**Statusmail 17.1.2017**

Godt nytår til alle!

**Wifi problemer**

Som Helle meldte ud, har vi nu fået løst de wifi problemer, vi havde i efteråret. Det viste sig at være et mismatch i konfigurationen mellem firewall og server-switchene, som egentlig burde have givet problemer på alle netværk, men som kun gav udslag på det trådløse.

**Fælles Docunote**

Ulrik har undervist superbrugere fra Rødovre og Ordrup, som nu har adgang til at benytte vores fælles Docunote server. De tester og tilretter opsætningen af filstrukturen samt adgangsrettigheder i samarbejde med Ulrik, så den passer bedst muligt til deres arbejdsgange.

**Nyt (fælles) trådløst**

Nærum skifter deres trådløse netværk til sommer. De går fra Meru til Cisco. I den forbindelse er det planen, at HTG og Nærum påbegynder et fælles trådløst setup i ITF regi, hvor de med deres 2 nye wireless controllere kan lave et mere driftssikkert trådløst miljø (redundans). Her vil det så være muligt for de andre gymnasier at købe sig ind, når de skal have opgraderet deres trådløse net. I stedet for at hvert gymnasium står med en ”single point of failure” og skal investere i egne wireless controllere, vil vi således samle det trådløse og spare udgifterne til 3-4 controllere samt få en bedre sikkerhed/oppetid. Win-win.

**Nyt pædagogisk net**

HTG blev flyttet til det nye pædagogiske net op til juleferien, og det gik ret smertefrit ikke mindst på grund af et godt stykke arbejde af de lokale it-folk. Som nævnt i sidste statusmail, skal alle gymnasier (på nær Gladsaxe) igennem samme flytning senest i den kommende sommerferie. Borupgaard, Ordrup og Rødovre har meddelt, de vil lave flytningen i sommerferien.

**EU forordning**

Som I sikkert er bekendt med, træder nye og skrappe regler for it-sikkerhed i kraft i april/maj 2018. ITF og ITF’s referencegruppe har allerede et stykke tid haft fokus på dette, sikkerhedsregler til forskellige medarbejdsgrupper er udarbejdet (og måske allerede implementeret på skolerne?), og vi forsøger fortsat at sætte os ind i alle vinkler af dette store felt. ITF vil efter bedste evne orientere jer og samtidig sørge for, at de data, vi opbevarer, og at en hver anden praksis lever op til kravene. Mht. praksis på den enkelte skole kan ITF imidlertid (kun) komme med anbefalinger, som vi allerede har gjort i forbindelse med eksempelvis dokumenthåndtering (i form af Docunote), men det er i høj grad op til hvert enkelt gymnasium at vurdere, hvad der skal til for at overholde reglerne, og informere ITF om eventuelle tiltag. Jeg vil anbefale, at I allerede nu begynder at gøre jer overvejelser om hvilke brugere, der bør være på det administrative net. Jeg tænker især på de medarbejdere, der håndterer mange personfølsomme data (studievejledere f.eks). Hvis man ikke allerede har dem på det administrative net, bør man kraftigt overveje det, og det vil nok være en god ide at træffe en beslutning inden næste skoleårs start, så de ikke skal flyttes midt i skoleåret. Der skal også findes en DPO (data protection officer), som er ansvarlig for, at de ansatte kender og overholder reglerne i omgang med data mm.

**Sikkermail**

Hvis man skal modtage sikre mails fra institutioner, firmaer eller enkeltpersoner, *som ikke er på Comendos sikkermail løsning*, så kan det faktisk godt lade sig gøre for afsenderen at kryptere mails og sende dem til jeres sikkermail ”hovedpostkasse”. Proceduren er at afsenderen tilgår: <https://www.medarbejdersignatur.dk/produkter/nemid_medarbejdersignatur/information_om_nemid/sikker_e-mail/soeg_certifikat/> og her finder gymnasiets certifikat og krypterer deres mail med dette (kræver nok en it-teknikers hjælp). Disse mails kan kun sendes til ”hovedpostkassen” og ikke til individuelle brugere. Man kan også sende sikre (krypterede) mails fra e-boks, hvilket er klart den nemmeste løsning, hvis afsender har den mulighed.

**Overvejelser omkring øget sikkerhed**

Brugerne udgør den største sikkerhedsrisiko. Vi kan ikke sikre os 100% med teknologiske hjælpemidler, medmindre vi lukker og spærrer på kryds og tværs - hvilket gør det pokkers besværligt for både it-folk og brugere. Med en kommende DPO (data protection officer), der er ekspert i persondata lovgivning og har ansvar for at medarbejdere er oplyst om regler og retningslinjer samt at disse overholdes, er vi godt på vej. Der findes også en række teknologiske hjælpemidler, der kan hjælpe os it-folk og jer brugere, uden at det behøver give alt for mange frustrationer. Nogle af de ting, jeg overvejer at kigge på (primært til det administrative), er:

* Certifikater på computere (så kun de, der har et certifikat kan logge på det administrative net),
* Cisco ISE (få styr på alle enheder der er tilknyttet netværket mm),
* SMS passcode (når man skal på VPN, får man en sms med sin kode – så dobbeltsikrer man, at det er den rigtige bruger, der forsøger at logge på)
* Heimdall security / Psi Software insector (software, der kontroller om de programmer, der er installeret på jeres computere, er fuldt opdateret)
* SSL dekryptering på firewall (mange websites sender krypteret trafik (https), hvilket er godt, men det betyder, at firewallen ikke kan se, om der er malware gemt i trafikken. Her kan man få firewallen sat op til at dekryptere, ved at den agerer mellemled for al krypteret trafik).