LEMVIGH-MÜLLER

CYBERSIKKERHED: DET UDFORDRENDE SAMSPIL MED DIREKTIONEN

Track 1: 12.15-12.35

AGENDA

- Hvem er Lemvigh-Müller
- Baggrund for cybersikkerhedsarbejdet
- Samspillet med bestyrelse og direktionen
- Anvendelse af Bestyrelsesforeningens materialer
- Læring

OM LEMVIGH-MÜLLER

NØGLETAL

1846
GRUNDLAGT

+20.000
KUNDER

+550.000
VARENUMRE

8
MIA. I OMSÆTNING

23
BUTIKKER

3
CENTRALLAGRE

6
FORRETNINGSOMRÅDER

1.421
MEDARBEJDERE

PRODUKTOMRÅDER

Stål, rustfri stål, aluminium og metaller

El-teknik

Belysning

Tele, data og sikkerhed

Energi og klima

Beklædning og PPE

Rør og fittings

Svejsning

Kabler, ledninger, afdækning og brandsikring

Mekanik og teknik

Procesteknik

Værktøj og maskiner

Varme

Bad og sanitet

Indretning, løft og transport

Kemi, smøring, miljø og forbrugsartikler

Befæstelse

SERVICEOMRÅDER

LEVERING

- Dag til dag
- Ekspres – 1 time
- Til specifikt arbejdssted

BUTIKKER

- Stort sortiment
- Pick up – ½ time
- Fagpersonale

SUPPORT

- Specialister indenfor alle produktområder
- Vagttelefon 24/7/365

INDKØBSOPTIMERING

- One stop shop
- E-handel – webshop, app, EDI, punchout

LAGERSTYRING

- VMI / SmartLager: Kanban, scannere, automater + vægte, mercher-service
- SCM-center – pakning, mærkning, eksport
- Sikkerhedslager, konsignationslager

KURSER

- 200 +fagkurser
- Teori, hands on
- Produkter, teknologier, lovgivning

BEARBEJDNING

- Egne, ISO-certificerede produktionscentre
- Stål, rustfrit stål og metaller, armering

DOKUMENTATION

- På mail, online, med varen
- Sikkerhedsdatablade
- Sporbarhed – 3.1-certifikater

BAGGRUND FOR CYBERSIKKERHEDSARBEJDET

CYBERSIKKERHED

Indtil 2020

- Regler for cybersikkerhed var I fokus og opbygget efter “hvad du ikke må”
- Cybersikkerhed indsats var typisk hændelsesstyret

I 2020

- Etableret en risikobaseret tilgang og arbejde med risiko og trusselsområder
- Udarbejdede en modenhedsanalyse baseret på ISO27001
- Opkvalificering af medarbejdere indenfor cybersikkerhed
- Plan for teknisk gæld og teknisk Cyberbeskyttelse.

CYBERSIKKERHED FORTSAT

2021

- Teknisk sikkerhed kom i fokus
- Awareness blev målrettet med ledelsesopfølgning

2022

- Fokus på ændringer i trusselsbilledet og mere teknisk beskyttelse
- Tilpasning af samarbejde med direktion og bestyrelse

