Powered by Knowledge.
Driven by Trust.

v5

Helsesektoren har skrevet ned oppskriften. I august viste forskerne hvorfor den ikke holder alene.

Webartikkel (del 1 ledelse, del 2 teknisk)

nLogic AS

Foretaksregisteret NO
821678102 MVA
nLogic.no

Innhold

1.	Klikk for å skrive inn overskrift	**Feil! Bokmerke er ikke definert.**
1.1	Bruk stiler for å strukturere dokumentet	**Feil! Bokmerke er ikke definert.**
1.2	Lim inn tekst på rett måte	**Feil! Bokmerke er ikke definert.**

Tittel: Helsesektoren har skrevet ned oppskriften. I august viste forskerne hvorfor den ikke holder alene.

Avsender: nLogic AS

Type: Webartikkel (del 1 ledelse, del 2 teknisk)

Versjon: v5

Dato: 13.08.2026

Dybdedokument: «Fem sammenhengende policyer for betinget tilgang i Microsoft 365» (kan bestilles fra oss)

Helse- og kommuneCERT hos Norsk helsenett har laget en sikringspyramide mot angriper-i-midten. Den sorterer tiltakene etter hvor godt de faktisk virker, og den er gratis, offentlig og skrevet på norsk.

Øverst står passnøkler, Windows Hello for Business og sertifikatbasert autentisering. Nederst, under overskriften «Hjelper IKKE», står Authenticator med nummermatching, tofaktor over telefon og tofaktor over SMS.

Det de fleste norske virksomheter i dag mener når de sier «vi har MFA», ligger altså i bunnen av pyramiden.

Så kom uka mellom 5. og 10. august, og tre uavhengige forskningsmiljøer viste at heller ikke toppen er absolutt.

Del 1: For ledelsen

Angriperne har lest de samme rådene som dere

Én av sakene vi meldte til en norsk kunde i månedsskiftet juli–august handlet om en pålogging fra en hostingleverandør som knapt brukes av noen. Kategorien «Login from Hosting ASN» dukket opp for første gang i juli 2026 i det året vi har gjennomgått hos denne kunden, sammen med feilkonfigurerte sertifikatmaler. To nye kategorier på tolv måneder er ikke tilfeldig støy: angrepsteknikken endrer seg.

Og den endrer seg raskere enn kontrollene. 7. august publiserte Arctic Wolf Labs en analyse av en kampanje mot Microsoft 365 der kompromitterte sesjoner ble holdt i live automatisk omtrent hver åttende time. Trafikken kom ikke fra et datasenter, men fra roterende noder på forbrukerlinjer i offerets eget land.

Lokkemiddelet var et varsel om en talemelding. Deretter fulgte en omdirigeringskjede i seks ledd, via Google Meet-lenker, annonseklikksporing og skylagring, før brukeren landet på noe som så ut som en helt vanlig Microsoft-innlogging. Hundrevis av virksomheter var mål for kampanjen i juli.

Kampanjen henger sammen med den Microsoft sporer som Storm-2657 og Storm-2755, kjent som «Payroll Pirate». Arctic Wolf varslet om den allerede 23. juli. Målet er lønns- og økonomikorrespondanse: angriperen leser med, venter på riktig øyeblikk, og endrer kontonummeret på en faktura.

Poenget for ledelsen er enkelt. Geografi og nettverkstilhørighet er kontroller som fortsatt fanger noe, men angriperne designer seg nå bevisst rundt dem, nettopp fordi kontrollene har virket.

Hva som skjedde med passnøkler i august

Tre funn på seks dager, og ingen av dem knekker kryptografien:

5. august, under Black Hat: SpecterOps viste at Windows Event Logging Service skrev signaturmateriale fra WebAuthn i klartekst, lesbart for en helt vanlig bruker. Kombinert med svak validering i Entra ID ble det til «Pass-the-Passkey», registrert som CVE-2026-34348.

