TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret

Skydd mot nätfiske och dataintrång i Microsoft Office 365

Traficoms publikation
12/2019

Innehåll

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret
ISSN 1799-0157 (webbpublikation)

Förord

Särskilt i början av 2018 fick Cybersäkerhetscentret kännedom om allt fler incidenter där organisationer drabbades av nätfiske i syfte att komma över anställdas inloggningsuppgifter. Nätfiske kan även riktas till såväl privatpersoner som organisationer. Globalt används allmänt termen business email compromise eller BEC för dataintrång i företagskonton.

Användarnas inloggningsuppgifter kunde utnyttjas på olika sätt beroende på exempelvis vilka angriparens motiv var eller vilken roll eller vilka uppgifter innehavaren av det angripna användarkontot hade i organisationen. I några fall försökte angriparen till exempel klart få en stor ekonomisk nytta genom att följa utbytet av meddelanden om betalningstransaktioner. Å andra sidan kan stulna inloggningsuppgifter även användas till exempel för att spionera och komma över företagshemligheter. Därtill kan ett lyckat nätfiske medföra bland annat olika anseende- och regleringsrisker.

Även om nätfiske som ett fenomen inte endast begränsas till vissa leverantörers tjänster hade dessa fall en gemensam spionera och komma över företagshemligheter: de stulna användaruppgifterna var för Microsoft Office 365-konton. Sådana fall kommer till Cybersäkerhetscentrets kännedom kontinuerligt. Cybersäkerhetscentret gav en varning om ämnet i juni 2018, och varningen gäller fortfarande nu när denna guide skrivs.

Vi har sett att ett antal nätfiskekampanjer utvecklats i olika riktningar sedan slutet av våren och början av sommaren. Enskilda exempel på dessa är att man skickar nätfiskemeddelanden som ser ut som krypterade e-postmeddelanden, kringgår en multifaktorautentisering genom att använda gamla metoder för e-postförbindelse och skräddarsyr nätfiskewebbplatsens utseende utifrån den e-posttjänst som användaren använder för att få tillgång till den aktuella tjänsten.

Att reagera på nya nätfiskekampanjer är en ändlös jakt och ofta ohjälpligen för sent i det skede där vågen redan har slagit mot stranden. Därför är det högst viktigt att i god tid införa informationssäkerhetsfunktioner i tjänster. Man kan på olika sätt försöka minska antalet nätfiskemeddelanden som redan skickats till användare, förhindra att någon lätt utnyttjar nätfiskade en ändlös jakt och bidra till att utreda incidenter eller begränsa konsekvenserna av ett lyckat nätfiske.

I denna guide har granskningen av fenomenet avsiktligen begränsats till skydd av Microsofts produkter. Utifrån det gångna året utgör produkterna en klar grupp föremål som enligt Cybersäkerhetscentrets kännedom särskilt har drabbats av kampanjer mot företag. Utifrån Cybersäkerhetscentret förekommer det dessutom ofta brister i införandet av skyddsåtgärder och skyddsinställningar för produkter i organisationerna.

Vi hoppas att organisationer kan hitta hjälp i guiden när de särskilt vill förbättra e-post- och molntjänstmiljön mot hot om nätfiske. Läsaren antas ha grundläggande förståelse av Microsofts molntjänster.

Sammanfattning

De senaste åren har vi ofta fått läsa om att användarnamn och lösenord har hamnat i orätta händer. Oftast har nyheterna handlat om att användardatabaser i olika tjänster har riskerats. Konsumenter har använt samma lösenord i olika tjänster, vilket har gett nätbrottslingar möjlighet att även använda avslöjade användaruppgifter i andra tjänster.

Användningen av molntjänster i organisationer har ökat snabbt. I Finland används Microsofts Office 365-tjänst i stor utsträckning inom både den offentliga och den privata sektorn. De identiteter som används av Office 365 sparas och administreras i tjänsten Azure Active Directory (AD). Ofta är det möjligt att även använda andra molntjänster med samma användaridentitet.

Nätfiske är ett av de vanligaste hoten mot informationssäkerheten. I februari 2019 publicerade Cybersäkerhetscentret årsöversikten Informationssäkerhet 2018. Enligt översikten var det största hotet mot informationssäkerheten 2018 Office 365-bedrägerier som nätfiskade information av användare, ett fenomen som spred sig steg för steg.

Office 365 och de övriga Microsoft-tjänsterna innehåller flera olika funktioner med vilka risken för ett lyckat nätfiske kan reduceras betydligt. Tjänsterna kan köpas i olika versioner, så kallade

prenumerationer, som skiljer sig från varandra. En prenumeration inkluderar ett önskat antal licenser som organisationens IKT-förvaltning delar ut till användare. Organisationen kan köpa likadana licenser för alla användare eller de lämpligaste tjänsterna och licenserna för tjänsterna till personer i olika roller.

Funktioner som kan användas för att begränsa nätfisket beror på vilka prenumerationer som används. I detta dokument presenteras olika skyddsmetoder oberoende av vilka prenumerationer eller licenser en organisation nu använder.

De viktigaste åtgärderna för att begränsa nätfisket är följande oberoende av prenumerationer och licenser:

1. Införa en modern autentisering och tvinga användaren att använda den
2. Införa tvåfaktorsautentisering
3. Säkerställa kvaliteten, mängden och lagringstiden för loggar.

1 Vad bör du skydda dig mot?

Informationssäkerheten består av flera delområden. Detta dokument fokuserar på att begränsa nätfisket.

Nätfiske kan ske på flera olika sätt. I allmänhet skickas meddelanden som används för nätfiske till stora grupper användare. Syftet med riktade bedrägeriförsök är till exempel att få kännedom om kontouppgifter lagrade i en molntjänst som en organisation använder och/eller uppgifter till systemadministratörskonton. Angriparen kan även rikta en attack mot personer i ett företags ledning eller andra personer som behandlar penningtransaktioner och fakturor.

1.1 Brottslingars avsikt är oftast att skapa bluffakturor

För tillfället finns det flera olika kriminella grupper som nätfiskar. Gruppernas kompetensnivå, vanligen använda verktyg och verksamhetsmål varierar något. I regel har brottslingar konstaterats tillämpa minst två olika tillvägagångssätt:

- Det vanligaste sättet är att brottslingar försöker komma över så många inloggningsuppgifter som möjligt. De loggar in på kontot och inhämtar sökord om fakturering. De använder informationen för en bluffaktura och sammanställer fakturan utifrån uppgifterna och kontexten i den rätta fakturan. Om ett konto inte anses vara intressant, använder brottslingarna kontot för att skicka nya nätfiskemeddelanden till offrets kontakter.
- Ett mindre vanligt sätt är att brottslingar försöker följa brevväxlingen i en e-postlåda för att inhämta information. Cybersäkerhetscentret har kännedom om incidenter där brottslingar har gjort intrång i e-postkonton för personer i central ställning och sedan följt utbytet av meddelanden. I sådana fall ställer brottslingar in kontona så att e-posten omsänds till en e-postlåda som hanteras av brottslingarna. Ett specifikt motiv har inte kunnat visas i sådana fall.

1.2 Brottslingar kan kringgå tvåfaktorsautentisering

Olika kriminella gruppers tekniska kunskaper varierar något. Skillnaderna mellan olika grupper har dock minskat. I dag kan de flesta grupper kringgå till exempel en tvåfaktorsautentisering. Tvåfaktorsautentisering har kringgåtts på minst två sätt:

- Det vanligare sättet är att brottslingar loggar in i en tjänst genom att utnyttja Office 365:s egenskap som möjliggör inloggning med enheter eller program som inte stöder tvåfaktorsautentisering. För närvarande kan brottslingar på många olika sätt utnyttja denna egenskap som möjliggör legacystöd. Denna guide innehåller anvisningar om att införa en så kallad modern authentication och förhindra legacyinloggning i en tjänst.
- Brottslingar loggar in i en tjänst med ett nätfiskat användarnamn och lösenord, varvid offret som lämnat uppgifterna får en äkta verifieringskod till exempel per sms. Brottslingarnas nätfiskewebbplats ber offret även ange denna tvåfaktorskod och med koden får brottslingarna åtkomst till den egentliga tjänsten.

1.3 Centralkriminalpolisens exempel på dataintrång i Office 365

Ur polisens synvinkel är nätfiske ett mycket oroväckande fenomen. Nätfisket har i regel genomförts genom att använda en mycket skickligt skapad webbplats. När gärningsmännen har fått åtkomst till ett företags Office 365-tjänst, kan det ha hänt att de har följt företagets e-posttrafik under mycket lång tid. Å andra sidan har polisen fått ett relativt litet antal polisanmälningar om sådana incidenter, vilket gör att polisen saknar en tillräckligt stor mängd data för att kunna identifiera gärningsmännen.

Finansföretaget A
Någon hade gjort ett intrång i företagets Office 365-molntjänst genom nätfiske, dvs. Skickat e-post till två anställda på företaget med en länk till nätfiskewebbplatsen. I systemet hade gärningsmännen följt företagets e-posttrafik under flera månader och skapat regeländringar i omsändningen av e-post utan att företaget haft kännedom om det. Företaget A hade ingen exakt uppfattning om hur länge dess e-posttrafik hade följts och inte heller om vilken information om företaget som eventuellt hade läckt ut. Dessutom hade gärningsmännen försökt lägga till fakturor i företagets betalningar i syfte att få företaget att betala fakturorna på gärningsmännens konto. På fakturorna hade gärningsmännen använt information från e-posttrafiken och på så sätt försökt få fakturorna att se så äkta ut som möjligt.

Industriföretaget B
Någon hade gjort ett intrång i företagets Office 365-molntjänst genom nätfiske på samma sätt som i exemplet ovan. Gärningsmännen hade skickat nätfiskelänkar från företagets e-postsystem till anställda på företagets dotterbolag och företagets underleverantörer och kunder. I företaget upptäckte man att någon hade gjort otillåtna omsändningsregler i e-postsystemet. Till polisens stora förtret upptäcktes dataintrånget så sent att loggdata om intrånget inte var tillgängliga längre.

2 Office 365 sett ur ett nätfiskeperspektiv

Microsoft Office 365 är en tjänst som också används i stor omfattning i Finland. Exchange Online, Sharepoint Online och Teams är de viktigaste delarna av tjänsten. Skype for Business Online kommer att avvecklas eftersom motsvarande kommunikationsfunktioner nu finns i Teams. I de flesta licensalternativ i Office 365 ingår även skrivbordsprogram, till exempel Outlook, Word, Excel och Powerpoint.

Enterprise Mobility + Security (EMS) samlar i sin tur hanterings- och informationssäkerhetstjänsterna för informationsarbete till en enda lösning. Den innehåller de mest omfattande versionerna av Azure Active Directory, Intune-tjänsten för hantering av klienter och Azure Information Protection för skydd av data.

Microsoft 365[1] inkluderar Office 365, Windows 10 och Enterprise Mobility + Security.

I regel används e-postadresser som verktyg för nätfiske av inloggningsuppgifter, och målet är att komma över användares inloggningsnamn och lösenord. Därför är tjänsten Exchange och Azure Active Directory, som tar emot inloggningar, de viktigaste Office 365-tjänsterna vad gäller nätfiske. Genom att förbättra skyddet av dem kan nätfiske sannolikt förhindras eller så kan åtminstone sannolikheten för ett lyckat nätfiske minskas betydligt.

Vid nätfiske kan till exempel SharePoint-rutor visas för användaren. Rutorna är dock vare sig äkta eller organisationens egna och därför hjälper det inte med att skydda den egna SharePoint-tjänsten.