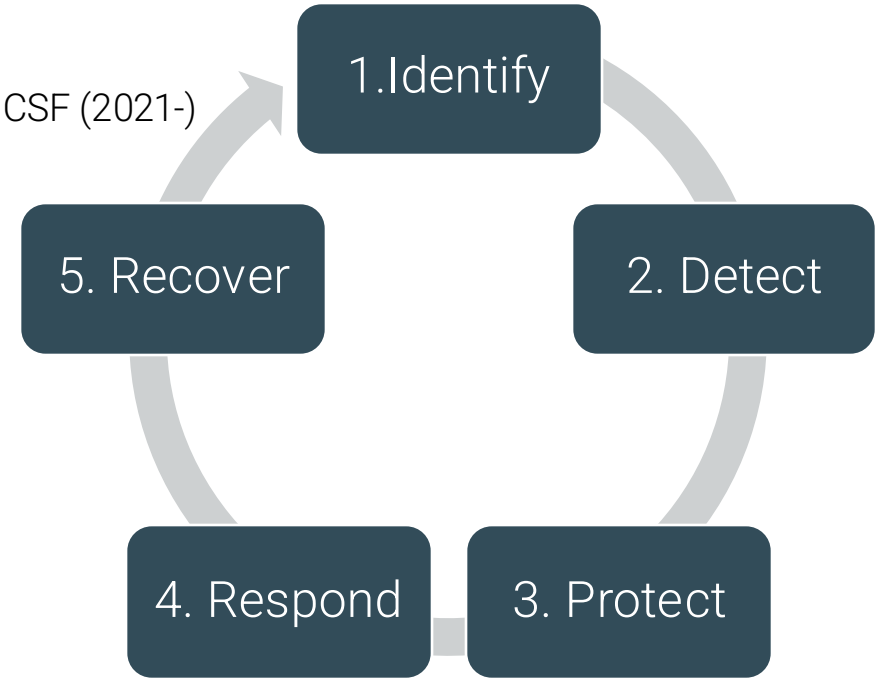
2023

- Rapportering til direktion og bestyrelse inspireret af bestyrelsesforeningen

2024

- Tilpasning af bestyrelsesrapportering

Inspiration NIST CSF (2021-)



Risici: it-nedbrud uanset årsag er forretningskritisk. Ingen IT = Ingen forretningsaktiviteter

SAMSPILLET MED BESTYRELSE OG DIREKTION

KOMMUNIKATION OG FAGLIGHED

Kommunikation er vigtig (det er indlysende men hele tiden nødvendig at minde sig selv, og andre om.

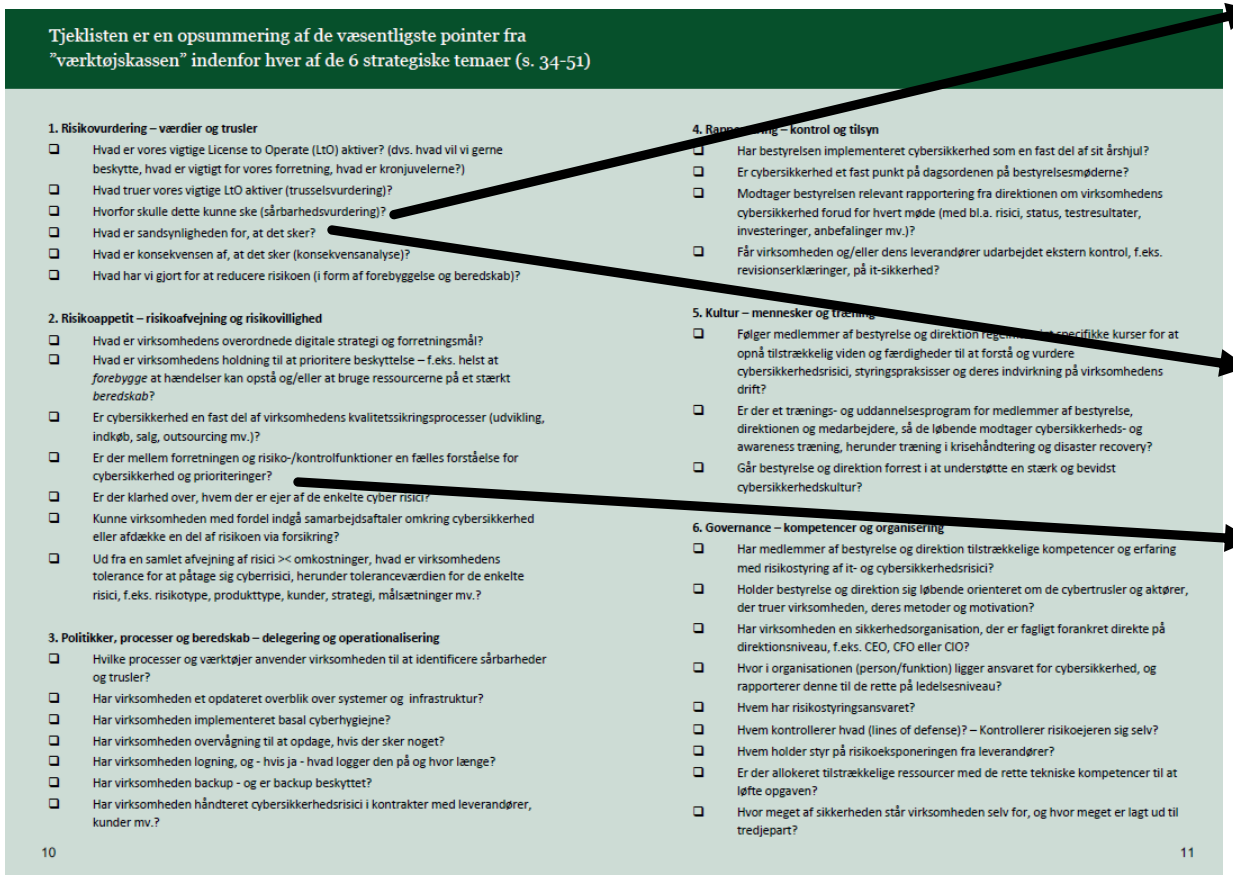
- Du kan som udgangspunkt IKKE forklare Cybersikkerhed med tekniske begreber
- Som sikkerhedsprofessionel SKAL du forstå hvad der er vigtigt for forretningen
- Du SKAL tillære dig, at kunne tale sikkerhed i en forretningskontekst – Det kræver øvelse
- Det handler om at formulere sig på et sprog som modtageren forstår - forstå hvad modtager finder vigtigt samt hvilke bekymringer de har.

