Grundlæggende IT-sikkerhed: "Cyberhygiejne" baseret på CIS CSC #1-6 (ikke vægtet)

DeciMax A/S
Your Security Is Our Passion

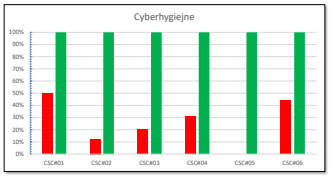
Er dette et problem?	
Nej/Utilstrækkelig	54%
Delvist/Mellem	32%
Ja/Tilstrækkelig	14%

Nej/Utilstrækkelig, 54% | **Delvist/Mellem, 32%** | **Ja/Tilstrækkelig, 14%**

Spørgsmål	Start	Slut	CSC#	Beskrivelse af problem	Kontrol	Nuværende score	Ønsket score
SPG: 01	✓	✓	#01	Der findes en liste med kendte, autoriserede noder, som må findes på netværket, i én samlet inventarliste.	CSC#01	50%	100%
SPG: 02	?	✓	#01	Uautoriserede noder forhindres aktivt i at få adgang til netværket.			
SPG: 03	?	✓	#01	Hele netværket scannes kontinuerligt for nye noder, og der er en aktiv proces, som håndterer de nye noder.			
SPG: 04	✗	✓	#01	Der findes en dokumenteret og implementeret proces for CSC #01 med tilhørende KPI.			
SPG: 05	✗	✓	#02	Der findes en liste med kendt, autoriseret software, som må findes på netværket, i én samlet inventarliste (samme som i SPG 01).	CSC#02	13%	100%
SPG: 06	✗	✓	#02	Uautoriseret software forhindres aktivt i at eksekvere.			
SPG: 07	?	✓	#02	Hele netværket scannes kontinuerligt for nyt software, og der er en aktiv proces, som håndterer softwaren.			
SPG: 08	✗	✓	#02	Der findes en dokumenteret og implementeret proces for CSC #02 med tilhørende KPI.			
SPG: 09	?	✓	#04	Hele netværket scannes regelmæssigt med en eller flere anerkendte sårbarhedsscannere.	CSC#03	20%	100%
SPG: 10	?	✓	#04	Sårbarheder rettes i prioriteret rækkefølge - både de, der kan patches (OS og tredjepart), og de, der kræver konfigurationsændringer.			
SPG: 11	✗	✓	#04	Der er særligt fokus på sårbarheder i kritiske systemer som webservere og databaser (og lign.).			
SPG: 12	✗	✓	#04	Der findes et risiko-feed og mitigation actions baseret på dette/disse feed/feeds vurderes.			
SPG: 13	✗	✓	#04	Der findes en dokumenteret og implementeret proces for CSC#04 med tilhørende KPI			
SPG: 14	✓	✓	#05	Alle servicekonti skal følge en specifik navnestandard.	CSC#04	31%	100%
SPG: 15	✗	✓	#05	Alle servicekonti skal automatisk skifte password mindst én gang hver 90. dag, men helst hver uge.			
SPG: 16	?	✓	#05	Alle servicekonti skal dokumenteres med en ejer, formål og tilknyttede systemer.			
SPG: 17	?	✓	#05	Servicekonti må ikke have RDP-rettigheder og må ikke være domain admins.			
SPG: 18	?	✓	#05	Alle servicekonti skal have komplekse passwords på mindst 14 karakterer (a-A, 0-1,5).			
SPG: 19	✗	✓	#05	Alle servicekonti skal have et unikt password.			
SPG: 20	✓	✓	#05	Alle administrative konti skal følge en specifik navnestandard.			
SPG: 21	?	✓	#05	Ingen administrativ konto må være ubrugt i mere end én måned. Så skal den disables eller fjernes.			
SPG: 22	✗	✓	#05	Alle administrative konti skal automatisk skifte password mindst én gang hver 30. dag, men helst hver uge.			
