Så säkert är Mac OS X

Apples framgångar med Mac OS X tycks vara oändliga. Men i takt med att det Unixbaserade operativsystemet blir allt mer komplext och funktionsrikt undrar allt fler om säkerheten verkligen hänger med. Här har vi tagit hjälp av några säkerhetsexperter för att räta ut frågetecknen.

TEXT: JOACIM MELIN FOTO: ANDREAS EKLUND

Apple var från mitten av 1990-talet fram till början på 2000-talet om inte dödförklarade så åtminstone hyfsat nära. Försäljningen gick uselt. När Apple väl lyckades få till en produkt som sålde bra, exempelvis den bärbara datorn Powerbook, kunde de antingen inte leverera tillräckligt många enheter till butikerna eller så var kvaliteten så usel att produkten fick dåligt rykte och försäljningen gick i botten.

Med den lilla datorn Imac och sedan Mac OS X vände Apple trenden. I mars 2001 släpptes den första versionen av företagets nya operativsystem. Mac OS X var fött – men helt nytt var det inte.

Mac OS X föddes ur något av en bastard kallad Rhapsody, ett kodnamn för vad som skulle bli Apples nästa operativsystem. Rhapsody byggde enkelt uttryckt på Nexts operativsystem Openstep i kombination med valda delar från Apples gamla trotjänare till operativsystem, Mac OS. I kombination med delar från Free BSD och Net BSD blev det här det som senare fick namnet Mac OS X.

De valda delarna från Mac OS var rent kosmetiska och fanns med i Rhapsody för att göra övergången från gamla Mac OS till ett nyare Unixbaserat operativsystem enklare för användarna. Efter att Steve Jobs återvänt till Apple i och med köpet av Next skrotades dock det gamla gränssnittet helt. Det ersattes av Aqua, ett nytt gränssnitt där vissa egenskaper hämtats från gamla Mac OS.

Kärnan i Mac OS X bygger på Mach-kärnan, som även användes i Nextstep och

"Säkerheten är lätt att hantera för användaren."

Dino Dai Zavi, säkerhetsexpert

Openstep. Operativsystemet är posix-kompatibelt och kärnan kallas XNU (vilket lär stå för X is Not Unix) och bygger på en kombination av version 3.0 av Mach-kärnan och version 4.3 av BSD-kärnan.

Kombinationen Mach och BSD kom till för att överbrygga begränsningarna i Mach-kärnan, som är en mikrokärna och som i vissa situationer kan drabbas av stora prestandaproblem när kärnan får mycket att göra. BSD-kärnan löste det problemet men bidrog också med posix-kompabilitet, processhantering, virtuell minneshantering och nätverksfunktionalitet.

Lätt för användaren

Sedan lanseringen av Mac OS X har säkerhetsfunktionerna hela tiden tagit ett steg framåt med varje ny version av operativsystemet. I version 10.4 introducerades exempelvis funktionen File Vault som är en krypteringsfunktion för användarens filer i hemkatalogen. Den bygger på en 256 bitars aes-kryptering vilket är samma funktion som numera också finns för image-filer.

I Mac OS X 10.5, som de flesta användare numera har på sina Macar, introducerades en ny funktion kallad trojan horse marking. Den markerar alla filer som laddas ner från internet. När användaren sedan vill öppna filen varnas denne för att filen kommer från en källa som inte kan garanteras vara säker. På samma tema har säkerheten runt hur program körs i operativsystemet förbättrats och varje program kapslas in för att hindra att program gör saker de inte ska.

Användarna märker väldigt lite av den här typen av skydd. Något som säkerhetsexperten Dino Dai Zavi håller med om. Han är mest känd för sin kunskap om säkerheten i Mac OS X och har vunnit säkerhetstävlingar där det gäller att hacka operativsystemet.

– Apple har verkligen lyckats när det gäller att skapa en tillräcklig säkerhet och sam-

tidigt göra den lätt att hantera för användaren, säger Dino Dai Zavi.