Faglig udfordring er fx at:

- Forstå hvor de største risici er for forretningen
- Kunne sammenfatte mange tekniske detaljer til en samlet helhed
- Iscenesætte at Cybersikkerhed er en kontinuerlig rejse, som skal tilpasses de forandringer og virkelighed vi møder.
- Når Direktion eller bestyrelse har fået nye input, kommer der spørgsmål –vær forberedt
    - Har vi styr på….
    - Kan det ske for os at….
    - Hvornår er vi færdige med…

IT-SIKKERHEDSVÆRKTØJSKASSEN (2023)

Bestyrelsen ønskede at vide hvor vi stod med IT-værktøjskassen - baseret på bestyrelsesforeningen guide.



Tjeklisten er en opsummering af de væsentligste pointer fra "værktøjskassen" indenfor hver af de 6 strategiske temaer (s. 34-51)

1. Risikovurdering – værdier og trusler

- ❑ Hvad er vores vigtige License to Operate (LtO) aktiver? (dvs. hvad vil vi gerne beskytte, hvad er vigtigt for vores forretning, hvad er kronjuvelerne?)
- ❑ Hvad truer vores vigtige LtO aktiver (trusselsvurdering)?
- ❑ Hvorfor skulle dette kunne ske (sårbarhedsvurdering)?
- ❑ Hvad er sandsynligheden for, at det sker?
- ❑ Hvad er konsekvensen af, at det sker (konsekvensanalyse)?
- ❑ Hvad har vi gjort for at reducere risikoen (i form af forebyggelse og beredskab)?

2. Risikoappetit – risikoafvejning og risikovillighed

- ❑ Hvad er virksomhedens overordnede digitale strategi og forretningsmål?
- ❑ Hvad er virksomhedens holdning til at prioritere beskyttelse – f.eks. helst at *forebygge* at hændelser kan opstå og/eller at bruge ressourcerne på et stærkt *beredskab*?
- ❑ Er cybersikkerhed en fast del af virksomhedens kvalitetssikringsprocesser (udvikling, indkøb, salg, outsourcing mv.)?
- ❑ Er der mellem forretningen og risiko-/kontrolfunktioner en fælles forståelse for cybersikkerhed og prioriteringer?
- ❑ Er der klarhed over, hvem der er ejer af de enkelte cyber risici?
- ❑ Kunne virksomheden med fordel indgå samarbejdsaftaler omkring cybersikkerhed eller afdække en del af risikoen via forsikring?
- ❑ Ud fra en samlet afvejning af risici >< omkostninger, hvad er virksomhedens tolerance for at påtage sig cyberrisici, herunder tolerancеværdien for de enkelte risici, f.eks. risikotype, produkttype, kunder, strategi, målsætninger mv.?

