Åtgärder för att hantera nätfiske i M365

CERT-SE

2025-05-06

Inledning

Detta dokument innehåller CERT-SE:s rekommendationer för att kunna utreda och hantera en incident där ett övertaget M365-konto skickat ut nätfiskemejl internt och externt. Rekommendationerna är inte uttömmande och bör ses som ett stöd vid en hantering av liknande incidenter.

CERT-SE uppmanar organisationer att ta höjd för fler scenarier i syfte att förebygga incidenter. CERT-SE:s rekommendationer bör ses som ett minimum vid misstänkt aktivitet för att minska risken att en hotaktör bibehåller ett fotfäste i en M365-miljö.

Dessa rekommendationer riktar sig till teknisk personal och utgår från en organisation som har den lägsta licensnivån. Genom att följa detta dokument kan er organisation skapa förhöjd säkerhet utan att ha tillgång till de mest avancerade funktionerna.

Innehållsförteckning

1.0 Initial utredning

Ifall ett nätfiskemejl skickats från ett konto i er organisation bör det första steget vara att åtgärda det misstänkt övertagna kontot. Se därefter till att:

1. Återta kontroll över de misstänkt övertagna kontona, *se punkt 2.1 till 2.4.*
2. Informera både externa och interna mottagare om händelsen, *se punkt 3.*

Dessa punkterna kan och bör genomföras i takt med att ny information framkommer under utredningens gång.

1.1 Utredningsskede

CERT-SE:s rekommendation är att följa de steg och checklistor som rekommenderas i Microsofts playbooks för att skapa sig en bild av omfattning samt vidare åtgärder.

För att ta del av Microsofts playbooks in sin helhet, se:
Microsoft. (06-11-24). Phishing investigation.
https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-phishing
Microsoft. (31-03-25). Respond to a compromised cloud email account.
https://learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-emejl -account
Microsoft. (07-03-24). Token theft playbook.
https://learn.microsoft.com/en-us/security/operations/token-theft-playbook
Microsoft. (12-03-25). Compromised and malicious applications investigation.
https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-compromised-malicious-app
Microsoft. (12-03-25). App consent grant investigation.
https://learn.microsoft.com/en-us/security/operations/incident-response-playbook-app-consent

Viktigt!

Dokumentera samtliga fynd samt åtgärder som vidtas under utredningen. Detta underlättar både för teknisk personal som utreder incidenten, vid eventuell kontakt med polis, samt om behovet finns att ta in extern hjälp.

En grundutredning bör åtminstone inkludera dokumentation gällande följande:

- ➔ Tidsstämplar (oavsett vilket tidsformat som används, tänk på att vara konsekvent).
- ➔ Vilket konto som utfört misstänkt aktivitet (användarnamn).
- ➔ Vilken misstänkt aktivitet som skett och vilken källinformation (exempelvis sign-in logs).
- ➔ Vilka åtgärder som vidtagits och av vem.

2. Återta kontrollen över ett konto

2.1 Inaktivera påverkade användare

Som första åtgärd vid misstänkt aktivitet bör användarkontot inaktiveras till att problemet är åtgärdat. Efter att användaren inaktiverats/blockerats behövs fortsatt övervakning av eventuell aktivitet från användarkontot då en hotaktör kan ha fortsatt åtkomst på grund av giltiga Access Tokens och Refresh Tokens.

Viktigt!
Detta steg avser moln-miljöer. Vid användning av hybrid-miljöer med Microsoft Identity Manager eller liknande funktioner bör man vara medveten om att återaktivering av användaren kan ske i bakgrunden.

Sign-in logs
Använd Sign-in logs i Microsoft Entra ID för att kontrollera inloggningar för den berörda användaren. I Sign-in logs kan värdefull information finnas, exempelvis IP-adresser, tidsstämplar, vilken enhet som använts, vilket protokoll som använts för inloggning och liknande.