Om nätfisket lyckas och brottslingarna kommer över vissa lösenord, kan spåren visas i loggarna över e-postadresser och inloggningar samt även över andra tjänster. Detta behandlas närmare i avsnittet Skyddsåtgärder.

[1] https://www.microsoft.com/sv-SE/microsoft-365

2.1 Office 365-versioner

Office 365 innehåller en Business-version för organisationer med högst 300 personer och en Enterprise-version för större organisationer. Det sistnämnda[2] innehåller nivåerna E1, E3 och E5. Dessutom ingår konsument- och utbildningsversioner (Education A1, A3 och A5).

Office 365 har kunnat köpas separat eller som en del av Microsoft 365. Microsoft 365 innehåller även en mer begränsad E3-nivå och en mer omfattande E5-nivå.

Inloggning i Office 365-tjänsterna sker med Azure Active Directory. Basic-versionen ingår alltid i Office 365 medan den mer omfattande Premium-versionen P1 eller P2 kan köpas som en del av EMS, med andra ord tillsammans med exempelvis Microsoft 365. Dessutom finns Microsoft 365 i versionen Microsoft 365 Firstline 1[3] som inkluderar bland annat Azure Active Directory Premium P1.

Tabellen nedan åskådliggör de olika alternativen. Office 365 Business finns i en separat kolumn, men som det ovan konstaterats kan Office 365 Enterprise dock även köpas separat.

Delområde	**Office 365 Business-version separat**	**Microsoft 365 E3**	**Microsoft 365 E5**
Office 365	Business	Enterprise E3	Enterprise E5
EMS		EMS E3, inklusive Azure AD P1 + annat	EMS E5, inklusive Azure AD P2 + annat
Windows 10		Enterprise	Enterprise + Windows Defender Advance Threat Protection

Prenumerationer och licenser som ingår i dem kan också kombineras. En adminstratör kan med andra ord ha en licens för Microsoft 365 F1, och dessutom kan en licens för Azure AD P2 köpas för personen så att till exempel funktionen Privileged Identity Management kan tas i bruk.

Den 1 februari 2019 lanserades nya tillägg till Microsoft 365 E3-prenumerationen, dvs. Identity and Threat Protection och Information Protection and Compliance, som innehåller säkerhetsfunktioner. Som det även framgår av namnen, inkluderar särskilt det förstnämnda de viktigaste tjänsterna för identitetshantering. På https://github.com/AaronDinnage/Licensing finns scheman över olika servicepaket och funktioner som ingår i paketen.

[2] https://products.office.com/sv-se/business/compare-more-office-365-for-business-plans
[3] https://www.microsoft.com/sv-se/microsoft-365/compare-all-microsoft-365-plans

2.2 Identitet (Azure Active Directory)

Azure Active Directory är en tjänst för identitetshantering. Tjänsten används av sammanlagt över en miljard personer i tiotals miljoner organisationer. En del av dessa använder Office 365, en del Azure AD för andra program. Olika organisationer och deras användare och data är logiskt fördelade på separata abonnenter (tenants) och åtskilda från varandra[4].

Det finns två identitetstyper i Azure AD: molnidentitet (managed) och federerad identitet (federated). I det förstnämnda identifieras användaren alltid genom Azure AD. I det sistnämnda sker identifieringen utanför Azure AD och utifrån en betrodd relation förlitar sig Azure AD på den externa identifieringen. En identitetstyp är specifik för en domän (domändelen av en e-postadress).

Antalet program som är integrerade i Azure AD är flera hundra tusen. Användare behöver inte separat logga in i programmen, utan det räcker med att logga in på Azure AD. Vid auktorisering av användning av programmen kan Azure AD-användargrupper användas.

Azure AD kan anslutas till tjänsten Active Directory Domain Services (AD DS) som finns i det organisationsinterna nätet (on-premises) och som ofta kallas Active Directory eller en aktiv katalog. Genom anslutningen kan samma identifieringsuppgifter användas både i tjänster i det organisationsinterna nätet och i molntjänster. Oftast genomförs anslutningen med programmet Azure Active Directory Connect som kan installeras på en server i ett internt nät.

I en integrerad miljö sker inloggningen på ett av följande sätt[5]:

1. Teckensträng som härletts från lösenord synkroniseras i Azure Active Directory.
   (Password Hash Synchronization - PHS)[6].
   Vid användning av molntjänster görs verifieringen av Microsofts tjänst Azure Active Directory.

2. Federerad inloggning: det är endast identiteterna som synkroniseras, inte de teckensträngar som härletts från lösenord. När en användare loggar in på en molntjänst dirigeras användaren till tjänsten Active Directory Federation Services (AD FS) i en on-premises-miljö. Oftast kräver denna lösning minst fyra servrar (två i det interna nätet och två i DMZ-zonen).
   Domänkontrollanten (domain controller) av Active Directory gör verifieringen.

3. I en on-premises-miljö används tjänsten Passthrough Authentication (PTA). Denna lösning kan ersätta tjänsten AD FS om organisationen inte har andra tjänster som har genomförts med AD FS och som kräver engångsinloggning.

4. I en on-premises-miljö används tjänsten PingFederate[7] som gör verifieringen.

Även om en organisation använder en federerad inloggning (alternativ 2 på listan ovan), kan teckensträngar som härletts från lösenord också synkroniseras i Azure AD (alternativ 1 på listan). Denna metod har två fördelar:

a) det går fortare att gå över till en molnidentitet i stället för en federerad identitet, om det eventuellt uppstår fel i on-premises-federeringstjänsten
b) identifieringsuppgifter som har hamnat i orätta händer kan identifieras (Azure AD-rapporten leaked credentials[8]).

Azure AD inkluderar enligt självbetjäningsprincipen även en funktion för att återställa lösenord. Synkroniserade användares lösenord som har återställts i en molntjänst kan återsynkroniseras i on-premises Active Directory. För detta behövs Azure AD Premium (P1 eller P2).

Med tanke på övergripande identitetsadministration och skydd mot nätfiske är följande de viktigaste funktionerna i Azure AD:

[4] http://aka.ms/Office365TI
[5] https://docs.microsoft.com/en-us/azure/security/azure-ad-choose-authn
[6] https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-password-hash-synchronization
[7] https://docs.pingidentity.com/bundle/O365IG20_sm_integrationGuide/page/O365IG_c_integrationGuide.html
[8] https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/Azure-Active-Directory-Premium-reporting-now-detects-leaked/ba-p/249200

Multifaktorautentisering (Multi Factor Authentication - MFA)

MFA möjliggör en ytterligare identitetskontroll efter en konventionell identifiering med kombination av användarnamn och lösenord. Alternativen för ytterligare kontroll är följande:

- engångskod per telefon
- engångskod per sms
- godkännande med mobilapp (Microsoft Authenticator)
- engångskod med mobilapp (Microsoft Authenticator).

Microsofts molnbaserade MFA finns i tre versioner:

1. Multi-Factor Authentication for Office 365. En mer begränsad version som medföljer Office 365 och som endast kan användas för att skydda Office 365-program. I denna version ska MFA-kravet aktiveras separat för varje användare.
2. Azure Multi-Factor Authentication. Azure AD Premium (P1 eller P2) tillåter aktivering av MFA-kravet enligt Conditional Access-villkoren eller separat för varje användare. För identifiering används tjänsten Azure MFA eller så kan en särskild server för identifiering installeras i ett internt nät.
   OBS! Till och med den 1 september 2018 kunde Azure MFA köpas med en separat licens. Numera kan den dock endast köpas i anslutning till en Azure AD Premium-prenumeration.
3. MFA for Azure Active Directory Global Administrators. Ursprungligen kunde MFA endast införas för användare som hade rollen Global Administrator med alla behörigheter för Azure AD. Senare har tjänsten utvidgats till att även omfatta andra användare. År 2018 lanserade Microsoft Global Administrator, en funktion som kan införas med ett särskilt Conditional Access baseline protection-protokoll. Microsoft ska aktivera protokollet i anslutning till lanseringen, dvs. när det når General Availability.

.

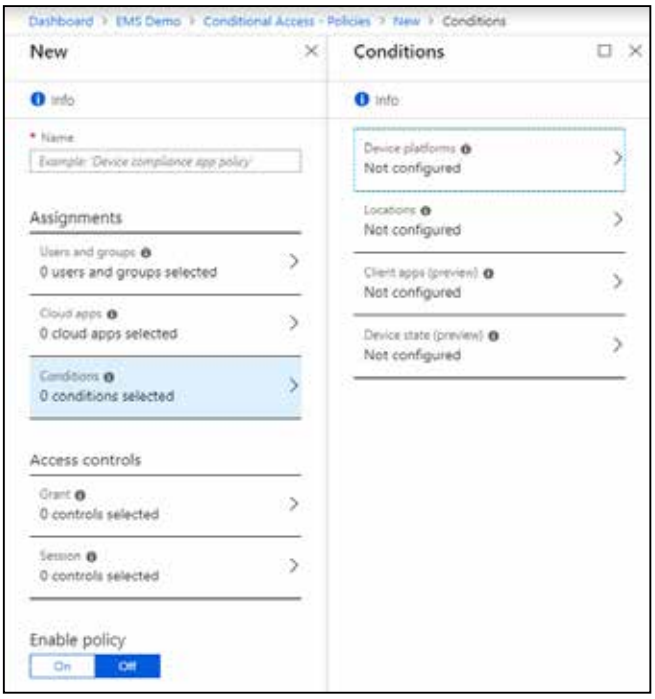
Conditional Access

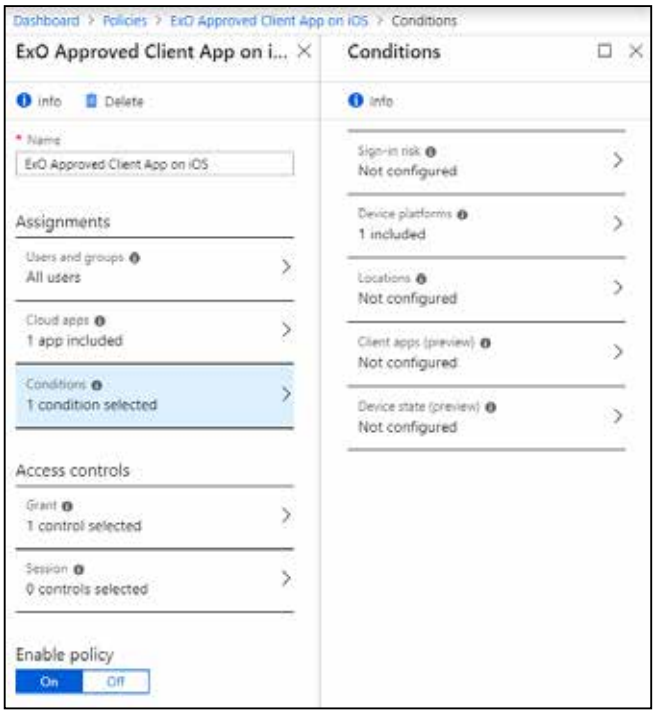
Conditional Access, eller villkorlig åtkomst, tillåter eller förhindrar användning av vissa bestämda tjänster, till exempel Office 365 och Exchange Online, när vissa villkor är uppfyllda. Åtkomst kan tillåtas för exempelvis en kombination av användarens position, enhet, tjänst och identifieringsmetod.

Vanligen är exempelvis en kombination av ett användarnamn och lösenord endast tillåten från ett internt nät medan tvåfaktorsautentisering krävs vid identifiering från ett offentligt nät. Ett annat vanligt exempel är att vissa tjänster endast kan användas med organisationens enheter. I så fall kan exempelvis Office 365-tjänster inte användas med hemdator.

