Titeln: Säkerhetsarkitektur

Råd för säkrare extern överföring av information

April 2021

Innehåll

1. Hur man gör extern överföring säkrare

Servrar som är exponerade mot internet bör använda sig av TLS för att säkra uppkopplingar mot avlyssning. Det räcker emellertid inte att slå på TLS utan det finns en hel del saker att fundera över och konfigurera för att det skall bli bra. När man har stegat sig igenom den här listan har man en säkrare server och man har samtidigt lärt sig en hel del.

Listans innehåll är inte det enda man behöver tänka på, men det kan tjäna som en komihåglista för när man kravställer såväl egna insatser som upphandlade tjänster.

Det finns externa tjänster som tillhandahåller tester för att se om en webbsajt eller epostmottagare eller epostsändare uppfyller dessa krav. Tyvärr finns det inte en som visar allt utan man kan behöva använda flera.

Genom att arbeta sig igenom denna lista är risken mindre att man gör onödiga misstag. Det finns inget facit för vilka konfigurationer som skall göras, det behöver man avgöra från fall till fall men de externa tjänsterna ger oss en bra idé om vilka värden som bör uppnås. När man går igenom listan kommer man dessutom att bygga upp sin kompetens på området.

1.1 Generella frågor

Denna första avdelning handlar om sådant som är generellt för externa servrar, såväl för webbservrar som e-postservrar.

1.1.1 IPv6

Detta är det moderna protokollet som gör att vi får tillräckligt många ip-adresser och slipper adressöversättningar vilket gör nätverkstrafiken snabbare. Det är inget lagkrav men det är dags att börja ta det i bruk. Vi skall inte bygga vår infrastruktur på gammal teknik. Däremot är det för tidigt att sluta använda ipv4 eftersom många inte har ipv6 ännu.

1.1.2 DNSSEC

DNSSEC innebär att vi signerar våra dnsposter kryptografiskt och det är en förutsättning för mycket av det som kommer senare i dokumentet. Det är inte helt enkelt att sätta upp men väl värt besväret.

1.1.3 TLS

TLS är det protokoll som används för att kryptera förbindelsen mellan en webbläsare och en webbserver eller mellan en mottagande e-postserver och sändande e-postserver eller klient. Det fungerar på ungefär samma sätt i bägge fallen. Det finns ett antal saker att tänka på här.

Tidigare hette protokollen SSL men de är numera betraktade som osäkra. Idag bör man använda TLS1.2 eller TLS1.3

TLS1.2 är den version som är mest spridda för närvarande och betraktas som tillräckligt bra.

TLS 1.3 är nästa version som är förhållandevis ny och den stöds inte av äldre utrustning.

1.1.4 Forward security

Detta handlar om hur man har en unik kryptering för varje session, så även om någon kommit över en privat nyckel så är det svårt att dekryptera en inspelad överföring.

DHE använder en statisk nyckel som idag bör vara minst 3072 bitar stor medan ECDHE använder en nyckel som genereras med hjälp av en elliptisk kurva.

DHE kräver mer beräkningar vilket påverkar lasten på servern.

1.1.5 Krypteringsalgoritmer

Krypteringsalgoritmerna påverkas av att det blir lättare att dekryptera dem utan nyckel när kunskap och beräkningskapacitet ökar. Det gör att krypteringsalgoritmer är färskvara och med tiden behöver de ersättas av mer kraftfulla algoritmer.

En vanlig källa för att avgöra vilka krypteringsalgoritmer som är tillräcklig är NIST (National Institute for Standards and Technology)
https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

1.1.6 Föredragen ordning

Detta handlar om att man skall konfigurera sin server till att föredra den starkaste krypteringsalgoritmen, gärna av typen ECDHE.

1.1.7 Cert org = önskad org

Kontrollera att organisationens namn står med i certifikatet.

1.2 Webb-servrar

Denna avdelning handlar om frågor som är specifika för webb-servrar.

1.2.1 Omdirigering till https

För en webbserver är det viktigt att man, om http är påslaget, gör en omdirigering från http till https. Detta för att undvika att förbindelsen avlyssnas på vägen.

1.2.2 HSTS

Detta är en header man sätter i https-svaret och som talar om för webbläsaren att under specificerad tid skall den byta ut http mot https mot den server eller domän som anges. Det innebär att man förhindrar att användare luras att koppla upp sig mot en falsk sajt med http. Den minsta tid man bör använda är 6 månader. Därför är det viktigt att man testat noggrant och börjar med en kortare tid under införandefasen.