SPG: 23	✗	✓	#05	Alle administrative konti skal have komplekse passwords på mindst 14 karakterer (a-A, 0-1,5).			
SPG: 24	✗	✓	#05	Administrative konti må ikke være domain admins, og de må ikke lave RDP med en domain admin-konto.			
SPG: 25	✓	✓	#05	Alle administrative konti skal have et unikt password.			
SPG: 26	✗	✓	#05	Alle administrative opgaver skal udføres med 2-faktorautentifikation eller fra jump-servere.			
SPG: 27	✗	✓	#05	Alle lokale administratorkonti skal have et unikt, komplekst password - både på servere og klienter.			
SPG: 28	✗	✓	#05	**Ingen brugere må have lokal administrator-privilegier på klienten.**			
SPG: 29	✗	✓	#05	Lokal administrator-kontoen "Administrator" skal omdøbes og disables (SID -500).			
SPG: 30	✗	✓	#05	Der skal indføres en ny "decoy"-konto ved navn "Administrator" på servere og klienter.			
SPG: 31	?	✓	#05	**Medlemskabet af alle systemiske grupper skal godkendes mindst én gang om måneden.**			
SPG: 32	✓	✓	#05	Der skal alarmeres på alle ændringer i systemiske grupper.			
SPG: 33	✗	✓	#05	Der skal alarmeres ved brug af "Administrator"-kontoen (som er decoy).			
SPG: 34	✗	✓	#05	Der skal alarmeres ved forandringer i lokal administrator-gruppen på klienter.			
SPG: 35	✗	✓	#05	Der skal alarmeres på lockout af alle administrative konti.			
SPG: 36	?	✓	#05	Der skal alarmeres på administrative konti og servicekonti, som ikke følger navnestandarden.			
SPG: 37	?	✓	#05	Der skal rapporteres på alle administrative events.			
SPG: 38	✗	✓	#05	Der skal rapporteres på alle administrative password reset og change events.			
SPG: 39	?	✓	#05	Der findes en dokumenteret og implementeret proces for CSC #05 med tilhørende KPI.			
SPG: 40	✗	✓	#03	De eksisterende templates for hardware og software er scannet med en anerkendt sårbarhedsscanner og rettet.	CSC#05	0%	100%
SPG: 41	✗	✓	#03	De ksisterende templates for hardware og software er benchmarket med CIS 20 CSC Benchmarks og ligeledes konfigureret.			
SPG: 42	✗	✓	#03	Der findes en dokumenteret og implementeret proces for CSC #03 med tilhørende KPI.			
SPG: 43	?	✓	#06	Der logges aktivt fra alle relevante noder (fx servere, firewalls, WLC o.lign.) til ét centralt LMS.	CSC#06	44%	100%
SPG: 44	✗	✓	#06	Der logges aktivt fra alle klienter til ét centralt LMS.			
SPG: 45	?	✓	#06	Der logges aktivt fra alle relevante systemer (AD, databaser, web, DNS, DHCP og lign.) til ét centralt LMS.			
SPG: 46	✓	✓	#06	Alle devices har samme NTP-server og derfor samme tidsstempel.			
SPG: 47	✗	✓	#06	Logge gennemgås regelmæssigt for anormaliteter.			
SPG: 48	?	✓	#06	LMS-systemet er velimplementeret og kan betjenes aktivt af organisationen eller af en outsourcet service.			
SPG: 49	✗	✓	#06	Alarmer, regler og dashboards er opsat efter best practice (som minimum som i #08-10)			
SPG: 50	✓	✓	#06	Der findes en dokumenteret og implementeret proces for CSC #05 med tilhørende KPI.			