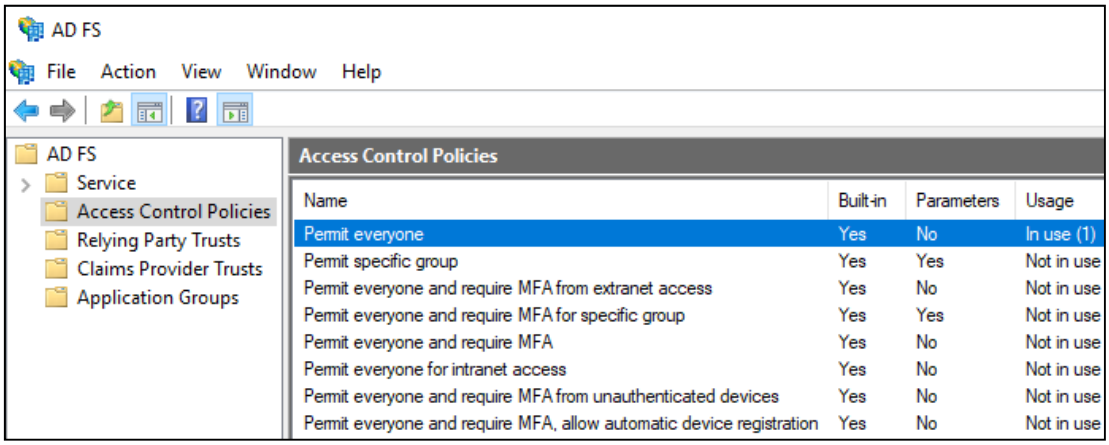
Azure Active Directory Conditional Access kan användas i Azure AD Premium-prenumerationer.

På bilden nedan visas standardprotokollen för tjänsten Windows Server 2019 AD FS.





Vid avsaknad av Azure AD Premium-licenser kan en motsvarande funktion införas med federerad identitet genom att använda Microsoft Active Directory Federation Services (AD FS). AD FS är en roll som ingår i Windows-serveroperativsystemen. På bilden ovan visas standardprotokollen för tjänsten Windows Server 2019 AD FS.

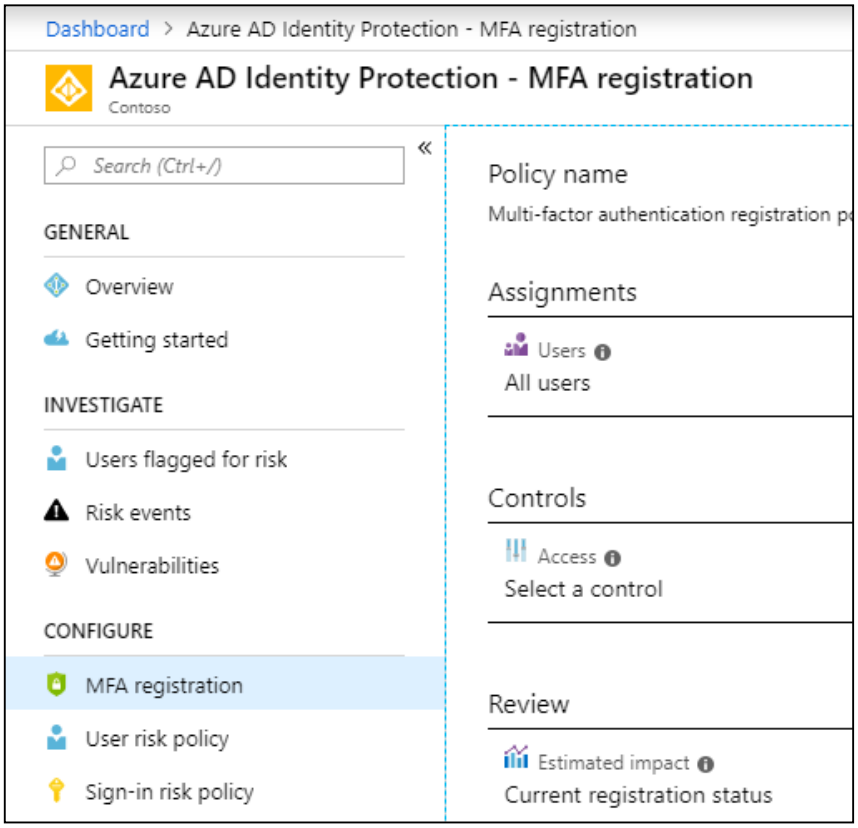


Identity Protection[9]

I Följande kan införas med Identity Protection:

1. Identifiering av sårbarheter som påverkar organisationens identiteter
2. Automatiska åtgärder vid upptäckta tvivelaktiga händelser gällande identiteter
3. Forensik och utredning av tvivelaktiga händelser.

I Identity Protection ingår även MFA Registration, en funktion med vilka önskade användare kan tvingas att registrera sig som användare av MFA. I januari 2019 infördes en del nya funktioner i tjänsten Identity Protection[10].



[9] https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/index

[10] https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Four-major-Azure-AD-Identity-Protection-enhancements-are-now-in/ba-p/326935

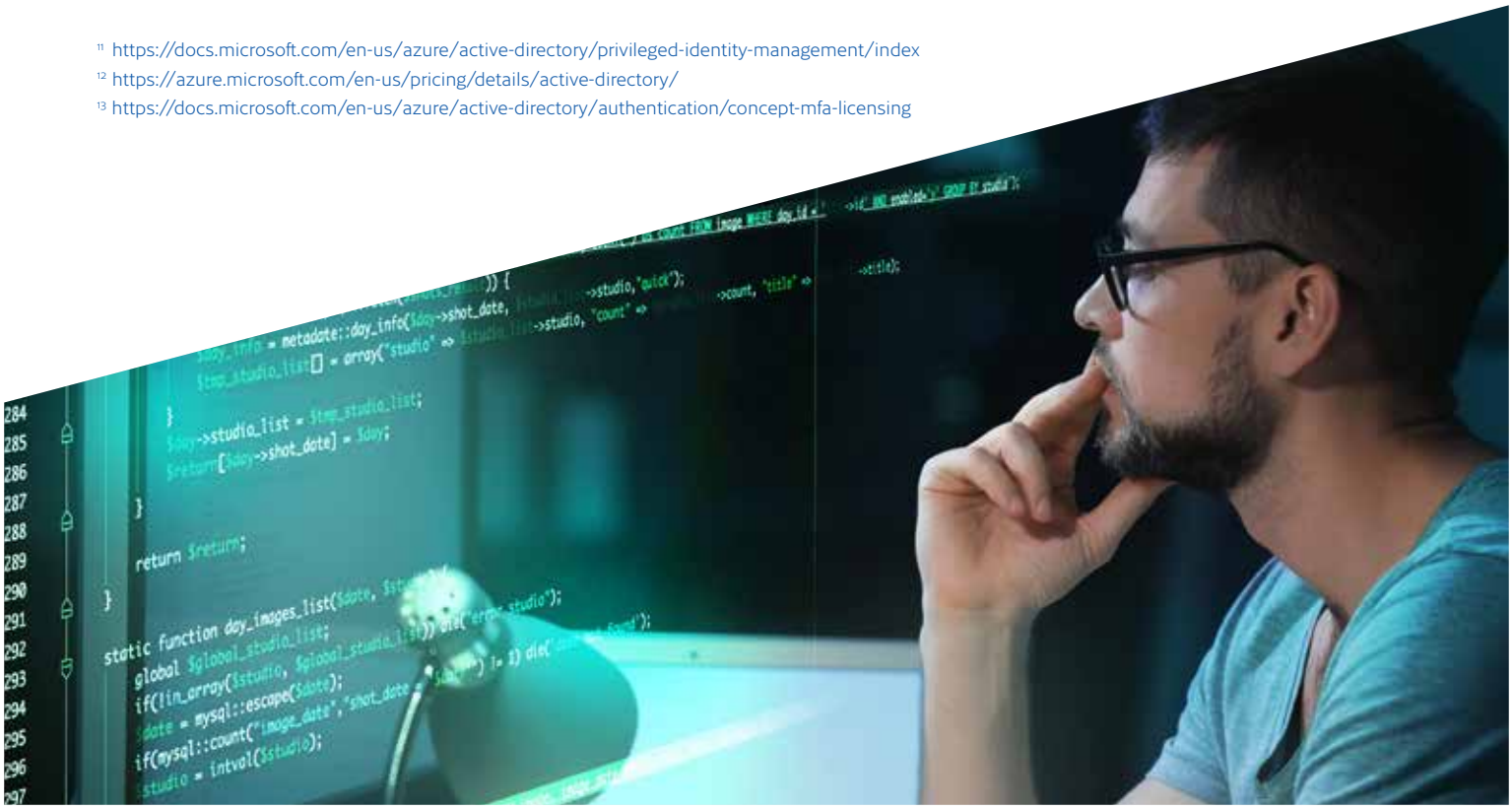
Azure Active Directory Privileged Identity Management[11]

Genom tjänsten Privileged Identity Management är det äntligen möjligt att ta kontroll över medlemskapet för Azure AD- och Azure-hanteringsrollerna så att systemadministratörernas roller är flexibla. I flera situationer kan antalet ordinarie systemadministratörer reduceras. Användare börjar använda roller och behörigheter om det behövs och användningen kan följas upp. Roller kan aktiveras genom ett förfarande för godkännande används, där endast bestämda personer kan godkänna att en person blir systemadministratör. Dessa funktioner visas i tabellen nedan.

		Azure AD-version		
Funktion		**Basic och Office 365**	**Azure AD P1**	**Azure AD P2**
Multi-Factor Authentication for Office 365		X	X	X
Azure Multi-Factor Authentication			X	X
Conditional Access	Baserat på terminal-utrustningens operativ-system, position, använd applikation eller utrustnin-gens status		X	X
	Baserat på risk			X
Identity Protection				X
Priviledged Identity Management				X

De olika AD-versionerna och deras funktioner presenteras närmare på sidan för prissättning av Azure AD-tjänsten[12].
Funktionerna i de olika versionerna av MFA-tjänsten presenteras på en separat sida[13].

[11] https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/index
[12] https://azure.microsoft.com/en-us/pricing/details/active-directory/
[13] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing



2.3 Tekniker för skydd av e-postadresser

E-postadresser kan skyddas genom olika tekniska åtgärder. Trafiken mellan e-postservrar kan krypteras och kryptering tvingas med TLS (Transport Layer Security). TLS bygger på certifikat vilket gör att det samtidigt är möjligt att styrka den andra partens identitet.

Dessutom finns det olika tekniker för hantering av skräppost[14]. Med de tekniker som presenteras i tabellen nedan är det möjligt att förhindra att e-post som skickats från Office 365-miljön markeras som skräppost. Det är inte möjligt att påverka inkommande e-post eftersom inställningarna alltid fastställs av avsändaren.

