5 cases til gruppearbejde

Case A: SafeMommyShopper

Hvad de laver: SafeMommyShopper er en online markedsplads, der tilbyder at formidle handler for de bedste og mest sikre produkter til børn. Virksomheden sigter mod at være den mest troværdige kilde for forældre, der ønsker at købe kvalitetsprodukter til deres børn. Man vil sine børn det bedste, og det er hvad SafeMommyShopper har fokus på.

Case B: AutoPartMasters

Hvad de laver: AutoPartMasters er en online auto-reservedelsforretning, der specialiserer sig i at matche reservedele med specifikke bilmodeller for at lette kundernes indkøbsoplevelse. De spottede et hul i markedet for 6 år siden, og har vækstet jævnt hvert år.

Case C: Jylland Vandforsyning

Hvad de laver: Jylland Vandforsyning er en mindre vandforsyningsvirksomhed, der leverer drikkevand til 4 kommuner i Jylland.

Case D: TimeTrackPro

Hvad de laver: TimeTrackPro udvikler et timeregistreringsværktøj, som er en Software as a Service (SaaS)-løsning, der hjælper virksomheder med at overholde den nye EU-lov, som stiller krav til nøjagtig og effektiv time-registrering af medarbejdere.

Case E: AC Byg TisvildeVirksomheden: AC Byg Tisvilde

Hvad de laver: AC Byg Tisvilde er en tømmerhandel og byggemarked, der leverer byggematerialer og værktøj til både private og professionelle kunder. De er en del af den landsdækkende kæde AC Byg, men drives som en franchise virksomhed.

Case A: SafeMommyShopper

Hvad de laver: SafeMommyShopper er en online markedsplads, der tilbyder at formidle handler for de bedste og mest sikre produkter til børn. Virksomheden sigter mod at være den mest troværdige kilde for forældre, der ønsker at købe kvalitetsprodukter til deres børn. Man vil sine børn det bedste, og det er hvad SafeMommyShopper har fokus på.

Antal ansatte: 25 medarbejdere

Teamets sammensætning: Teamet er relativt ungt, hvor de fleste medarbejdere er mellem 25-40 år. De består af en blanding af tekniske folk (udviklere), en håndfuld marketing- og kommunikationsspecialister, samt en hands-on ledelse som er de der fik ideen til markedspladsen, ledelsen er meget involveret i de daglige opgaver og sætter retningen for virksomheden. Teamet er ambitiøst og fokuseret på at bygge en succesfuld startup, som vokser efter planen og holder investorerne tilfredse.

Kultur inden for cybersikkerhed: SafeMommyShopper har traditionelt haft en lav bevidsthed om cybersikkerhed og har ikke prioriteret investeringer i sikkerhedsforanstaltninger. Det er ledelsen der sætter retningen, og de har mere fokus på profit-optimering og vækst, hvilket har været opmærksomhedspunkter fra investorerne.

Hvordan anses cybersikkerhed? Direktøren har det man kan kalde en laissez-faire holdning til cybersikkerhed og er mere optaget af vækst og ekspansion. Cybersikkerhed anses som en bagvedliggende opgave, hvilket har efterladt virksomheden sårbar over for potentielle trusler. Fokus har været på at vækste hurtigt og imødekomme investorenes krav, hvilket har ført til, at sikkerhedstiltag ofte er blevet nedprioriteret.

Hvor SafeMommyShopper kan være udsatte: På grund af deres lave niveau af investering i cybersikkerhed kan SafeMommyShopper potentielt set være sårbare over for trusler som phishing-angreb rettet mod kunders konti, malware-inficerede betalingstransaktioner og datalækager på grund af manglende sikkerhedsforanstaltninger. Som en online markedsplads, hører de under NIS2-direktivet, og derfor kan man vurdere at disse risici er betydelige og kan have alvorlige konsekvenser for både virksomheden og kunderne.

