då signerar man med sin privata nyckel och alla som har den motsvarande publika nyckeln kan se att det enbart kan vara innehavaren av den privata som har skickat mejlet.

15.5 Lästips

För mer detaljer om kryptering, men ändå lättläst, kan jag rekommendera boken: *Cryptography, A Very Short Introduction* av Piper & Murphy, från Oxford University Press.

För datorsäkerhet i allmänhet är en mycket läsvärd bok *Secrets & Lies, Digital security in a networked world* av Bruce Schneier.

Två andra bra böcker är *Hardening Linux* av James Turnbull. Apress (2005) och *Hacking The Next Generation* av Dhanjani, Rios & Hardin. O'Reilly (2009).