DATO
8. maj 2023

Cyber- og informationssikkerhed i Kalundborg Kommune 2023

I øjeblikket er der en høj grad af cybertrusler og -angreb rettet mod offentlige myndigheder i EU. Dette faktum er blevet påpeget i rapporten "Cybertruslen mod Danmark 2023", udgivet af Center for Cybersikkerhed (CFCS). I rapporten har CFCS vurderet trusselsniveauerne inden for tre områder som følgende:

- *"Truslen fra cyberkriminalitet mod Danmark er fortsat MEGET HØJ. Velorganiserede ransomware-grupper går efter alle dele af samfundet."* Typisk via økonomisk afpresning

- *"Truslen fra cyberspionage mod Danmark er MEGET HØJ. Herunder kritisk infrastruktur."* For Kalundborg Kommunes vedkommende Sundhedsområdet

- *"Truslen fra cyberaktivisme mod Danmark er HØJ. Det er sandsynligt, at danske virksomheder og myndigheder vil blive ramt af aktivistiske cyberangreb på kort sigt. Pro-russiske cyberaktivister har et højt aktivitetsniveau mod NATO-lande, herunder Danmark, og har i stigende grad formaliseret deres angrebsmodus og forøget deres kapacitet."*

I Danmark giver digitaliseringen anledning til sårbarhed ift. ondsindede aktører, som forsøger at udnytte svagheder i vores digitale infrastruktur, især i den offentlige sektor. Samtidig stiger kravene til Cybersikkerhedshåndtering, både gennem politiske aftaler og strategier samt formel regulering såsom senest EU's NIS2-direktiv. Dette direktiv forventes at påvirke kommunerne bredt, da det stiller bredere krav til ledelse, risikostyring, forretningskontinuitet og rapportering til myndighederne.
Regeringen har med den nationale strategi for cyber- og informationssikkerhed 2022-2024 fokuseret på sikkerheden i den kritiske IT-infrastruktur, som understøtter samfundsvigtige funktioner. Dette stiller større og mere nødvendige krav til arbejdet med Cyber- og informationssikkerhed.

Det anbefales af professionelle, fortsat at implementere tekniske og organisatoriske løsninger, der kan hjælpe med at beskytte mod ondsindede cyberangreb og andre trusler, for at forebygge og håndtere deres stigende antal.

I Kalundborg Kommune har vi i løbet af de seneste år investeret i og implementeret tekniske sikkerheds- og overvågningsløsninger af høj kvalitet fra førende leverandører inden for Cybersikkerhed og informationssikkerhed. Disse tekniske løsninger er med til at støtte og beskytte alle medarbejdere i deres daglige arbejde mod at klikke på ondsindede links eller utilsigtet dele personlige data, og omfatter avancerede cybersikkerhedsløsninger såsom firewalls, antivirusprogrammer, 24/7 overvågning,

Kontakt

Sagsansvarlig:
Bjarne Østergaard
Digitalisering og IT
Telefon, direkte: 59 53 48 20

Kalundborg Kommune
Holbækvej 141 B
4400 Kalundborg

analyse og proaktiv alarm på IT-infrastruktur såsom trafik på vores IT-netværk, pc'er, servere, Microsoft sikkerhedslicenser, automatisk bruger- og rettighedsstyring mm. Den afledte økonomi er ca. 5.800.000 kr. årligt, hvoraf de ca. 2.000.000 kr. betales ude i organisationen, de resterende 3.800.000 kr. har været finansieret af bevilgede puljer og overførselssum fra tidligere år. Fokus har primært været på at sikre det administrative IT-miljø, men de samme sikringsbehov gælder også for skolernes IT-miljø, hvor en lignende sikring er en nødvendighed.

Kravene til at sikre borgeres data bliver stadig større i fremtiden. EU- og nationale standarder og direktiver er med til at sikre en høj grad af beskyttelse mod Cybertrusler. Som kommune er det nødvendigt at være på forkant med udviklingen og løbende investere i nye sikkerhedsløsninger og vedligeholde og optimere de eksisterende løsninger både i det administrative og på skoleområdet. Dette medfører dog øgede omkostninger, som ikke kan dækkes af eksisterende budget eller bevillinger, og derfor er der ikke længere budget til nye tiltag eller videreudvikling af nuværende løsninger.

For at opfylde kravene fra EU og national side er der behov for større investeringer i scannings- og overvågningsløsninger samt tekniske sikkerhedsløsninger til højere sikkerhed på PCere, servere og netværk. Det er også nødvendigt at implementere yderligere tekniske tiltag for at støtte de organisatoriske tiltag og sikre borgernes data.

Implementering af IT-Sikkerhed kan dog have afledte omkostninger, da det ikke altid gør hverdagen nemmere for os ansatte. Der kan derfor være behov for andre teknologier, såsom biometri og højere kvalitetskrav til IT-udstyr, for at mindske de gener, som sikkerhedsløsningerne kan medføre, og samtidig sikre højere brugervenlighed og sikkerhed.