10. august: Unit 42 viste at private nøkler for synkroniserte passnøkler kan hentes ut via en hovednøkkel på 32 byte i nettleseren. Den nøkkelen kan ikke roteres eller trekkes tilbake.

10. august: Dirk-jan Mollema viste at en nøkkel fra Windows Hello for Business kan brukes fra en allerede kompromittert sesjon uten at brukeren må oppgi PIN eller biometri på nytt. Entras påloggingsutfordring er gyldig i fem minutter, og er ikke bundet til hverken sesjon, bruker eller tenant.

Alle tre forutsetter at maskinen allerede er kompromittert. Den nyansen er viktig, og den forsvinner fort i overskriftene: passnøkler stopper phishing, og gjør det svært godt, men beskytter ikke mot en angriper som allerede har fotfeste på maskinen.

Vi anbefaler fortsatt passnøkler, men ikke at dere legger hele forsvaret på ett tiltak.

Datoene som gjør dette til en beslutning nå

Microsoft har satt to datoer, og de kommer uansett hva dere bestemmer.

Figur 1: Microsofts to frister for overgangen fra SMS og tale til passnøkler.

1. september 2026: Brukere som i dag bruker SMS eller taleoppringing, blir automatisk aktivert for passnøkler, og får en oppfordring ved pålogging.

1. februar 2027: Microsoft-levert SMS og tale pensjoneres. Brukere som bare har disse metodene, møter en registreringsdialog de ikke kommer forbi. Microsofts egen formulering er «There is no opt out from this February 1 behavior. It will be enforced for all tenants.»

Dere skal altså gjennom denne overgangen. Det eneste dere velger, er om den planlegges eller om den bare skjer.

Del 2: Teknisk

Sikringspyramiden i sin helhet

De to nivåene folk siterer er topp og bunn. De tre i midten er de som avgjør hva dere gjør på mandag:

Figur 2: De fem nivåene i Norsk helsenetts pyramide, med tiltakene som hører til hvert av dem.

1. **Stopper AitM:** passnøkler, fysiske nøkler, Windows Hello for Business, Microsoft Authenticator med passkey, sertifikatbasert autentisering
2. **Stopper innloggingen, men passordet er fortsatt på avveie:** Global Secure Access, krav om registrert, innrullert eller compliant enhet, innlogging fra sikker IP
3. **Stopper noen innlogginger:** geoblokkering, HelseCERTs blokkeringslister, URL-filtrering i nettleser og e-post, Defender for Identity
4. **Kan oppdage angrepsforsøk:** AitM-honeytokens
5. **Hjelper ikke:** token protection, Authenticator med nummermatching, telefon-MFA, SMS-MFA, ingen MFA

Token protection står nederst med en presis begrunnelse fra Norsk helsenett selv: AitM-angrepet går mot nettleserversjonen av Microsoft 365, og token protection støtter ikke nettlesere.

Nivå 4 er nivået folk hopper over. Det er også det eneste nivået en SOC har å jobbe med når de tre øverste er omgått.

Rammeverksforankring

Prinsipp eller tiltak	Hva det krever
2.6.7 Bruk multi-faktor autentisering	Minst på kontoer med tilgang til kritiske data og systemer, og på driftsbrukere
2.6.6 Styr tilganger til enheter	Grunnlaget for kravet om kjent enhet
2.5.2 Begrens tilgangen til interne tjenester fra eksterne lokasjoner	Betinget tilgang er den moderne formen for dette
2.8 Beskytt e-post og nettleser	Hele omdirigeringskjeden i AitM-kampanjen gikk gjennom nettleseren

CIS Controls v8.1 legger all flerfaktor i IG1:

- **6.3 Require MFA for Externally-Exposed Applications** (IG1)
- **6.4 Require MFA for Remote Network Access** (IG1)
- **6.5 Require MFA for Administrative Access** (IG1)
- **4.7 Manage Default Accounts on Enterprise Assets and Software** (IG1)
- **6.7 Centralize Access Control** (IG2)

CIS skiller ikke mellom flerfaktormetoder i teksten. Det gjør sikringspyramiden, og det er nettopp derfor de to hører sammen: CIS sier at dere skal ha flerfaktor, pyramiden sier hvilken.