Viktigt!
Sign-in logs kan ha en fördröjning på upp till 15 min innan de syns i listan. Det finns två olika typer av inloggningar:

1. User sign-ins (interactive)
User sign-ins (interactive) listar inloggningar som har genomförts av användaren.

- ➔ Här loggas på vilket sätt användaren har loggat in och till vilka resurser som getts åtkomst. Exempelvis kan vara via lösenord, MFA, via Device Code-flöde eller liknande. Ur en utredningssynpunkt kan detta vara viktigt att hålla koll på då det kan visa på vilket sätt en eventuell hotaktör har fått åtkomst.
- ➔ För att se vilken metod som använts för inloggning, gå in på en specifik logghändelse och skrolla ner till **Original transfer method**, som visar vilken metod som användes för att

initiera inloggningen, samt **Authentication protocol**, som visar vilket autentiseringsprotokoll som använts.

För vidare information:
Microsoft. (09-02-26). What are interactive user sign-ins in Microsoft Entra?
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-interactive-sign-ins

2. User sign-ins (non-interactive)

Här listas icke-interaktiva inloggningar, sådana som genomförts i egenskap av användaren, exempelvis en klientapplikation som användaren delegerat behörigheter åt eller SSO-flöden (Single Sign-On).

- Tidigare observationer har visat att hotaktörer använder legitima applikationer för att komma åt användares mejlkorgar för att kunna hämta ner mejl lokalt till sina klienter. Därför kan detta vara viktigt att undersöka vid en utredning.
- I dessa loggar registreras det även när användarens Access Token förnyas (med hjälp av Refresh Token) och andra bakgrundsaktiviteter. Detta kan också vara viktigt att hålla koll på ur utredningssynpunkt.

För vidare information:
Microsoft. (09-02-26). What are non-interactive user sign-ins in Microsoft Entra?
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-noninteractive-sign-ins

Audit logs

Audit-loggarna innehåller detaljerad information om samtliga händelser och förändringar som sker i Microsoft Entra, och kan vara en viktig källa för att förstå vad som skett vid en utredning. I audit-loggarna går det att bland annat ta del av:

- lösenords-, grupp- och rollförändringar eller
- om användare registrerat nya MFA-metoder,
- vem som initierat det och vem förändringen gjordes på,
- vilka attribut som förändrats samt IP-adressen som det utförts ifrån.

För vidare information:

Microsoft. (18-11-25). What are Microsoft Entra audit logs?

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-audit-logs

2.2 Revokera session för påverkade användare

Revokera sessionen för det påverkade kontot för att kontots Refresh Token och i särskilda fall[1] även Access Token blir ogiltiga. Detta gör att användaren behöver logga in på nytt och på detta sätt kan åtkomsten brytas för en eventuell hotaktör.

Ifall **Continuous Access Evaluation** är aktivt bör detta ta max 15 minuter innan dessa är ogiltiga, annars beror det på när Access Token skapades, dessa har en genomsnittlig livslängd på 75 min från utfärdandet.

Refresh Tokens har en livslängd på upp till 90 dagar om de inte används under denna period.

Viktigt!
Från att ni revokerar sessionen tills att giltighetstiden för Access Token har gått ut behövs övervakning av eventuell kontoaktivitet, s*e information om Sign-in logs och Audit logs under punkt 2.1*.

Steg för steg:

1. Navigera till **Entra ID Admin Center** (https://entra.microsoft.com).
2. Expandera fliken **Users**.
3. Välj **All users**.
4. Välj den användare du vill revokera sessionen för.
5. Klicka på **Revoke sessions** och välj **Yes** på den efterföljande frågan.
6. Repetera ovanstående steg för samtliga berörda användare.
   För att genomföra revokering via PowerShell, *se Microsoft dokumentation:*
   https://learn.microsoft.com/en-us/entra/identity/users/users-revoke-access

1Ifall er organisation inte nyttjar **Continuous Access Evaluation** går det inte att revokera Access Tokens. Dessa har en standardlivslängd på mellan 60-90 min, i genomsnitt 75 min, från utfärdandet och kommer därför vara giltiga resterande del av denna tid.

2.3 Revokera användares MFA-session och se över MFA-metoder

När det påverkade användarkontot har inaktiverats och sessioner revokerats bör man revokera den påverkade användarens nuvarande MFA-session för att ogiltigförklara den session som är aktiv. Det gör att nästa gång en åtgärd genomförs som kräver MFA måste en MFA-autentisering genomföras på nytt. Det tvingar exempelvis en användare att genomgå MFA igen även om användaren tidigare valt **Kom ihåg den här enheten** vid inloggning.

