TEKNISKE MINIMUMSSTANDARDER

14. November 2022

Ved Christian Christensen

Hvad og hvorfor?

Som leverandører er I med til at understøtte løsningen af en række samfundsopgaver, herunder cyber- og informationssikkerheden.

Konkret:

- **En række anbefalinger, der er vendt imod kommunerne**
- **Som leverandør er det klogt at orientere sig imod de krav, hvor man selv leverer ydelser/tjenester**
- **Ikke en tjekliste som kan efterleves af hver enkelt leverandør.**

Kravene i overblik

Der er 35 krav i alt. Kravene findes i nedenstående kategorier:

1. **Klient / PC**
2. **Mail**
3. **Autentifikation**
4. **Mobile enheder**
5. **Logning**
6. **Domæner (tidligere kendt som web)**
7. **Netværk**
8. **Diverse**

Mange af kravene er meget specifikke på den kommunale infrastruktur.

De kommende slides forsøger at dykke ned i de mere generiske krav der er af almen bred interesse.

Kravene i overblik

Der er 35 krav i alt. Kravene findes i nedenstående kategorier:

1. **Klient / PC**
2. Mail
3. Autentifikation
4. Mobile enheder
5. Logning
6. Domæner (tidligere kendt som web)
7. Netværk
8. Diverse

”S6 - Administrative rettigheder for brugere tildeles kun tidsbegrænset og med veldokumenterede behov.”

Som leverandør betyder det, at jeres brugerstyringsmodel skal være så moden, at administrative opgaver skal kunne adskilles fra alm. brugere i systemet OG fra andre krav, at rettigheder skal kunne styres fra et central system, f.eks. ADFS.

Kravene i overblik

Der er 35 krav i alt. Kravene findes i nedenstående kategorier:

1. Klient / PC
2. **Mail**
3. Autentifikation
4. Mobile enheder
5. Logning
6. Domæner (tidligere kendt som web)
7. Netværk
8. Diverse

Kun relevant hvis Jeres system har mail interaktion. Men open mail relay er ”forbudt”, og TLS1.2 kryptering er minimumsstandard.

Kravene i overblik

Der er 35 krav i alt. Kravene findes i nedenstående kategorier:

1. Klient / PC
2. Mail
3. Autentifikation
4. Mobile enheder
5. Logning
6. Domæner (tidligere kendt som web)
7. Netværk
8. **Diverse**

”K9 – passwords skal udformes, opdateres og opbevares i overensstemmelse med CFCS anbefalinger”

”K11 - Internet-of-Things enheder skal være beskyttet med ikke-default password og skal være koblet på et behørigt segmenteret netværk.”

Kort – passwords skal være komplekse, de skal kunne ændres, de skal gemmes i en krypteret database, og de må ikke kunne tilgås.

HVIS I arbejder med https-baserede løsninger, mailsystemer eller infrastrukturrelaterede løsninger …

- Så er der en række af kravene der er langt mere interessante for dig
- Fokuser på ”Diverse”, ”Mail” og ”Mobile enheder”

Den samlede liste kan ses her på KL’s Videnscenter hjemmeside.

Spørgsmål til overvejelse

1. Kan I se værdi i de tekniske minimumsstandarder, set fra Jeres perspektiv?

2. Ser I andre områder hvor I som leverandører, kan bidrage til at højne cyber- og informationssikkerhedsniveauet i kommunerne?

Spørgsmål og kommentarer

Jette Larsson
JELA@kl.dk
Konsulent
Digitalisering og Teknologi

Christian Christensen
CHCH@kl.dk
Konsulent
Digitalisering og Teknologi