Password Modenhedsmodel © Dediko A/S

Start her: Angiv status i kol. D

NR	Tiltag	Relevans	Status på tiltag
Kontrol	Typer af password angreb		
#01	Tiltag som modvirker phishing, spear phishing, whaling og Voice phishing	✓	0. Ikke igangsat
#02	Tiltag som modvirker malware som keyloggers og screen scraping	✓	1. Påbegyndt
#03	Tiltag som målrettet modvirker social engineering (Guillibility)	✓	2. Delvist gennemført
#04	Tiltag som modvirker brute force password angreb og credential stuffing	✓	3. Næsten komplet
#05	Tiltag som modvirker dictionary angreb	✓	4. Gennemført
#06	Tiltag som modvirker spidering (brugt i brite force og dictionary angreb)	✓	
#07	Tiltag som modvirker password gæt blandt de mest brugte passwords	✓	
#08	Tiltag som modvirker password angreb baseret på rainbow tabeller	✓	

Kontrol	Management ejerskab, budget og rapportering	Relevans	Status på tiltag
#09	Kender ledelsen til en målbar password risiko i organisationen og står ledelsen bag en plan for at mitigere denne risiko	✓	
#10	Har ledelsen aftalt tilstrækkeligt budget, kompetencer og manpower af til at mitigere risikoen indenfor en planlagt tidsramme?	✓	
#11	Rapporteres status på passwordsmitigerings projektet regelmæssigt til ledelsen og tager ledelsen korrigerende tiltag på basis af rapporteringen?	✓	

Kontrol	Minimumskrav til password styrke i organisationen	Relevans	Status på tiltag
#12	Følges anbefalingerne fra CIS Password Policy Guide eller bruges et andet relevant rammeværk for passwords	✓	
#13	Er der opsat ganulerede politikker for styrken af passwords for brugere, administratorer, eksterne konsulenter og servicekonti (maskin brugere)	✓	
#14	Er brugerpasswords på mindst 12 karakterer med fuld kompleksitet, skift ved breach, ikke genbrug af de sidste 12 passwords, lås ved 5 forkerte forsøg, maksimum skift 1 dag	✓	
#15	Får brugerne undervisning i oprettelse og håndtering af password efter den anbefalede password politik?	✓	
#16	Får brugerne en password husker stillet til rådighed af organisationen?	✓	
#17	Er admin, konsulent og service konti passwords på mindst 16 karakterer, fuld kompleksitet, ingen genrbug af de sidste 12 passwords, lås ved 3 forkerte forsøg, ingen automatisk oplåsning	✓	
#18	Skiftes passwords på service konti automatisk så ingen (eller stort set ingen) konti er sat til never expire?	✓	
#19	Er alle passwords i organisationen (inklusive Administrator brugerne) unikke?	✓	
#20	Bruges ENTROPY aktivt i udregningen af password styrken?	✓	
#21	Sikres det at humane passwords (alle andre end service konti) ikke indeholder dictionary ord, gentagne tegn, ord som relaterer til organisationen eller medarbejderen eller forbudte kombinationer (fx qwerty)	✓	
#22	Har alle bruger konti et udløb og sammenkædes åbningen af kontoen med bestået awareness træning i organisations it-sikkerheds- / informationssikkerheds politik?	✓	
#23	Ved reset/nulstilling/fornyelse af password for menneskelige konti vises der en password styrke indikator, er password hints fjernet og forklares det tydeligt hvorfor et password evt. bliver afvist?	✓	
#24	Er der indtænkt sikre koder / sikker adgangskontrol på andre typer af devices som fx tablets og mobiltelefoner?	✓	

Kontrol	2 Faktor Godkendelse (Auth)	Relevans	Status på tiltag
#25	Er alt eksternt arbejde (fx cloud services og VPN) ledsaget af 2FA/MFA?	✓	
#26	Er alt internt administrativt arbejde ledsaget af 2FA/MFA (hvor det er teknisk muligt)?	✓	

Kontrol	Overvågning af konti	Relevans	Status på tiltag
#27	Overvåges password reset forsøg mønster på administrative konti og kan dette give anledning til en alarm?	✓	
#28	Overvåges fejlede logins på bruger og admin konti og kan dette give anledning til en alarm?	✓	
#29	Overvåges lækkede passwords rettidigt og giver fører dette til et krav om tvungent password skift hos konto ejeren?	✓	
#30	Er alle passwords i organisationen blevet undersøgt for at de ikke er på lister over lækkede passwords - regelmæssigt?	✓	
#31	Undersøges User and Entity Analytics (Behaviour analyse) og giver dette anledning til password skift?	✓	