Han gör gärna en jämförelse mellan Mac OS X 10.5 och Windows Vista när det gäller hur användarna måste godkänna operationer. Dino Dai Zavi menar att Apples modell är betydligt enklare för användarna att arbeta med och att den inte alls stör och förvirrar. Det gör att användarna inte är benägna att stänga av funktionen helt, något som användare av Windows Vista gärna gör efter en tid.

Daniel Ström driver konsultfirman och webbhotellet MacDaddy i Boden. Han håller med Dino Dai Zavi:

– It-säkerhet handlar om att förstå hotbilden och hantera sannolikheter att utsättas för skada för att sedan använda rätt verktyg för att minimera möjligheten. Vi tycker att Mac OS X är ett utmärkt verktyg eftersom det är ett operativsystem som inte är i vägen för användaren utan att för den sakens skull tumma på säkerheten.

Servern kan sluta fungera

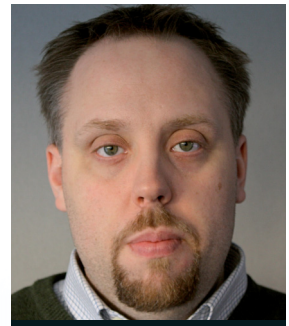
Ett av de största problemen med att arbeta professionellt med Mac OS X är Apples hemlighetsmakeri. Apple släpper regelbundet säkerhetsuppdateringar för sina operativsystem men det är långt ifrån alltid som Apple berättar vad dessa innehåller.

Arbetar man dessutom med Mac OS X Server, där en stor del av administrationen kan innebära att man kringgår Apples grafiska gränssnitt och i stället gör ändringar via terminalen, kan en säkerhetsuppdatering innebära att saker slutar att fungera.

Man kan använda den i skrivande stund senaste säkerhetsuppdateringen, Security Update 2008-007, som innehåller en uppsjö av buggfixar av exempelvis Apache, My SQL, Postfix, Clam AV, php, rlogin, med mera. Men Apple berättar inte vad de gör när de uppdaterar de här tjänsterna. Inga säkerhetskopior tas på befintliga konfigurationsfiler när uppdateringen sker eftersom Apple antar att alla modifieringar som gjorts av operativsystemet har gjorts på det sätt som de föreskriver. Har du otur står du där med en delvis defekt server som inte fungerar.

Apple hymlar inte med att de inte vill diskutera, eller ens avslöja, att ett säkerhetsproblem existerar förrän de själva har undersökt problemet och producerat en lösning. Företaget menar att de gör på det viset för att de vill skydda sina kunder.

Leif-Olof Wallin är analytiker på Gartner Group och han är kritisk till hur Apple håller kunderna informerade.



Daniel Ström, MacDaddy

”Apple berättar inte vad de gör när de uppdaterar de här tjänsterna.”

– För företag är det här ett stort problem. Företag efterfrågar en ”roadmap” för att kunna planera. Bolag som Microsoft, Intel och många av pc-tillverkarna är ganska duktiga på att kunna tala om vad som kommer och upprätthåller därför stabilitet och planerbarhet för företagen, säger Leif-Olof Wallin.

Daniel Ström är nöjd med valet av Mac OS X Server som operativsystem på sina webbservrar men inte heller han är helt nöjd med hur Apple håller kunderna informerade:

– Uppdateringar från Apple för Mac OS X Server får vi vänta ett tag med att installera eftersom de inte sällan förstör något som fungerade bra innan.

Hemlighetsmakeriet frustrerande

Daniel Ström anser inte att Apples hemlighetsmakeri är ett stort problem förutom när det är dags att investera i en ny server. Däremot är bristen på information om vad en viss uppdatering innehåller mycket frustrerande, i synnerhet om man dras med en bugg som man bara måste få bort.

