PRODUKTBLAD / CYBER SECURITY

CONSCIA SECURITY ASSESSMENT

Få det store sikkerhedsoverblik og en prioriteret plan med CIS-kontrollerne

conscia

Hvorfor CIS-kontrollerne?

For at få skabt en fælles anerkendt reference-ramme omkring IT-sikkerhed og gøre indsatsen målbar. Rammen bygger på flere store virksomheders erfaring med angreb og processer.

Hvad er CIS-kontrollerne?

Center for Internet Security (CIS) kontrollerne dækker over en række håndgribelige og operationelle kontroller, som er udledt af mange års erfaring med bekæmpelse af cyberangreb.

Kontrollerne er udviklet af førende sikkerheds-eksperter fra hele verden og raffineres, prioriteres og valideres med jævne mellemrum.

Retningslinjerne består af 18 kritiske sikkerheds-kontroller, Critical Security Controls - CSC, som implementeres for at opdage og forhindre angreb.

Kontrolelementerne er designet, så primært automatiserede løsninger kan anvendes til at implementere, håndhæve og overvåge kontrollerne.

Sikkerhedskontrollerne giver anbefalinger til cybersikkerhed, skrevet i et sprog, der er let at forstå.

Kontrollerne er prioriterede, så de let kan anvendes til at lave en struktureret plan for cybersikkerhed.

Ved at anvende kontrollerne opnår I blandt andet overblik over, hvad der skal prioriteres for at højne cybersikkerheden.

Ved blot at gennemføre de 6 første kontroller kan I, ifølge Center for Internet Security, mindske sandsynligheden for en sikkerhedsbrist med omkring 85%.

CIS Controls

Version 8

1	Inventory and Control of Enterprise Assests	10	Malware Defenses
2	Inventory and Control of Software Assets	11	Data Recovery
3	Data Protection	12	Network Infrastructure Management
4	Secure Configuration of Enterprise Assets and Software	13	Network Monitoring and Defense
5	Account Management	14	Security Awareness and Skills Training
6	Access Control Management	15	Service Provider Management
7	Continuous Vulnerability Management	16	Application Software Security
8	Audit Log Management	17	Incident Response Management
9	Email and Web Browser Protections	18	Penetration Testing

conscia

Hvordan forløber et Conscia Security Assessment?

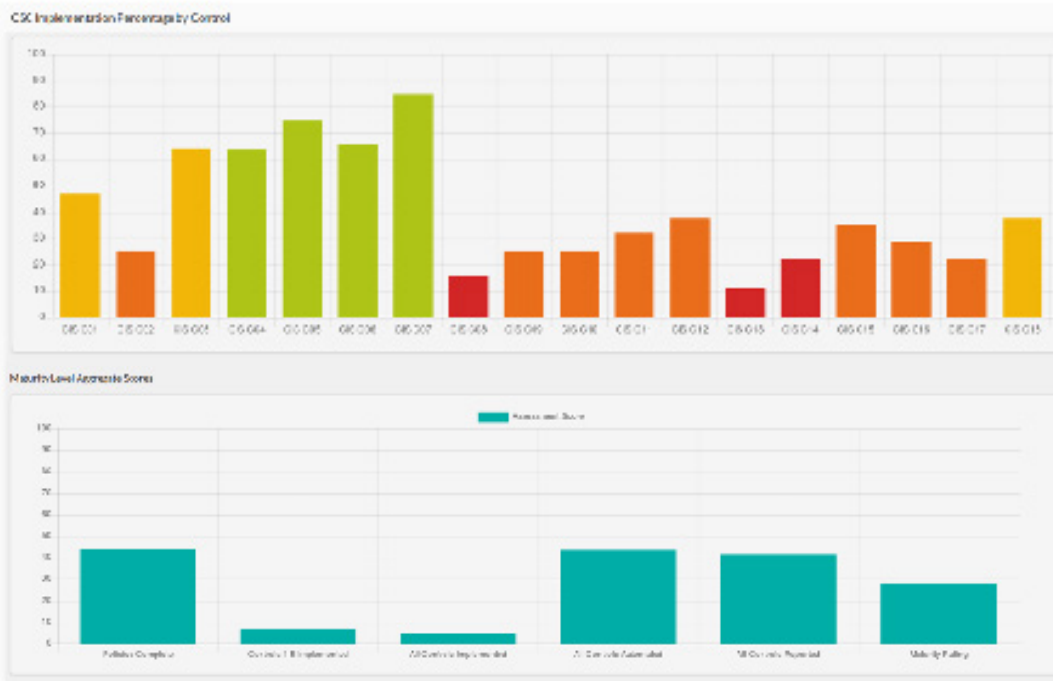
Conscia Security Assessment-forløbet varierer fra projekt til projekt, men indeholder en række faste elementer:

Workshop - Afhængigt af behov kan en workshop strække sig over alt fra en til tre dage. På workshoppen deltager personer med indsigt i det nuværende it-sikkerhedssetup, eksempelvis en CISO, sikkerhedsarkitekter, sikkerhedsdriftsansvarlige og netværksarkitekter. Baseret på virksomhedens risikoprofil gennemgår projektlederen fra Conscia de 18 hovedkontroller og 153 beskyttelsesforanstaltninger med hver af de ansvarlige i interviewsessioner. Formålet med workshoppen er at få belyst de områder, hvor virksomhedens nuværende it-sikkerhedsarbejde er henholdsvis mindst og mest robust

Rapport - Projektlederen udarbejder på baggrund af workshoppen en Security Assessment-rapport. Rapporten giver et her-og-nu-overblik over sikkerhedsniveauet i virksomheden og angiver resultatet med en sikkerhedsscore. Rapporten kommer også med anbefalinger til, hvor virksomheden bør sætte ind med tiltag, og hvilken effekt disse tiltag vil have for den samlede sikkerhedsscore

Afrapporteringsmøde - Conscia fremlægger resultaterne af rapporten, så virksomheden får tegnet et tydeligt billede af, hvordan de kan forbedre deres sikkerhedsprogram

Forløbet tager 3-6 uger



Samlet kontrol implementering og modenhed.

Vil du høre mere om CIS-kontrollerne og Conscias Security Assessment?

Kontakt Jesper Hessner, Sales Director
Mail: jhs@conscia.com
Mobil: +45 31 31 78 89

Læs mere på conscia.dk/cis-kontroller