Implementering af EU og nationale standarder

NSIS (National Standard for Identiteters Sikringsniveau)
NSIS er en national standard, der er udviklet som følge af en EU-forordning, der har til formål at sikre en fælles ramme for digital identifikation på tværs af EU. For at overholde standarden kræves der specifikke organisatoriske og tekniske krav til IT-sikkerheden for de myndigheder og virksomheder, der er omfattet af standarden. Dette inkluderer implementering af en lang række procedurer og retningslinjer, samt nødvendige tekniske IT-løsninger for at sikre en høj grad af IT-Sikkerhed. Standarden kræver også, at der årligt udarbejdes en uvildig revisionserklæring fra en autoriseret IT-revisor, som derefter skal godkendes af Digitaliseringsstyrelsen for at sikre fortsat overholdelse af sikkerhedskravene.

Kravene i NSIS-standarden gælder også for undervisningssektoren, og derfor er det nødvendigt at implementere og vedligeholde samme krav på skolernes IT-platforme.

KL-Cyberværn
I 2019 blev der lavet en aftale mellem KL, Danske Regioner og Staten om at højne sikkerheden for cyber- og informationssikkerhed. For at leve op til denne strategi og NIS2-direktivet har KL arbejdet med kommunerne og PWC for at udarbejde en rapport om, hvordan sikkerheden kan forbedres. Rapporten anbefaler oprettelsen af et fælleskommunalt overvågnings- og analysecenter for cybersikkerhed, der skal være et supplement til andre sikkerhedstiltag. Planen er at etablere centeret i 2023 efter kommunerne har implementeret de nødvendige tekniske og organisatoriske tiltag. Det

forventes at omkostningerne vil være mellem 94-123 mio. kr. om året for alle kommuner, hvilket vil svare til 775-1.020.000 kr. for Kalundborg Kommune. KL arbejder på at få omkostningerne dækket i de årlige økonomiforhandlinger med regeringen, så omkostningerne er ikke medtaget i nedenstående oversigt.

NIS2 EU-direktivet

I maj 2022 blev NIS2-direktivet vedtaget i EU, og alle medlemsstater skal implementere det senest den 17. oktober 2024. Det forventes, at den danske lov vil være på plads kort tid før denne frist, og KL og andre eksperter forventer, at kommunerne vil blive omfattet på sundhedsområdet og dele af det administrative område. Direktivet kræver, at alle medlemsstater sikrer den kritiske nationale infrastruktur mod cyberkriminalitet. For at sikre implementeringen og den fortsatte fokus vil der blive indført krav om hændelsesrapportering til en national tilsynsmyndighed inden for 24 timer, og der vil kunne udstedes bøder for manglende overholdelse af direktivet.

For Kalundborg kommune betyder dette, at der er behov for yderligere sikkerhedstiltag, herunder organisatoriske tiltag såsom yderligere risiko- og beredskabsstyring, uddannelse i informationssikkerhed samt udvidelse af en 24/7 vagtordning. Det vil også være nødvendigt at implementere yderligere tekniske foranstaltninger såsom udvidelse af nuværende sikkerhedsløsninger og løbende anskaffelse af nye tekniske sikringsværktøjer, overvågnings- og sikkerhedsskanningsløsninger osv. Omkostningerne til dette er en del af omkostningsoverblikket nedenfor.

Hvis Kalundborg Kommune ønsker at sikre det nuværende og kommende trusselsniveau på IT-sikkerheden, vil der være behov for at øge budgettet til videreudvikling af eksisterende løsninger samt tilkøb af flere og nye løsninger. Omkostningerne er opgjort for 2024 og 2025 og er henholdsvis 3.664.504 kr. og 3.815.200 kr. Behovet er opgjort ud fra en liste over nuværende og nødvendige IT-sikkerhedsløsninger m.m.

	Tiltag	**Budget 2024**	**Budget 2025**	**Budget 2026**	**Budget 2027**
1	Cybersikkerhedstiltag servere og firewall herunder overvågning, licenser, services, skanninger, beredskab m.m.	1.407.616	1.558.312	1.558.312	1.558.312
2	Cybersikkerhedstiltag internet- og netværkstrafik herunder sikring mod DDOS-angreb, cyberkriminalitet, skanninger m.m.	1.614.710	1.614.710	1.614.710	1.614.710
3	Sikkerhedstiltag PC-arbejdspladser herunder endpoint protection, skanningssoftware, sikkerhedsopdaterings software m.m.	223.000	223.000	223.000	223.000
4	Sikkerhedstiltag til hjælp for medarbejderne herunder yderligere optimering af sikkerhedssoftware fra Microsoft, awareness m.m.	75.000	75.000	75.000	75.000
5	Sikkerhedstiltag i forbindelse med implementering af NSIS	344.178	344.178	344.178	344.178

	herunder årlig revisionserklæring, sikkerhedsløsning til kommunikation og brug af NemLogin til eks. FMK m.m.				
	Total	**3.664.504**	**3.815.200**	**3.815.200**	**3.815.200**

De fortsatte og nødvendige investeringer, som er beskrevet ovenfor, kan sammenlignes med internationale analyser af cyberangreb. Disse analyser viser, at angreb, hvor hackere krypterer alle eller dele af en virksomheds data og kræver løsepenge, i gennemsnit koster omkring 24 mio. kr. som konsekvens. Desuden tager det i gennemsnit 280 dage, før organisationen er tilbage på samme produktionsniveau som før angrebet. Dette understøtter behovet for fortsat optimering af Datatilsynets afgørelser, hvor de inden for det seneste år gentagne gange har udtalt "Alvorlig kritik" og indstillet til bøder for manglende modenhed i organisatoriske og tekniske sikkerhedsforanstaltninger til kommuner, andre offentlige myndigheder og private leverandører.