Notat

Dato: 28-10-2026
IT og Digitalisering

Redegørelse om IT-sikkerhedshændelser oktober 2026

De seneste uger har været præget af flere alvorlige IT-sikkerhedshændelser, som har betydning for den generelle cybertrussel mod kommunerne. For Norddjurs Kommune har der særligt været opmærksomhed på læk af oplysninger fra CPR-registeret samt en kritisk sårbarhed i programmeringssproget PHP.

Læk af CPR-oplysninger
Primo oktober blev der på landsplan konstateret uautoriseret adgang til personoplysninger fra CPR-registeret, hvor ca. 8,8 mio. cpr-numre blev lækket.

Hændelsen er ikke et sikkerhedsbrud hos Norddjurs Kommune, og der er således ikke tale om, at oplysningerne er lækket fra kommunens IT-systemer.

Hændelsen er imidlertid relevant for kommunen, fordi personoplysninger, der er kommet uvedkommende i hænde, efterfølgende kan anvendes til blandt andet svindel, phishing og målrettede angreb mod borgere eller offentlige myndigheder.

Hændelsen medfører derfor en generelt skærpet opmærksomhed på informationssikkerhed. IT & Digitalisering følger anbefalingerne fra Styrelsen for Samfundssikkerhed (SAMSIK), herunder anbefalingerne om skærpet overvågning og håndtering af relevante cyberhændelser.

Ledere og medarbejdere er orienteret om, hvordan vi skal forholde os i situationen. Det er bl.a. sket via intranettet og med afsæt i anbefalinger fra centrale myndigheder og KL.

Kritisk sårbarhed i programmeringssproget PHP
Onsdag den 21. oktober blev der på verdensplan identificeret en kritisk sikkerhedssårbarhed i PHP, der anvendes i en række webbaserede IT-løsninger.

Medarbejdere i IT & Digitalisering arbejdede fra onsdag eftermiddag og gennem aftenen og natten med at undersøge Norddjurs Kommunes eksponering og overvåge situationen sammen med kommunens IT-sikkerhedsleverandør.

Som en forebyggende sikkerhedsforanstaltning blev enkelte webbaserede IT-løsninger midlertidigt lukket ned, herunder AULA og bibliotekssystemet. Relevante leverandører blev samtidig kontaktet med henblik på afklaring og aftaler om nødvendige sikkerhedsopdateringer af IT-systemerne.

Der er ikke konstateret tegn på, at Norddjurs Kommunes IT-systemer eller data er blevet kompromitteret som følge af PHP-sårbarheden.

Det er i forbindelse med denne sårbarhed vigtigt at nævne, at disse sikkerhedshuller ikke er et nyt fænomen. Det har altid været en fast del af arbejdet i IT-afdelingen at lukke disse sårbarheder, når de bliver opdaget. Det nye i forhold til denne PHP-sag er hastigheden, hvormed hackere udnytter sikkerhedshuller. Fra tidligere erfaringer kunne der gå uger og måneder inden hackere begyndte at udnytte opdagede sikkerhedshuller, men med AI som værktøj er der nu tale om dage eller timer fra et sikkerhedshul opdages til man ser de første angreb. Samtidig får det en helt anden bevågenhed fra offentligheden, end det tidligere har været tilfældet.

Samlet vurdering
De aktuelle hændelser understreger et skærpet cybertrusselsbillede, hvor sikkerhedshændelser både hos centrale myndigheder og eksterne leverandører hurtigt kan få betydning for kommunerne.

IT & Digitalisering følger det aktuelle trusselsbillede tæt og arbejder efter anbefalingerne fra bl.a. SAMSIK og KL.