3. Politikker, processer og beredskab – delegering og operationalisering

- ❑ Hvilke processer og værktøjer anvender virksomheden til at identificere sårbarheder og trusler?
- ❑ Har virksomheden et opdateret overblik over systemer og infrastruktur?
- ❑ Har virksomheden implementeret basal cyberhygiejne?
- ❑ Har virksomheden overvågning til at opdage, hvis der sker noget?
- ❑ Har virksomheden logning, og - hvis ja - hvad logger den på og hvor længe?
- ❑ Har virksomheden backup - og er backup beskyttet?
- ❑ Har virksomheden håndteret cybersikkerhedsrisici i kontrakter med leverandører, kunder mv.?

10

4. Rapportering – kontrol og tilsyn

- ❑ Har bestyrelsen implementeret cybersikkerhed som en fast del af sit årshjul?
- ❑ Er cybersikkerhed et fast punkt på dagsordenen på bestyrelsesmøderne?
- ❑ Modtager bestyrelsen relevant rapportering fra direktionen om virksomhedens cybersikkerhed forud for hvert møde (med bl.a. risici, status, testresultater, investeringer, anbefalinger mv.)?
- ❑ Får virksomheden og/eller dens leverandører udarbejdet ekstern kontrol, f.eks. revisionserklæringer, på it-sikkerhed?

5. Kultur – mennesker og træning

- ❑ Følger medlemmer af bestyrelse og direktion regelmæssigt specifikke kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici, styringspraksisser og deres indvirkning på virksomhedens drift?
- ❑ Er der et trænings- og uddannelsesprogram for medlemmer af bestyrelse, direktionen og medarbejdere, så de løbende modtager cybersikkerheds- og awareness træning, herunder træning i krisehåndtering og disaster recovery?
- ❑ Går bestyrelse og direktion forrest i at understøtte en stærk og bevidst cybersikkerhedskultur?

6. Governance – kompetencer og organisering

- ❑ Har medlemmer af bestyrelse og direktion tilstrækkelige kompetencer og erfaring med risikostyring af it- og cybersikkerhedsrisici?
- ❑ Holder bestyrelse og direktion sig løbende orienteret om de cybertrusler og aktører, der truer virksomheden, deres metoder og motivation?
- ❑ Har virksomheden en sikkerhedsorganisation, der er fagligt forankret direkte på direktionsniveau, f.eks. CEO, CFO eller CIO?
- ❑ Hvor i organisationen (person/funktion) ligger ansvaret for cybersikkerhed, og rapporterer denne til de rette på ledelsesniveau?
- ❑ Hvem har risikostyringsansvaret?
- ❑ Hvem kontrollerer hvad (lines of defense)? – Kontrollerer risikoejeren sig selv?
- ❑ Hvem holder styr på risikoeksponeringen fra leverandører?
- ❑ Er der allokeret tilstrækkelige ressourcer med de rette tekniske kompetencer til at løfte opgaven?
- ❑ Hvor meget af sikkerheden står virksomheden selv for, og hvor meget er lagt ud til tredjepart?

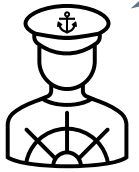
11

Svaret var en sammenfatning pr. område da tjekmark ikke er en mulighed. (det samlede svar fylder 8 A4 sider)

