Indikation af organisationens sandsynlige sårbarhed relateret til ransomware og anden malware

Samlet risiko	Område	Måling	Risiko
75%	CIS 1-6	28	83%
	Klienten	24	56%
	Backup og data-beskyttelse	13	75%
	Modsvar	25	86%
	mTrends 2021 anbefalinger	78	75%

Cybersnack - anti-malware

Helt og fuldt	2	4%
Næsten dækkende	7	13%
Delvist	20	38%
Slet/stort set ikke	23	44%

Start herunder…

Risikoområde	Svar	Spørgsmål
CIS 1-6	3. Delvist	Er alle devices i organisationen opdaget og mitigeret med 802.1x / NAC
	4. Nej, slet ikke eller stort set ikke	Er alt software i organisationen opdaget og mitigeret med Application Whitelisting (fx ManageEngine DesktopCentral eller Application Control)
	4. Nej, slet ikke eller stort set ikke	Scannes hele netværket med en bedst-i-klasse sårbarhedsscanner (fx Tenable.IO eller .SC)
	3. Delvist	Rettes sårbarheder på servere og klienter (og alle OS) rettidigt - både Microsoft og 3rdie part (fx ManageEngine DesktopCentral)
	4. Nej, slet ikke eller stort set ikke	Er alle systemer, OS og devices opsat efter CIS benchmarks
	3. Delvist	Er der implementeret brug af mindste privilegier og sikker opsætning af AD/Azure AD (fx ManageEngine ADManager og ADAudit)
	4. Nej, slet ikke eller stort set ikke	Bruges der sikre passwords og granulerede passwords policies sammen med 2FA/MFA ved administrative opgaver og på Internet vendte services
	3. Delvist	Bruges logning aktivt til at opdage malware aktivitet efter bedste praksis
Klienten	2. Ja, næsten dækkende	Minimale rettigheder ved login og ingen mulighed for at brugeren kan tiltage sig admin rettigheder
	3. Delvist	**Et "bedst i klasse" anti-malware system som er sat korrekt op til at blokere trusler (fx Sophos, CrowdStrike, SentinelOne…)**
	4. Nej, slet ikke eller stort set ikke	Lokal firewall opsat med "default deny"
	4. Nej, slet ikke eller stort set ikke	Opsætning af OS og applikationer efter CIS benchmarks (https://www.cisecurity.org/cis-benchmarks/)
	2. Ja, næsten dækkende	E-mail gateway med sandbox (fx ProofPoint)
	2. Ja, næsten dækkende	Web gateway med sandbox (fx ProofPoint)
	4. Nej, slet ikke eller stort set ikke	IPS (HIPS)
	1. Ja, helt og fuldt dækkende	Harddisk kryptering
	2. Ja, næsten dækkende	Firewall med L7 på netværket (fx Cisco, Palo Alto, Fortigate, Checkpoint…)
Backup og data-beskyttelse	3. Delvist	Komplet backup som er testet korrekt og regelmæssigt (fx Veeam)
	3. Delvist	Backup er 100% sikkert ikke sårbar overfor ransomware
	3. Delvist	Alle sensitive data er kendte (vi ved hvor de er, hvor de må være og hvem der har adgang til dem) og beskyttet med ACL og kryptering (Fx SolarWinds A
	4. Nej, slet ikke eller stort set ikke	Der er indført Data Loss Prevention mekanismer i netværket (klienter, servere, mail) (fx ForcePoint DLP eller ManageEngine Data Security Plus)
Modsvar	3. Delvist	Logningen overvåges 24/7/365 af intern eller ekstern SOC (CIS 6)
	4. Nej, slet ikke eller stort set ikke	Der er etableret en CSIRP og CSIRT som er veldokumenteret og afprøvet. Evt. eksternt IR team (CIS 19)
	4. Nej, slet ikke eller stort set ikke	Cybersikkerheden er trykprøvet med relevante pentest baseret på MITRE ATT&CK TTP (CIS 20)
	3. Delvist	Der er indført et awareness trænings program efter bedste praksis (SANS MGT433) med hyppige phishing tests (CIS 17) (fx ProofPoint Wombat)
	4. Nej, slet ikke eller stort set ikke	Er der implementeret et målbart og regelmæssigt program for "Clear Desk Policy"?
	4. Nej, slet ikke eller stort set ikke	Uddannes brugerne regelmæssigt og målbart i organisationens IT-sikkerhedspolitik?
