IT-SIKKERHED

IT FORUM GRUPPENS IT-SIKKERHEDSTJEK

Baseret på CIS 18-kontrollerne

IT FORUM GRUPPEN

IT FORUM GRUPPEN A/S
IT-SIKKERHEDSTJEK

En central del af at drive virksomhed involverer IT-systemer

På trods af IT-systemers afgørende betydning viser det sig, at 1 ud af 4 små og mellemstore virksomheder ikke har implementeret essentielle sikkerhedstiltag, såsom overvågning eller opdatering af software og hardware. IT-kriminelle forsøger konstant at udnytte sårbarheder i IT-infrastrukturen til at angribe virksomheder.

Ofte kan det være en uoverskuelig og ressource-krævende proces at sikre sig imod en eventuel kompromittering. Et godt sted at starte er ved at få skabt et overblik over kritiske systemer og data, og dermed blive gjort opmærksom på, hvor i organisationen det er særligt vigtigt at sikre sig imod angreb.

Med et IT-sikkerhedstjek fra IT Forum Gruppen får du en avanceret og systematisk gennemgang af din samlede IT-infrastruktur baseret på CIS 18-kontrollerne.

Alle tekniske enheder, software og netværk bliver behandlet. Også de menneskelige IT-sikkerhedsforanstaltninger såsom IT-politikker bliver kontrolleret, da IT-sikkerhed i høj grad også handler om den daglige anvendelse af IT i en organisation.

MED ET SIKKERHEDS-TJEK FÅR DU:

- **Komplet rapport over IT-infrastruktur**
  (Brugere, enheder, software, hardware og systemer)
- **Praktisk handlingsplan i prioriteret rækkefølge - baseret på CIS 18-kontrollerne**
- **Styrket dokumentation ift. compliance eller NIS2**
- **Rapportering til ledelse eller bestyrelse**

IT-SIKKERHEDSTJEK
CIS-KONTROLLERNE

IT FORUM GRUPPEN

CONTROL 01	Inventory and Control of Enterprise Assets	5 Safeguards	IG1 2/5	IG2 4/5	IG3 5/5
CONTROL 02	Inventory and Control of Software Assets	7 Safeguards	IG1 3/7	IG2 6/7	IG3 7/7
CONTROL 03	Data Protection	14 Safeguards	IG1 6/14	IG2 12/14	IG3 14/14
CONTROL 04	Secure Configuration of Enterprise Assets and Software	12 Safeguards	IG1 7/12	IG2 11/12	IG3 12/12
CONTROL 05	Account Management	6 Safeguards	IG1 4/6	IG2 6/6	IG3 6/6
CONTROL 06	Access Control Management	8 Safeguards	IG1 5/8	IG2 7/8	IG3 8/8
CONTROL 07	Continuous Vulnerability Management	7 Safeguards	IG1 4/7	IG2 7/7	IG3 7/7
CONTROL 08	Audit Log Management	12 Safeguards	IG1 3/12	IG2 11/12	IG3 12/12
CONTROL 09	Email and Web Browser Protections	7 Safeguards	IG1 2/7	IG2 6/7	IG3 7/7
CONTROL 10	Malware Defenses	7 Safeguards	IG1 3/7	IG2 7/7	IG3 7/7
CONTROL 11	Data Recovery	5 Safeguards	IG1 4/5	IG2 5/5	IG3 5/5
CONTROL 12	Network Infrastructure Management	8 Safeguards	IG1 1/8	IG2 7/8	IG3 8/8
CONTROL 13	Network Monitoring and Defense	11 Safeguards	IG1 0/11	IG2 6/11	IG3 11/11
CONTROL 14	Security Awareness and Skills Training	9 Safeguards	IG1 8/9	IG2 9/9	IG3 9/9
CONTROL 15	Service Provider Management	7 Safeguards	IG1 1/7	IG2 4/7	IG3 7/7
CONTROL 16	Applications Software Security	14 Safeguards	IG1 0/14	IG2 11/14	IG3 14/14
CONTROL 17	Incident Response Management	9 Safeguards	IG1 3/9	IG2 8/9	IG3 9/9
CONTROL 18	Penetration Testing	5 Safeguards	IG1 0/5	IG2 3/5	IG3 5/5

HVAD ER CIS 18-KONTROLLERNE?

Center for Internet Security (CIS) har udviklet et internationalt anerkendt rammeværktøj for IT-sikkerhed, kaldet CIS 18. Kontrollerne indeholder en række prioriterede, pragmatiske og operationelle anbefalinger udviklet af brancheeksperter fra hele verden.

Disse bliver løbende revideret i takt med at trusselsbilledet ændrer sig. CIS fokuserer på de mest forebyggende indsatser imod cyberangreb såsom malware, ransomware, misbrug af rettigheder, målrettet indtrængen og applikationshacking.

