

Håndtering av kompromittert M365-konto i 7 steg



Helse- og
kommuneCERT

1. Avslutt sesjoner
2. Tilbakestill passord
3. Sjekk MFA-metoder
4. Sjekk applikasjoner
5. Slett app-passord
6. Sjekk innboksregler
7. Gjennomgå audit-logg

1) Avslutt sesjoner

Gå til <https://entra.microsoft.com/> (som administrator)

Velg: -> Users -> All users

Finn og velg rammet bruker fra listen

Velg "Revoke sessions" -> "Yes"

2) Tilbakestill passord

Velg: Reset password -> Reset password

Kopier midl.passord og send dette til bruker **via alternativ kanal**. Ikke til den kompromitterte e-posten

3) Sjekk MFA-metoder

Slett innlagte MFA-er:

Authentication methods -> tre prikker -> delete

Om du ikke med sikkerhet kan si hvilke metoder angriper har lagt til:

Tilbakestill alle:

authentication methods -> require re-register multifactor authentication -> OK

4) Sjekk etter applikasjoner

Gå til applications -> velg innlagt applikasjon som ikke hører til -> remove

5) Slett app-passord

Gå til:

<https://account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx>

Velg bruker I listen -> Manage user settings

Check: Delete all existing app passwords generated by the selected users -> save

6) Sjekk etter innboksregler*

security.microsoft.com/v2/advanced-hunting

Bruk søk

```
CloudAppEvents
| where AccountObjectID == @"<GUID>"
| where ActionType in ('Set-Mailbox', 'New-InboxRule', 'UpdateInboxRules', 'Set-inboxRule')
```

Ved treff

Gå til admin.exchange.microsoft.com

Velg bruker -> Mailbox delegation -> Velg deg selv

Gå til outlook.office.com

Trykk på deg selv -> open another mailbox -> velg bruker

Slett innboksregler og forwardingregler

***) Business standard kan finne innbokseregler med PowerShellsøk:**

```
$adminAccount = "admin@domene.no"
$mailbox = "bruker@domene.no"
Import-Module
ExchangeOnlineManagement
Connect-ExchangeOnline -
UserPrincipalName $adminAccount
Get-InboxRule -Mailbox $mailbox
```

7) Gjennomgå audit-logg

Gå til

<https://purview.microsoft.com/audit/auditsearch>

Velg tidsrom og bruker

Gjennomgå

S
a
m
m
e

v
i
n
d
u

Varsle: incidents@helsecert.no