Deloitte.

Draware

IT Security Review™

Læs mere på security.draware.dk

Indholdsfortegnelse

CIS 20 Critical Security Controls

Draware IT Security Review™ er baseret på Center for Internet Security's 20 Critical Security Controls®. Kontrollerne er rangeret efter kritikalitet og er derfor et oplagt rammeværk at anvende, når organisationer ønsker en konkret og målrettet indsats for IT-sikkerheden.

Basale kontroller

1. AUTORISEREDE/UAUTORISEREDE NODER
2. AUTORISERET/UAUTORISERET SOFTWARE
3. KONTINUERLIG SÅRBARHEDSVURDERING
4. MINIMERET BRUG AF ADMINRETTIGHEDER
5. KONFIG. AF HARD- OG SOFTWARE

Essentielle kontroller

6. OVERVÅGNING AF AUDIT LOGS
7. E-MAIL- OG BROWSERBESKYTTELSE
8. MALWAREFORSVAR
9. BEGRÆNSNING OG KONTROL AF NETVÆRK
10. MULIGHED FOR GENDANNELSE AF DATA
11. KONFIG. AF NETVÆRKSNODER
12. PERIMETERBESKYTTELSE
13. DATABESKYTTELSE
14. ADGANG EFTER NØDVENDIGHED
15. KONTROLLERET ADGANG TIL WiFi
16. OVERVÅGNING AF BRUGERKONTI

Organisatoriske kontroller

17. AWARENESSTRÆNING
18. SIKKERHED PÅ APPLIKATIONER
19. CYBERBEREDSKAB
20. PENETRATION TESTS

CIS 20 Critical Security Controls og ISO

Draware IT Security Review™ er baseret på Center for Internet Security's 20 Critical Security Controls - et rammeværk udviklet med formålet at hjælpe organisationer implementere de mest passende IT-sikkerhedstiltag. Men hvad er i grunden forskellen på ISO 2700x og CIS 20 CSC?

Compliance og konsensus

ISO27001 er et compliance rammeværk (her kan organisationen blive certificeret af et officielt certificeringsorgan). CIS Kontroller er et konsensus rammeværk (her kan organisationen ikke blive certificeret men måle, om den lever op til de relevante kontroller). ISO27001 er sidste revideret i 2013, mens CIS kontrollerne revideres en eller flere gange om året.

Risikomanagement

ISO27001 bygger på princippet om risikomanagement, men beskrivelsen af risikomanagement ligger i ISO 31000. CIS kontroller indeholder CIS RAM – Risk Assessment Method. CIS kontroller indeholder desuden et komplet sæt af KPI relateret til de relevante risici.

Kontroller og tiltag

ISO27001 beskriver principperne for, hvad der skal udføres af organisatoriske og tekniske tiltag, og SOA giver scopet relevans. Der er ingen prioritering af kontroller (processer/procedurer). ISO27002 beskriver, hvad der skal gøres for at leve op til alle/SOA (Statement of Applicability) relevante principper i ISO27001. CIS 20 forklarer i detaljer hvordan tekniske kontroller (66/114 Annex A kontroller) skal udføres på en prioriteret og målbar måde.

Vores add-on analyser

Kontrolprofil

En dybdegående GAP-analyse som danner baggrund for arbejdet med kommende IT-sikkerhedsprojekter og grundlaget for en konkret accepteret risiko. Profilen er baseret på CIS® 20 CSC og 66 ud af 114 Annex A ISO 27001/2 kontroller.

Procesprofil

Denne profil sikrer en korrekt beskrivelse af processerne for organisationens mitigeringstiltag. Her refereres til kontrolprofilen. Profilen danner et overblik over samspillet mellem medarbejdere, roller, mitigeringstiltag og kontroller.

Ledelsesprofil

Profilen forankrer IT-sikkerhedstiltag hos ledelsen på en konkret og målbar måde. Ledelsesprofilen muliggør en vurdering af sikkerhedsniveauet ud fra udvalgte processer og områder med ledelsens prioritering. Samtidigt gør ledelsesprofilen det muligt at præsentere de vigtigste nøgletal (KRI/KPI) enkelt og visuelt.