Ydermere tager CIS 18-kontrollerne udgangspunkt i omkostningseffektive sikkerhedsaktiviteter, hvilket vil sige den højeste værdi på kortest tid.

Du kan læse mere om CIS 18-kontrollerne her.

IT FORUM GRUPPEN A/S
IT-SIKKERHEDSTJEK

Kan CIS-kontrollerne bidrage til implementering af standarder som NIS2 og ISO?

Det kan være en ressourcekrævende opgave at blive ISO certificeret eller imødekomme europæiske myndighedskrav som NIS2-direktivet. Sidstnævnte er et EU-direktiv, som skal øge og ikke mindst strømline IT-modstandsdygtigheden på tværs af samfundsmæssige tjenesteudbydere og samtidig forbedre håndteringen af IT-angreb. Et fælles kendetegn for standarderne er, at de ofte er formuleret abstrakt og bredt, hvilket betyder, at det kræver en gradvis afkodning af kravene før disse kan omsættes til konkrete løsninger – og det er her CIS-kontrollerne kan bidrage.

CIS-kontrollerne er konkrete og pragmatiske anbefalinger til IT-sikkerhed, som kan implementeres og i prioriterede rækkefølge. Emnerne i CIS 18-kontrollerne vil næsten uundgåeligt være krævet i standarder som ISO og NIS2, så derfor vil det være et godt sted at starte ift. arbejdet med compliance og operationalisering.

Så det korte svar på, om CIS-kontrollerne kan bidrage til implementering af ISO eller NIS2 standarder er:
Ja, CIS-kontrollerne kan bidrage til at gøre arbejdet med standarder mere konkrete og håndgribelige.

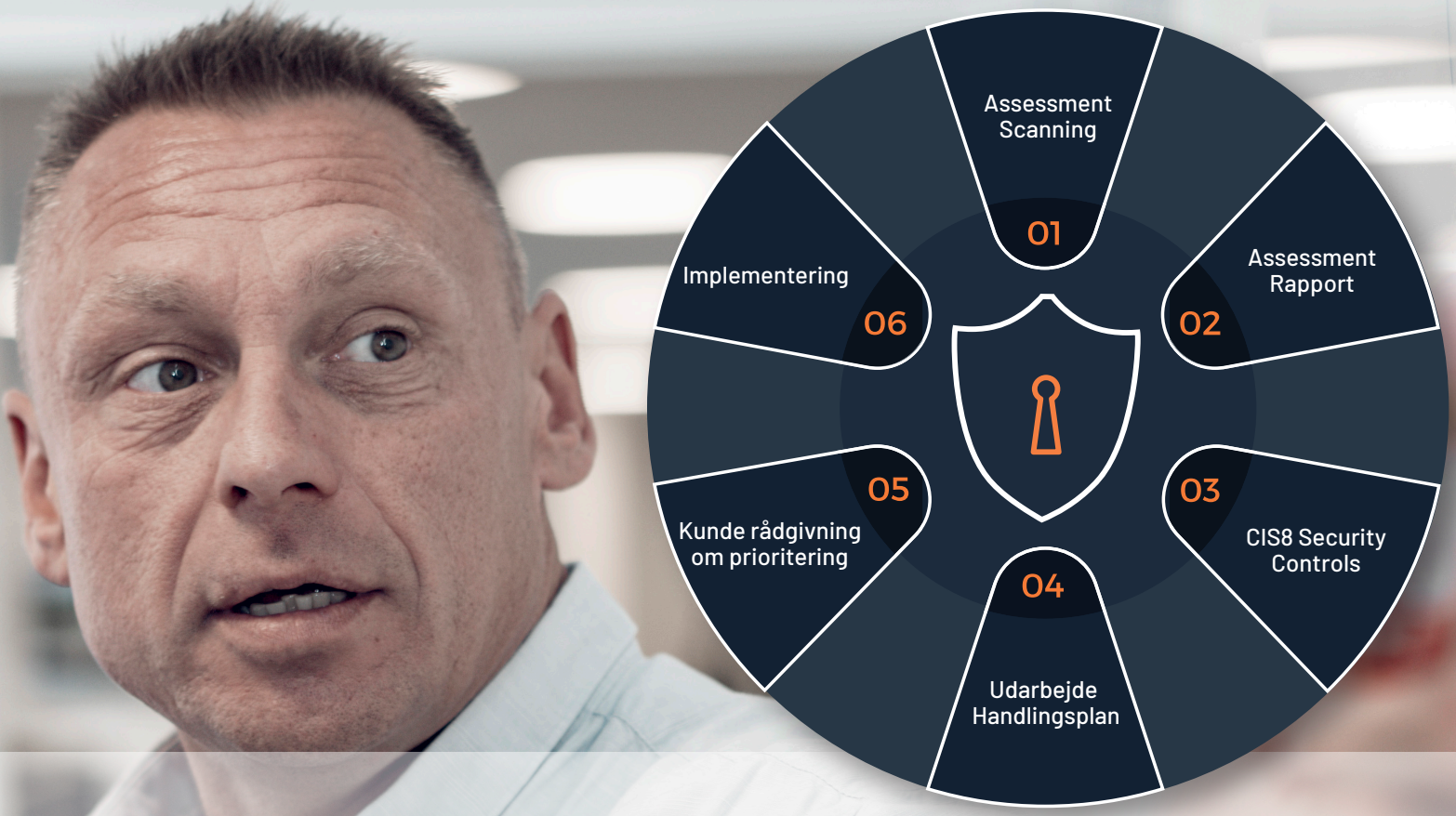
Hvad er NIS2 direktivet?