	SPF	DKIM	DMARC
Vad betyder?	Sender Policy Framework	DomainKeys Identified Email	Domain-Based Message Authentication, Reporting, and Conformance
Vad är det?	Ett system som anger och verifierar vem som kan skicka e-postmeddelanden från en viss domän.	Ett identifieringssystem för e-post, som bygger på asymmetriska krypteringsnycklar.	Ett identifieringssystem för e-post, som hjälper till att utreda vad som ska göras om ett meddelande inte godkänns i SPF- eller DKIM-kontrollerna.
På vilket sätt fungerar det?	Mottagaren kontrollerar om avsändaren har behörighet att skicka e-postmeddelanden från domänen. Informationen är lagrad i TXT-posten i domänens DNS-system.	Avsändaren undertecknar e-postmeddelandet och/eller rubrikinformationen. Mottagaren kontrollerar signaturen och försäkrar sig om att informationen inte har förändrats. Den offentliga nyckeln införs i TXT-posten i domänens DNS-system.	Mottagaren gör SPF- och DKIM-kontrollerna. Om kontrollerna misslyckas, kontrollerar den avsändarens DMARC-protokoll och beslutar vad som ska göras: stoppar meddelandet, sätter det i karantän, skickar det normalt, rapporterar till avsändaren. DMARC-protokollet införs i TXT-posten i domänens DNS-system.
Varför är det viktigt?	Minskar sannolikheten för att utgående meddelanden markeras som skräppost.	Minskar betydligt sannolikheten för att utgående meddelanden markeras som skräppost.	Hjälper den mottagande organisationen att besluta vad denna ska göra med e-postmeddelanden som inte godkänns i kontrollerna. Fungerar även som responskanal för avsändaren.

2.4 Dela information i olika tjänster

I Office 365 kan egna filer delas till parter utanför organisationen i syfte att främja samarbete. Delningen sker framför allt från SharePoint-dokumentbibliotek, antingen direkt med SharePoint-funktioner eller med Teams- eller OneDrive for Business-funktioner baserade på SharePoint.

Åtkomsten för gästanvändare till organisationens dokument kan regleras i följande versioner:

- Azure AD. Bastjänst för identitet och identitet hantering.
- SharePoint Online och OneDrive for Business. OneDrive for Business fungerar också baserat på SharePoint-dokumentbibliotek.
- Office 365 Groups. Dessa grupper kan användas vid auktorisering och gruppkommunikation.
- Teams. Varje team bygger på ett Office 365 Groups-team och ett SharePoint-dokumentbibliotek.

Under länken i fotnoten finns en beskrivning av åtkomsten för gästanvändare till dokument i Teams[15].

Cloud App Security[16] är Microsofts CASB-lösning (Cloud Access Security Broker) för uppföljning av användningen av data som lagras i Office 365 och även i andra molntjänster samt för skydd av data. Med lösningen går det att:

- följa upp de molntjänster som organisationen använder och riskerna i tjänsterna

[14] https://blogs.technet.microsoft.com/fasttracktips/2016/07/16/spf-dkim-dmarc-and-exchange-online/

[15] https://docs.microsoft.com/en-us/microsoftteams/teams-dependencies

[16] https://docs.microsoft.com/en-us/cloud-app-security/

- skydda data genom att följa upp och hantera användningen av molntjänster
- identifiera avvikande beteende och informationssäkerhetskränkningar och att automatiskt reagera på dem. Detta kan realiseras till exempel när ett nätfiske har lyckats och filer delas med nätfiskade användarkoder i en molntjänst till externa användare.

Tjänsten finns i två versioner[17]: Office 365 Cloud App Security och Microsoft Cloud App Security. Den förstnämnda ingår i Office 365 E5-paketet och den sistnämnda i EMS E5-paketet.

2.5 Informationssäkerhetsarkitektur

Azure Active Directorys informationssäkerhetsarkitektur skiljer sig betydligt från konventionella Active Directorys. I tabellen nedan presenteras vissa skillnader mellan Active Directory Domain Service, som har integrerats i operativsystemet Windows Server, och Azure Active Directory.

	Active Directory (Domain Services)	**Azure Active Directory**
Användningsändamål	On-premises identitetshantering för Windows-maskiner	Identitetstjänst för molneran (Identity as a Service IDaaS)
Verifiering	Kerberos och NTLM	OpenID Connect Security Assertion Markup Language (SAML), WS-Federation, ADAL
Auktorisering	Tjänster för operativsystem	OAuth2
Informationsinhämtning	LDAP	REST API, dvs. HTTP eller HTTPS
Hanteringsgränser	Skog, träd, domän	Hyresgäst (tenant)
Åtkomst	Främst organisationens interna nät; vissa funktioner, t.ex. verifiering, kan också användas via andra tjänster från ett externt nät	Från vilket som helst ställe
Integration mellan organisationer	Arbetskrävande	Enkel

En av Microsofts identitetstjänster är Azure Active Directory Domain Services[18]. Den är en begränsad version av konventionella Active Directory. Dess användningsändamål är att tillhandahålla Active Directorys tjänster (verifiering, sökning och Group Policy) till tjänster som fungerar med virtuella maskiner som förs över till Azure.

2.5.1 Azure Active Directorys kontrollmodell

Azure AD är försedd med en rollbaserad kontrollmodell (Role-Based Access Control, RBAC). Modellen omfattar flera olika roller och Global Administrator har de största behörigheterna bland alla roller. Endast de som ingår i denna roll har behörighet att bevilja andra användare administratörsbehörigheter och till exempel att lägga till nya domäner. Användare (User) är i sin tur den minsta behörighetsrollen och beviljas automatiskt alla användare av Azure AD-katalogen. Rollen ”User Account Administrator” räcker till för daglig kontroll över användare, till exempel för licenshantering och återställande av lösenord.

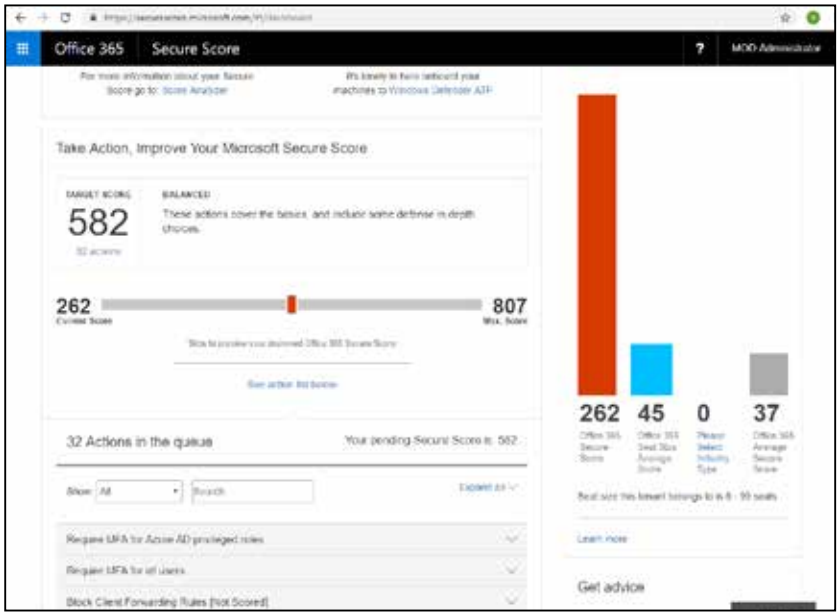
I Azure AD ingår samma informationssäkerhetsgrupper som i Active Directory. Dessa grupper kan användas till exempel för administration av åtkomstbehörigheter i SharePoint Online. Till skillnad från Active Directory kan grupper i Azure AD inte beviljas RBAC-roller. Om Azure AD har anslutits till Active Directory kan grupperna administreras i Active Directory.

När Azure AD:s skyddsfunktioner används ska åtkomsten säkerställas genom olika undantagsarrangemang. Microsoft har berett en instruktion[19] för hur man kan förbereda sig för olika undantagssituationer.

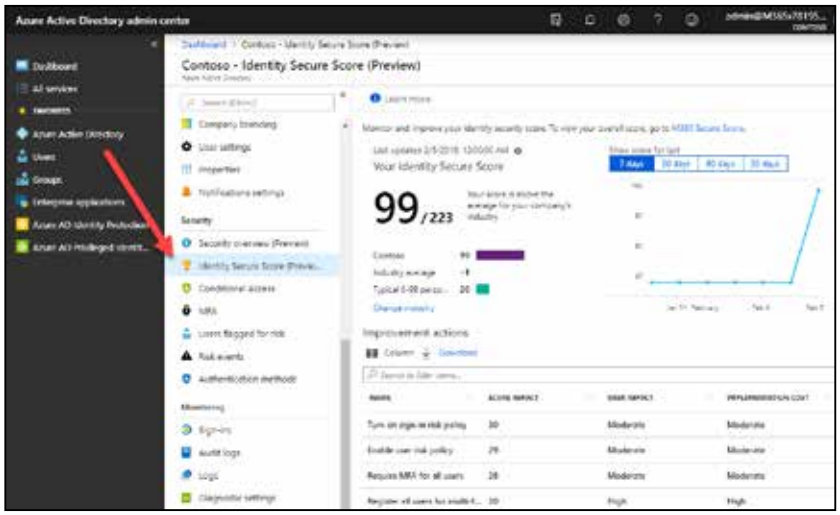
[17] https://docs.microsoft.com/en-us/cloud-app-security/editions-cloud-app-security-o365
[18] https://docs.microsoft.com/en-us/azure/active-directory-domain-services/
[19] https://aka.ms/resilientaad

2.6 Microsoft Secure Score

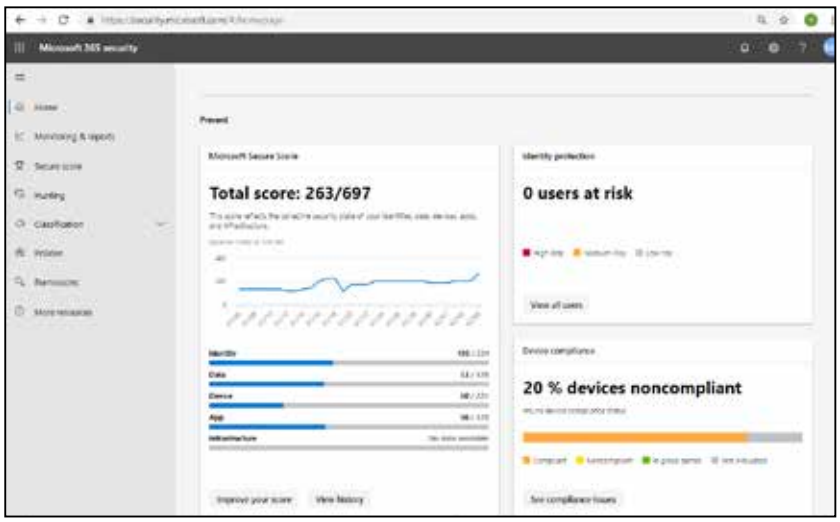
Microsoft Office 365 Secure Score[20] lanserades hösten 2016. Med verktyget ser organisationens systemadministratörer en analys av organisationens kuranta Office 365-informationssäkerhetsläge och får rekommendationer om åtgärder för att förbättra läget. I anslutning till varje åtgärd beskrivs de hot som bekämpas genom åtgärden. Det beskrivs också vilken inverkan åtgärden har på användares verksamhet och hur komplicerat införandet är.



Identity Secure Score lanserades i sin tur hösten 2018. Det kan användas som en del av Azure AD-hanteringsportalen.



I januari 2019 lanserade Microsoft nya Microsoft 365 security center- och compliance center-portalerna[21]. De kan användas med Microsoft 365 E3- eller E5-prenumeration. I Security center är Secure Score indelat i olika avsnitt. Samma verktyg inkluderar även till exempel en kombination av olika forensiska funktioner. Genom portalen Security center har informationen ur olika källor kombinerats, och därför behöver användaren inte öppna många olika portaler.