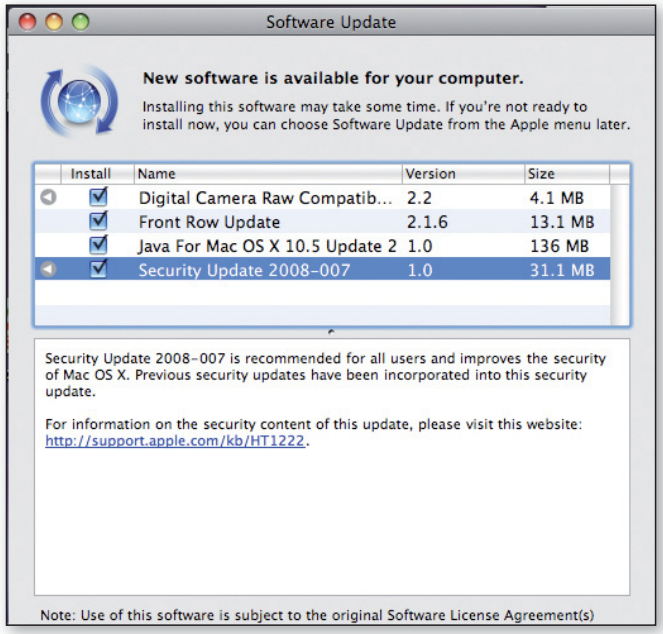
Dino Dai Zavi anser ändå att Apples förebyggande säkerhetsarbete är väldigt effektivt. Han menar också att Apple tar säkerheten på allvar genom sina återkommande säkerhetsuppdateringar:

– I princip alla andra programleverantörer säkrar och reparerar sina produkter först efter att luckor och fel rapporterats »

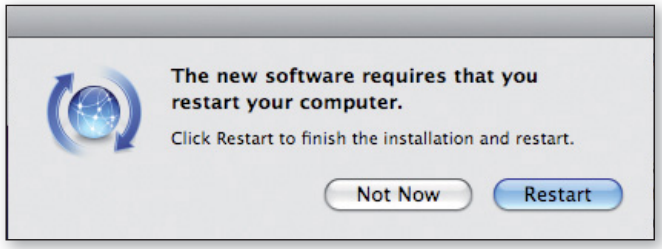
Fotnot: Vi kontaktade Apple, F-Secure och Symantec för kommentarer om hur de ser på säkerheten i Mac OS X. Apple vägrade att ge några kommentarer. F-Secure meddelade att det svenska kontoret inte hade tid. Symantec sa sig gärna vilja medverka men har inte återkommit.

Den inbyggda krypteringsfunktionen i Mac OS X är säker med dagens mått mätt. Använd den!

To boldly go, where no backup has gone before. Endast storleken på din backup-volym begränsar hur långt bak i tiden du kan gå för att hitta en fil du råkat radera.



Via Software Update erbjuder Apple regelbundet uppdateringar av många funktioner och program som finns i datorn. Användare av Mac OS X Server bör dock tänka sig för innan de installerar – ta en säkerhetskopia först!



Skjut inte upp det du kan göra i dag. Med andra ord: starta om direkt när du har lagt på en uppdatering.

av en extern part. Skulle de hitta ett fel genom sitt interna utvecklingsarbete bakas den nya koden ofta in i stora uppgraderingspaket, vilket exponerar användarna för problemen under en onödigt lång tid.

Ett bra exempel på det kan man hämta från Security Update 2008-007 där Apple upptäckte och fixade en bugg i programmet Colorsync, ett program för att med hjälp av icc-profiler kalibrera skärmar. Innan uppdateringen var det möjligt att via en bild med en tillhörande icc-profil exekvera kod på datorn. Det här är kanske inte den typ av säkerhetshål man först tänker på när man funderar på hur man håller en dator säker.

Dino Dai Zavi menar dock att många av de synliga säkerhetsmekanismerna i Mac OS X inte riktigt håller måttet om man börjar syna dem i sömmarna. Det beror helt och hållet på Apples oförmåga att skriva tillräckligt bra kod. Operativsystemet skulle må bra av en rejäl översyn av säkerhetsfunktionerna, något som Dino Dai Zavi tror pågår i skrivande stund. Det kommer vi att få se resultatet av i nästa version av Mac OS X, som går under kodnamnet Snow Leopard.

