Risikovurdering af TimeTrackingPRO

Gruppe 3

Agenda

- The Why
- Nuværende risikovurdering
- Vores centrale risici
- Risikovurdering efter tiltag
- Løsningsforslag, ressourcer og tidsplan

Hvorfor har vi fokus på IT-sikkerhed?
Sikkerhed og compliance

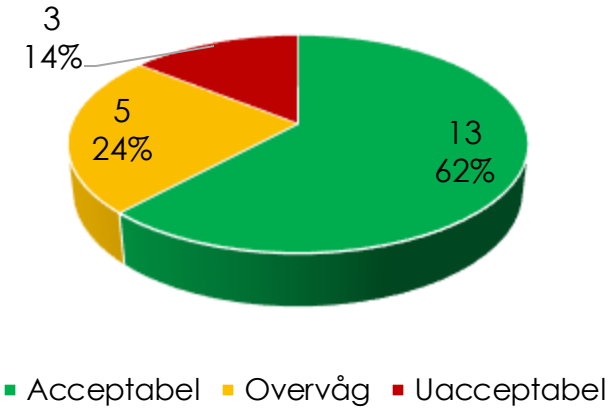
- Sikkerhed og compliance
- Vores nuværende kunder bliver omfattet NIS2
- Beskyttelse af vores kritiske aktiver
  - En stabil SaaS-platform
  - Kundernes data
  - Vores udviklingsmiljø (softwarearkitektur, konfigurationer og kode)
  - Omdømme som sikker SaaS
- Understøtter vores strategi om at bejle til C20-virksomheder

Krav til NIS2- leverandører (risikogruppe 2)
Defineret og implementeret cyber- og informationssikkerhedspolitik
Udpeget it-sikkerhedsansvarlig
Defineret og testet beredskabsplan
Udvidet awareness-træning af ledelse og medarbejdere
Adgangskontrol og rettighedsstyring
Beskyttet fjernadgang til systemer (kryptering og flerfaktor-autentifikation)
Fysisk sikring af it-infrastruktur, systemer, klienter og data

Risikovurdering Vi er langt – men ikke langt nok

Risiko	Beskrivelse	Risikoscore (S x K = R)*
Manglende kontrol med brugerrettigheder	Medarbejderes unødige adgang til en administratorkonti kan udnyttes pga. en vej ind til vores data og vores netværk	3 x 2 = **6**
Manglende dokumentation over netværk og opsætning	Uden en oversigt er det vanskeligt at identificere trafikken og tilrette konfigurationen af netværket, hvilket gør netværket sårbart over for hackere og malware.	2 x 3 = **6**
Manglende kontrol med enheder (og applikationer)	Et manglende overblik over accepterede og installerede applikationer kan resultere i ondsindet eller uopdateret software på enheder og netværk	3 x 3 = **9**
Ikke opdateret netværk	Det er ofte via forældede versioner af netværksenhedernes software (routere, firewalls, DNS-servere, DHCP-servere etc.), at hackere tvinger sig adgang til netværket.	2 x 3 = **6**
Manglende kontrol med back-ups af data	Kun ad hoc testing af back-ups kan blive fatalt i tilfælde af nedbrud	2 x 4 = **8**
Uønsket aktivitet på netværket	Ondsindet netværksaktivitet kan foregå uopdaget uden aktiv logning. Og ved manglende netværkssegmentering kan aktiviteten foregå på tværs af netværket.	2 x 4 = **8**
Manglende kontrol med leverandører	Hvis vi ikke kender vores leverandørers sikkerhedspolitik eller har serviceaftaler, kan vi risikere nedbrud el.lign. pga. manglende due diligence fra leverandørens side (og dermed vores)	3 x 4 = **12**
Manglende overordnet IT-sikkerhedsstyring	Manglende overblik over vores IT-sikkerhedstyring samt dokumentation kan føre til oversights og store fejl	4 x 3 = **12**