Om NIS2 og norsk rett. NIS2 er ikke gjennomført i norsk rett. Direktivet er ennå ikke tatt inn i EØS-avtalen, og det finnes ingen fastsatt ikrafttredelsesdato. Det som gjelder i dag er digitalsikkerhetsloven (lov 20.12.2023 nr. 108), som trådte i kraft 1. oktober 2025 og gjennomfører NIS1. NIS2 ventes innført i løpet av 2026, og utvider virkeområdet fra rundt 600 norske virksomheter til rundt 5 000. Vi tar det med fordi tiltaket i denne artikkelen treffer artikkel 21(2)(j) (*«the use of multi-factor authentication or continuous authentication solutions …»*), altså flerfaktor eller kontinuerlig autentisering. Og den som planlegger nå, slipper å gjøre arbeidet to ganger.

Forbeholdet skal med: setningen ender med *«where appropriate»*, og direktivet overlater dermed vurderingen til virksomheten. Tilgangsstyringen står tydeligere i 21(2)(i), *«access control policies»*.

GDPR gjelder allerede, gjennom personopplysningsloven. Artikkel 32(1)(b) krever *«the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services»*, altså vedvarende og ikke bare ved oppstart. Artikkel 25 heter *«Data protection by design and by default»*, innebygd personvern, og krever at tiltakene bygges inn når behandlingen bestemmes, ikke ryddes på plass etterpå. Tilgangsmodellen er dermed et designvalg som skal tas før systemet settes i drift, og en usikker metode dere lar ligge igjen som reserve, er også et designvalg.

Slik anbefaler vi at dere går fram

Norsk helsenett bygger på to prinsipper vi gjerne gjentar.

Ikke alt eller ingenting. Hver brukergruppe dere sikrer, reduserer sannsynligheten for kompromittering. Dere trenger ikke ta alle samtidig, og et prosjekt som venter på at alt skal være klart, blir aldri ferdig.

En gruppe er ikke sikret før de usikre metodene er fjernet. Dette er punktet flest bommer på. Innfører dere passnøkler og lar SMS ligge igjen som reserve, har dere ikke sikret noen ting, for angriperen velger den svakeste metoden som fremdeles er tillatt.

Rekkefølgen vi anbefaler:

1. Kartlegg hvilke metoder som faktisk er i bruk, per bruker og ikke per policy. Rapporten fra policyen forteller hva som er tillatt, ikke hva folk gjør.

2. Start med drift og ledelse. Færrest brukere, høyest verdi, og de beste forutsetningene for å tåle litt friksjon underveis.

3. Krev registrert eller innrullert enhet før dere krever phishing-resistent metode. Enhetskravet er nivå 2 i pyramiden, og det løfter alle tiltakene som kommer etterpå.