Viktigt!
Det kan ta upp till 15 min innan MFA-sessionen är revokerad.

Steg för steg (molnmiljö):

1. Navigera till **Entra ID Admin Center** (https://entra.microsoft.com).
2. Expandera fliken **Users**.
3. Välj **All users**.
4. Välj den användare du vill revokera sessionen för.
5. Välj **Authentication Methods**.
6. Klicka på **Revoke multifactor authentication sessions**.
7. Repetera ovan steg för samtliga påverkade användare.

Därefter bör det kontrolleras om det lagts till fler MFA-enheter och metoder för den påverkade användaren under det misstänkta tidsfönstret. Om möjligt, välj att kräva omregistrering av MFA för att säkerställa att inte hotaktören kontrollerar någon MFA-metod.

För vidare information:
Microsoft. (02-02-26). Manage user authentication methods for Microsoft Entra multifactor authentication.
https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-userdevicesettings#manage-user-authentication-options

2.4 Kontrollera och revokera applikationsbehörigheter

Som tidigare nämnt under Audit logs har CERT-SE tidigare observerat utnyttjandet av legitima applikationer i samband med övertagna konton för att exempelvis exfiltrera mejl. I samband med misstänkt aktivitet bör det därför även utredas om några applikationer registrerats av användaren under tidsfönstret för den misstänkta aktiviteten och vilka behörigheter användaren delegerat till en eventuell sådan applikation.

Vid upptäckt av misstänkta applikationer bör behörigheter för dessa revokeras omgående och applikationerna tas bort.

För vidare information:
Microsoft. (06-03-25). Review permissions granted to enterprise applications. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-application-permissions?pivots=portal#review-and-revoke-permissions

2.5 Kontrollera vilka administrativa roller som är tilldelade användaren

Kontrollera vilka administrativa roller en användare är tilldelad för att minska risken för ytterligare påverkan i er miljö. En administratör har ofta högre behörigheter vilket kan öppna upp fler attackytor för en hotaktör. Det kan dels handla om att lägga in bakdörrar såväl som att förflytta sig eller eskalera sin åtkomst. Exempelvis, en Exchange-administratör har behörigheter som medger åtkomst till samtliga användares mejlkorgar och kan därmed utnyttjas för att komma åt samt exfiltrera känslig information i dessa.

Exempel på administrativa roller med höga/känsliga behörigheter:

- Global Administrator.
- Contributor.
- Owner.
- Role Based Access Control Administrator.
- User Access Administrator.
- Help Desk Administrator.
- Exchange Administrator.
- M365 Backup Administrator.

Ta även hänsyn till egenskapade roller, så kallade Custom Roles, då även dessa kan ha höga/känsliga behörigheter.

1. Börja med att ta bort dessa roller för användaren.
2. Se över vilka administrativa roller användaren hade tillgång till för att ta reda på om ni eventuellt behöver utöka er utredning.

För vidare information:

Microsoft. (31-03-25). Respond to a compromised cloud email account. https://learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-email-account

Microsoft. (09-04-26). Azure built-in roles.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

Microsoft. (29-04-26). Microsoft Entra built-in roles.

https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

2.6 Kontrollera eventuella mejlregler i mejlkorgen

Ett sätt för hotaktörer att undvika upptäckt vid utskick av nätfiskemejl är att lägga till regler i den övertagna användarens mejlkorg. På detta sätt säkerställer hotaktören att exempelvis svar på nätfiske omdirigeras till en annan mapp eller raderas så att inte användaren ska se dessa.

Utöver detta har de i vissa fall lagt till vidarebefordringsregler för att omdirigera mejl till externa adresser. På detta sätt har hotaktören kunnat övervaka mejltrafik samt exfiltrera information/data.

Följ dessa steg:

1. Kontrollera och ta bort eventuella tillagda mejlregler i användarens mejlkorg.
2. Undersök användarens mejlkorg efter mappar som kan ha använts för att dölja mejl.
3. Kontrollera och ta bort eventuella tillagda vidarebefordringsregler i användarens mejlkorg.