1.3	Hvorfor skulle dette kunne ske (sårbarheds-vurdering)?	Cyberkriminelle øger angrebstyperne, og de er blevet bedre til at hacke. Medarbejdere er en typisk angrebsflade. Som en moderne digital virksomhed har vi mange tekniske integrationer med samarbejdspartnere, som er potentielle sårbare områder, med mere eller mindre direkte adgang til vores systemer.
1.4	Hvad er sandsynlighe den for, at det sker?	Cyberangreb sker hver dag. Sandsynligheden for nedbrud af IT-systemer er medium, som konsekvens af ydre angreb, personale, almindelige software- og hardwarenedbrud, personafhængighed mv.
2.4	Er der mellem forretningen og risiko-/kontrolfunkti oner en fælles forståelse for cybersikkerhe d og prioriteringer?	For cybersikkerhed er det IT Sikkerhedschefen som er kontrolfunktionen, og i sidste ende IT Direktøren. For GDPR, er der en særskilt kontrolfunktion, en GDPR Koordinator i Compliance Der er en fælles forståelse af cybersikkerhed og prioriteringer mellem kontrolfunktioner og forretningen. I realiteten er der tale om funktioner som har forskelligt mindset, forudsætninger og kompetencer. Denne forskellighed kan føre til gode kreative løsninger, men også løsninger som har sikkerhedsmæssige sårbarheder.

EKSEMPEL PÅ PROBLEMSTILLING OG KOMMUNIKATION

Har vi styr på brugeradgange?



Her er reference til Cyberhygiejne

Multi-faktor brugervalidering

Anvend som minimum to-faktor brugervalidering på alle former for fjernadgang (VPN-løsninger, fjernskrivebord, Citrix m.v.) og på alle (væsentlige) cloud services, f.eks. Microsoft Office 365, Google Gmail m.v. Særlig fokus skal være på brugere med administrative adgange, da disse adgange kan gøre stor skade, samt konsulenter og andre eksterne brugere, der også måtte have adgang, og ofte glemmes ved implementering af tofaktor brugervalidering.

IT refleksion:
Spørgsmål kunne være; "*Har vi det?*"

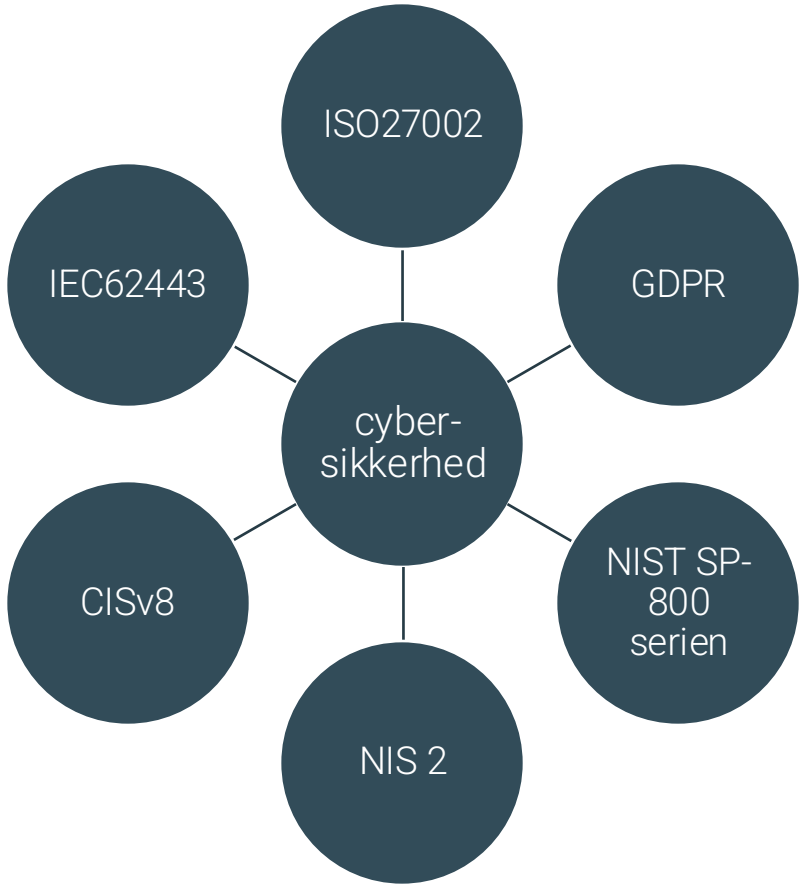
Hvad er dit svar?

Kan du svare Ja, 100% eller er jeres tekniske løsninger differentieret ift. valg af adgangstype, teknologi mv.?

Hvad skal svaret så være?

Her kommer viden om risici, og teknologi i spil.