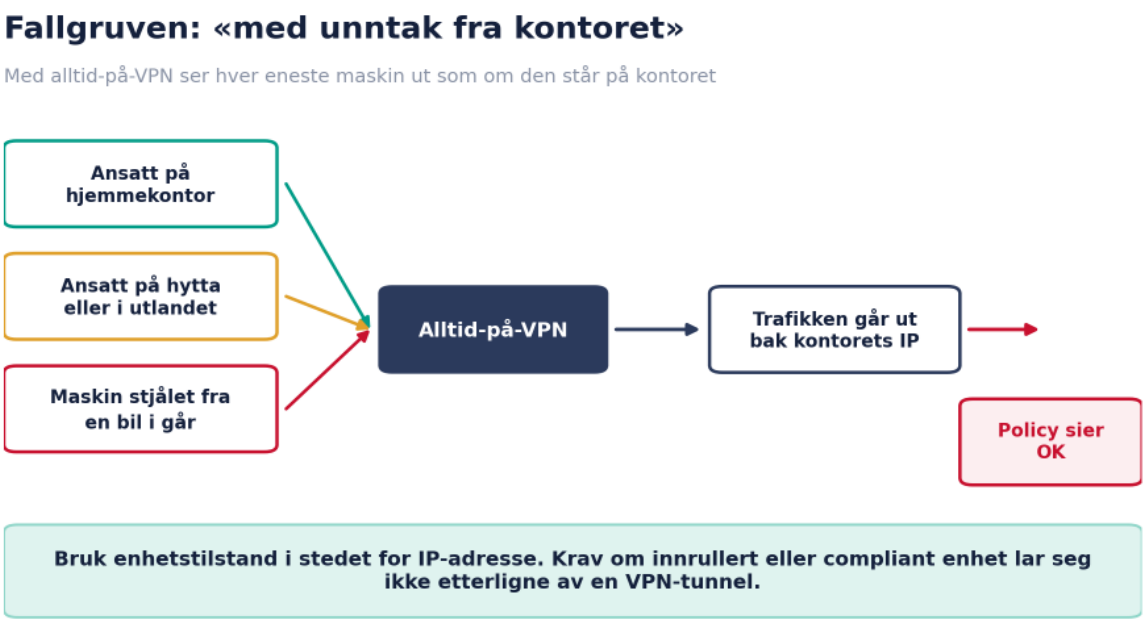
4. Fjern de usikre metodene for gruppen dere nettopp sikret, før dere går videre til neste gruppe.

5. Blokker pålogging med enhetskode. NSM anbefaler at den slås av eller begrenses kraftig. Den er fast inventar i verktøykassene som brukes mot Microsoft 365.

6. Legg deteksjon på selve sesjonen. Se avsnittet om SOC-kontroller nedenfor.

Fallgruven vi vil advare særskilt mot

Flere av policymønstrene bruker formuleringen «med unntak fra kontoret». Det høres fornuftig ut, og i mange miljøer er det direkte farlig.



Figur 3: Slik bryter alltid-på-VPN et unntak dere trodde gjaldt en fysisk lokasjon.

Årsaken er alltid-på-VPN. I moderne oppsett kobler maskinen seg til VPN-en før brukeren i det hele tatt har logget inn. Slik skal pålogging mot domenet, gruppepolicy og innlogging virke uten

problemer, uansett hvor den ansatte befinner seg. Det er godt driftshåndverk, og nettopp derfor bryter det kontrollen: maskinen kommer ut på internett bak kontorets IP-adresse hele tiden.

Den ansatte som sitter på hytta, på et hotellrom i Málaga eller på en flyplass, ser ut som om hun sitter på kontoret. Det gjør også maskinen som ble stjålet fra en bil på parkeringsplassen forrige uke, helt til den blir sperret.

I praksis betyr det at et unntak dere trodde gjaldt en fysisk lokasjon, gjelder hver eneste maskin i porteføljen, hele døgnet.

Slik anbefaler vi at dere håndterer det:

- **Sjekk først om alltid-på-VPN er i bruk**, og om VPN-trafikken går ut via kontorets utgående IP-adresser. Dette tar ti minutter å slå fast, og svaret overrasker overraskende ofte.
- **Bruk enhetstilstand i stedet for IP-adresse.** Krav om innrullert eller compliant enhet er nivå 2 i pyramiden og lar seg ikke etterligne av en VPN-tunnel.
- **Er kontor-IP likevel nødvendig**, bør den kombineres med et krav som følger brukeren og ikke nettverket, for eksempel innrullert enhet i tillegg.
- **Bruk Global Secure Access eller tilsvarende** der dere trenger et stedsuavhengig alternativ som faktisk sier noe om hvem som sitter der.

Andre fallgruver

Nødkontoer som aldri blir testet. Å låse seg selv ute av egen tenant er en reell risiko i dette arbeidet. Nødkontoene skal være unntatt policyene, ha lange tilfeldige passord, og testes med jevne mellomrom, ikke bare opprettes.