*Risikovillighed: Acceptabel <5, Overvåg <9, Uacceptabel >=9



- Vi vil have svært ved at nå videre uden ekstra midler (max. kapacitet)
- Flere af disse risici er underlagt NIS2

VORES FOKUS Vi skal være i grøn (med lidt gule undertoner)

Risiko	Beskrivelse	Risikoscore (S x K = R)*
Manglende kontrol med enheder (og applikationer)	Et manglende overblik over accepterede og installerede applikationer kan resultere i ondsindet eller forældet software på enheder og netværk	3 x 3 = **9**
Manglende kontrol med leverandører	Hvis vi ikke kender vores leverandørers sikkerhedspolitik eller har serviceaftaler, kan vi risikere nedbrud el.lign. pga. manglende due diligence fra leverandørens side (og dermed vores)	3 x 4 = **12**
Manglende overordnet IT-sikkerhedsstyring	Manglende overblik over vores IT-sikkerhedstyring samt dokumentation kan føre til oversights og store fejl	4 x 3 = **12**

Risiko 1 – Manglende kontrol af enheder og brugere

Risiko	Beskrivelse	Risikoscore (S x K = R)*
Manglende kontrol med enheder (og applikationer)	Et manglende overblik over accepterede og installerede applikationer kan resultere i ondsindet eller forældet software på enheder og netværk	3 x 3 = **9**

Nuværende situation

- Ingen central kontrol med enheder
- Egne admin-rights til alle (undtagen sælgere)
- Man kan downloade alt
- Vi har dog firewall og antivirus

Problematik

- "farlig" software kan downloades
- Forældet software og styresystem kan blive et entry point for hackere
- NIS2-krav

Risiko 1 – Manglende kontrol af enheder og brugere

Risiko	Beskrivelse	Risikoscore (S x K = R)*	Efter tiltag
Manglende kontrol med enheder (og applikationer)	Et manglende overblik over accepterede og installerede applikationer kan resultere i ondsindet eller forældet software på enheder og netværk	3 x 3 = **9**	1 x 2 = **2**

Udbedringstiltag

- Centralstyring af enheder
  - Auto-updates
  - Whitelisting af software
  - Admin skal godkende ikke-whitelistede softwares
- Protokol for bruger-administration (slet gamle ansatte mv.)

Ressourcer

DKK	Engangs	Kontinuerlig
Upgrade MS 365 til at inkludere InTune		12.000
Opsætning (ca. 3 ugers udviklertid månedsløn 70K)	52.500	
Vedligehold (5 dage/år udviklerløn 70K)		17.500
Total	**52.500**	**29.500**

Risiko 2 – Manglende kontrol af underleverandører

Risiko	Beskrivelse	Risikoscore (S x K = R)*
Manglende kontrol med leverandører	Hvis vi ikke kender vores leverandørers sikkerhedspolitik eller har serviceaftaler, kan vi risikere nedbrud el.lign. pga. manglende due diligence fra leverandørens side (og dermed vores)	3 x 4 = **12**

Nuværende situation

- Store aktører med høj tillidsgrad
- Ingen kontrol – ad hoc eller planlagt
- Serviceaftaler med de kritiske underleverandører (ex. AWS)

Problematik

- Vi risikerer større nedbrud, datatab el.lign., hvis vores leverandører ikke har sikkerheden i orden
- NIS2-kunder kræver det

Risiko 2 – Manglende kontrol af underleverandører

Risiko	Beskrivelse	Risikoscore (S x K = R)*	Efter tiltag
Manglende kontrol med leverandører	Hvis vi ikke kender vores leverandørers sikkerhedspolitik eller har serviceaftaler, kan vi risikere nedbrud el.lign. pga. manglende due diligence fra leverandørens side (og dermed vores)	3 x 4 = **12**	2 x 2 = **4**

Udbedringstiltag

- Dokumentation på leverandørers sikkerhedsprotokoller, vores serviceaftaler, kontakter, mv.
- Screeningsproces for eventuelle nye leverandører

