M365 Sikkerhedstjek

Ledelsesresumé · November 2026

SAMLET VURDERING

Høj risiko

Gennemgangen viser huller hos Eksempelfonden, som gør det realistisk for en angriber at overtage en mailkonto og bruge den til svindel. Microsofts egen måling placerer jer på 31 %, hvor organisationer af samme størrelse i gennemsnit ligger på 55 %. De 4 kritiske punkter kan typisk løses på få dage med de licenser I allerede har. Der kan spares ca. 29.500 kr. om året på licenser, der ikke bliver brugt.

ADGANG OG IDENTITET

Høj risiko

5 medarbejdere er ikke beskyttet af to-trinsbekræftelse.

APPS OG INTEGRATIONER

Forhøjet risiko

Medarbejdere kan selv give ukendte apps adgang til deres mail og filer, hvilket svindlere udnytter med falske apps.

DATA OG DELING

Forhøjet risiko

Filer kan deles med alle der har linket, uden login. Det giver risiko for datalæk og gør Copilot mindre sikkert.

MAIL OG SVINDEL

Forhøjet risiko

Svindlere kan sende mails, der ser ud til at komme fra jer, til samarbejdspartnere og modtagere af betalinger.

PC'ER OG ENHEDER

Forhøjet risiko

Pc'erne mangler beskyttelse mod de mest almindelige angreb via vedhæftede filer og makroer.

LICENSER OG ØKONOMI

Besparelse mulig

ca. 29.500 kr. om året ekskl. moms

9 licenser er købt uden at være tildelt nogen. 1 licens er tildelt lukkede konti. 2 licenser er tildelt personer, der ikke har logget ind i 90 dage.

Det vigtigste for ledelsen

1. 5 medarbejdere er ikke beskyttet af to-trinsbekræftelse.
2. Angribere kan logge ind uden om to-trinsbekræftelse via ældre mailprogrammer.
3. Medarbejdere kan selv give ukendte apps adgang til deres mail og filer, hvilket svindlere udnytter med falske apps.

Sammenlignet med andre

Eksempelfonden	**31 %**
Organisationer af jeres størrelse	**55 %**
Alle Microsoft 365 kunder	**48 %**

Microsoft Secure Score: andelen af Microsofts anbefalede sikkerhedsindstillinger, der er taget i brug.

Anbefalet beslutning

Godkend at de kritiske punkter løses inden for 2 uger, og at resten planlægges inden for 3 måneder.

De kritiske punkter er anslået til 12 timer (16.500 kr.), og hele handlingsplanen til 59 timer (81.125 kr.) ekskl. moms.

Udpeg en ansvarlig, som følger op over for ledelsen, og gentag sikkerhedstjekket om 3 måneder.

Teknisk gennemgang

Grundlag, detaljer og handlingsplan til IT ansvarlig eller leverandør

Organisation	Eksempelfonden
Dato	25. november 2026
Udarbejdet af	Michael Dyrhauge, xSafety ApS
Klassifikation	Fortrolig
Grundlag	Read-only Graph API export: 26 interne brugere og 14 gæster, 3 Conditional Access policies, Microsoft Secure Score, 30 dages Defender hændelser

1. Nøgletal

31 % Secure Score (67 af 217)	**79 %** Brugere med MFA	**4** Kritiske fund	**9** Ledige betalte licenser

2. Microsoft Secure Score

Secure Score er Microsofts egen måling af hvor mange af de anbefalede sikkerhedsindstillinger der er taget i brug. Scoren er 67 af 217 mulige point. Gennemsnittet for alle Microsoft 365 kunder er 48 %.

Område	Point	Andel
Enheder	30,0 / 116	26 %
Identitet	24,0 / 50	48 %
Apps	13,0 / 26	50 %
Data	0,0 / 25	0 %

Største forbedringsmuligheder

Handling	Område	Point at hente	Brugerpåvirkning	Indsats
Create a DLP policy	Data	10,0	Moderate	Moderate
Apply sensitivity labels	Data	10,0	Moderate	High
Block Office applications from injecting code into other processes	Enheder	9,0	Moderate	Low
Block JavaScript or VBScript from launching downloaded executable content	Enheder	9,0	Moderate	Low

Handling	Område	Point at hente	Brugerpåvirkning	Indsats
Block execution of potentially obfuscated scripts	Enheder	9,0	Moderate	Low
Block Win32 API calls from Office macros	Enheder	9,0	Moderate	Low
Block credential stealing from the Windows local security authority subsystem	Enheder	9,0	Moderate	Low
Block persistence through WMI event subscription	Enheder	9,0	Moderate	Low
Block untrusted and unsigned processes that run from USB	Enheder	9,0	Moderate	Low
Use advanced protection against ransomware	Enheder	9,0	Moderate	Low
Block abuse of exploited vulnerable signed drivers	Enheder	9,0	Moderate	Low
Enable policy to block legacy authentication	Identitet	8,0	Moderate	Moderate

3. Attack Surface Reduction

ASR regler i Defender for Endpoint stopper typiske angrebsteknikker, for eksempel makroer der starter programmer eller scripts hentet fra mails. De er blandt de mest effektive og billigste tiltag på Windows.