	3. Delvist	Bruges der aktivt og regelmæssigt et rammeværk til at måle effektiviteten af IT-sikkerhedstiltagene (kontroller som fx CIS Measures and Metrics)? (Delo
FireEye Mandiant 2021 m-trends rapport anbefalinger (https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html)	3. Delvist	AD konti med delegere rettigheder på domæne root niveau - fx DS-Replication-Get-Changes og DS-Replication-Get-Changes-All (som kan bruges til at s
	3. Delvist	AD konti som direkte har fået elevere rettigheder på domain controllers (fx Thycotic Secret Server eller XTON tech)
	3. Delvist	AD Konti med delegerede rettigheder for organizational units (OUs) som indeholder computer og bruger objekter
	2. Ja, næsten dækkende	AD Konti som har lokale admin rettigheder på mange klienter / servere
	4. Nej, slet ikke eller stort set ikke	AD Konti som er konfigureret til ubegrænset eller begrænset Kerberos delegation
	4. Nej, slet ikke eller stort set ikke	AD Konti som ikke er beskyttet mod delegering (ikke medlem af "Protected Users Security Group" eller ikke har "Sensitive and Cannot Be Delegated"
	4. Nej, slet ikke eller stort set ikke	AD Konti som er beskyttet med AdminSDHolder
	3. Delvist	AD Konti som har mulighed for at redigere, linke og fjene links til Group Policy Objects (GPOs)
	3. Delvist	AD Konti der har rettigheder til at ændre passwords for mange konti (User-Force-Change-Password permissions)
	3. Delvist	AD Konti der har rettighed til at tildele bruger rettigheder som er konfigureret i Group Policy som tillader fjernlogin på mange klienter
	3. Delvist	AD Konti der har høje privilegier til ikke-computer konti konfigureret med Service Principal Names (SPNs)
	4. Nej, slet ikke eller stort set ikke	**IT-Sikkerhedskontroller som skal sikre minimering af brug og sårbarhed for brug at priviligerede konti på tværs af mange klienter (se note)**
	4. Nej, slet ikke eller stort set ikke	Kan du opdage og forhindre hackere i at modificere konti med rediger rettigheder til Group Policy Objects (GPOs) til er linket til domain root som fx "Defa
	4. Nej, slet ikke eller stort set ikke	Bruger du beskyttede bruger sikkerhedsgrupper til at placere priviligere "ikke-service" konti i
	2. Ja, næsten dækkende	Inaktiverer du metoder som kan gemme rettigheder (passwords) i klar tekt i hukommelsen på klienter (som fx WDigest og Windows Credential Manager
	2. Ja, næsten dækkende	Tilkobler du Credential Guard og Remote Credential Guard på Windows 10/2016+ klienter/servere eller "Restricted Admin Mode" til RDP med priviligere
	1. Ja, helt og fuldt dækkende	Bruger du Microsoft LAPS eller andre værktøjer til at rotere passwords for indbyggede administrator konti på klienter
	3. Delvist	Bruger du en enterprise "tiered" model for admin adgang
	4. Nej, slet ikke eller stort set ikke	Sørg for at admin tiltag kun startes fra priviligere dedikerede klienter eller jump servere
	4. Nej, slet ikke eller stort set ikke	Beskyt priviligerede konti mod delegering (fx med "Sensitive and Cannot Be Delegated")
	3. Delvist	Aktiver Windows Firewall til at forhindre brug af protokoller som kan bruges til spredning af malware, fjernadgang og ransomware
	4. Nej, slet ikke eller stort set ikke	Begræns antallet af klienter som konti og grupper med rettigheder der tillader spredning af malware til klienter (Se GPO SeDenyNetworkLogonRight, Set
	4. Nej, slet ikke eller stort set ikke	Begræns antallet af klienter som konti og grupper med rettigheder der tillader elevering af rettigheder (Se GPO SeDebugPrivilege, SeBackupPrivilege, Se
	4. Nej, slet ikke eller stort set ikke	Sørg for at begrænse hackeres mulighed for at bruge GPO til spredning af ransomware