Ressourcer

DKK	Engangs	Kontinuerlig
Vedligehold af aftaler og screening (3 dage/år funktionær 50K/måned)		7.500
Opsætning og samling af dokumentation (ca. 2 ugers funktionær 50K/måned)	25.000	
Total	**25.000**	**7.500**

Risiko 3 – Manglende IT-sikkerhedsstyring

Risiko	Beskrivelse	Risikoscore (S x K = R)*
Manglende overordnet IT-sikkerhedsstyring	Manglende overblik med vores IT-sikkerhedstyring samt dokumentation kan føre til oversights og store fejl	4 x 3 = **12**

Nuværende situation

- Vi gør mange ting, men vi kan ikke vise det
- Generel håndtering og dokumentation mangler
- De fleste ting foregår ad hoc og at random
- Ingen standardisering og nedskrevne regler

Problematik

- Ad hoc = Afhængighed af personer, risiko for fejl og glemsomhed
- Krav fra NIS2 – vi vil være compliant

Risiko 3 – Manglende IT-sikkerhedsstyring

Risiko	Beskrivelse	Risikoscore (S x K = R)*	Efter tiltag
Manglende overordnet IT-sikkerhedsstyring	Manglende overblik med vores IT-sikkerhedstyring samt dokumentation kan føre til oversights og store fejl	4 x 3 = **12**	2 x 2 = **4**

Udbedringstiltag

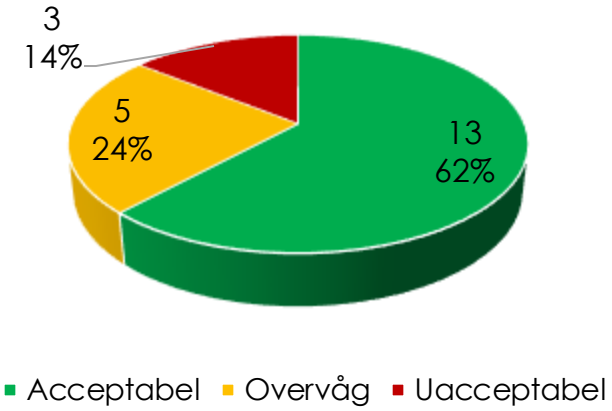
- Sikkerhedspolitik
  - Roller
  - Awareness-træning
  - Kontinuerlig opdatering regler for opsætning
  - Risikovurderinger
  - Dokumentation af sikkerhedsforanstaltninger
- Beredskabsplaner
- Årshjul med drift af vores sikkerhedspolitik
- Opsætning af cybersecurity-backlog

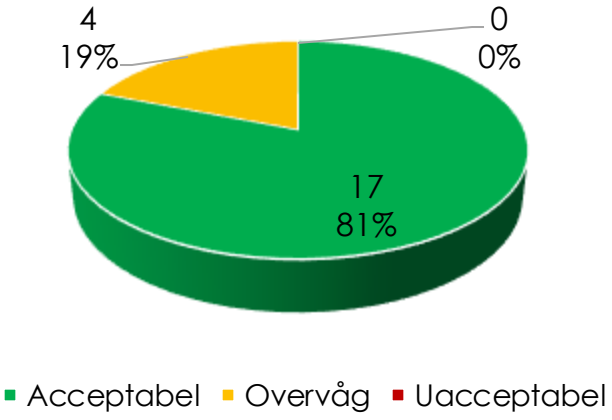
Ressourcer

DKK	Engangs	Kontinuerlig
Udarbejdelse af dokumenter (1 måned funktionær 50K/måned)	50.000	
Kontinuerlig udvikling af sikkerhed (1 måned/år udvikler 70K/måned)		70.000
Kontinuerlig drift og arbejde med cybersecurity (1 måned/år funktionær 50K/måned)		50.000
Total	**50.000**	**120.000**