Ansvar for cybersikkerhed: En softwareudvikler i det tekniske team. har fået ansvaret for cybersikkerheden i SafeMommyShopper, men bruger størstedelen af sin tid på produktudvikling. Med et stramt roadmap for de næste seks måneder, hvor nye features skal lanceres, har medarbejderen gentagne gange nævnt for deres CEO, at der er behov for en mere dedikeret ressource eller et team til at tackle cybersikkerhedsudfordringer. Disse bekymringer er dog blevet overset til fordel for vækstrelaterede mål.

Planer om vækst: SafeMommyShopper har planer om at styrke deres digitale tilstedeværelse og lancere nye online transaktionstjenester, der gør det nemmere at gennemføre handler og imødekomme kundernes behov for en nem og sikker handelsoplevelse. Med en målsætning om at sælge virksomheden inden for de næste otte år, har de sat ambitiøse vækstmål og planer om at udvide til Norden i samarbejde med deres investorer.

Case B: AutoPartMasters

Virksomheden: AutoPartMasters

Hvad de laver: AutoPartMasters er en online auto-reservedelsforretning, der specialiserer sig i at matche reservedele med specifikke bilmodeller for at lette kundernes indkøbsoplevelse. De spottede et hul i markedet for 6 år siden, og har vækstet jævnt hvert år.

Antal ansatte: 25 medarbejdere

Teamets sammensætning: Teamet er ungt, dynamisk og består primært af lager-, fragt- og pakningspersonale. Ledelsen er hands-on og udvikler selv den digitale platform med assistance fra et par udviklere. Platformen er kritisk for virksomhedens vækststrategi - da det er her kerneydelsen ligger - Uden deres digitale platform har de ikke en forretning.

Kultur inden for cybersikkerhed: Cybersikkerhed er ikke blevet prioriteret i AutoPartMasters. Fokus har været på vækst og udvikling af den digitale platform for at tiltrække større markedsaktører og potentielt blive opkøbt. Der er ingen i virksomheden som har en naturlig interesse for dette, eller ser truslerne tydeligt.

Hvordan anses cybersikkerhed? Ledelsen har en laissez-faire holdning til cybersikkerhed, i det deres hovedfokus har været på vækst og optimering af kundeoplevelsen. Dette har resulteret i utilstrækkelige sikkerhedsforanstaltninger, hvilket gør virksomheden sårbar over for angreb.

Hvor AutoPartMasters kan være udsatte: Uden passende sikkerhedsforanstaltninger kan AutoPartMasters være sårbar over for fx phishing-angreb, malware, og datalækager. Specielt deres online betalingssystemer og kundedata kan blive mål for cyberkriminelle, eller måske endda konkurrenter.

Ansvar for cybersikkerhed: Der er ingen dedikeret medarbejder til cybersikkerhed. Udviklerne, der hjælper til, med arbejdet på platformen, har nævnt en gang eller 2 behovet for sikkerhedsforanstaltninger, men disse forslag bliver ofte overset til fordel for funktionalitets- og vækstfokuserede opdateringer af ledelsen/ejerne.

Planer om vækst: AutoPartMasters planlægger at udvide deres digitale platform og integrere avancerede tekniske løsninger for at forbedre kundernes evne til at matche reservedele med deres biler. De har oplevet markant vækst de sidste tre år og sigter efter at blive solgt til en større aktør på markedet indenfor de næste 5 år.

Case C: Jylland Vandforsyning

Virksomheden: Jylland Vandforsyning

Hvad de laver: Jylland Vandforsyning er en mindre vandforsyningsvirksomhed, der leverer drikkevand til 4 kommuner i Jylland.

Antal ansatte: 30 medarbejdere

Teamets sammensætning: De fleste medarbejdere er over 50 år og har arbejdet i virksomheden i mange år og har avanceret løbende i deres opgaver. Der er en 50/50 fordeling på køn. De fleste arbejder med daglige operationelle opgaver og vedligeholdelse af vandforsyningssystemerne.

Kultur inden for cybersikkerhed: Der er lav bevidsthed og forståelse for cybersikkerhed i Jylland Vandforsyning. Medarbejderne er usikre på, hvad NIS2-direktivet indebærer, og hvad de konkret skal gøre for at opfylde kravene, dog er de blevet gjort opmærksom på det via telefonsælgere, netværk m.m. - så de ved det er noget de bør være mere obs omkring.