[20] https://securescore.microsoft.com/

[21] https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Introducing-the-new-Microsoft-365-security-center-and-Microsoft/ba-p/326959

3 Skyddsåtgärder

Genom åren har det kunnat hända att en viss teknikskuld har uppstått i organisationens egna tjänster när tjänsterna inte av olika skäl har uppdaterats med de senaste versionerna. Ett gott exempel är Windows 7-operativsystemet som fortfarande används i stor utsträckning. När systemet förr i tiden planerades kunde hänsyn inte tas till dagens hot.

Molntjänsterna uppdateras till och med varje vecka. Därför har särskilt underhållet och stödfunktionerna utmaningar med att följa utvecklingen.

När dessa två verkligheter förenas med varandra kan konsekvensen vara ett komplicerat införandeprojekt.

3.1 Skydd av identiteter

Vid skydd är det viktigast att skydda användares identiteter. I dag används tjänster i alla slags moln med olika klienter och var som helst. Därför är de konventionella skyddsåtgärderna inte längre tillräckliga.

3.1.1 Skräddarsy inloggningssidorna enligt din organisations grafiska utseende

Inloggningssidorna för Office 365-tjänsten kan skräddarsys enligt organisationens grafiska utseende[22]. Samtidigt blir användare vana vid utseendet och det blir svårare att lyckas med ett nätfiske genom att förfalska skräddarsydda sidor.

En användare kan dock inte helt lita på utseendet eftersom de förfalskade sidorna kan likna de ursprungliga sidorna fullständigt. Även i sådana situationer kan förfalskningen avslöjas utifrån adressraden och certifikatuppgifterna.

3.1.2 Skydda lösenord

Det är viktigt att se till att lösenorden är komplicerade och tillräckligt långa. På så sätt minskar sannolikheten för att någon lyckas knäcka lösenord. Vid nätfiske hjälper dock ett komplicerat lösenord inte särskilt mycket om användaren anger ett lösenord som består av fraser eller något annat starkt lösenord på fel webbplats.

I dag kan allmänt använda teckensträngar förhindras i både Azure AD och on-premises Active Directory[23]. För att begränsa lösenord med denna funktion i en on-premises-miljö krävs det Azure AD Premium-licenser.

Det finns flera olika tekniker för att förhindra att lösenord gissas eller knäcks genom grov beräkning. Microsoft har infört rekommenderade åtgärder för att förhindra att lösenord gissas eller knäcks[24].

Vid federerad inloggning finns det skäl att kontrollera att det används Extranet Lockout[25]. Funktionen blev tillgänglig i versionen Windows Server 2012 R2 och har vidareutvecklats i de senare operativsystemen (Windows Server 2016 och 2019).

3.1.3 Skydda Azure Active Directory

Särskilt i en miljö som är ansluten till Azure AD är det också viktigt att hantera lokala Active Directory.

År 2000 lanserades Active Directory integrerat i Windows Server 2000. Under de senaste närmare 20 åren har det skapats flera rekommendabla metoder för att administrera och skydda tjänsten. Dessutom har tjänsten i den senaste versionen nästan inte alls utvecklats längre, eftersom Microsoft har fokuserat sina insatser på att utveckla molntjänster, inbegripet Azure Active Directory.

[22] https://docs.microsoft.com/en-us/office365/admin/setup/customize-sign-in-page?view=o365-worldwide
[23] https://aka.ms/aadpasswordprotectiondocs
[24] https://www.microsoft.com/en-us/microsoft-365/blog/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/
[25] https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection

Informationssäkerhetsfunktioner i Active Directory är bland annat:

- hantering
- administration av inloggningsuppgifter och användargrupper
- centraliserad hantering av inställningar med Group Policy
- observation
- loggdata och larm.

Det är krävande att specificera tusentals Group Policy-inställningar manuellt. Därför har Microsoft i åratal gett ut Security Baseline-dokument där dessa inställningar är specificerade på olika informationssäkerhetsnivåer. Det senaste verktyget är Security Compliance Toolkit (SCT)[26].

Ett av de delområden som hanteras med Group Policy är kraven på lösenord. I Azure AD krävs det att lösenordet ska bestå av 8–16 tecken och enligt komplexitetskravet minst tre av följande: stora bokstäver, små bokstäver, siffror och specialtecken. I en lokal AD som är ansluten till Azure AD gäller dock lösenordspraxis i Azure AD inte nödvändigtvis. I värsta fall är det med andra ord möjligt att det skapas lösenord med ett tecken för synkroniserade användarkoder i Azure AD.

I regel görs specifikationerna för auditeringsloggarna också centraliserat med Group Policy. I detta dokument behandlas inte enskilda loggar och deras inställningar. Med tanke på nätfiske finns det skäl att säkerställa loggdata om enskilda inloggningar. Loggdata om enskilda maskiner och särskilt servrar ska lagras centralt. Detta lyckas med funktionen Windows Event Forwarding[27] i Windows-operativsystemet. Konsoliderade loggdata kan införas i SIEM-system där händelser kan analyseras noggrannare och larm kan ställas in.

3.1.4 Modern Authentication är en förutsättning för säker tvåfaktorsautentisering

Modern Authentication[28], dvs. modern autentisering, är en paraplyterm som omfattar olika kombinationer av identifierings- och auktoriseringsmetoder. En säkert genomförd tvåfaktorsautentisering kräver en modern autentisering.

Modern autentisering är en standardautentisering i Office 365- abonnenter som har skapats efter den 1 juli 2017. Användningen av en modern autentisering säkerställs eller en modern autentisering införs med PowerShell-kommandon:

- Exchange Online[29]
- SharePoint Online[30]
- Skype for Business Online[31].

Vid användning av en hybridmiljö ska den moderna autentiseringen även aktiveras i den lokala Exchange[32]- och Skype for Business[33]-miljön. I en federerad miljö har införandet fler faser.

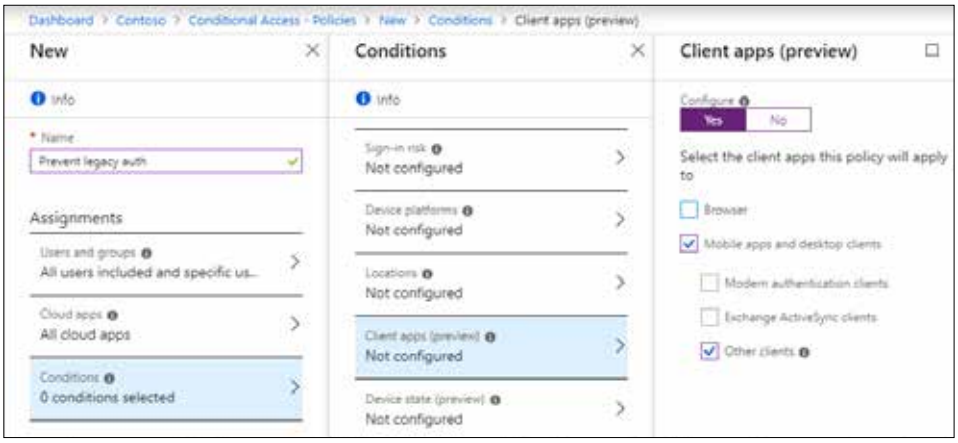
[26] https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10
[27] https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection
[28] https://docs.microsoft.com/en-us/office365/enterprise/hybrid-modern-auth-overview#BKMK_WhatisModAuth
[29] https://docs.microsoft.com/en-us/Exchange/clients-and-mobile-in-exchange-online/enable-or-disable-modern-authentication-in-exchange-online
[30] https://docs.microsoft.com/ga-ie/azure/active-directory/conditional-access/conditional-access-for-exo-and-spo
[31] https://social.technet.microsoft.com/wiki/contents/articles/34339.skype-for-business-online-enable-your-tenant-for-modern-authentication.aspx
[32] https://docs.microsoft.com/en-us/office365/enterprise/configure-exchange-server-for-hybrid-modern-authentication
[33] https://docs.microsoft.com/en-gb/skypeforbusiness/manage/authentication/use-adal

3.1.5 Förhindra metoder som inte stöder tvåfaktorsautentisering

De konventionella e-postprotokollen, som POP, IMAP, SMTP och ActiveSync, stöder inte modern autentisering. Vid användning av tvåfaktorsautentisering går det fortfarande att via dessa protokoll identifiera sig med en kombination av ett användarnamn och lösenord. Därför gäller det att förhindra användning av dessa protokoll och att använda Office-kundprogram eller andra program som stöder modern autentisering på både datorer och mobila enheter.

Tjänsten Exchange har den viktigaste rollen i begränsningen av nätfisket. Användning av Modern Authentication kan vara tvingad i en federerad miljö med regler som har specificerats i tjänsten AD FS[34]. Hösten 2018 blev det möjligt att i Exchange förhindra Basic Authentication med autentiseringspraxis som kan riktas till och med till enskilda användare[35].

Sedan sommaren 2018[36] kan användning av program som inte använder modern autentisering (inkl. Exchange) förhindras i Azure Active Directory med Conditional Access-regler. På bilden nedan specificeras Client apps-villkoret så att användning av program som inte använder modern autentisering förhindras.



Alternativen för att tvinga modern autentisering presenteras i tabellen nedan.

Genomförandemetod	Fördelar	Utmaningar
AD FS-regler	Existerande tjänst i operativsystemet. Genom tjänsten går det att förhindra att osäkra protokoll och identifiering används utifrån interna nätet.	Kan endast användas i federerade miljöer. En mer komplicerad specifikation (ett eget ”programmeringsspråk”).
Inställning på servicenivå (Exchange Online)	Kan med protokoll ställas in även för enskilda användare.	Om den inte är ett standardprotokoll måste den aktiveras separat för varje användare.
Conditional Access	Enkel att genomföra.	Kräver en Azure AD Premium-prenumeration.

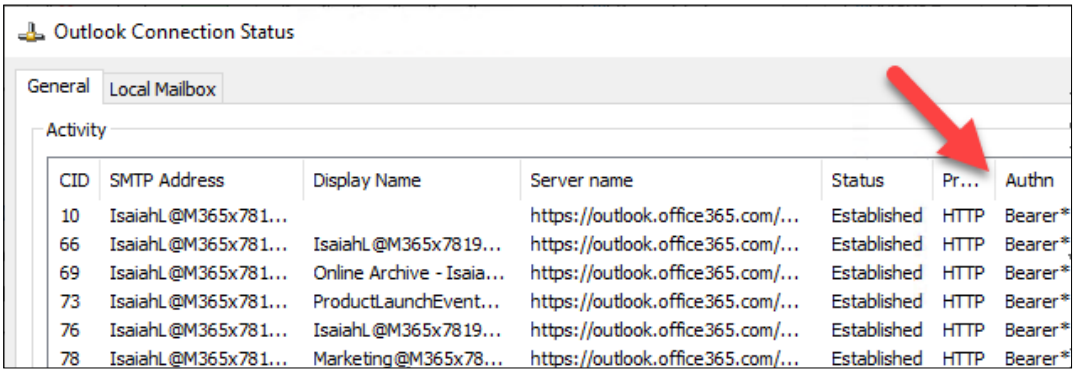
[34] https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditional-access-for-exo-and-spo
[35] https://blogs.technet.microsoft.com/exchange/2018/10/17/disabling-basic-authentication-in-exchange-online-public-preview-now-available/
[36] https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Conditional-Access-support-for-blocking-legacy-auth-is/ba-p/245417

3.1.6 Modern Authentication-stöd för program

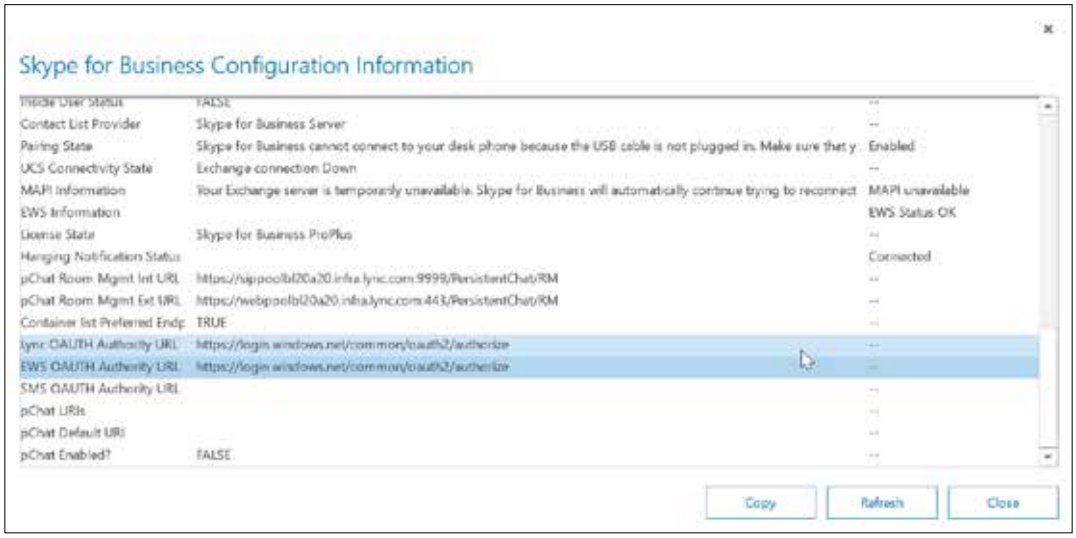
Modern Authentication kräver ett stöd och eventuellt också åtgärder i de program som används.