Regel	Status	Point
Block executable content from email client and webmail	OK	9,0 / 9
Block all Office applications from creating child processes	OK	9,0 / 9
Block Office applications from creating executable content	OK	9,0 / 9
Block Office applications from injecting code into other processes	MANGLER	0,0 / 9
Block JavaScript or VBScript from launching downloaded executable content	MANGLER	0,0 / 9
Block execution of potentially obfuscated scripts	MANGLER	0,0 / 9
Block Win32 API calls from Office macros	MANGLER	0,0 / 9
Block credential stealing from the Windows local security authority subsystem	MANGLER	0,0 / 9
Block persistence through WMI event subscription	MANGLER	0,0 / 9
Block untrusted and unsigned processes that run from USB	MANGLER	0,0 / 9
Use advanced protection against ransomware	MANGLER	0,0 / 9
Block abuse of exploited vulnerable signed drivers	MANGLER	0,0 / 9

15 enheder har rapporteret til Defender de seneste 30 dage. ASR har registreret 1.739 hændelser i audit og 3 blokeringer.

Regel	Tilstand	Hændelser	Enheder
Lsass Credential Theft	Audit	1.290	15
Office Child Process	Audit	412	9

Regel	Tilstand	Hændelser	Enheder
Obfuscated Script	Audit	37	4
Executable Email Content	Blokeret	3	2

4. Licenser

Licens	Købt	Tildelt	Kan frigøres	Pris pr. md.	Besparelse pr. år
Microsoft 365 Business Premium	30	23	10	206,94 kr.	24.833 kr.
Microsoft 365 Copilot	5	3	2	194,00 kr.	4.656 kr.
Exchange Online (Plan 1)	1	1	0	30,00 kr.	–

Priser er Microsofts vejledende priser (MSRP) ekskl. moms ved årligt abonnement. Kan frigøres omfatter ledige licenser og licenser på lukkede eller inaktive konti.

Sikkerhedsfunktioner tenanten har licens til: Entra ID P1, Intune, Defender for Endpoint, Defender for Office 365.

Licenser der kan frigøres

Navn	Bruger	Bemærkning
Laura Mose	laura.mose@eksempelfonden.dk	Deaktiveret konto med licens
Signe Friis	signe.friis@eksempelfonden.dk	Sidste login 8. juli 2026
Morten Toft	morten.toft@eksempelfonden.dk	Aldrig logget ind

5. Identitet og adgang

Conditional Access policy	Status
CA01 - Kræv MFA: Alle brugere	Report-only
CA02 - Kræv MFA: Administratorer	Aktiv
Block legacy auth (gammel)	Deaktiveret

19 af 24 licenserede brugere har registreret MFA.

Brugere uden MFA	Bruger
Kasper Berg	kasper.berg@eksempelfonden.dk
Line Dahl	line.dahl@eksempelfonden.dk
Rasmus Vang	rasmus.vang@eksempelfonden.dk
Emma Skov	emma.skov@eksempelfonden.dk
Niels Bak	niels.bak@eksempelfonden.dk

Globale administratorer	Bruger
Anne Holm	anne.holm@eksempelfonden.dk
Peter Krog	peter.krog@eksempelfonden.dk
Mette Lund	mette.lund@eksempelfonden.dk

Globale administratorer	Bruger
BG Admin 1	bg-admin1@eksempelfonden.onmicrosoft.com
Jens Vang	jens.vang@eksempelfonden.dk

21 enheder er tilmeldt Intune (Windows 17, iOS 4), og 16 er compliant.

6. Apps og deling

Tredjepartsapps med brede rettigheder for hele organisationen. Microsofts egne apps er udeladt.

App	Udgiver	Rettigheder	Type
Nyhedsbrev Connector	Eksempel Marketing ApS	Mail.ReadWrite, Mail.Send	Delegeret, alle brugere
Gammel backupintegration	Ukendt	Mail.Read, Files.Read.All	Applikation

Deling i SharePoint og OneDrive: **Alle med linket, også uden login**.