2.7 Undersök och ta bort skadlig SharePoint-sida

I flera nätfiskekampanjer under 2024-2026 har hotaktörer använt sig av användares OneDrive-lagringsytor och organisationers SharePoint-ytor för att sprida dokument med skadliga länkar i. I flera fall har skadliga länkar lett till fejkade inloggningsportaler med syftet att samla in inloggningsuppgifter.

Om dessa ytor eller dokument tas bort kommer en användare som fått ett nätfiskemejl inte kunna nå den fejkade inloggningsportalen.

Steg för steg (molnmiljö):

1. Navigera till **Microsoft 365 admin center** (https://admin.cloud.microsoft).
2. Expandera fliken **Users** och välj **Active users**.
3. Markera den berörda användaren.
4. På den ruta som dyker upp, välj fliken **OneDrive**.
5. Under **Get access to files**, klicka på **Create link to files**.
6. Klicka på länken som skapas vilket leder till användarens OneDrive-lagringsyta.
7. Markera det dokument som inkluderar den skadliga länken och klicka på **Delete** i menyn ovanför.

2.8 Återställ lösenord för påverkade användare

Säkerställ att er organisation har inaktiverat användaren/blockerat inloggning för den påverkade användaren och revokerat sessionen. När utredningen är klar och kontot ska aktiveras bör det genomföras en lösenordsåterställning för att säkerställa att en eventuell hotaktör inte kan återta kontrollen över användarkontot.

Viktigt!
Om användaren är en hybrid-användare (lösenordet synkas från Active Directory) behöver nedanstående process genomföras två gånger. Detta beror på cachningsmekanismer i Active Directory där NTLM-hashar eller Kerberos-tickets kan ta längre tid på sig att uppdateras och/eller ogiltigförklaras. Genom att återställa lösenordet en andra gång tvingar man fram en ogiltigförklaring av dessa hashar/tickets snabbare.

För vidare information:
Microsoft. (03-04-26). Revoke user access in Microsoft Entra ID.
https://learn.microsoft.com/en-us/entra/identity/users/users-revoke-access

Steg för steg (molnmiljö):

1. Navigera till **Entra ID Admin Center** (https://entra.microsoft.com).
2. Expandera fliken **Users**.
3. Välj **All users**.
4. Välj den användare du vill revokera sessionen för.
5. Klicka på **Reset password**.
6. I rutan som kommer upp till höger, klicka på knappen **Reset password** för att visa användarens nya automatiskt genererade tillfälliga lösenord.
7. Repetera ovanstående steg för samtliga berörda användare.

Viktigt!
Det tillfälliga lösenordet behöver förmedlas till användaren på ett säkert sätt. Tänk på att

användaren eventuellt inte längre har access till sitt mejlkonto då sessionen är revokerad.

Observera! Giltighetstiden för detta tillfälliga lösenord löper aldrig ut.

2.9 Övervaka åtgärdade användare

När användarkontot väl är återaktiverat måste kontot fortsätta övervakas för att säkerställa att det inte fortsatt sker misstänkt aktivitet. Om misstänkt aktivitet upptäcks bör ovanstående åtgärder repeteras.

Tidsramen för övervakning är upp till varje organisation att avgöra. CERT-SE rekommenderar dock att detta görs under minst 3 månader genom daglig kontroll.

Övervakning bör genomföras åtminstone via ovan beskrivna metoder som:

- Sign-in logs och Audit logs.
- Behörighetssamtycken.
- MFA-metoder.
- Applikationer.

Denna lista är inte uttömmande utan bör ses som en grund.

3. Informera interna och externa mottagare

Organisationen bör skyndsamt informera berörda mottagare av ett nätfiskemejl för att förhindra vidare spridning.

Ifall din organisation är en kommun rekommenderar CERT-SE att IT-avdelningarna inom respektive kommun skapar en kommunikationskanal till övriga kommuners IT-avdelningar, om detta inte redan finns på plats, i syfte att:

- ➔ Skyndsamt kunna informera om händelser som kräver tidskritisk hantering.
- ➔ Dela agerbar information, tips och rekommendationer.
- ➔ Utbyta erfarenheter kring liknande händelser.

Viktigt!
CERT-SE vill förtydliga att detta arbete bör vara en del i det förebyggande arbetet och inte prioriteras i händelse av en incident.