Risikovurdering Tiltag vil påvirke flere risici

Risiko	Beskrivelse	Risikoscore (S x K = R)*	Efter tiltag
Manglende kontrol med brugerrettigheder	Medarbejderes unødige adgang til en administratorkonti kan udnyttes pga. en vej ind til vores data og vores netværk	3 x 2 = **6**	2 x 2 = **4**
Manglende dokumentation over netværk og opsætning	Uden en oversigt er det vanskeligt at identificere trafikken og tilrette konfigurationen af netværket, hvilket gør netværket sårbart over for hackere og malware.	2 x 3 = **6**	2 x 3 = **6**
Manglende kontrol med enheder (og applikationer)	Et manglende overblik over accepterede og installerede applikationer kan resultere i ondsindet eller uopdateret software på enheder og netværk	3 x 3 = **9**	1 x 2 = **2**
Ikke opdateret netværk	Det er ofte via forældede versioner af netværksenhedernes software (routere, firewalls, DNS-servere, DHCP-servere etc.), at hackere tvinger sig adgang til netværket.	2 x 3 = **6**	2 x 3 = **6**
Manglende kontrol med back-ups af data	Kun ad hoc testing af back-ups kan blive fatalt i tilfælde af nedbrud	2 x 4 = **8**	2 x 4 = **8**
Uønsket aktivitet på netværket	Ondsindet netværksaktivitet kan foregå uopdaget uden aktiv logning. Og ved manglende netværkssegmentering kan aktiviteten foregå på tværs af netværket.	2 x 4 = **8**	2 x 4 = **8**
Manglende kontrol med leverandører	Hvis vi ikke kender vores leverandørers sikkerhedspolitik eller har serviceaftaler, kan vi risikere nedbrud el.lign. pga. manglende due diligence fra leverandørens side (og dermed vores)	3 x 4 = **12**	2 x 2 = **4**
Manglende overordnet IT-sikkerhedsstyring	Manglende overblik over vores IT-sikkerhedstyring samt dokumentation kan føre til oversights og store fejl	4 x 3 = **12**	4 x 3 = **12**





*Risikovillighed: **Acceptabel <5**, **Overvåg <9**, **Uacceptabel >=9**

Løsningsforslag, ressourcer og tidsplan

Løsningsforslag	Konsekvens
Dedikeret InfoSec-ansættelse	• **720.000-840.000 DKK/år**
Dedikere nuværende udvikler til InfoSec	• Nedskalering af ny udvikling (og potentiel manglende viden)
Ingen ændringer	• Tab på **800.000 DKK/år** i abonnementsindtægter (Frafald af nuværende kunder (NIS2) • Strategi skal ændres – C20-kunder vil kigge anden vej

Risiko	Engangs-udgifter (DKK)	Drifts-udgifter (DKK/år)
Manglende kontrol med enheder (og applikationer)	52.500	29.500
Manglende kontrol med leverandører	25.000	7.500
Manglende overordnet IT-sikkerhedsstyring	50.000	120.000
	127.500	**157.500**

- Mange muligheder for funding (ex. Innobooster, NCC, Industriens Fond)
  - Realistisk funding på **50.000 DKK**

