

Senaste veckan har det kommit uppdateringar till webbläsaren Firefox och epostprogrammet Thunderbird, först till 6.0.1 och så 6.0.2 (samma versionsnummer för bägge). Det "enda" som hänt är att rot-certifikatet för DigiNotar i Holland tagits bort. Även Windows Update lär ha skickat ut uppdateringar till Windows med rensat rot-certifikat, och motsvarande för andra operativsystem.

Det som hänt är att DigiNotar i Holland som ger ut säkerhetscertifikat har haft "inbrott" och blivit av med sina "nycklar". Med hjälp av dessa nycklar kan tjuvarna utfärda nya certifikat som för alla programvaror som innehållit DigiNotar som en betrodd utgivare (ett rot-certifikat) kan lura besökaren att man faktiskt kommunicerar med den part man tror det är, som banken eller webaffärens betalfunktion.

Då detta är en klart avancerad stöld och kräver avancerade kunskaper för att användas kan man spekulera i vem som ligger bakom, men det är just spekulationer då det lika gärna kan vara en tekniskt intresserad/avancerad yngling som en subversiv nations säkerhetstjänst. För oss som användare innebär det dock:

- Säkerheten är beroende av uppdaterade programvaror
- Säkerheten baseras på ett antal betrodda certifikatutgivare
- Om certifikatutgivarna misslyckas så har vi som användare ingen säkerhet

Att "ingen kedja är starkare än den svagaste länken" gäller sålunda även här.

För företaget DigiNotar blir det svårt att återskapa förtroendet utan kommer troligen avvecklas. Holländska staten som säkrat upp sina myndigheter med certifikat från DigiNotar drabbas också då myndighetsfunktionerna inte är betrodda förrän nya certifikat installeras.

Skrivet av Erik Liljencrantz

2011-09-08 08:55 - Senast uppdaterad 2011-09-08 09:27

---

Att DigiNotar ingår i företaget Vasco som skapat flera av de svenska bankernas inloggningslösningar med dosor kan på sikt få ännu större konsekvenser.

*Rekommenderade åtgärder är att uppdatera operativsystemet (Windows Update och motsvarande) samt kontrollera att man kör senaste versionen av viktiga program som epost och webb-läsare.*

Intressant läsning: [betanews](#) , [eWeek](#) , [PC För Alla](#)