1.2.3 Förladdad HSTS

Förladdad HSTS använder man när man inom domänen helt slutat använda http och infört https för all webbtrafik, även internt. Det innebär att man anmäler sin domän till browsertillverkarna och den läggs in permanent i webbläsarna. Det innebär att man måste ha testat under tillräckligt lång tid på grund av den låga omsättningstakten av webbläsare. Vill man inte ha förladdad HSTS så kan man välja bort det, men den kommer inte försvinna förrän webbläsarna uppdaterats.

1.2.4 OCSP stapling

Detta är ett sätt att undvika att webbläsare behöver kontakta certifikatutgivaren för att verifiera certifikat. Man publicerar en signerad ”försäkran” från certifikatutfärdaren. Det genererar bland annat snabbare sajter och certifikatutfärdaren vet inte vilka som besöker varje webbsajt.

1.2.5 CSP

Content Security Policy ger möjlighet att förhindra vissa attackvägar genom att man bland annat specificerar vilka sajter som får leverera innehåll till webbsajten. Om man använder json-data från ett API på en annan server så måste man deklarera att den servern är tillåten att leverera svaret. till webbläsaren. Det motverkar olika försök att lura webbläsaren att hämta innehåll från fel ställe men kräver att man håller sin policy uppdaterad.

CSP kan vara lurigt att slå på gamla sajter, men bör vara ett krav på nya sajter.

1.2.6 EV-certifikat

Detta är certifikat med en extra validering av vem det är som använder det.

1.2.7 Security.txt finns

Security.txt kommer från en kommande standard som specificerar en textfil med information som skall läggas på en välkänd plats på servern. Där kan den som vill kontakta ägaren i säkerhetsfrågor hitta en epostadress och den som så vill kan lägga en publik krypteringsnyckel för överföring av information om säkerhetsbrister. I stället för att skriva till registrator@myndighet.se kommer informationen direkt till någon som förstår vad det handlar om och vad som behöver göras.

1.2.8 Stöder CAA i DNS

Detta innebär att man i DNS lägger in uppgifter om vilka certifikatutfärdare som är giltiga för domänen och vilka som får utfärda wildcard-certifikat-.

1.2.9 Övriga security headers

Det finns ett antal headers man kan lägga till i sina svar till webbläsaren och kontrollera delar av dess beteende. Vilka man använder beror på behovet.

1.3 Epost

Denna avdelning handlar om frågor som är specifika för epostservrar.

1.3.1 DKIM

DKIM innebär att man signerar utgående mail med en nyckel och mottagaren kan verifiera denna mot ett fält i domänens DNS

1.3.2 SPF

SPF innebär att man i DNS publicerar uppgifter om vilka IP-adresser som får skicka epost med domänen som avsändare.

1.3.3 DMARC

DMARC är en policy vi publicerar i DNS och där vi talar om vad mottagaren skall gör med epost som inte följer någon av SPF eller DKIM.

1.3.4 DANE

Används för att ge möjlighet att verifiera att egensignerade certifikat är genuina och ersätter därigenom certifikat från certifikatutfärdare.

eSam är ett medlemsdrivet program för samverkan mellan myndigheter och Sveriges Kommuner och Regioner (SKR) för att underlätta och påskynda digitaliseringen inom det offentliga. eSam bildades 2015 som en frivillig fortsättning på E-delegationen. En viktig uppgift för eSam är att ta fram vägledningar som ger förutsättningar för att öka den digitala samverkan inom offentlig förvaltning.

Vägledningarna finns på esamverka.se

I eSam ingår Arbetsförmedlingen, Bolagsverket, Boverket, Centrala Studiestödsnämnden, Domstolsverket, eHälso-myndigheten, Försäkringskassan, Jordbruksverket, Kriminalvården, Kronofogdemyndigheten, Lantmäteriet, Migrationsverket, Naturvårdsverket, Patent- och Registreringsverket, Pensionsmyndigheten, Polisen, Riksarkivet, Sida, Skatteverket, Skolverket, Sveriges Kommuner och Regioner, Statens servicecenter, Statens tjänstepensionsverk, Statistiska centralbyrån, Tillväxtverket, Trafikverket, Transportstyrelsen, Tullverket och Universitets- och högskolerådet (okt 2020)