Alla Office 365-tjänster stöder modern autentisering. När tjänster används med webbläsare är modern autentisering den enda användbara identifieringsmetoden. De övriga kundprogrammen, som e-post (Outlook) och snabbmeddelanden (Skype for Business), kan dock kräva åtgärder på användares arbetsstationer beroende på vilka versioner av Office-programmen som används. Modern autentisering är standardidentifiering i Office 2016 medan den i Office 2013 måste aktiveras separat[37].

Användning av modern autentisering kan även kontrolleras i klientapplikationen. I detta dokument presenteras Outlook och Skype for Business. I båda programmen har man klickat på programikonen i aktivitetsfältet samtidigt med <Ctrl> och sedan valt Connection Status (Outlook) och Configuration Information (Skype for Business).



I Apples iOS-operativsystem infördes stödet för modern autentisering i version 11. Det finns dock vissa brister i versionen och de korrigerades i version 12. Apple macOS 10.14 var den första versionen som innehöll stöd för modern autentisering. De ursprungliga e-postprogrammen i operativsystemet Android stöder inte modern autentisering. Stödet finns i vissa av tredje parters kundprogram, bland annat 9Folders Nine[38].



[37] https://docs.microsoft.com/en-us/office365/enterprise/modern-auth-for-office-2013-and-2016
[38] http://www.9folders.com/

3.1.7 Inför tvåfaktorsautentisering

Kontrollera att Modern Authentication har införts enligt de skeden som beskrivs ovan. På så sätt utesluts möjligheten till bakdörrar, dvs. tvåfaktorsautentiseringen är verkligt säker.

Tvåfaktorsautentisering kan införas antingen separat för enskilda användare eller med hjälp av Conditional Access. Specifikationen av införandet separat för varje användare blev tillgänglig tidigare och kan genomföras utan Azure AD Premium-licenser. Dessutom är det möjligt att specificera att en kontroll inte behöver göras inom nästa 1–60 dagar om identifieringen har lyckats. Detta rekommenderas dock inte. Om enheten blir stulen går det att logga in med enheten utan tvåfaktorsautentisering.

Med Azure MFA går det att specificera sådana önskade IPv4-subnät som inte ska kontrolleras. Vid användning av en federerad identitet och AD FS kan detta även genomföras med AD FS-regler.

Om man vill ha en ännu mångsidigare lösning för en on-premises-miljö, kan en MFA Server[39] ställas in på on-premises-servern. Med den kan tvåfaktorsautentisering även införas för andra tjänster än dem som är integrerade i Azure Active Directory. Sådana andra tjänster är exempelvis Remote Desktop, lokala IIS-webbapplikationer och program som använder AD FS för inloggning.

Användare ska specificera inställningarna för tvåfaktorsautentisering[40]. Specifikationen görs i användarens Access Panel-portal på https://myapps.microsoft.com eller direkt på https://aka.ms/mfasetup. För att förbättra kundupplevelsen har det tagits fram en webbplats för administration av självbetjäningsportalen för lösenord och webbplatsen har integrerats i MFA. I februari 2019 när detta dokument skrevs var webbplatsen i testskedet[41]. Webbplatsen måste aktiveras i abonnentens inställningar.

En utmaning med tvåfaktorsautentisering är användare som ännu inte har aktiverat dessa kontrollfunktioner i enlighet med specifika metoder. Den som nätfiskar identifieringsuppgifter kan lyckas få sin egen MFA registrerad istället för kontoägarens MFA.

Som det sägs ovan innehåller Azure AD Identity Protection en funktion som tvingar användaren att registrera sig. Om Identity Protection inte är i bruk, kan användares MFA-status följas upp via MFA-portalen eller PowerShell[42].

Tvåfaktorsautentisering medför också ytterligare faser i systemadministratörernas användning av PowerShell. Beroende på tjänst kan det till exempel hända att den PowerShell-modul som används måste bytas ut eller att förbindelsen med molntjänsten måste genomföras på ett sätt som skiljer sig från den tidigare använda kombinationen av användarnamn och lösenord.

3.1.8 Inför Conditional Access

Conditional Access bör införas genom att skapa flera protokoll. Först bör funktionen testas med en liten målgrupp. Microsoft har en instruktion om införande av Conditional Access[43].

Nedan finns modellprotokoll som lämpar sig för testning och en liten miljö:

1. Tvinga systemadministratörer att använda MFA, gäller inte “break-glass”-administratörer[44].
2. Ställ in MFA obligatorisk vid användning av okända enheter.
3. Förhindra alla andra identifieringsmetoder än modern autentisering för alla användare.
4. Förhindra användning av ActiveSync för alla användare.

I bilaga 1 presenteras mer omfattande exempelprotokoll som införs i en testmiljö. Specifikationer av liknande protokoll presenteras i en närmare instruktion[45].

[39] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-whichversion

[40] https://support.office.com/sv-se/article/office-365-n-kaksivaiheisen-tarkistamisen-määrittäminen-ace1d096-61e5-449b-a875-58eb3d74de14?ui=fi-FI&rs=fi-FI&ad=FI

[41] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-converged

[42] https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates

[43] https://aka.ms/deploymentplans

[44] https://aka.ms/breakglass; break-glass är en anlogi till en nödknapp täckt av glas eller motsvarande koder som endast ska används i undantagsfall och som fungerar utan MFA och Conditional Access.

[45] https://bloggerz.cloud/2019/01/02/conditional-access-are-you-really-getting-the-most-out-of-it-part-2-of-2/

3.1.9 Skydd av on-premises Active Directory-verifiering

I Azure AD ingår många olika skyddsfunktioner som Microsoft kan införa för att tjänsten är så stor. I on-premises-miljöer finns det inte nödvändigtvis motsvarande resurser tillgängliga, och operativsystemet saknar inbyggda avancerade funktioner för att upptäcka attacker.

Microsoft lanserade funktionen Advanced Threat Analytics (ATA)[46] sommaren 2015. Med funktionen är det möjligt att genom att följa upp trafiken på on-premises AD domain controller-servrar upptäcka om identiteter beter sig onormalt och om någon försöker utnyttja flera olika sårbarheter. Uppföljning av trafik kan genomföras antingen med port mirroring eller genom att installera ATA Lightweight Gateway på önskade domain controller-servrar. Funktionen ingår i EMS E3-licenspaketet.

Azure Advanced Threat Protection (Azure ATP)[47] är en molnversion av ATA. Vid användning av molnversionen behöver lokala ATA-servrar inte installeras. På domain controller-servrar installeras Azure ATP sensor. Funktionen lanserades i mars 2018 och ingår i EMS E5-licenspaketet.

3.1.10 Kontroll över innehavare av systemadministratörsroller

När det gäller hanteringskoder för Active Directory är ett av de rekommenderade protokollen att skapa särskilda systemadministratörsuppgifter. Sådana koder har dock kontinuerligt alla gruppmedlemskap och är därför kronjuveler som angriparen försöker komma över.

I Azure AD kan sådana försök förhindras effektivt med Privileged Identity Management. Microsoft rekommenderar att antalet ordinarie systemadministratörer enbart är två och inte mer än fem ens i stora miljöer. Conditional Access och tvåfaktorsautentisering ska inte införas för dessa användare så att det är möjligt att logga in i tjänsterna även om det finns vissa utmaningar med tjänsterna.

Microsoft Identity Manager (MIM) 2016 möjliggör en motsvarande funktion även i on-premises-miljöer. Lösningen är Privileged Access Management for Active Directory Domain Services[48]. Det krävs stora resurser för att införa och underhålla lösningen.

Informationssäkerheten kan förbättras genom att begränsa underhållsåtgärder på dedikerade härdade åtkomstarbetsstationer (på engelska Privileged Access Workstation - PAW).

3.1.11 Utmaningar som har förekommit i skyddsfunktioner

Azure AD har federerats med WS-Federation-protokoll och SAML-standard. I federeringen av Azure AD har en brist hittats i informationssäkerheten[49]. Den gör att Global Administrator-systemadministratörer kan logga in som vilken användare som helst utan lösenord och även kringgå MFA. Enligt Microsoft är bristen en egenskap och behöver därför inte åtgärdas. Med anledning av detta ska antalet systemadministratörer med rollen Global Admin minimeras och åtgärder som systemadministratörer vidtar för att utnyttja bristen ska övervakas.

Det finns också vissa utmaningar med tvåfaktorsautentisering. Särskilt i större organisationer kan antalet IP-subnät och underhållet av näten i inställningarna för MFA-tjänsten i sig medföra utmaningar. Landspecifika begränsningar kan kringgås genom olika VPN-lösningar. Det är möjligt att i realtid kringgå tvåfaktorsautentisering, åtminstone i teorin.

[46] https://docs.microsoft.com/en-us/advanced-threat-analytics/
[47] https://docs.microsoft.com/en-us/azure-advanced-threat-protection/
[48] https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services
[49] https://ieeexplore.ieee.org/abstract/document/8456101

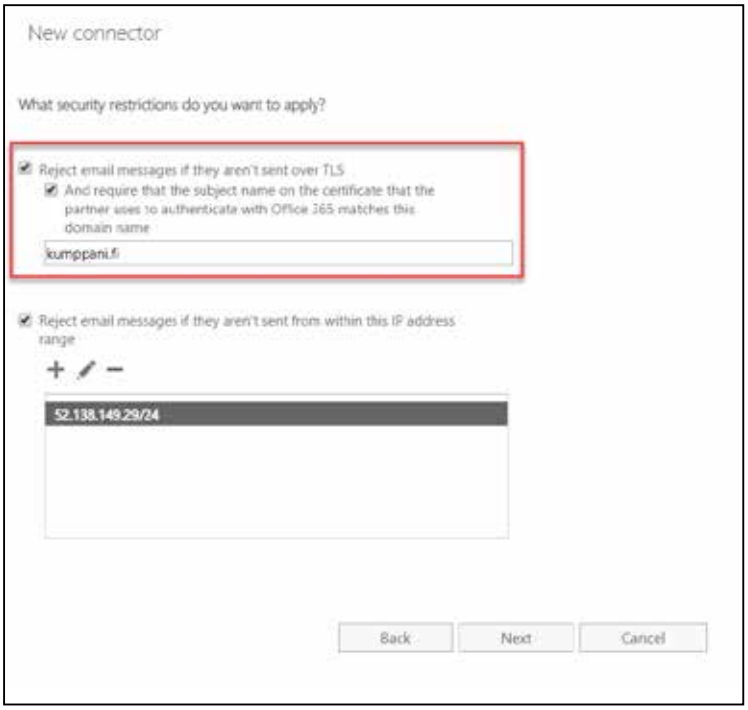
3.2 Skydd av e-post

3.2.1 Skydda routing av e-post

Med Exchange Online kan e-posttrafiken skyddas till exempel i inställningarna för e-postkontaktdon[50] (Connectors) tillsammans med betrodda partner eller på en intern e-postserver.

