CYBER PARTNERS

Sikkerhedstjek

CYBER PARTNERS

SIKKERHEDSTJEK

CSSLP ISC2 CISSP ISC2

Indledning

Et sikkerhedstjek er et vigtigt første skridt i at forstå og styrke sikkerheden omkring virksomhedens IT-setup - særligt når løsningen i høj grad er baseret på cloudtjenester som f.eks. Microsoft 365. I en cloudbaseret virkelighed, hvor infrastrukturen styres af leverandører, ligger ansvaret for den konkrete konfiguration og sikkerhedsopsætning hos virksomheden selv.

Selvom de fleste større cloududbydere tilbyder dokumentation i form af f.eks. SOC 3-rapporter, siger disse intet om, hvordan jeres specifikke opsætning er sat op og sikret. Det er netop her et sikkerhedstjek bliver relevant

Der skal afdækkes eventuelle konfigurationsfejl, manglende kontroller eller områder, hvor opsætningen kan styrkes i forhold til best practices og gældende krav.

Sikkerhedstjekket består af en **struktureret analyse** af virksomhedens konfigurationer og opsætninger på tværs af cloudtjenester og relevante systemer. Det giver et konkret indblik i, hvor godt jeres løsning er beskyttet mod trusler, og hvor der eventuelt bør sættes ind.

I det følgende præsenterer vi vores tilgang, metode og de leverancer, der følger med et sikkerhedstjek.

Pris og beskrivelse

Sikkerhedstjek - Indhold, pris og tidsplan

Et sikkerhedstjek fungerer som et eftersyn af jeres IT-miljø, hvor vi gennemgår de mest kritiske kontroller for at give jer et klart og brugbart overblik over sikkerhedsniveauet - og hvor der er behov for forbedringer. Formålet er at identificere de mest oplagte sårbarheder, før nogen udnytter dem.

Omfang:

- Ca. 30 nøje udvalgte kontroller baseret på branchestandarder, bedste praksis og cloud-udbydernes egne sikkerhedsanbefalinger.
- Kontrollerne dækker typisk områder som adgangsstyring, patchniveau, netværkssegmentering, logging og backup-rutiner.
- Der tages også højde for eventuelle særlige ønsker eller risikoområder.

Leverancer:

- 1 dags on-site gennemgang med en erfaren sikkerhedskonsulent
- Rapport leveret senest 5 arbejdsdage efter besøget, som indeholder:
  - Et kort executive summary med de vigtigste konklusioner (på dansk)
  - En detaljeret kontrolmatrix med vurderinger og anbefalinger (på engelsk)
- 1-times online møde til gennemgang og sparring

Tidsplan:

- **Analysefase:** Gennemføres som udgangspunkt inden for 1-2 uger fra opstart
- **Rapportlevering:** Senest 5 arbejdsdage efter analysen
- **Afsluttende møde:** Aftales umiddelbart efter levering

Tidsplanen tilpasses altid efter virksomhedens behov og tilgængelighed.

Resultat:
En overskuelig og handlingsrettet tjekliste, der viser hvordan jeres nuværende setup står - og hvad der bør prioriteres for at øge sikkerheden. Alt sammen leveret i et sprog og format, der kan omsættes direkte til jeres drift.

19.000 DKK ekskl. moms

Hvorfor vælge Cyber Partners?

Vi arbejder som hackere, ikke som traditionelle konsulenter. I stedet for at gennemgå tjeklister, udfører vi realistiske simulationer, der afspejler de trusler, I faktisk står overfor. Resultatet er konkret viden frem for generiske rapporter, og I modtager praktiske handlingsplaner, som I kan tage i brug med det samme. Hele indsatsen er nøje tilpasset jeres branche, systemer og specifikke behov.

CYBER PARTNERS

Enkelt, forståeligt og tilgængeligt

Se mere på cyberpartners.dk