VI HAR VALGT EN OPERATIONEL TILGANG



HVOR ER VI MED RAPPORTERING NU?

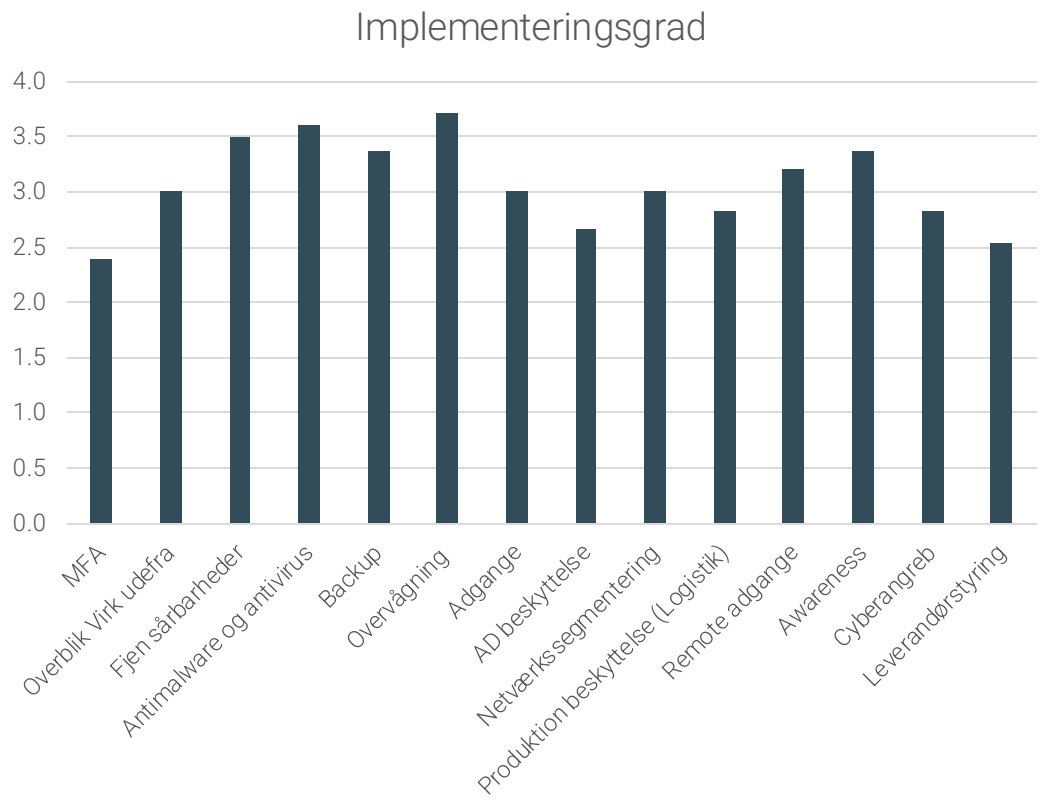
Rapportering er pt forankrede Cyberhygiejne tilpasset med 2 punkter Cyberangreb og Leverandørstyring.

Definitioner på Score – dvs. hvor godt krav er implementeret.

Niveau	Emne	Beskrivelse
4	Implementeret	• Krav efterleves både i form af retningslinjer, tekniske og/eller organisatoriske foranstaltninger
3	Delvist implementeret eller der er supplerende kontroller	• God risikodækning via delvis implementering af tekniske løsninger og/eller organisatoriske foranstaltninger • Delvist implementeret kan også dække over kompenserende kontroller.
2	Fravalgt ift risikovurdering	• Krav er fravalgt som følge af en lav risikovurdering • Der er foretaget en dispensation i en periode.
1	Ikke implementeret	• Risici er identificeret • Der er ved at blive designet en løsning

RAPPORTERINGSFORM

Tal står ikke alene der kommer kort tekst forklaring med.