Bilag - Sandsynlighedsskema

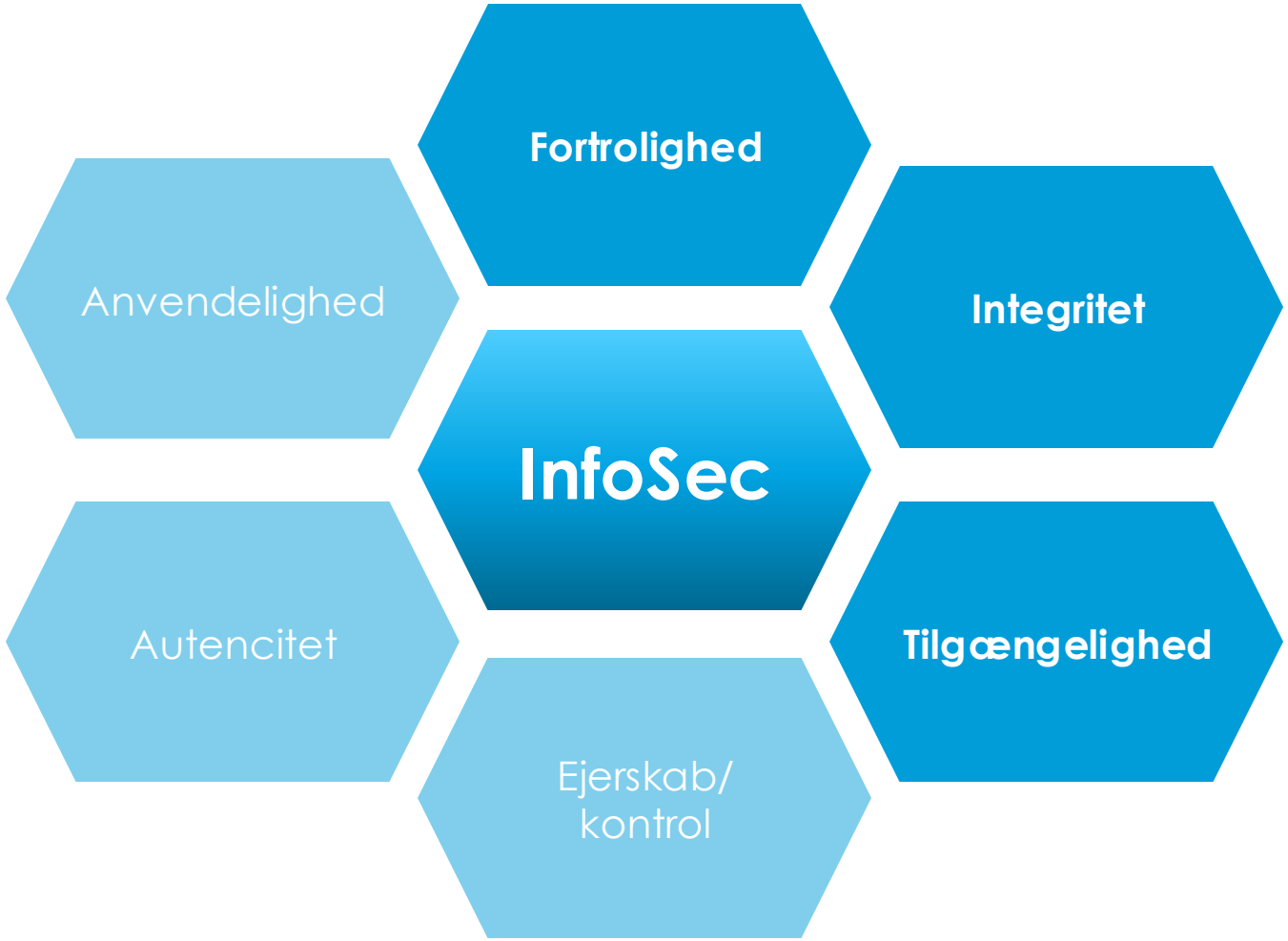
Sandsynlighed	Eksempelbeskrivelse
Usandsynligt Score: 1	Det anses for næsten udelukket, at hændelsen nogensinde kan forekomme • Ingen erfaring med hændelsen • Kendes kun fra få offentlige og private virksomheder
Mindre sandsynligt Score: 2	Hændelsen forventes ikke at komme • Mindre erfaring med hændelsen • Kendes fra offentlige og private virksomheder
Sandsynligt Score: 3	Det er sandsynligt, at hændelsen vil forekomme • Man har erfaring med hændelsen, men ikke inden for de sidste 12 måneder • Kendes fra offentlige og private virksomheder (omtales årligt i pressen)
Forventet Score: 4	Det forventes, at hændelsen vil forekomme • Man har erfaring med hændelsen inden for de sidste 12 måneder • Hænder jævnligt i andre offentlige og private virksomheder (omtales ofte i pressen)

