Dette dokument uddyber kravene til en 360-grader IT-sikkerhedsanalyse som EUC Nordvest (herefter betegnet EUC NV) på vegne af IT-fællesskabet Nordvest ønsker tilbud fra ekstern leverandør:

1. Info om vores systemarkitektur og hvem vi er:

Vi er et IT-fællesskab bestående af i alt 5 skoler:

- EUC Nordvest (EUC NV)
- FGU Nordvest
- Fjerritslev Gymnasium
- Morsø Gymnasium
- VUC Thy-Mors

Antal brugere fordeler sig så lededes.

Skole	**Ca. Antal ansate 2024**	**Antal ÅrsElever (2022 tal)***
EUC Nordvest:	335	1325
FGU Nordvest:	50	209
Fjerritslev Gymnasium:	53	303
Morsø Gymnasium:	26	227
VUCTM:	58	329

**Bemærk at der er flere IT-brugere end dette årligt. Antal unikke årlige brugere/elever skal ca. ganges med en faktor 3.*

1.1 IT-ansvar:

Hver skole har deres egen IT-ansvarlige medarbejdere.
EUC Nordvest har en egentlig IT-afdeling bestående af 3 systemadministratorer, en IT-elev og en Digitaliseringschef. EUC Nordvest står for driften af IT-fællesskabet.

1.2 IT-fællesskabet Nordvest:

IT-fællesskabet Nordvest er et samarbejde skolerne i mellem, hvor EUC Nordvest er drift ansvarlig skole og modtager en årlig økonomisk godtgørelse for driften af infrastrukturen.

Infrastrukturen består overordnet af:

- En On-præmis server løsning placeret fysisk på EUC Nordvest, inkl. backup server (bånd)
- Netværk/internet: herunder Firewall, Login-Portal løsning, MPLS forbindelser og coreswitch samt hjælp med korrekt konfiguration af Access switche og Access Points.

- De enkelte skoler ejer/køber selv access switche, APer og licenser hertil.
- De enkelte skoler står selv for patching og opdatering af switche og AP'er
- Fælles Active Directory (som dog er delt op i en instans per skole, hvor hver skoles IT-ansvarlig selv).

VUC og FGU køre i enkelte afdelinger deres eget netværk og internet opsætning uden for IT-fællesskabet.

EUC NV on-premis serverløsning består hovedsageligt af Microsoft VM-servere ca. 100instanser (hvoraf flere drifter SQL servere og ISS servere), firewall, portal server, Core switche, 2x Wireless controllere, backupserver (Via fysiske bånd og Veeam) samt SAN.

1.3 Yderligere systemer:

Alle skoler anvender Microsoft Azure og Microsoft office 365. Backup af ansattes data foretages via Veeam. Hver skole anvender hver deres regnskabs, LMS og studieadministrative systemer, som ofte driftes på statslige løsninger/aftaler af eksterne leverandører.

EUC Nordvest anvender MSSC til styring af domæne enheder, FGU er netop gået i gang med at anvende Intune. De resterende skoler har manual enhedshåndtering.

EUC Nordvest/IT-fællesskabet har et tæt samarbejde med konsulentvirksomheden NetIP, som via en support og drift aftale hjælper med IT-sikkerhed, backup, restore-test, overvågning af systemer/hardware samt patching og drift af de mere drift kritiske systemer.

2. Kravspecifikation til tilbud:

2.1 Overordnet krav

4 af skolerne i IT-fællesskabet (alle skoler på nær VUC Thy-Mors) ønsker et grundigt 360-graders tjek af vores IT-sikkerhedsniveau. Så vi kan se om det er acceptabelt ift. det nuværende og fremtidige IT-sikkerheds risikobillede, herunder anbefalinger til hvor vi bør sætte ind for at forbedre niveauet - om noget er kritisk at gøre nu og her.

Analysen skal helt overordnet indeholde:

A. En analyse og redegørelse af IT-sikkerhedsniveauerne for hver skole
B. En analyse og redegørelse af IT-sikkerheden for IT-fællesskabet

Både analyse A og B skal indeholde et executive summary og en prioriteret anbefalingsplan til forbedringer af hvor man bør sætte ind, inkl. konkrete løsningsforslag til hvad bør gøres og estimat på omkostninger for at gøre dette.

Kriterier for anbefaling skal som minimum tage højde for disse 3 parametre:

1. Sandsynlighed for ulykke/angreb
2. Alvorlighed ved ulykke/angreb
3. Omkostninger eller arbejdsindsats krævet for mitigering

Da analyserne har til formål at sikre at de IT-ansvarlige (i sidste ende direktører og bestyrelser) ved om det nuværende IT-sikkerhedsniveau er tilstrækkelig, er det vigtigt at analysen er grundig nok til at vi kommer hele vejen rundt om IT-sikkerheden.