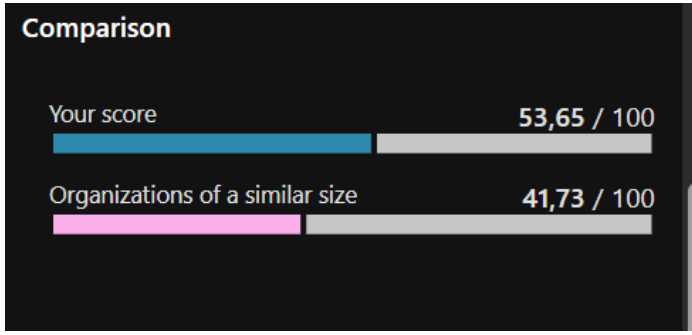


Baggrund er sikkerhedskrav og kontroller sammenstillet med sikkerhedsstandarder

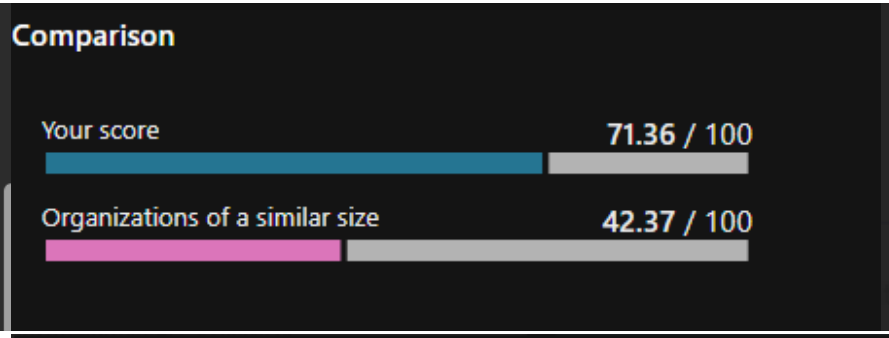
Kontrolbeskrivelse	Implementeringsniveau
Minimer Administratoradgang: Begræns antallet af domæneadministratorer og andre højtstående konti. Brug rollebaseret adgangskontrol (RBAC) for at begrænse adgangen.	
Brug af Stærke Adgangskoder og Multi-Faktor Godkendelse (MFA): Sikre alle brugerkonti, især administratorer, med komplekse adgangskoder og MFA.	
Regelmæssig Overvågning og Revision: Implementer overvågningsløsninger for at spore og logge AD-aktivitet, herunder loginforsøg, ændringer i gruppemedlemskab og adgang til følsomme oplysninger.	
Sikkerhedskopiering og Gendannelse: Oprethold regelmæssige og sikre sikkerhedskopier af AD-databasen og test jævnligt gendannelsesprocedurer.	
Implementering af Least Privilege: Giv kun den nødvendige adgang til brugere og tjenester baseret på deres arbejdsbehov. Undgå at give unødvendige administrative rettigheder.	
Adgangskontrol til Administrative Grupper: Kontroller regelmæssigt medlemskabet af kritiske grupper som Domain Admins, Enterprise Admins og Schema Admins.	
Beskyttelse mod Pass-the-Hash og Pass-the-Ticket Angreb: Brug teknologier som Windows Defender Credential Guard og privilegeret adgangshåndtering (PAM) for at beskytte mod disse typer angreb.	
Sikring af Domain Controllers: Anvend strenge sikkerhedspolitikker og fysiske sikkerhedsforanstaltninger for domænecontrollere, og sørg for, at de kun udfører nødvendige roller.	
Brug af Separate Administrationskonti:	