Bilag - Konsekvenstyper

	Økonomisk Medfører økonomiske meromkostninger eller tab	**Administrativ/proces** Medfører administrative belastninger	**Omdømme** Påvirker omdømme negativt	**Politisk/Strategisk** Medfører indskrænkninger i evne til at handle i en periode	**Interessentforhold** Påvirker forhold til interessenter	**Lovbrud** Medfører brud på lovgivning, fx. forvaltningslov og straffelov
Ubetydelig (uvæsentlig) Score: 1	Ingen særlig påvirkning	Ingen særlige påvirkning	Ingen særlig påvirkning	Ingen særlig påvirkning	Ingen særlig påvirkning	Ingen særlig påvirkning
Mindre alvorlig (generende) Score: 2	Meromkostninger og tab i begrænset niveau, som kan kræve mindre budgetændringer	Håndteres inden for rimeligt ekstra administrativt ressourcetræk	Forbigående opmærksomhed fra enkelte grupper	Planlagte aktiviteter kan gennemføres med mindre justeringer	Forringet samarbejde med interessenter i enkeltsager	Manglende overholdelse af administrative procedurer og regler, som ikke er af kritisk karakter
Meget alvorlig (kritisk) Score: 3	Store økonomiske tab med risiko for at blive sat under administration	Der må trækkes væsentligt på eksisterende og nye administrative ressourcer	Offentligheden fatter generel negativ interesse for organisationen	Medfører revurdering af vigtige aktiviteter	Generelt forringet samarbejde med interessenter	Lovbrud, der er kritiske og kan stille ministeriet i miskredit
Graverende /ødelæggende (uacceptabelt) Score: 4	Væsentlige økonomiske tab. Bliver sat under administration	Eksisterende og nye administrative ressourcer er ikke tilstrækkelige	Væsentlig skade på omdømme. Der vil være personale- og ledelsesmæssige konsekvenser	Bliver ude af stand til at gennemføre vigtige aktiviteter. Der vil være personale- og ledelsesmæssige konsekvenser	Væsentligt nedbrud i det generelle samarbejde med interessenter	Brud på kritisk lovgivning, fx straffeloven brydes. Der vil være personale- og ledelsesmæssige konsekvenser

Hvad vi arbejder ud fra?