Å tro at «phishing-resistent» betyr «uangripelig». Alle funnene fra 5. til 10. august handler om hva som skjer etter at maskinen er kompromittert. Passnøkler flytter angrepet, de avlyser det ikke.

Å anta at trafikk fra Norge er trygg trafikk. Kampanjen Arctic Wolf Labs beskriver bruker med vilje noder i offerets eget land.

Hvilke SOC-kontroller som virker her

Når nivå 1 til 3 er omgått, er det deteksjonen som står igjen. Dette er kontrollene som faktisk fanger en AitM-kompromittering:

- **Pålogging fra hostingleverandør eller uvanlig nettverk.** Fortsatt nyttig, og fortsatt ikke nok alene.
- **Sesjonsanomali etter en vellykket innlogging.** En sesjon som fornyes med jevn maskinell rytme, oppfører seg ikke som et menneske. Det var nøyaktig dette mønsteret Arctic Wolf Labs kjente igjen.
- **Endring av autentiseringsmetoder på en konto.** En ny flerfaktormetode registrert er ett av de tidligste tegnene på at noen andre har overtatt kontoen.
- **Nye eller endrede innboksregler og videresendinger.** «Payroll Pirate» gikk etter lønns- og økonomikorrespondanse, og regelen som skjuler svarene kommer rett etter innloggingen.
- **AitM-honeytokens.** Nivå 4 i pyramiden. Undervurdert, rimelig, og den eneste kontrollen som er bygget for å oppdage akkurat dette angrepet.
- **Samtidige sesjoner fra ulike kilder** mot samme konto.

Kontrollene på nivå 1 til 3 setter dere opp én gang. Kontrollene i listen over må noen se på hver dag. Det er forskjellen mellom betinget tilgang og en SOC, og de to erstatter ikke hverandre.

Kilder

- AitM sikringspyramide, Helse- og kommuneCERT, Norsk helsenett SF
- Herdeguider for M365 conditional access, Helse- og kommuneCERT, Norsk helsenett SF
- Microsoft 365 AitM Phishing Hijacks Accounts to Collect Payroll and Finance Emails, The Hacker News om Arctic Wolf Labs, 07.08.2026
- Microsoft 365 & Workday Payroll Pirate AiTM Session Hijacking Campaign, Arctic Wolf sikkerhetsbulletin, 23.07.2026 (tilgjengelig for Arctic Wolf-kunder)
- New Passkey Attacks Can Recover Synced Private Keys or Bypass Phishing-Resistant MFA, The Hacker News, 10.08.2026
- Passkeys by default and retirement of Microsoft-provided SMS and voice authentication, Microsoft Learn, sist oppdatert 10.08.2026
- Advarsel om stor digital angrepsaktivitet, Sikkert.no (NSM, Politiet, Datatilsynet, Digdir), oppdatert 07.08.2026
- NSMs grunnprinsipper for IKT-sikkerhet 2.1
- CIS Critical Security Controls v8.1
- Direktiv (EU) 2022/2555 (NIS2), EUR-Lex. Artikkel 21(2)(i) og (j)
- Forordning (EU) 2016/679 (GDPR), EUR-Lex. Artikkel 25 og artikkel 32(1)(b)
- Lov om digital sikkerhet (lov 20.12.2023 nr. 108), Lovdata. I kraft 1. oktober 2025
- Personopplysningsloven, lov 15.06.2018 nr. 38 (gjør GDPR til norsk rett)

Tallene fra egen overvåking bygger på tolv månedsrapporter for én anonymisert kunde, august 2025 til juli 2026. Ingen opplysninger som kan identifisere virksomheten, systemene eller enkeltpersoner er gjengitt.

Kim Hansen

Solution Architect Security
+47 40448800
kim.hansen@nlogic.no

Kontakt oss

nLogic AS
Karenslyst Allé 20, 0278 Oslo
Org.nr.: 821 678 102
info@nlogic.no

Powered by Knowledge.
Driven by Trust.