EKSEMPEL MICROSOFT SECURE SCORE

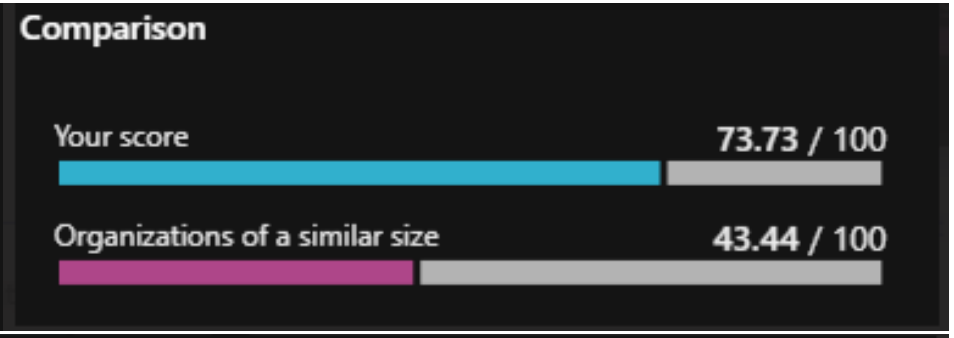
Ultimo Jan 2024

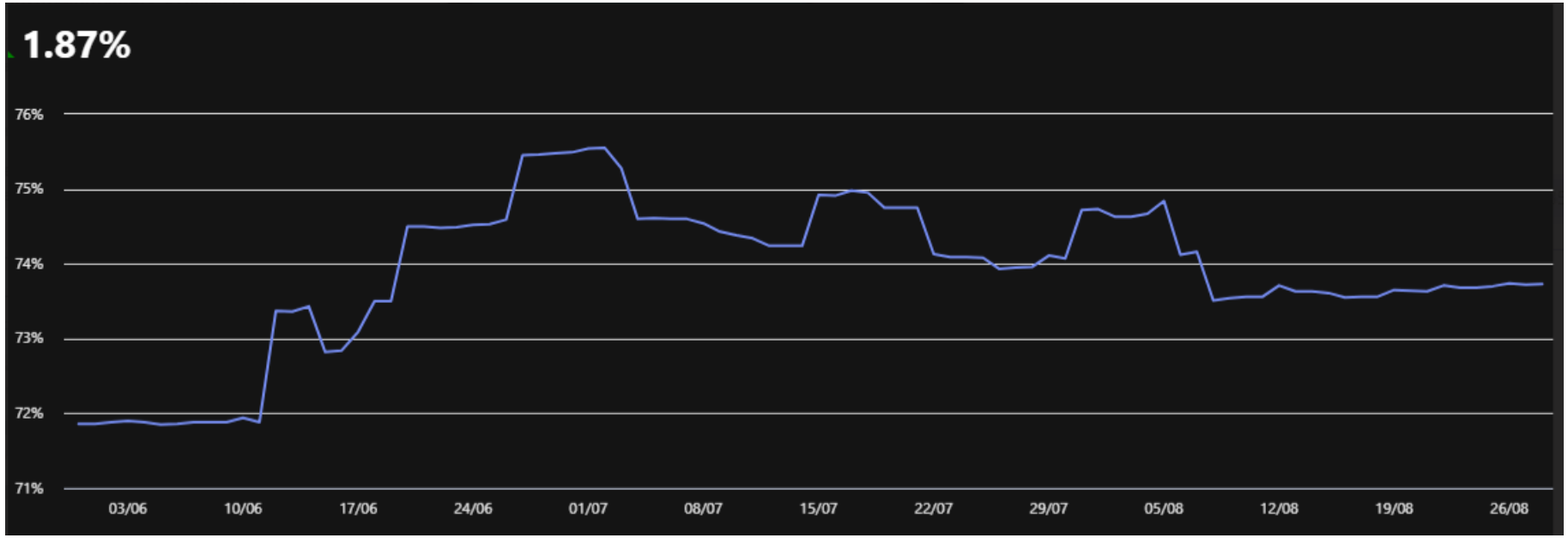


Primo Maj 2024



Ultimo August 2024





LÆRING

Hvad har jeg lært/hvad kan virke?

- Jeg har lært at Cybersikkerhed kan løses på mange måder
- Vær ærlig- gør ikke sikkerheden bedre eller dårligere end den er
- Vær varsom med at formulere dig, så du hænger nogen ud
- Hav modet til at spørge, så du er mere sikker på, at du forstår hvad spørgsmålet omhandler
- Vær på forkant med løbende orientering, også det som ikke er behageligt
- Inddrag IT-organisationen

Hvad bør du undgå

- Hop ikke til konklusionen – du skal arbejde mere med problemstillingen, inden du giver et svar
- At du vil have alt med = være 100%
- At måling ikke er absolutte værdier, så kan fokus blive på ”tallet” fremfor udviklingen/forbedringer

NÅR ERFARING SKABER FREMTID