- Gfdfdsf
- Dafdfdfda
- fdafdafdafd



TimeTrackingPro

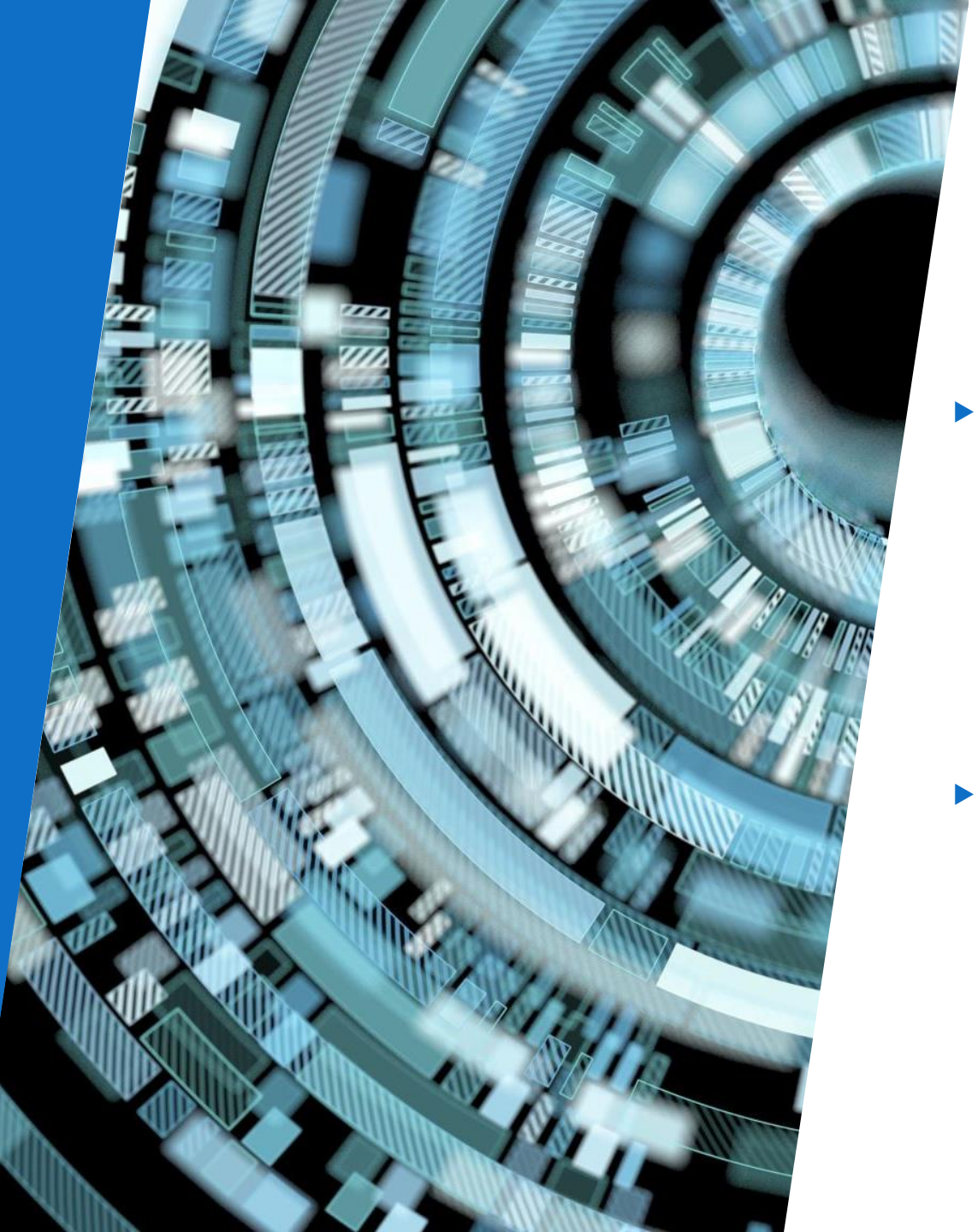
Virksomhed	Timeregistreringsværktøj Software as a Service (SaaS) 12 medarbejdere
Antagelser	Kun tidsregistrering Integration til kunders systemer Ingen HR-data el.lign.
Kundegruppe	C20-virksomheder - Krav om NIS2
Fokus	Datalækager Systemintegritet Cyberangreb

Angrebsvektorer

- Malware
  - Eksterne trusler: Social Engineering, phishing (/vishing/smishing), ransomware
  - Interne trusler: Security awareness, sårbarheder i software
- Netværksangreb
  - Eksterne trusler: (D)DoS, credential attacks
  - Interne trusler: Security awareness, adgangskontrol

DATA:
CIS-controller 3, 8 og 11

- Control 3 - Data Protection:
  - 3.3 Sikker databasehygiejne: Konfigurere lister over dataadgangskontrolelementer.
  - 3.5 Opsigelse af kunde - sletning af data.
- Control 8 - Audit Log Management
  - Logging af data: Brugerlogin og logouts, Ændringer i konfigurationen.
  - Procedure for historik logs:
    Gem overvågningslogge på tværs af virksomhedsaktiver i mindst 90 dage.
- Control 11 - Data Recovery:
  Procedure for data recovery proces.
  - Sikre at backup ligger segmenteret fra produktion.
  - Test af backup.



ACCESS:
CIS-controller 5, 6

- Control 5 – Account Management
  - Overblik over brugere/kontier
  - Procedure for kontrol af brugere
    - IAM program (Identify and Access Management)
  - Minimere antal administratorer og adskillelse fra ordinær bruger
- Control 6 – Access Control Management
  - Brugerstyring
    - Salg har ikke brug for adgang til f.eks. data
    - MFA (Multi-Factor Authentication)

Next steps

- Budgetter
- Definer team
  - CISO
  - Response team
- Udarbejd sikkerhedspolitik
- Lav en roadmap med nye tiltag
- Kontinuerlig opfølgning
  - Revidering
  - Træning af team