Europa-Parlamentet har indgået en ny aftale vedr. cyber- og informationssikkerhed – det såkaldte NIS2-direktiv. Danske virksomheder skal forvente at disse krav skal efterleves i løbet af 2024. Med de nye regler stilles der krav til topledelsen, som skal stå til ansvar for at føre tilsyn med IT-sikkerhedsindsatsen og godkende sikkerhedsforanstaltningerne – og der er lagt op til væsentlige bødeafgifter, såfremt disse krav ikke efterkommes.

KRAVENE FOR NIS2 DIREKTIVET ER BL.A.

- **Politikker for risikoanalyse og informationssystemsikkerhed.**
- **Håndtering af hændelser (Incident Response).**
- **Retningslinjer for kontinuert enhedsopdatering og Awareness træning.**
- **Sikring af intern kommunikation, adgang og data.**
- **Driftskontinuitet og krisestyring (Back-up, gendannelse m.m.)**
- **Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.**
- **Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici (Penetrationstest).**
- **Brug af kryptografi og kryptering.**

IT FORUM GRUPPEN A/S
IT-SIKKERHEDSTJEK



2 - 4 UGER

TRIN 1 / 2 — SCANNING

TRIN 3 — CIS SPØRGESKEMA

TRIN 4 / 5 / 6 — SIKKERHEDSRAPPORT

HVORDAN GENNEMFØRES ET IT-SIKKERHEDSTJEK MED IT FORUM GRUPPEN?

TRIN 1 / 2

IT-sikkerhedstjekket igangsættes med at sikkerhedskonsulenten fra IT Forum Gruppen starter en scanning af jeres samlede IT-miljø. Denne proces vil typisk strække sig over en periode på et par uger.

Scanningen summeres i **Trin 2** til en teknisk rapport, som giver konsulenten den nødvendige grundviden samt overblik over enheder på netværket, software, hardware m.m. og heraf potentielle sårbarheder.

TRIN 3

Næste trin i processen kræver involvering fra relevante nøgle-personer i jeres virksomhed, som har den nødvendige viden om jeres nuværende IT-miljø. Afhængig af den tekniske indsigt og forudgående aftale udfyldes CIS-spørgeskemaet i større eller mindre grad i samarbejde med konsulenten fra IT Forum Gruppen.

Formålet er at få belyst IT-sikkerhedsprocesser som f.eks. IT-politikker, IT-beredskabsplan, awareness niveau m.m.

TRIN 4 / 5 / 6

IT Forum Gruppen udarbejder en samlet sikkerhedsrapport, som giver et aktuelt overblik over sikkerhedsniveauet.

Rapporten indeholder også den anbefalede handlingsplan i forhold til, hvilke sikkerhedsinitiativer I som virksomhed bør sætte i gang, og hvilken effekt disse vil have på det samlede sikkerhedsniveau.

Rapporten og handlingsplanen fremlægges for jer og hvis det ønskes, aftales en eventuel implementeringsplan.

SKAL VI STYRKE JERES FORSVAR IMOD CYPERANGREB?

JA TAK

SIKKERHED FOR FREMDRIFT

Hos IT Forum Gruppen A/S sætter vi en ære i at forstå vores kunders drift, for kun sådan kan vi sikre de løsninger, der forhindrer nedbrud.

Vi ser ikke kun på virksomhedens udfordringer, men også på dens potentialer. Ved siden af den løbende kontakt i hverdagen, afholder vi IT-Facts-møder med det direkte formål at fordybe os i vores kunders behov og potentiale. Her byder vores specialister ind med forslag og løsninger, der understøtter virksomhedens kultur og krav.

Vi har blikket rettet mod fremtiden og de stadig nye trusler og muligheder indenfor IT. Samtidig er vi lokalt forankret med begge ben på jorden, mens vi stræber efter at skabe værdi i hver time, vi bruger.

IT Forum Gruppen A/S sikrer ikke alene den daglige drift. Vi udfordrer dig, så vi sikrer bedre udnyttelse af dine systemer, og vi inspirerer dig til at bruge nye løsninger. Kun sådan kan vi leve op til vores løfte.

KONTAKT OS PÅ 70 100 150