"För företag är det här ett stort problem – de vill ha en roadmap."

Leif-Olof Wallin, Gartner

Autentisering gånger 5

Mac OS X 10.5 erbjuder fem olika autentiseringsmetoder. Den första är den lokala autentiseringen där användaren loggar in med det login och lösenord som registrerats i den lokala databasen. Den säkerheten är inte tillräcklig eftersom man med en installations-cd eller -dvd för Mac OS X kan starta datorn och nollställa root-lösenordet på maskinen. Används den här inloggningsmetoden, vilken är den överlägset vanligaste, är en kryptering av alla känsliga filer med File Vault eller någon annan krypteringsmetod minst sagt ett krav.

Stödet för katalogtjänster har också blivit bättre och numera klarar Mac OS X open directory, active directory och inloggningar via Kerberos. Open directory är en katalogtjänst som Apple även har implementerat på Mac OS X Server. Den kan hantera alla former av resurser i ett Macbaserat nätverk.

Stödet för active directory i Mac OS X har varit omdiskuterat ända sedan det infördes i Mac OS X 10.4. I version 10.5 har buggarna varit många och de som hade en fungerande autentisering mot active directory i 10.4 fick se hur det helt slutade att fungera efter en uppdatering till 10.5.

Det tog ett antal månader innan de värsta buggarna hade hamrats ut ur koden i Mac

6 tips för en säkrare Mac

1 Det användarkonto som skapas som standard när Mac OS X installeras är inte särskilt säkert. Detta på grund av att kontot ges fullständiga administratörsrättigheter som standard. Vi rekommenderar att du skapar ytterligare ett användarkonto som används för daglig drift. Alternativt att du slår på root-kontot, loggar in som root och sedan tar bort administratörsrättigheterna på det konto som skapades vid installationen av operativsystemet.

2 Om du arbetar mycket i terminalen, motstå frestelsen att logga in som root eller att köra *su*. Använd i stället *sudo* så långt det går.

3 Ett annat tips är att det kan vara bra att använda olika webbläsare för att exempelvis göra sina bankärenden och för sitt vanliga surfande. Alla användare rekommenderas också att slå på den inbyggda krypteringen för alla användardata som lagras på hårddisken.

4 Till skillnad från i Windows är det inte helt självklart att man har ett lösenordsskydd aktiverat för skärmsläckaren, men det bör slås på så snart datorn är installerad.

5 Om du kör Mac OS X på din skrivbordsdator rekommenderas det som regel att låta Software Update kolla efter nya uppdateringar varje natt. Kör du däremot Mac OS X Server rekommenderas det att du sätter upp en testserver med samma version av operativsystem och samma konfiguration av tjänster och program som på servern och sedan testar nya uppdateringar på den innan du installerar uppdateringarna på en server som går i skarp drift.

6 I Mac OS X 10.5, både server och klient, finns en ypperlig funktion vid namn Time Machine. I praktiken fungerar den som en funktion för säkerhetskopiering som i realtid tar en säkerhetskopia på innehållet på din hårddisk. Det kan antingen göras mot en nätverksvolym eller mot en extern hårddisk direkt ansluten till datorn.

Vi rekommenderar att säkerhetskopiorna tas mot en nätverksvolym eftersom de data som kopierats till den externa hårddisken kan vara okrypterade om du inte tidigare har aktiverat krypteringsfunktionen.

Värt att notera är också att det snygga rymdinspirerade grafiska gränssnittet i Time Machine inte går att använda när du vill återställa filer från en hemkatalog krypterad med File Vault. I stället får man söka fram den säkerhetskopierade informationen manuellt genom att titta igenom kataloger och filer på disken med säkerhetskopior.

OS X. I och med version 10.5.3 ska dock active directory-bindningar och inloggningar fungera som utlovat.

Buggar kan komma igen

Säkerhetsproblemen finns och de bör tas på största allvar. Ofta är det buggar inte bara i operativsystemet utan också i de program som Apple producerar. Man kan heller aldrig vara helt säker på att buggarna är borta när de tidigare har fixats.