Hvordan anses cybersikkerhed? Cybersikkerhed anses som en uklar og sekundær prioritet. Ledelsen har ikke taget konkrete skridt for at styrke sikkerheden, selvom de er begyndt at modtage flere salgsopkald fra virksomheder, der tilbyder hjælp med cybersikkerhed. Den manglende handling, bunder nok også i deres mangel på viden om feltet, og svært ved at vide hvor de skal starte.

Hvor Jylland Vandforsyning kan være udsatte: Med en mangel på dedikerede sikkerhedsforanstaltninger er Jylland Vandforsyning sårbar over for cyberangreb, der kan kompromittere vandforsyningens kontrolsystemer. Dette kan føre til serviceafbrydelser eller forurening af vandforsyningen.

Ansvar for cybersikkerhed: Der er ingen specifik medarbejder ansvarlig for cybersikkerhed. Den generelle IT-støtte bliver håndteret af en ekstern leverandør, der ikke har fokus på cybersikkerhed. Ledelsen begynder at blive nervøse over den stigende mængde salgsopkald fra sikkerhedsleverandører og erkender behovet for at tage aktion.

Planer om vækst: Der er ingen specifikke planer om vækst, men der er et øget fokus på at sikre pålidelig og sikker vandforsyning. Virksomheden indser behovet for at opdatere deres systemer og procedurer for at opfylde NIS2-kravene og beskytte deres kritiske infrastruktur mod potentielle cybertrusler.

Case D: TimeTrackPro

Virksomheden: TimeTrackPro

Hvad de laver: TimeTrackPro udvikler et timeregistreringsværktøj, som er en Software as a Service (SaaS)-løsning, der hjælper virksomheder med at overholde den nye EU-lov, som stiller krav til nøjagtig og effektiv time-registrering af medarbejdere.

Antal ansatte: 12 medarbejdere

Teamets sammensætning: Teamet består af et lille, men meget erfarent ingeniørteam, som tidligere har arbejdet med produktudvikling for store danske virksomheder (Siemensa, NordLight, ArloFoodies). Derudover har de ansat 2 sælgere, som skal hjælpe med at drive salget, tiltrække samt onboarde nye kunder.

Kultur inden for cybersikkerhed: På grund af teamets baggrund og erfaring med at arbejde for store virksomheder, har TimeTrackPro en høj bevidsthed om vigtigheden af cybersikkerhed. De er opmærksomme på de potentielle risici og har implementeret basis sikkerhedsforanstaltninger, men er stadig i gang med at finde den rette balance mellem udvikling og sikkerhed, og hvor meget det bør vægtes for at det ikke går ud over bundlinjen. Selvom de er bevidste omkring det, er det ikke helt realiseret - da der er meget fokus på at levere på produkt-features, så det kan nå at blive klar jvf roadmap.

Hvordan anses cybersikkerhed? Direktøren og teamet ser cybersikkerhed som en nødvendighed og en potentiel konkurrenceparameter. De forstår, at hvis de skal tiltrække store kunder, især C20-virksomheder, skal de kunne dokumentere robuste sikkerhedsforanstaltninger og overholdelse af relevante love og reguleringer, herunder NIS2-direktivet.

Hvor TimeTrackPro kan være udsatte: Som leverandør til store virksomheder, der er underlagt NIS2-direktivet, er TimeTrackPro under øget pres for at sikre, at deres løsninger er sikre og pålidelige. Dette inkluderer beskyttelse mod datalækager, sikring af systemintegritet og beskyttelse mod cyberangreb. Hvis deres system kompromitteres, kan det have alvorlige konsekvenser for både TimeTrackPro og deres kunder.

Ansvar for cybersikkerhed: Den tekniske leder har hovedansvaret for cybersikkerhed. Han har et ønske om regelmæssige sikkerhedsgennemgange og opdateringer for at sikre, at de lever op til de højeste standarder. Men der er ikke helt medvind til at allokere tid til dette, han mener dog det er nødvendigt næste gang at de rejser kapital.

Planer om vækst: TimeTrackPro har store ambitioner om vækst og planlægger at rejse kapital senere. For at tiltrække investorer forventer de at kunne dokumentere, at de har en række C20-virksomheder som kunder.

De skal finde en måde de kan differentiere dem fra konkurrenterne og gøre dem mere attraktive for både kunder og investorer. De er blevet bevidste om, at øget pres på leverandørstyring betyder, at de skal kunne demonstrere robuste sikkerhedsforanstaltninger for at opfylde kravene fra deres store kunder, og er derfor også blevet i tvivl om vægtningen er den rigtige.

Case E: AC Byg TisvildeVirksomheden: AC Byg Tisvilde

Hvad de laver: AC Byg Tisvilde er en tømmerhandel og byggemarked, der leverer byggematerialer og værktøj til både private og professionelle kunder. De er en del af den landsdækkende kæde AC Byg, men drives som en franchise virksomhed.

Antal ansatte: 70 medarbejdere

Teamets sammensætning: Størstedelen af medarbejderne er butiksmedarbejdere, som står for kundeservice, salg og lagerarbejde. Derudover er der flere administrative medarbejdere, der håndterer kontoropgaver og bogholderi.

IT-infrastruktur: AC Byg Tisvilde har adgang til en række fælles systemer og databaser, som drives og vedligeholdes af hovedkontoret for AC Byg. De har ingen IT-medarbejdere i butikken og trækker derfor på hovedkontorets IT-kompetencer.

Ejeren: Gert, 55 år **-** er erfaren i byggebranchen og ved, hvordan man driver en butik effektivt. Hans kendskab til cybersikkerhed er dog meget begrænset. Han er ikke ligeglad, men han har ingen bevidsthed om, at cybersikkerhed kan have en betydelig betydning for hans butik, og det er derfor hellere ikke en prioritet.

Kultur inden for cybersikkerhed: Cybersikkerhed er ikke en prioritet i butikken i Tisvilde. Der er ingen bevidsthed om potentielle trusler eller vigtigheden af at beskytte digitale aktiver. Fokus er primært på at levere god kundeservice og drive butikken effektivt.

Hvordan anses cybersikkerhed? Gert har ikke overvejet cybersikkerhed som en vigtig faktor for hans butik. Han har tillid til, at hovedkontoret håndterer de nødvendige IT- og sikkerhedsforanstaltninger, men han er ikke klar over de specifikke risici, som butikken står overfor.

Hvor AC Byg Tisvilde *kan* være udsatte: På grund af manglende lokal bevidsthed og initiativer omkring cybersikkerhed er butikken sårbar over for flere typer af trusler:

Phishing-angreb: Medarbejdere kan blive mål for phishing-forsøg, hvilket kan føre til kompromittering af personlige oplysninger eller adgang til virksomhedens systemer.

Malware: Uden lokal sikkerhedsuddannelse og procedurer kan butikken være modtagelig for malware, der kan forstyrre operationer eller kompromittere kundedata.

Datalækager: Adgang til fælles systemer og databaser betyder, at en sikkerhedsbrist i butikken kan påvirke hele kæden.

Ansvar for cybersikkerhed: Det er hovedkontorets ansvar at håndtere IT-sikkerheden, men der er ingen dedikeret medarbejder i butikken til at overvåge eller håndtere lokale sikkerhedsproblemer. Gert og hans team er afhængige af hovedkontorets retningslinjer og support.

Planer om vækst: Butikken i Tisvilde har ingen specifikke planer om vækst udover den naturlige vækst, der kommer med øget kundeflow og udvidelse af produktudvalget. De fokuserer på at opretholde et højt serviceniveau og sikre, at kunderne får den bedste oplevelse.Ved at være en del af en større kæde, kan butikken i Tisvilde drage fordel af

centraliserede sikkerhedstiltag fra hovedkontoret, men det er også vigtigt, at Gert og hans team bliver mere bevidste om cybersikkerhedsrisici og følger de retningslinjer og procedurer, der er sat op for at beskytte butikken og deres kunder.