Håndtering kompromittert M365-konto

Entra.microsoft.com

1) Blokkér innlogging

Gå til https://admin.microsoft365.com/ som administrator

Velg brukeren

Block sign-in -> huk av -> "save changes"

2) Avslutt økter

Gå til https://entra.microsoft.com/ som administrator

Velg: -> Users -> All users

Velg bruker fra listen

"Revoke sessions" -> "Yes"

3) Reset passord

Velg: Reset password -> Reset password

Send midlertidig passord til brukeren i en annen kanal. Angriper kan ha tilgang til e-posten.

4) Slett MFA

Slett MFA-er angriper har lagt inn:

Authentication methods -> tre prikker -> delete

Om du er usikker

Tilbakestill alle:

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

5) Slett applikasjoner

Gå til applications -> fjern alle

Vi opplever jevnlig at folk ikke har kontroll på hva som hører hjermme. Reset alt.

6) Slett app-passord

Gå til: https://account.activedirectory.windowsazure.com/UserManagement/MultifactorVerification.aspx

Velg bruker -> Manage user settings-> Delete all existing app passwords generated by the selected users -> save

7) Aktiver bruker igjen

Velg: Unblock sign-in -> fjern kryss -> "save changes"

Admin.microsoft365.com

8) Sjekk innboksregler*

security.microsoft.com/v2/advanced-hunting

Søk etter

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

Om dere har 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
```

9) Varsle oss med det dere har av:

- Avsender
- Lenken til phishingen
- E-posten med phishingen i (som vedlegg)
- IP-ene angriperen brukte
- Hva angriperen gjorde

Send til: incidents@helsecert.no

Helse- og kommuneCERT

Laget for utskrift i A3 eller A4 for enkelt oppslag