Administrator med daglig konto	Roller
Anne Holm	Global Administrator
Peter Krog	Global Administrator
Mette Lund	Global Administrator
Jens Vang	Global Administrator
Lars Berg	Exchange Administrator

7. Mail og domæner

Domæne	SPF	DMARC	DKIM
eksempelfonden.dk	v=spf1 include:spf.protection.outlook.com -all	v=DMARC1; p=none; rua=mailto:dmarc@eksempelfonden.dk	Mangler

8. Gap-analyse mod best practice

Område	Kontrol	Status	Bemærkning
Identitet	MFA registrering for brugere	FEJL	79,2 % af licenserede brugere har registreret MFA (19 af 24).
Licenser	Licenser på deaktiverede konti	MANGLER	1 deaktiveret konto har stadig betalte licenser.
Enheder	ASR regler i blok tilstand	MANGLER	9 af 12 ASR regler er ikke fuldt slået til.
Identitet	Bloker legacy authentication	MANGLER	Ældre protokoller uden MFA er ikke blokeret.
Identitet	Beskyttelse af MFA registrering	MANGLER	En angriber med adgangskoden kan registrere sin egen MFA metode.
Identitet	Globale administratorer	MANGLER	5 globale administratorer. Microsoft anbefaler under 5.
Apps	Brugeres samtykke til apps	MANGLER	Alle brugere kan give enhver app adgang til deres mail og filer.
Data	Deling med alle der har linket	MANGLER	Filer kan deles med alle der har linket, uden login.
Mail	DKIM for eksempelfonden.dk	MANGLER	DKIM for Microsoft 365 er ikke sat op.
Licenser	Ledige betalte licenser	DELVIS	9 købte licenser er ikke tildelt nogen.
Licenser	Inaktive brugere med licens	DELVIS	2 aktive konti med betalt licens har ikke logget ind i 90 dage.
Enheder	Intune enhedsstyring	DELVIS	21 enheder tilmeldt, 5 er ikke compliant.
Identitet	MFA for alle brugere	DELVIS	Policyen findes, men står kun i report-only.
Identitet	Policies i report-only	DELVIS	1 policy håndhæves ikke.
Identitet	Deaktiverede policies	DELVIS	1 policy er slået fra.
Identitet	Phishingresistent MFA for administratorer	DELVIS	3 af 4 administratorer har ingen passkey, FIDO2 nøgle eller Windows Hello.
Identitet	Brugere med kun SMS eller opkald	DELVIS	2 brugere har kun SMS eller telefonopkald som metode.
Identitet	Separate administratorkonti	DELVIS	5 administratorer bruger samme konto til daglig mail og administration.
Identitet	Break-glass konti	DELVIS	Kun én mulig nødkonto: BG Admin 1.
Identitet	Svage MFA metoder tilladt	DELVIS	SMS er tilladt som totrinsbekræftelse.
Identitet	Passkeys og FIDO2	DELVIS	Passkeys og FIDO2 nøgler er ikke slået til.

Område	Kontrol	Status	Bemærkning
Apps	Brugere kan registrere apps	DELVIS	Almindelige brugere kan oprette app registreringer.
Apps	Apps med brede rettigheder	DELVIS	2 apps har adgang til mail, filer eller mappen for hele organisationen.
Data	Eksterne kan dele videre	DELVIS	Eksterne brugere kan dele jeres filer videre med andre.
Identitet	Inaktive gæster	DELVIS	9 af 14 gæster har ikke logget ind i 90 dage.
Mail	DMARC for eksempelfonden.dk	DELVIS	DMARC overvåger, men afviser ikke forfalskede mails (p=none).
Identitet	MFA for administratorer	OK	Administratorer er dækket af MFA krav.
Mail	SPF for eksempelfonden.dk	OK	v=spf1 include:spf.protection.outlook.com -all
Identitet	Risikobaseret adgang	IKKE RELEVANT	Kræver Entra ID P2, som tenanten ikke har.

9. Handlingsplan

Prio 1 = Kritisk, udføres hurtigst muligt. Prio 2 = Vigtigt, inden for 2 uger. Prio 3 = Anbefalet, inden for 30 dage.

Timepris: 1.375 kr. ekskl. moms. Timerne er anslåede.