Kontrol	Nuværende status	Ønsket status	Kategori
CSC#01	50%	100%	Hardware inventory
CSC#02	13%	100%	Software inventory
CSC#03	20%	100%	Sårbarhedshåndtering
CSC#04	31%	100%	Administrative privilegier
CSC#05	0%	100%	Benchmarking
CSC#06	44%	100%	Logning/Auditing

Nuværende score	Ønsket score
26%	100%



Dedikio A/S

Tjekliste til administrative rettigheder

Bemærkninger

>>> Angiv dine valg i kolonne E "Svar": 0=nej, 1=delvist og 2=Ja. Er spørgsmålet ikke relevant, skrives 0 i kolonne D "relevans".

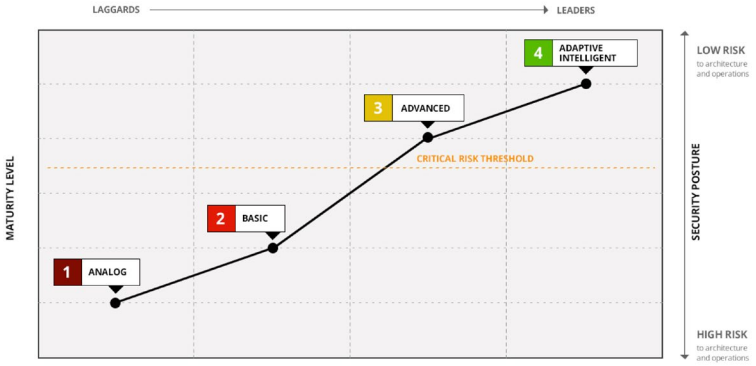
Kategori	Relevans	Start	Slut	Implementeret	Spørgsmål	Dine bemærkninger
Forank-ring	✗	✓	✓	FALSK	Forankring: Undersøg og få opbakning og ressourcer til nedenstående aktiviteter for målbart at nå den accepterede risiko inden for en given tidsramme	
	✓	✓	✓	SAND	Forankring: Foretag en PAM-vurdering, og opsæt en målsætning for organisationens fremtidige rejse mht. administrative rettigheder	
Begræns-ning	✓	✓	✓	SAND	**Begrænsning: Undersøg og begræns lokale admin-rettigheder på en struktureret måde (LAPS eller anden løsning)**	
	✓	!	✓	FALSK	**Begrænsning: Brug den administrative "Tiering"-model" – Tier 0,1,2 (0 = Critical, 1 = Members og 3 = End-devices)**	
	✓	!	✓	FALSK	Begrænsning: Indfør håndtering af/politik om passwords efter bedste praksis** (inkl. differentieret politik på forskellige grupper)	
	✓	✗	✓	FALSK	Begrænsning: Indfør tidsbestemt medlemskab af grupper*, hvor det er relevant og muligt	
	✓	✗	✓	FALSK	Begrænsning: Skift password på krbtgt***-kontoen min. en gang årligt	
	✓	!	✓	FALSK	**Begrænsning: Brug 2FA/MFA overalt, hvor det er muligt og relevant**	
Kontroller	✓	✓	✓	SAND	Kontroller: Undersøg og ensret AD og Azure (navngivning af admin-, service-, eksterne og brugerkonti)	
	✓	✓	✓	SAND	**Kontroller: Gå på jagt efter aktive konti med passwords sat til "never expire" – inklusive servicekonti og "dårlig praksis" på brugerkonti**	
	✓	!	✓	FALSK	**Kontroller: Undersøg og overvåg kritiske*** sikkerhedsgrupper i AD og Azure**	
	✓	!	✓	FALSK	Kontroller: Kontroller og miljøer non-conformity (skift mellem status, ændring og kontrol med miljøering)	
	✓	✗	✓	FALSK	Kontroller: Lav halvårligt (mindst) ACL review på dit AD	
	✓	✗	✓	FALSK	Kontroller: Lav halvårligt (mindst) en søgning efter skjulte objekter i AD	
Processer	✓	!	✓	FALSK	**Processer: Beskyt dine domain controllers (segmentering, backup/recovery, adgang, next-gen AV, beredskab)**	
	✓	!	✓	FALSK	Processer: Indfør en sund proces for oprettelse af nye medarbejdere og fratagelse af rettigheder for betroede medarbejdere	
	✓	✓	✓	SAND	Processer: Beskriv livscyklus for admin-, service-, eksterne og brugerkonti	
	✓	✗	✓	FALSK	Processer: Automatiser af oprydning i AD	
	✓	!	✓	FALSK	**Processer: Uddan brugerne målrettet og målbart i sikker håndtering af konti og adgangskoder**	
Overvåg-ning	✓	!	✓	FALSK	Overvågning: Sørg for logning efter bedste praksis	
	✓	!	✓	FALSK	**Overvågning: Overvåg tegn på intern og ekstern misbrug af rettigheder**	
	✓	!	✓	FALSK	Overvågning: Brug fx Microsoft ATA / ATP eller et tredjepartsværktøj som fx ManageEngine ADAudit eller StealthBits	
Egne kontroller, metoder, processer, idéer	✓			FALSK	Har vi tilstrækkelig viden om administrative rettigheder i Azure AD?	
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		
	✗			FALSK		

Dashboard

Forankring	Begrænsning
100%	42%
Kontroller	**Processer**
50%	50%
Overvågning	**Egne kontroller, metoder, p**
50%	50%
Nej svar	**Delis svar**
23%	50%
Ja svar	
27%	

PAM Maturity Model (Thycotic)