Bemærk herunder kompleksiteten med at en af partnerskolerne (af økonomiske årsager) ikke ønsker at være en del af denne IT-sikkerhedsanalyse, men i stedet har kørt deres egen light-udgave, hvor de har brugt få timer sammen med en ekstern konsulent for at gennemgå It-sikkerheden. Dette vil vi også gerne have med i analysen hvad reelt betyder for os andre som ønsker analysen, da det er jo også en potentiel sårbarhed - at vi ikke kender vores partnerskoles IT-sikkerhedsniveau. Spørgsmålet er herunder i hvor høj grad dette påvirker os andre og hvad der anbefales at vi gør ved udfordringen. Om vi f.eks. IT-teknisk kan/bør opsætte barrierer, bør sætte nogle særlige IT-sikkerhedskrav til denne partnerskole eller måske helt bør indstille dem til at forlade IT-fællesskabet?

2.2 Krav til format, metode og indhold:

- Vi ønsker et samlet tilbud i danske kroner ex. moms
- Prisen skal indeholde ALLE udgifter til projektet, herunder evt. projektledelse/koordinerings omkostninger
- Tilbuddet skal vise hvor mange arbejdstimer i forventer at bruge på arbejdet
- Tilbuddet skal vise et estimat på hvor mange timer i vurderer den enkelte skole skal ligge i forbindelse med analysen (f.eks. til interviews/dokumentationsindhentning)
- Tilbuddet skal vise et estimat på hvor mange timer NetIP og evt. andre leverandører skal forvente at bruge på analysen (f.eks. til interviews/dokumentationsindhentning og -udarbejdelse)
- Tilbuddet skal indeholde en redegørelse af hvordan I vil gå til opgaven, hvordan slut rapporten vil se ud (f.eks. med grafer/visualiseringer osv.) og hvorfor netop I kvalificer jer til opgaven (Case-henvisninger, erfaring, certificering etc.)
- I tilbuddet skal inkluderes en mundtlig/visuel præsentation af resultaterne, hvor repræsentanter for hver skole har mulighed for at spørge indtil analysen og rapporterne.
- Er der punkter i forbindelse med denne kravspecificering i ikke mener at kunne opfylde skal dette fremgå af tilbuddet.
- Endelig skal det fremgå hvornår I forventer at I vil kunne igangsætte analysen og deadline for færdiggørelse af analysen.
    - Bemærk: Det er vigtigt for os, at analysen ikke trækker ud og vi ønsker derfor at indføre en SLA på deadlinen. Således at vi for hver uge projektet overskrider den aftalte deadline kompenseres med 3% af aftalebeløbet.
- Betaling vil falde umiddelbart efter leverancen er fuldført, men hvis ønskes kan et forudbetalt beløb overføres til deponi konto.

Metoden bør være et mix af:

- Scanninger
- Interviews
- Gennemgang af teknisk dokumentation
- Evt. godartet forsøg på phishing eller hacking (er dog ikke et krav)

Yderligere specificering af metode krav:

- Analysen skal foretages af IT-konsulenter som er uddannet inden for IT-sikkerhedsområdet og hvor mindst en person på holdet har mere end 3års erfaring med IT-sikkerheds analyser af organisationer/virksomheder
- Sikkerheds- og Risikovurdering skal tage udgangspunkt i kendte frameworks for cyber security. Umiddelbart ønske er CIS18 og NIST. Tages der udgangspunkt i andre frameworks skal det fremgå af tilbuddet hvilke og argumenteres hvorfor.
- Rapporten skal indeholde minimum 150 forskellige observationspunkter, som vurderes med en score fra 1-5.
- De ovennævnte sikkerhedsframeworks skal danne grundlag for anbefalinger for risikovurdering på alle observationer.
- Der skal tilknyttes anbefalinger til udbedring/mitigering til samtlige observationer – inkl. en vurdering af, hvordan anbefalingerne forventes at påvirke scoren.
- Der skal anvendes et eller flere IT-sikkerheds scanningsværktøjer til analysen f.eks.: CSAT-scanning eller Nessus sårbarhedsscanning.
- Interviews: Der skal gennemføres interviews med minimum 7 nøglepersoner og der skal gennemgås materialer/dokumentation, processer/procedurer samt roller og ansvar.
- Vurderingerne skal tage afsæt i, en general sammenligning/forholdningstagning til risikoprofilen for den branche vi befinder os i og til typen af organisation vi er (skoler under et samlet IT-fællesskab)
- Resultatet af rapporten skal være konkret og håndgribelig således der umiddelbart kan iværksættes indsatser for udbedring/mitigering – hvor muligt inddelt i faser og anbefalinger efter risiko og prioritering.
- Man er som leverandør velkommen til at komme med eget tilbud i forbindelse med mitigering, men vi fastholder os også retten til selv at mitigere fejlen og/eller gå med andre eksterne parter.

Er noget uklart i forhold til krav og ønsker kan Digitaliseringschef Christian Homann kontaktes på:

Mail: Cho@Eucnordvest.dk
Tlf.: 92721911