Trafiken mellan olika partner ska alltid krypteras med TLS och den andra parten ska identifiera sig med certifikat. Det rekommenderas att certifikatet ska bestå av en teckensträng som den andra parten har identifierat, till exempel företagets namn eller e-postadressens domän. Om ip-adresserna till den andra partens e-postservrar är kända, är det vid behov möjligt att tillåta enbart post som skickas från dessa adresser.

Tillåtna adresser som fastställts av avsändaren kan utredas utifrån SPF-posten med följande Windows-kommandon: nslookup -q=TXT kumppani.fi.



Ett e-postmeddelande som används för nätfiske kan skickas från en adress utanför organisationen, och avsändaren är organisationens e-postadress som har förfalskats. Denna rutt kan spärras med SPF. Först ska SPF-posten fastställas rätt i DNS. Sedan ska SPF Record: hard fail aktiveras i inställningarna för skräppost i Exchange Online (Exchange admin center => protection => spam filter). Det bestämmer att e-postmeddelanden i den egna organisationens namn endast kan tas emot ur sådana lagliga källor som anges i SPF-posten.

[50] https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/use-connectors-to-configure-mail-flow

3.2.2 Skydd av användare mot skadeprogram och skräppost

Office 365 Advanced Threat Protection (Office 365 ATP)[51] är en tjänst för att skydda användare mot skadeprogram, skräppost och nätfiske.

ATP Safe Attachments är en funktion mot nolldagsattacker. Sådana bilagor till meddelanden som godkänns i kontrollerna av kända skade- och virusprogram dirigeras för en åtskild verifiering där de öppnas. Bilagorna undersöks med maskininlärningsteknik med tanke på okända hot. Om en fil verkar innehålla något illvilligt, raderas det och det övriga meddelandet och bilagorna vidarebefordras till användarens postlåda.

En annan Office 365 ATP-funktion är säkra länkar (ATP Safe Links). Med funktionen ersätts misstänkta länkar med felsidor som meddelar att länken kan innehålla skadeprogram och nätfiske.

Skyddet mot nätfiske (ATP Antiphishing) undersöker om inkommande meddelanden handlar om nätfiskeförsök eller försök till imitation (Impersonation). Även i denna undersökning tillämpas olika maskininlärningstekniker för att analysera meddelanden.

Office 365 ATP ingår i prenumerationerna Office 365 Enterprise E5, Office 365 Education A5 och Microsoft 365 Business.

Antinätfiske-funktion (Antiphishing) ingår även utan ATP, men är mer begränsad än ATP. Inkommande meddelanden kontrolleras med tanke på bedrägerier (Spoofing) medan Impersonation-kontroll saknas.

3.3 Loggar och integration i SIEM-system

De olika Office 365-tjänsterna lagrar användarnas aktiviteter i loggar. Azure AD:s loggar och Office 365-auditlogg är de viktigaste loggarna. Office 365-auditloggen måste aktiveras separat[52] medan de övriga loggarna aktiveras automatiskt beroende på vilken version av Azure AD som används. Tabellen nedan innehåller en förteckning över de olika loggarna och lagringstiderna, som är mycket begränsade.

I auditloggen lagras åtgärder som systemadministratörer har vidtagit, till exempel skapat nya användare eller återställt lösenord.

Loggen över inloggningsaktiviteter innehåller data om enskilda användares inloggningar. Detta ingår endast i Azure AD Premium-prenumerationer.

Office 365-auditloggen samlar data om både administratörers och slutanvändares åtgärder. I loggen samlas åtgärder från alla tjänster, inbegripet Azure AD:s auditlogg och loggen över inloggningsaktiviteter. Till skillnad från andra loggar är lagringstiderna längre.

Dröjsmålet i Azure AD:s loggar, dvs. hur snabbt händelser lagras, är cirka 15 minuter. Dröjsmålet i Office 365-auditloggen är i regel 30 minuter medan det i Azure AD-loggarna är 24 timmar.

Genom kontroll över loggar kan nätfiskeförsök upptäckas genast när de har påbörjats. I praktiken förutsätter realtidskontroll prenumeration på Azure AD Premium eftersom dröjsmålet i Office 365-auditloggen är 24 timmar.

	Azure AD-version och tid dygn		
Logg	**Basic**	**Azure AD P1**	**Azure AD P2**
Auditlogg	7	30	30
Inloggningsaktivitet	-	30	30
Användning	30	30	30
Riskfyllda användare	7	30	30
Riskfyllda inloggningar	7	30	30
Office 365-auditlogg	90	365	365

[51] https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description

[52] https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

Det rekommenderas att loggarna införs i ett externt system där de kan lagras och analyseras vid behov under längre tid. Microsoft tillhandahåller också sådana tjänster i Azure.

Azure Monitor inkluderar en kombination av kontroll, analys och automatisk reaktion i både moln-miljöer och on-premises-miljöer. Auditloggarna och loggarna över inloggningsaktiviteter importeras ännu från Azure Monitor till tjänsten Log Analytics för fortsatt analys eller visualisering. De kan importeras till Azure för lagring (Storage Account). Då kan lagringstiden ställas in för 1–365 dygn eller för en obegränsad tid. Kostnaden för lagring ska beaktas särskilt i mer omfattande miljöer, där speciellt antalet inloggningsaktiviteter är stort och antalet logghändelser därmed också stort.

Loggarna kan även importeras till tjänsten Azure Event Hub och vidarebefordras därifrån till andra tillverkares SIEM-system (security information and event management). Bland annat Sumologic[53], Splunk[54], IBM QRadar[55] och Micro Focus ArcSight[56] är SIEM-system som kan integreras i Azure.

Användning av Azure Monitor-tjänster kräver en separat Azure-prenumeration som inte ingår i Microsoft 365- och Office 365-prenumerationer.

3.4 Uppföljning

Både Office 365 och Azure AD inkluderar flera hanteringsportaler som i sin tur innehåller olika rapporter. Microsoft är medvetet om utmaningen med flera portaler och har börjat förena dessa. Hösten 2018 arrangerades en Ignitekonferens som presenterade nya portaler för hantering av tjänster, till exempel Microsoft 365 admin center https://admin.microsoft.com som fortfarande fanns i en betaversion i februari 2019 när detta dokument skrevs.

Power BI är ett verktyg som snabbt blir allt allmännare vid analys och rapportering av olika tjänster. I februari 2019 införde Microsoft en metod för att använda Power BI vid rapportering av larm från olika tjänster[57]. Verktyget kan även användas vid analys av inloggningsloggar med Azure Active Directory Power BI content pack[58].

3.5 Ha kontroll över och skydda klienter

Office 365-tjänster används med olika typer av klienter som kan ägas av personen själv (Bring Your Own Device) eller organisationen.

Informationssäkerheten i klienten är en väsentlig del av informationssäkerheten i hela systemet. Om ett skadeprogram som till exempel följer upp användarens åtgärder har installerats i klienten eller om operativsystemet i utrustningen har ersatts med en inofficiell version, riskeras alla användares användning av Office 365-tjänsterna med utrustningen.

Det finns olika alternativ för hantering av utrustning och program som används med utrustningen, bland annat:

- Office 365 Mobile Device Management[59]; en mer begränsad MDM-hantering än vad Intune ger. Inkluderar vare sig programhantering (MAM), programdelning, profilhantering eller hantering av PC- och macOS-enheter.
- Microsoft Intune (både enhetshanteringen Mobile Device Management - MDM och programhanteringen Mobile Application Management - MAM).
- Andra MDM-tillverkares lösningar, till exempel Citrix Endpoint Management (tidigare XenMobile), MobileIron Unified Endpoint Management, IBM MaaS360 och VMware Workspace ONE (tidigare AirWatch).

Bland lösningarna ovan är Microsofts egna lösningar närmare integrerade i Azure Active Directory. Med dem kan en klient registreras i Azure Active Directory och utrustningens överensstämmelse med kraven därmed lagras i inställningarna för utrustningsobjektet. Dessa data kan i sin tur utnyttjas i till exempel Conditional Access-protokollen genom att det krävs att en klient som använder en viss tjänst ska stämma överens med kraven.

Windows-klienter har i flera årtionden hanterats i Group Policy-inställningarna (på svenska gruppolicy) som har specificerats i Active Directory. Microsofts System Center Configuration Manager (SCCM) har i sin tur genom åren blivit ett mycket brett använt system för programhantering och inventering särskilt i större miljöer.

[53] https://help.sumologic.com/07Sumo-Logic-Apps/04Microsoft-and-Azure/Azure_Active_Directory/Install_the_Azure_Active_Directory_App_and_View_the_Dashboards
[54] https://splunkbase.splunk.com/app/3534/
[55] https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/t_dsm_guide_microsoft_azure_enable_event_hubs.html
[56] https://community.softwaregrp.com/t5/ArcSight-Connectors/SmartConnector-for-Microsoft-Azure-Monitor-Event-Hub/ta-p/1671292
[57] https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Gain-rich-insights-with-the-new-Microsoft-Graph-Security-Power/ba-p/334467
[58] https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-power-bi-content-pack
[59] https://support.office.com/en-us/article/Frequently-asked-questions-about-Mobile-Device-Management-for-Office-365-3871f99c-c9db-4a23-86f9-902c1b02f58d

I och med Windows 10 och konsumentisering kommer läget dock att förändras. Det senaste året har Microsoft utvecklat en AutoPilot-tjänst som motsvarar Apples Device Enrollment Program (DEP). Genom tjänsten kan Windows 10-arbetsstationer anpassas efter organisationens behov utan ett konventionellt skräddarsytt installationspaket. Inställningarna på arbetsstationerna kan hanteras med MDM-lösningar, inklusive Microsofts Intune-tjänst.

En Windows 10-utrustning kan anslutas till Azure AD med följande metoder:

- Azure AD Registered; en klient som ägs av den anställda och som registreras i Azure Active Directory och eventuellt i organisationens MDM-system
- Azure AD Joined; en klient som ägs av organisationen är endast ansluten till Azure Active Directory
- Azure AD Hybrid Joined; en klient är ansluten till både on-premises Active Directory och Azure Active Directory.

Vid användning av en federerad identitet och AD FS kan användningen av Office 365 med regler begränsas till organisationens egna klienter.

3.6 Ordna utbildning för användare och systemadministratörer

Det är mycket viktigt att utbilda användare eftersom det ofta är just användaren som är den svagaste länken i informationssäkerheten. Å andra sidan är det till exempel i en organisation med tusen personer omöjligt att nå ett läge där inte en enda användare genom åren ska begå ett misstag när man försöker nätfiska användarens uppgifter. Om användare däremot är mer kompetenta och mer medvetna har angriparen sämre möjligheter att lyckas.