Stadie	Relevans	Score %	Måling / Beskrivelse	Compliance
Analog (ikke aktiv)	✓	100%	Papirbaseret adgangskode og legitimationssporing	95%
	✓	80%	Brug af standard adgangskoder	
	✓	100%	Ingen rotation af adgangskoder	
	✓	100%	Ingen eller minimale adgangskompleksitetskrav	
Basal (reaktivt)	✓	0%	Automatisk opdagelse af privilegeret konti	8%
	✓	10%	Arkivering af adgangskoder i et sikkert arkiv	
	✓	10%	Brug af passwords der ikke er standard	
	✓	10%	Multi-faktor godkendelse	
Avanceret (proaktiv)	✓	0%	Skjul / tilsløring af adgangskoder	2%
	✓	0%	Privilegeret session proxy	
	✓	0%	Dobbelt kontrol & 2-persons protokoller	
	✓	0%	Overvågning af sessioner	
	✓	0%	Spor af privilegeret aktivitet som ikke kan ændres og rev	
	✓	10%	Endpoint mindsteprivilege & applikationskontrol	
Adaptiv Intelligent (kontinuerlig forbedring)	✓	0%	Automatisk afvigelse og afhjælpning af anomali	0%
	✓	0%	Automatiseret privilegeret kontolivscyklusstyring	
	✗	0%	DevOps-arbejdsgang privilegeret kontoadministration	
#4	?		Inkluderer du privilegerede konti i din bredere it-cybersi	
	?		Opdager du automatisk privilegerede konti i din organis	
	?		Hvor mange af dine privilegerede konti bruger automati	
	?		Hvor mange af dine privilegerede konti gemmes i et sikk	
	?		Bruger du værktøjer til at forhindre, at adgangskoder bli	
	?		Håndhæver du 2FA eller MFA, der skal bruges med privil	
	?		Opretholder du en uforanderlig revisionsspor med privil	
	?		Har du en måde at automatisk opdage og svare på en at	
	?		Fjerner du automatisk privilegerede konti, der ikke læng	
	?		Bruger du et legitimationsstyringsværktøj under dine sol	
	?		Hvilken procentdel af noder/enheder er beskyttet af pri	



#5: Bedste praksis for Priviledge Account management (PAM) implementering		
Definer	**#1**	Start med at definere, hvad 'privilegeret adgang' betyder, og identificer, hvad en privilegeret konto er for din organisation. Det er forskellige for enhver virksomhed, så det er vigtigt, at du kortlægger, hvilke vigtige
Find	**#2**	Identificer dine privilegerede konti og implementer kontinuerlig opdagelse for at bremse privilegeret kontospredning, identificere potentielt misbrug af insider og afsløre eksterne trusler. Dette hjælper med at sikre
Administrer og beskyt	**#3**	Proaktivt styring og kontrol af privilegeret kontotilgang, planlægning af adgangskodedrejning, revision, analyse og styring af individuel privilegeret sessionaktivitet. For brugere af IT-administratorer, som er konti, skal du kontrollere adgangen og implementere superbrugerprivilegihåndtering for at forhindre, at angribere kører ondsindede applikationer.
Overvåg	**#4**	Overvåg og registrer privilegeret kontoaktivitet. Dette vil hjælpe med at håndhæve korrekt opførsel og undgå fejl. Hvis der sker en overtrædelse, hjælper overvågning af privilegeret kontobrug også digitale forensics med at
Opdag	**#5**	At sikre synlighed til adgangen og aktiviteten til dine privilegerede konti i realtid vil hjælpe med at få mistanke om kompromis og mulig misbrug af brugere. Adfærdsanalyse fokuserer på centrale datapunkter for at etablere individuelle brugerbaserlinjer, herunder
Svar	**#6**	Når en privilegeret konto overtrædes, er det ikke tilstrækkeligt at ændre adgangskoden eller deaktivere kontoen. Mens de var inde, kunne hackere have installeret malware og endda oprette deres egne privilegerede konti. Hvis en domæneadministratorkonto
Reager og auditer	**#7**	Hvis du løbende observerer, hvor privilegerede konti der bruges gennem revisioner og rapporter, vil det hjælpe med at identificere usædvanlig adfærd, der kan indikere brud eller misbrug. Automatiske rapporter hjælper med at spore årsagen til sikkerhedshændelser og demonstrerer overholdelse af politikker og forskrifter.