Prio 1 · Kritisk

Område	Hvad	Handling	Timer	Pris
Identitet	MFA for alle brugere	Aktiver MFA policyen for alle brugere efter test i What If.	4	5.500 kr.
Identitet	Bloker legacy authentication	Opret en policy der blokerer Exchange ActiveSync og andre klienter.	2	2.750 kr.
Identitet	MFA registrering for brugere	Kontakt brugerne uden MFA og få dem registreret, eller deaktiver konti der ikke bruges.	4	5.500 kr.
Apps	Brugeres samtykke til apps	Begræns brugersamtykke til verificerede udgivere og lavrisiko rettigheder, eller slå det fra.	2	2.750 kr.
	I alt		**12**	**16.500 kr.**

Prio 2 · Vigtigt

Område	Hvad	Handling	Timer	Pris
Licenser	Licenser på deaktiverede konti	Fjern licenserne, eller konverter postkasser til delte postkasser.	1	1.375 kr.
Licenser	Inaktive brugere med licens	Bekræft om personerne stadig er ansat. Deaktiver og frigør licens hvis ikke.	1	1.375 kr.
Enheder	ASR regler i blok tilstand	Slå reglerne til i audit, gennemgå hændelser i 2 til 4 uger, og skift derefter til blok.	6	8.250 kr.

Område	Hvad	Handling	Timer	Pris
Enheder	Intune enhedsstyring	Undersøg hvorfor enhederne ikke overholder politikkerne.	4	5.500 kr.
Identitet	Beskyttelse af MFA registrering	Opret en policy for brugerhandlingen Registrer sikkerhedsoplysninger.	1	1.375 kr.
Identitet	Policies i report-only	Gennemgå resultaterne og aktiver eller slet dem.	2	2.750 kr.
Identitet	Globale administratorer	Reducer antallet og brug mere afgrænsede roller.	2	2.750 kr.
Identitet	Separate administratorkonti	Opret separate administratorkonti uden licens og postkasse, og fjern rollerne fra de daglige konti.	3	4.125 kr.
Identitet	Break-glass konti	Opret en nødkonto mere, undtaget fra alle policies, og overvåg login på begge.	2	2.750 kr.
Apps	Apps med brede rettigheder	Gennemgå apps og rettigheder, og fjern dem der ikke bruges eller ikke kan forklares.	3	4.125 kr.
Data	Deling med alle der har linket	Begræns deling til navngivne eksterne, og sæt standardlinket til kun personer i organisationen.	3	4.125 kr.
Mail	DMARC for eksempelfonden.dk	Stram til p=quarantine og derefter p=reject.	2	2.750 kr.
Mail	DKIM for eksempelfonden.dk	Publicer DKIM CNAME poster og slå signering til i Defender.	1	1.375 kr.
	I alt		**31**	**42.625 kr.**

Prio 3 · Anbefalet

Område	Hvad	Handling	Timer	Pris
Licenser	Ledige betalte licenser	Reducer antallet ved næste fornyelse eller tildel dem bevidst.	1	1.375 kr.
Identitet	Deaktiverede policies	Ryd op, så kun aktive og planlagte policies findes.	1	1.375 kr.
Identitet	Phishingresistent MFA for administratorer	Udrul passkeys eller FIDO2 nøgler til administratorer og kræv dem via Authentication Strength.	4	5.500 kr.
Identitet	Brugere med kun SMS eller opkald	Flyt brugerne til Microsoft Authenticator eller passkeys.	2	2.750 kr.
Identitet	Svage MFA metoder tilladt	Slå SMS og opkald fra, når brugerne er flyttet til Microsoft Authenticator eller passkeys.	2	2.750 kr.
Identitet	Passkeys og FIDO2	Slå passkeys til i politikken for godkendelsesmetoder, så phishingresistent MFA kan bruges.	2	2.750 kr.
Apps	Brugere kan registrere apps	Slå det fra, så kun administratorer kan oprette apps.	1	1.375 kr.
Data	Eksterne kan dele videre	Slå videredeling fra for eksterne.	1	1.375 kr.

Område	Hvad	Handling	Timer	Pris
Identitet	Inaktive gæster	Fjern gæster der ikke længere bruges, eller indfør access reviews.	2	2.750 kr.
	I alt		**16**	**22.000 kr.**

Hele handlingsplanen: 59 timer, 81.125 kr. ekskl. moms.

10. Næste skridt

Gennemgå rapporten sammen og afklar omfang og tidsplan for Prio 1.

Udfør Prio 1 i et planlagt servicevindue og test ændringer i Conditional Access med What If værktøjet før aktivering.

Planlæg Prio 2 og 3, og gentag sikkerhedstjekket om 3 måneder for at måle fremskridt.

Datagrundlag og begrænsninger

Data er hentet read-only via Microsoft Graph 25. november 2026 med xSafety M365 Snapshot 1.1.0. Rapporten er et øjebliksbillede og erstatter ikke en fuld sikkerhedsrevision. Punkter markeret MANUEL eller IKKE VURDERET kræver opfølgning.