Ett bra exempel på det är en sällsynt envis bugg i det inbyggda e-postprogrammet Mail som fixades i mars 2006 då Mac OS X fortfarande bar versionsnumret 10.4. Vid uppdateringen till 10.5 dök den här buggen upp igen. Den gjorde det möjligt att via e-post få in ett illasinnat program, som maskerats som till exempel en jpeg-bild, i maskinen.

Apple hade helt enkelt fipplat lite för mycket med koden i Mac OS X 10.5 och tagit bort den varning som användaren får när denne öppnar en bifogad fil till ett mejl. Buggen fixades till slut av Apple.

Mac OS X bygger till viss del också på öppen källkod. Php, Samba, nfs, Apache, Bind och Perl är några av de program som följer med både klient- och serverversionen. Dem har Apple ingen direkt kontroll över, förutom att de precis som alla andra kan fixa buggar och sedan skicka över dem till respektive projekt och hoppas på att koden antas och att en buggfix skickas ut. Tack och lov är Apple flitiga på att lägga in buggfixar med mera från tredjepartsleverantörer.

Apple menar att de är snabba på att reagera och att de är aktiva i exempelvis Forum of Incident Response and Security Teams (First) och i säkerhetsgänget som utvecklar Free BSD. Ändå tog det Apple över tre veckor längre att posta den uppdatering av Mac OS X som fixade en bugg i dns-servern Bind jämfört med andra leverantörer. Microsoft, Cisco och Sun fixade samma bugg i sina operativsystem betydligt snabbare.

Det tog dessutom ytterligare över en månad innan samma bugg även fixades på klientdatorernas implementation av Bind. Apple menade att de inte tyckte att det var ett säkerhetsproblem i klientversionen av Mac OS X 10.5, men det fanns gott om andra som tyckte annorlunda. Det är ingen överdrift att påstå att Apples trovärdighet fick sig en rejäl törn efter den fadäsen.

"Security by obscurity"

Daniel Ström menar att diskussionen om säkerheten i Mac OS X är något överdriven:

– Mac OS X har som alla andra system kod som måste rättas och uppdateringar som måste installeras. Det är ett konstant förbättringsarbete och inget system är säkrare än de tjänster som körs. Vår erfarenhet är att Mac OS X är ett modernt, säkert och problemfritt system. Ingen av våra kunder har haft intrång eller problem med vare sig maskar, trojaner eller virus.

Daniel Ström tillägger att hans företag förmodligen är den it-konsult som säljer minst licenser av antivirus under ett år.

Mac OS X har så här långt överlevt på "security by obscurity", det vill säga en säkerhet som bara existerar tack vare att plattformen fortfarande inte är populär och vanlig nog för att de som utnyttjar säkerhetshål ska lägga tid och energi på att utnyttja dem som finns i Mac OS X.

En fråga som verkligen är värd att ställa är huruvida Apple är redo den dagen kanonerna riktas mot Mac OS X och dess användare. Just nu kan Mac OS X jämföras med Sverige och vårt militära försvar: vi är säkra tills någon bestämmer sig för att anfalla.

Joacim Melin är testredaktör och skribent med säkerhet som sitt specialområde. Du når honom på joacim@melin.org.

Så går du vidare

» **Apple uppmärksammar alla** som rapporterat om säkerhetsproblem: support.apple.com/kb/HT1318

» **Apples Mac OS X 10.5 Security Brief:** images.apple.com/macosx/pdf/MacOSX_Leopard_Security_TB.pdf

» **Dino Dai Zovis blogg** med återkommande säkerhetsinformation om Mac OS X: blog.trailofbits.com

» **Active directory och Mac OS X 10.5 Leopard:** www.macwindows.com/leopardAD.html

» **AFP548,** webbsajten för dem som arbetar med Mac OS X Server: www.afp548.com/

» **Ars Technicas guide** till säkerhet i Mac OS X: http://arstechnica.com/guides/tweaks/mac-os-x-security.ars

» **Mac OS X, version för version:** http://en.wikipedia.org/wiki/Mac_os_x