E2EE (och varför du behöver det)

Vem skall ha rätt, eller ens möjlighet, att läsa dina e-postmeddelanden? Det självklara svaret borde vara: jag som skickar och du som tar emot meddelandet.

I verkligheten fungerar det inte alls på det sättet. Faktum är att det är ganska många som har tillgång till din digitala kommunikation; allt från den personal som har hand om de system som hanterar dina meddelanden, till cyberbrottslingar som bryter sig in eller stjäl på vägen, till myndigheter som under olika förevändningar begär access.

När ett meddelande skickas så skapas och sparas data i form av cache, mellanlagring, olika loggar, metadata osv. I vissa fall kan tex ditt meddelande sparas komplett med, inte bara innehållet i klartext, utan också info om avsändare, mottagare, tidpunkt och en mängd annan känslig data i en bortglömd serverlogg någonstans.

Detta gäller också alla de webbformulär som använder e-post som transport, något som ofta glöms bort i de här sammanhangen. När vi nämner “e-postklient” i den här artikeln så inkluderar vi alltså också de webbformulär som sänds via e-post.

“Vanlig e-post” sänds alltid helt i klartext via osäkra transportvägar.

Vissa e-postservers och e-postklienter skapar krypterade tunnlar för själva transporten, andra inte. Allt sparas i klartext i e-postlådorna, allt loggas och är spårbart, ofta kan hela meddelanden i klartext hamna i tex felloggar. Säkerheten och anonymiteten är i praktiken obefintlig.

Vanlig e-post, allt sänds och sparas i klartext, ibland krypteras transporten

Ett viktigt första steg i att skydda e-postmeddelanden är att kräva att det skapas en säker transport mellan avsändare och mottagare via en krypterad tunnel (SSH/TLS). Meddelandet är fortfarande sänt och sparat i klartext och skapar ett spår men skyddas mot att bli stulet under under själva transporten (MITM, Man-In-The-Middle attacker) mellan klienterna och server systemen.

E-post sänds och sparas i klartext men med säker transport via krypterad överföring

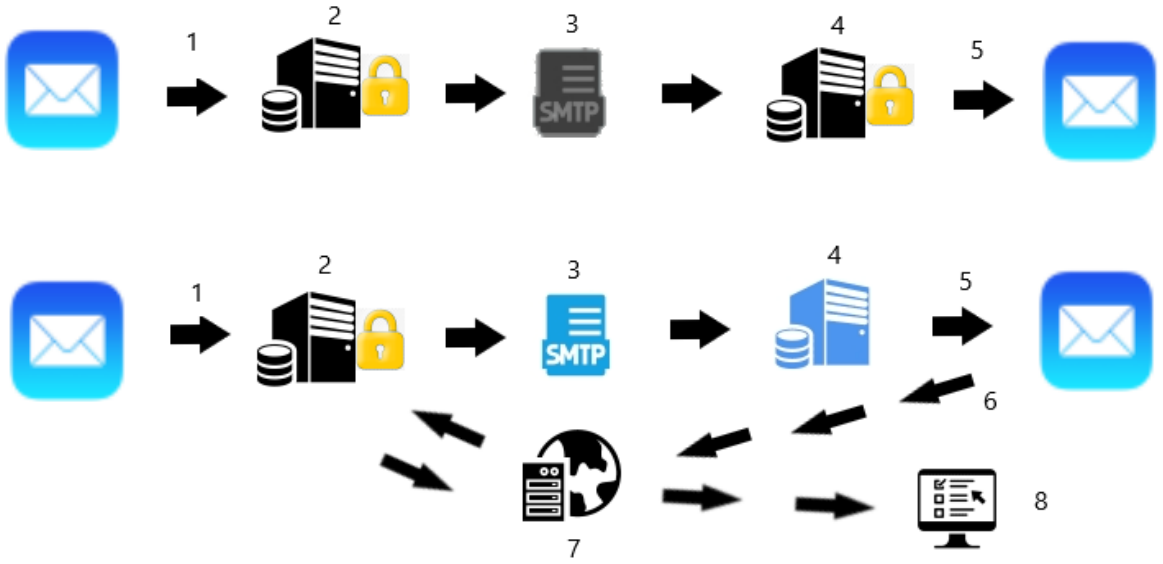
Nästa viktiga steg är att också skydda serversystemen genom kryptering av hårddiskar och databaser som skydd mot dataförlust genom tex inbrott eller stöld av hårdvara.

E-post sänds och sparas i klartext med säker transport och säkra servers

I det tredje steget, som blir allt vanligare, krypteras även själva meddelandet när det transporteras mellan servers och när det sparas i serversystemet. Detta marknadsförs ofta som ett säkert system med kryptering men det är viktigt att notera att meddelandet fortfarande kan läsas av systemen och alla som har access till dem.

Om ett krypterat e-postmeddelande sänds till någon som saknar funktionen så får mottagaren ett e-postmeddelande med en länk till en webbaserad e-

postklient där det krypterade meddelandet kan läsas och ofta också svaras på.



E-post krypterad i och mellan servers

I ett fjärde steg på säkerhetstrappan så krypteras/dekrypteras e-postmeddelandet i e-postklienten, sk E2EE (End-to-end encryption), och kan alltså inte läsas av obehöriga i något som helst sammanhang. I övrigt så fungerar det mesta som i steg tre, men med skillnaden att meddelandet är och förblir krypterat under hela transporten och när det arkiveras.

E2EE krypterad e-post, kryptering/dekryptering sker i e-postklienten

Anonymitet är också mycket viktig i de här sammanhangen men ofta helt förbisedd. Förutom själva e-postmeddelandet skapas en mängd information om meddelandet i olika cache, i cookies, som metadata och inte minst i olika loggar. Detta sker i alla delar av kedjan; på klientdatorn, i klientens webbläsare och i alla serversystem som på något sätt hanterar meddelandet. Med rätt verktyg och kunskap kan faktiskt de flesta e-postmeddelanden, också “säkra” sådana, både spåras hela vägen och ibland tom helt rekonstrueras.

Du som på något sätt hanterar känslig information och behöver kommunicera via e-post och webbformulär behöver alltså anonymiserad E2EE för din kommunikation.

Låt oss hjälpa dig med detta, tag kontakt!

Ps. Läs gärna också vår artikel om säker e-post med råd, om för och nackdelar och hur man löser en del praktiska problem mm.