Organisationsprofil

En måling og sammenligning af sikkerhedsniveauet I organisationens afdelinger. Profilens tekniske del gør det nemt hhv. at udbrede bedste praksis og awarenesstræning efter afdelingernes individuelle behov.

Risikoprofil

Profilen hjælper med at omsætte Sikkerhedsprofilen til en risikoanalyse og korrelere projekternes nødvendighed for at mitigere den fundne risiko til et acceptabelt niveau og ressourceforbrug. Profilen gør en prioritering af budgetallokeringer nemmere for ledelsen.

Behandlingssikkerhed

Profilen beregner det nuværende og ønskede risikoniveau for organisationens persondatabehandling. Samtidigt dannes et overblik over behandlingsaktiviteter og relevante tekniske og organisatoriske tiltag anvises med målet om at opfylde lovkravet om risikobaseret behandlingssikkerhed.

ISO-profil

Profilen danner en praktisk vejledning og et fundament for ISO27001 certificering. Det inkluderer bl.a. en måling af ISO27001 parathed, nøglepersoner, nøgledokumenter, overblik og kommunikation af ISO27001 til ledelsen.

Awarenessprofil

Profilen danner grundlaget for et awarenessprogram, der ikke alene er tilpasset organisationen men også er effektivt og målbart. Profilen fungerer herudover som essentiel dokumentation.

Leverandørprofil

Ved at stille krav til underleverandører/partnere i form af en prædefineret IT-sikkerhedsprofil kan leverandøren sikre og dokumentere, at underleverandører og partnere ikke udgør en risiko for organisationen.

Hvad får du ud af Draware IT Security Review?

Med Draware IT Security Review får din virksomhed et grundigt og konkret overblik over jeres ITsikkerhed. Analysen danner grundlag for dialog med virksomhedens ledelse omkring ønsket ITsikkerhed og accepteret risikoniveau.

Det er vores erfaring, at organisationer efter at have foretaget Draware IT Security Review:

1. Forstår deres nuværende IT-sikkerhedsprofil (hvilket ofte er en profil med adskilligt flere brister end forventet).
2. Forstår hvad der skal til – både teknisk og organisatorisk – for at opnå en IT sikkerhedsprofil, der passer til den aktuelle risiko.
3. Forstår den store forskel på IT-sikkerhed, der bygger på gode intentioner og IT-sikkerhed, der bygger på kontroller.
4. Forstår hvilke af de nuværende IT-sikkerhedsløsninger, der skal implementeres bedre og suppleres med organisatoriske kontroller, hvilke løsninger, der overlapper og hvilke løsninger, der mangler.
5. Får et nyt klippe-solidt grundlag for at træffe informerede beslutninger om IT-sikkerhed.
6. Får et værktøj/en metode, der hjælper med at formidle IT-sikkerhedsbudskabet og risikoen til ledelsen, som derefter kan træffe beslutningerne om tildeling af de nødvendige ressourcer på et informeret grundlag (IT-sikkerhed der matcher den accepterede risiko).

Hvordan foretages Draware IT Security Review?

Vi sidder on-site sammen med din organisations ledende medarbejdere fra IT afdelingen i 2-3 dage. Her foretages de nødvendige målinger og et nyt niveau af sikkerhed målsættes og formuleres.

Draware udarbejder derefter en præsentation, som du internt i organisationen kan bruge til at synliggøre den aktuelle risiko for ledelsen. Bl.a. på basis af dette dokument kan ledelsen så træffe en informeret beslutning om, hvilket niveau af risiko man vil acceptere og bevilge de nødvendige ressourcer.

Kontakt os

security.draware.dk
www.draware.dk

chrschmidt@deloitte.dk

+45 36 10 20 30 /
30 93 60 09

Weidekampsgade 6,
DK-2300 København S

Deloitte.