

Case: Hyper Medical Security A/S

Cybersikkerhed som konkurrencefordel

Contents

Baggrund	1
Hyper Medical Security A/S	2
Mission	2
Vision	2
Hyper Medical Security A/S Strategi 2024-2028.....	2
Strategisk Udgangspunkt	2
Strategiske Mål	3
Udfordringer	3

Baggrund

Hyper Medical Security A/S, eller i daglig tale HMS, er en mellemstor dansk innovationsvirksomhed, der udvikler og leverer automations- robot-, droneteknologi til sundhedssektoren. Virksomheden har oplevet kraftig vækst de seneste 4 år, men står nu over for øget konkurrence og strengere krav til patient- og datasikkerhed samt forsvarlig forsyningskædestyring.

Virksomheden sælger sine produkter og ydelser til en række lande, dog primært Danmark og Sverige. Den omsætter for ca. 90 millioner danske kroner årligt og beskæftiger ca. 60 fastansatte medarbejdere + ca. 5 til 25 løst tilknyttede konsulenter afhængig af projekter.

Denne case beskrivelse giver et indblik i HMS's Mission, Vision samt Strategi for årene 2024-2028.

Hyper Medical Security A/S

Mission

Vores mission her hos Hyper Medical Security A/S er at revolutionere sundhedssektoren gennem innovative automations-, robot- og droneteknologier, der forbedrer patientpleje, øger effektiviteten og sikrer den højeste standard for datasikkerhed.

Vi stræber efter at levere banebrydende teknologi, der gør en mærkbar forskel i menneskers liv, samtidig med at vi opretholder de strengeste sikkerhedsprotokoller i vores produkter og forsyningskæde.

Vision

Vi ser en fremtid, hvor Hyper Medical Security A/S er den førende leverandør af sikre, innovative teknologiløsninger til sundhedssektoren i Danmark og internationalt. Vores vision er at:

- I. Være på forkant med teknologisk innovation, såsom AI, machine learning og lign. inden for automations-, robot- og droneteknologi i sundhedssektoren.
- II. Sætte nye standarder for datasikkerhed og forsyningskædestyring i branchen.
- III. Forbedre patientpleje og sundhedspersonalets arbejdsvilkår gennem vores løsninger.
- IV. Være den foretrukne partner for sundhedsinstitutioner, der søger sikre og effektive teknologiløsninger.
- V. Bidrage til et mere effektivt og patientsikkert sundhedssystem gennem vores teknologi.
- VI. Inspirere og lede den næste generation af sundhedsteknologivirksomheder i Danmark og globalt.

Gennem vores dedikation til innovation, sikkerhed og excellence stræber vi efter at skabe en sundere og sikrere verden, én teknologisk løsning ad gangen.

Hyper Medical Security A/S Strategi 2024-2028

Strategisk Udgangspunkt

Hyper Medical Security A/S er en mellemstor dansk innovationsvirksomhed, der udvikler og leverer automations-, robot- og droneteknologi til sundhedssektoren. I lyset af de stigende udfordringer i sundhedssektorens forsyningskæde og de voksende krav til kvalitet, compliance og datasikkerhed, positionerer vi os som en nøgleaktør i transformationen af sundhedssektorens teknologiske infrastruktur.

Strategiske Mål

- I. Øge markedsandelen i Danmark med 30% og etablere stærk tilstedeværelse i mindst tre nye europæiske markeder inden 2028.
- II. Udvikle og lancere mindst to banebrydende teknologiløsninger årligt, der adresserer specifikke udfordringer i sundhedssektorens forsyningskæde.
- III. Opnå ISO 27001 certificering og blive anerkendt som branchens førende inden for datasikkerhed og forsyningskædestyring.
- IV. Etablere strategiske partnerskaber med mindst fem ledende farmaceutiske virksomheder og medicinalproducenter inden 2026.
- V. Reducere produktionslead-tider med 40% og hjælpe vores kunder med at reducere deres lagerbeholdninger med 25% gennem vores teknologiløsninger.

Udfordringer

Til trods for disse visioner oplever HMS udfordringer med at eksekverer på de strategiske mål. Det udmønter sig specielt på 4 områder:

1. Som leverandør oplever HMS et stigende pres fra deres kunder (hospitaller og klinikker) om at dokumentere cybersikkerheden i deres produkter og ydelser allerede i dag.
2. Som kunde skal HMS sikre, at deres egne leverandører og underleverandører lever op til høje sikkerhedsstandarder i hele forsyningskæden.
3. Konkurrencen i markedet er intensiveret, og HMS leder efter håndgribelige metoder og processer at differentiere sin forretning med.
4. HMS har en kompleks forsyningskæde med mange led, hvilket gør det udfordrende at opretholde et klart overblik og kontrol over virksomhedens teknologiløsninger.

Beredskabsplan

For at kunne modgå de øgede trusler fra Cyberkriminalitet, har HMS udformet følgende templates. Planen er at tage en kritisk situation i opløbet og med de ressourcer organisationen i forvejen råder over. I tillæg har HMS oprettet en IR aftale med Dubex.

Skabelon til handlingsplan for virus- og hackerangreb

Nr.	Handling	Ansvar	Tid
1	Vurder situationen Vurder situationen. Hvis der er risiko for, at data kan blive kompromitteret, afbrydes internetforbindelsen.		Start: Slut:
2	Luk systemer Vurder om der er behov for at lukke systemer for at undgå spredning af angrebet. Informer relevante systemejere, brugere mv.		Start: Slut:
3	Iværksæt undersøgelse Iværksæt en undersøgelse af angrebet. Kontakt Dubex.		Start: Slut:
4	Skift adgangskoder Det vurderes, om adgangskoder bør skiftes.		Start: Slut:
5	Aktiver ekstra systemlogging Det vurderes, om der bør iværksættes ekstra logging af systemer og netværk for at opklare og indsamle beviser om hændelsen.		Start: Slut:
6	Kontakt leverandører Hvis de ramte områder driftes eksternt kontaktes leverandørerne.		Start: Slut:
7	Kontakt myndigheder Det skal vurderes, om der skal foretages politianmeldelse, og om der er andre myndigheder, som bør kontaktes fx Datatilsynet		Start: Slut:
8	Informér interessenter Eventuelle øvrige interessenter informeres.		Start: Slut:

Leverandør samarbejde

Nr.	Handling	Ansvar	Tid
1	Undersøg leverandørforhold Det undersøges, hvilke opgaver som er outsourcet til en ekstern leverandør.		Start: Slut:
2	Kontakt leverandør Hvis ikke dette allerede er sket, fx i tilfælde af det er leverandøren der har konstateret og informeret om hændelsen, tages kontakt til leverandøren.		Start: Slut:
3	Vurder situationen Status gennemgås, og situationen vurderes i samarbejde med leverandøren. Hvis leverandøren har behov for adgang til organisationens lokation, aftales det, hvordan adgangen finder sted.		Start: Slut:
4	Planlæg indsatsen Planlæg opgaver og aftal det videre forløb. Er it-systemerne outsourcet, planlægges indsatsen i samarbejde med leverandøren.		Start: Slut:
5	Kommunikation og kontakter Planlæg hvordan kommunikationen med leverandøren skal foregå, og oplys kontaktoplysninger til eventuelle øvrige parter som leverandøren skal kommunikere med.		Start: Slut:

