Bilag 1 - Kravspecifikation

Indholdsfortegnelse

1. KRAV

1.1 OVERVÅGNING AF KUNDENS IT-SYSTEM

Leverandøren skal overvåge alle Kundens netværksforbundne enheder med henblik på at identificere eventuelle uregelmæssigheder.

Leverandørens løsning skal være en standard løsning.

Kunden skal i Aftalens løbetid have online adgang til Løsningen

Løsningen skal benytte kundens eksisterende installation af Endpoint Security (Cisco AMP).

Leverandøren skal levere overvågning 24/7, hele året, og Leverandøren skal i tilfælde af uregelmæssigheder, levere øjeblikkelig respons og analyse af uregelmæssighederne.

Det er et krav, at leverandøren registrerer en uregelmæssighed i løbet af 5 minutter og reagerer på uregelmæssigheden i indenfor 30 minutter fra registreringen enten ved at eskalere til Kundens IT-afdeling (i løbet af aftalte dagtimer) eller ved at respondere og håndtere uregelmæssigheden i forhold til aftalt procedure (f.eks. lukke en brugerkonto eller lign).

Leverandøren skal en gang om måneden, inden månedens udgang, skriftligt rapportere, at disse servicemål bliver overholdt. Leverandørens rapporter gennemgås hver tredje måned på et styregruppemøde.

Leverandøren skal gemme overvågningsdata i minimum 6 måneder for at sikre sporbarhed tilbage i dette tidsrum.

1.2 KUNDENS IT-ARKITEKTUR OG ENHEDER

Kundens nuværende IT-arkitektur er primært baseret på on-premise løsninger.

Nedenstående er en ikke komplet liste over eksempler på Kundens eksisterende enhedstyper som skal overvåges af Leverandøren igennem Løsningen:

- Servere (Vmware): 174
- Klient- Pc'er: 16002.06 Leveringskontrakt (udkast 09.11.22)
- IPhone: 140
- Firewall: 2
- Switche: 13
- Trådløse: 1
- Brugere: 204

Servere og netværksudstyr befinder sig på tre lokationer i hhv. København, Århus og et eksternt datacenter.

Klient-PC 'er er bærbare PC'er, der kan forbinde sig til det interne netværk via VPN. De er tilsluttet en hybrid AD mellem on-premise og Office365, hvor Exchange og Intune også benyttes.

1.3 RÅDGIVNING

Leverandøren skal stille et dedikeret team på 2 navngivne IT-sikkerhedsspecialister til rådighed for Kunden. Leverandørens medarbejdere skal, efter anmodning fra Kunden, rådgive og sparre med Kunden vedrørende alle aspekter af IT-sikkerhed. Rådgivningen skal baseres på Kundens

til enhver tid aktuelle IT-infrastruktur. Kunden skal have en ubegrænset adgang til Leverandørens medarbejdere.

Leverandørens IT-sikkerhedsspecialister skal være senior konsulenter som har dokumenterbar erfaring med det procesmæssige, tekniske og aktuelle trusselsniveau i forhold til Kundens profil.

IT-sikkerhedspecialisterne skal være i stand til løbende på opfordring og også proaktivt at rådgive om gode procedurer og konkrete tekniske løsninger for at undgå angreb og evt. rydde op efter angreb dvs. proaktiv bekæmpelse af hackere, ransomware DDOS-angreb o. lign. Det vil bl.a. være ifm arbejde med CIS20 kontroller.

Det er et krav, at disse IT-sikkerhedspecialister løbende er opdateret på nyeste standarder og viden inden for cybersikkerhed som er relevant for kundens miljø og geografi.

Et eksempel på rådgivning fra Leverandørens medarbejdere er implementering af CIS20, og hvilke forbedringer der bør indføres i en prioriteret rækkefølge. Et andet eksempel er rådgivning om sikkerhed i forbindelse med indførelse nye produkter/services hos Kunden. Endvidere vil det betragtes som positivt, hvis Leverandørens medarbejdere proaktivt og løbende kan levere status på det aktuelle IT-sikkerheds billede i verden, således at Kunden præventivt kan indføre tiltag for at mindske risici.