Kontrol	Password governance		
#32	Nulstilles en brugers konti og passwords når brugeren (inkl administratoren) forlader organisationen?	✓	
#33	Er denne nulstilling understøttet med teknik og automatiske rutiner (i stedet for manuelle procedurer som kan være fejlbehæftede)?	✓	
#34	Er det implementeret et PAM system til at understøtte sikkerhåndtering af passwords?	✓	
#35	Hvis ikke, er alle passwords gemt i et vault som er krypteret, med AD authentikeret adgang og 2FA?	✓	

Password dashboard	
Samlet score	16%
Typer af password angreb	31%
Management ejerskab, budget og rapportering	0%
Minimumskrav til password styrke i organisationen	0%
2 Faktor Godkendelse (Auth)	0%
Overvågning af konti	0%
Password governance	0%
Password håndtering til i forbindelse med et angreb	0%
Systemunderstøttelse til passord og kontohåndtering	100%

#36	Er alle lokale passwords dokumenteret og følger de samme policies og governance som AD passwords?	✔	
#37	Er alle fælles administrative konti fjernet eller disablet?	✔	
#38	Deles passwords sikkert i organisationen - dvs. de ikke sendes i klar tekst eller udvekles i et regneark / på mail?	✔	
#39	Tillades password copy og paste i relevante felter for at gøre det nemmere for brugerne at håndtere passwords?	✔	
#40	Tillades det brugerne at se det password de indtaster i passwordfeltet for at gøre det nemmere for brugerne at håndtere passwords?	✔	
#41	Gennemføres der regelmæssige password audits for at sigre at håndteringen af passwords og passwords ikke fjerner sig for de indførte passwordpolitikker?	✔	
#42	Sikres det at der ikke er eller kan installeres keyloggers eller screen scrapers på klienter og servere?	✔	

Kontrol	Password håndtering til i forbindelse med et angreb	Relevans	Systemnavn
#43	Nulstiller du virksomhedens KRBTGT konto to gange pr. domæne med mindst ti timers mellemrum?	✔	
#44	Nulstiller du effektivt ALLE virksomhedens privilegered, bruger, service og lokale konti med fokus først på kompromiterede konti og dernæst på priviligerede konti?	✔	
#45	Nulstiller du den unikke (pr DC) irectory Services Restore Mode (DSRM) konto som er en lokal nødkonto og gemmer password sikkert?	✔	
#46	Nulstiller du Domain Trust Keys som gemmes på hver DC og som er afgørende for trust mellem domæner i en AD Forest og en begrænsende faktor for lateral movement af malware?	✔	
#47	Nulstiller du Active Directory Federated Services (AD FS) Service Account? S nærmere på https://www.mandiant.com/resources/blog/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452 og https://www.mandiant.com/media/17656 (Remediation and Hardening Strategies for Microsoft 365 to Defend Against APT29 - v1.3)	✔	
#48	Nulstiller du kerberos dekrypteringsnøglen for AZUREADSSOACC Account (hvis der er SSO mellem AD og AAD)?	✔	
#48	Skifter du alle password med regelmæssige mellemrum - spcielt på priviligerede konti - også selvom de ikke er blevet breached?	✔	
#49	Nulstiller du synkroniserings konti passwords for konti mellem AD og AAD. Fx Azure AD Connector konto, Azure AD DS konto og ADSync Service Account?	✔	

Kontrol	Systemunderstøttelse til passord og kontohåndtering	Relevans	Systemnavn
#43	Har du et velimplementeret PAM system og hvad hedder det?	✔	ManageEngine PAM, ManageEngine Password Manager Pro (PMP), Thycotic Secret Server, Xton Tech
#44	Har du et velimplementeret password vault med individuel adgang, 2FA implementeret efter bedste praksis og hvad hedder det?	✔	ManageEngine PMP
#45	Har du et velimplementeret system til at hjælpe brugerne med at skifte passwords?	✔	SpecOps
#46	Har du et velimplementeret system til at opdage og håndtere lækkede passwords?	✔	SpyCloud
#47	Har du et velimplementeret system til at hjælpe brugerne med at håndtere Internet passwords og andre koder?	✔	LastPass / Keeper Security
#48	Har du et velimplementeret system tilat hjælpe medarbejdere i organisationen med at dele passwords sikkert?	✔	Thycotic, ManageEngine PAM, LastPass, Keeper Security
#49	Har du et velimplementeret system til Identity Access Management (IAM)?	✔	SailPoint

Dediko A/S
www.dediko.dk
Tel: +45 45 76 20 21