Varje användare av Office 365 bör ha kännedom om på vilket sätt denne ska skydda sitt lösenord, känna igen bluffmeddelanden och agera vid bedrägeriförsök eller lyckat bedrägeri.

På närmare plan kan utbildningen bestå av följande teman:

- Vilken typ av lösenord ska du använda? Till exempel https://pidempiparempi.fi/
- Angripare kontaktar vanligen per e-post, men även per telefon eller sms.
- Om meddelandet är dåligt skrivet är det sannolikt ett bluffmeddelande.
- Om den synliga delen av hyperlänken är en annan än den bakomliggande länken, handlar det sannolikt om ett bedrägeri.
- Om hyperlänkens måladress är numerisk handlar det troligen om ett bluffmeddelande.
- Om hyperlänkens måladress liknar ett hederligt företag, handlar det troligen om ett bluffmeddelande. Till exempel www.gigamtti.fi i stället för www.gigantti.fi.
- Om meddelandet begär att du ska skynda dig och hotar att du kan förlora pengar, är det troligen ett bluffmeddelande.
- Om sättet att tilltala är krystat handlar det troligen om ett bluffmeddelande.
- Meddelandet kan vara ett äkta meddelande i det hänseendet att det kommer från din chefs eller medarbetares e-postadress. Det är dock angriparen som har gett upphov till sändningen av meddelandet, och därför är begäran eller även ordern också en bluff.
- Hur kan du skilja på ett äkta meddelande och ett bluffmeddelande på inloggningsrutan?
- Om du får ett bluffmeddelande per e-post och du inte godtar det, ska du radera meddelandet och behöver inte göra en anmälan.
- Om du av misstag anger ditt löseord på fel ställe och du upptäcker eller misstänker att det handlar om ett bedrägeri, ska du genast göra en anmälan enligt din organisations anvisningar.

Dessa frågor är viktiga och å andra sidan begränsade. Därför kan det vara bra att varje användare genom test eller på något annat sätt måste kvittera att denne är medveten om frågorna.

Utbildningen ska också uppdateras eftersom teknikerna och situationerna förändras.

Utöver utbildningen kan användare testas, vilket dock också är en del av utbildningen. Organisationens informationsförvaltning kan skicka nätfiskemeddelanden till användare. Om användare råkar klicka på länken går de till en webbadress där de informeras om situationen.

I Office 365 ingår funktionen Attack Simulator för att skapa simulerade attacker. Motsvarande övningar och utbildning kan även köpas som tjänster.

Det gäller även att säkerställa att systemadministratörernas kompetens är uppdaterad. Från och med hösten 2018 har Microsoft ändrat sitt certifieringsprogram. Bland annat följande nya certifieringar baserade på arbetsroller och utbildningar i certifieringarna handlar om hur skyddet av Microsoft 365-miljön och upprätthållandet av informationssäkerheten kan utvecklas:

- Microsoft 365 Certified: Security Administrator Associate[60]
- Microsoft 365 Certified: Enterprise Administrator Expert[61].

3.7 Använd checklistor

Nätfiske är mycket allmänt och därför finns det flera olika checklistor för att förhindra det. Microsoft har publicerat en mångsidig serie av bloggartiklar på https://blogs.technet.microsoft.com/cloud-ready/2018/07/31/introduction-email-phishing-protection-guide-enhancing-your-organizations-security-posture/. Trots att en del av de detaljerade artiklarna inte är helt aktuella längre, kan instruktionerna tillämpas tillsammans med de informationskällor som anges i detta dokument.

De olika skedena av införandet av Microsoft 365-identitetsinfrastruktur på https://docs.microsoft.com/en-us/microsoft-365/enterprise/identity-infrastructure räknar i sin tur upp de åtgärder med vilka en hybrididentitet och dess viktigaste funktioner kan införas.

De ovan beskrivna Secure Score-portalerna räknar upp funktioner av vilka de flesta hjälper till att begränsa möjligheterna till nätfiske.

3.8 Logga in utan lösenord

Som det i detta dokument flera gånger konstaterats, är huvudsyftet med nätfiske att utreda en användares identifieringsuppgifter, dvs. användarnamn och lösenord, och att missbruka dem på något sätt. Vid identifiering är det möjligt att använda metoder där ett lösenord inte behöver användas.

Microsoft har i sina tjänster presenterat till exempel funktionen Hello for Business[62] i Windows 10. I funktionen identifierar sig användaren med sin pinkod eller biometriskt.

Med AD FS kan Azure MFA i federerade miljöer fastställas som primär verifieringsmetod[63]. Minimikravet är Windows Server 2016 AD FS.

Identifiering utan lösenord kan även genomföras med Microsoft Authenticator, ett program som installeras i telefonen[64]. I så fall visas en rad siffror för användaren, och användaren ska klicka på en motsvarande punkt i vyn i sin telefon för att godkänna inloggningen.

Dessutom används smartkortsautentisering i vissa branscher och organisationer. Då känner användaren inte nödvändigtvis till sitt lösenord och inloggningen bygger på ett smartkort och en pinkod.

[60] https://www.microsoft.com/en-us/learning/m365-security-administrator.aspx
[61] https://www.microsoft.com/en-us/learning/m365-enterprise-administrator.aspx
[62] https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification
[63] https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-and-azure-mfa
[64] https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-phone-sign-in

Hot som nätfiske medför och begränsning av hoten

	Tjänsten SaaS			Verifiering och auktorisering (identitet)		
	Office 365 -version			AAD-version		
Hot	**Business**	**E3**	**E5**	**Basic och Office 365**	**AAD P1**	**AAD P2**
Nätfiskemeddelande till användare						
Anti-spoofing-bluffmeddelanden	Med vissa partner används TLS	‹	‹			
Kontroll av att länkar är säkra	›	›	Safe-länkar			
Identifieringsuppgifter hamnar i orätta händer						
Lösenord knäcks (Brute force)				Skydda lösenord Vid användning av federerad autentisering, Extranet Lockout	‹	‹
Inloggningssidorna visas enklare för användare				Skräddarsy inloggningssidor	‹	‹
Otillräcklig kombination av användarnamn och lösenord				Tvåfaktors-autentisering (MFA for Office 365) av enskilda användare Vid användning av federerad autentisering införs AD FS Conditional Access-regler	Tvåfaktors-autentisering (Azure MFA) Conditional Access	‹ + tvingad MFA-registrering Identity Protection
Kringgå MFA						
Användning av legacyprotokoll	Basic Authentication-spärr i Exchange	‹	‹	Basic Authentication -spärr i Exchange (i Office 365-funktionen, ej som AAD-funktion) eller ›	Tvingad Modern Authentication genom Conditional Access	‹
MFA Phishing i realtid (t.ex. nätfiske av sms-bekräftelser)						
Informationsläcka - e-postmeddelande						
Förhindra regler för omsändning av e-postmeddelanden (mail forward)	Automatic Forward-spärr i en förinställd Remote Domain-konfiguration Transport Rules	‹ + Data Loss Prevention (DLP)	‹			
Förhindra regler för sortering av e-postmeddelanden (Inbox rules)						
Utgående skräppost	Begränsning av förmedlade e-postmeddelanden (throttling) Inställningar för connectors, t.ex. identifiering	‹	‹			
Informationsläcka från andra tjänster						
Identifiering i andra system med funktionen Single sign-on					Monitoring - Sign-ins	‹
Obehörig delning av dokument från SaaS	›	›	Office 365 Cloud App Security Microsoft Cloud App Security finns att tillgå med EMS-licens.			
Annat missbruk av koder						
Lateral movement				›	ATA	Azure ATP
Utnyttjande av svagheter i protokoll				›	ATA	Azure ATP
Missbruk av administrationskoder						Privileged Identity Management

Förklaringar av tecknen: › VKan genomföras genom att köpa dyrare licenser till höger ‹ Kan genomföras på samma sätt som det beskrivs till vänster

Hotet är inte relevant i denna kontext eller så är det inte möjligt att skydda sig mot hotet

Observation och forensik

	Tjänsten SaaS			Verifiering och auktorisering (identitet)		
	Office 365 -version*			AAD-version		
Hot	**Business**	**E3**	**E5**	**Basic och Office 365**	**AAD P1**	**AAD P2**
Loggdata						
Lösenord knäcks (Brute force eller spray attack) - on-premises				Uppföljning av loggdata	‹	‹
Lösenord knäcks (Brute force eller spray attack) - AAD				Uppföljning av loggdata om inloggningsaktiviteter	‹	‹
Försök till missbruk av koder - on-premises				On-premises: uppföljning av loggdata	‹	‹
Försök till missbruk av koder - AAD				Uppföljning av loggdata om inloggningsaktiviteter	‹	‹
Utredning av läsandet av meddelanden						
Utredning av sökningar i innehållet i e-postlådor	Granskning av loggdata	‹	‹			
Hittande av regler för omsändning av e-postmeddelanden	Granskning av loggdata, Granskning av inställningar för e-postlådor	‹	‹			
Hittande av regler för sortering av e-postmeddelanden (Inbox rules)	Granskning av loggdata, Granskning av inställningar för e-postlådor	‹	‹			
Hittande av e-postmeddelanden som skickats från ett hackat konto	Granskning av loggdata	‹	‹			
Utredning av sökningar i innehållet i e-postlådor				›	Sign-in logs	‹
Förebyggande uppföljning (Monitoring)						
Upptäckt av missbruk av koder				›	Azure Active Directory risk events	‹
Identifiering av lyckat nätfiske				›	Azure Active Directory risk events	‹

Förklaringar av tecknen: › Kan genomföras genom att köpa dyrare licenser till höger ‹ Kan genomföras på samma sätt som det beskrivs till vänster

Hotet är inte relevant i denna kontext eller så är det inte möjligt att skydda sig mot hotet

I tabellen sammanfattas de hot som Office 365-nätfiske och dataintrång medför, attackmetoderna och de skydds- och observationsmetoder som finns tillgängliga på de vanligaste licensnivåerna i Finland. Tabellen är inte en heltäckande servicebeskrivning. Inom ramen för de nuvarande licenserna kan den dock användas som hjälpmedel vid fastställande av befintliga metoder.

4 Åtgärder efter en attack

En organisations anvisningar om informationssäkerhet bör omfatta en intern instruktion, dvs. en process för informationssäkerhetsincidenter. Anvisningarna i detta dokument bör i tillämpliga delar integreras i organisationens anvisningar.

En kort minneslista om åtgärder efter en attack:

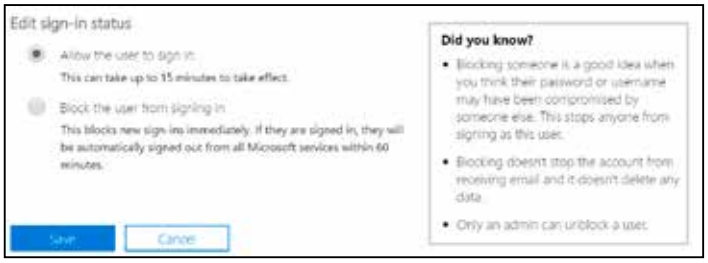
1. Identifiera offer och konton som har attackerats och förhindra ytterligare skador (ta över användarkonton, utesluta angriparna, omedelbara spärråtgärder).
2. Intern information om incidenten i syfte att minimera ytterligare skador.
3. En preliminär bedömning av angriparnas åtgärder och skadornas omfattning i möjligaste mån.
4. Extern information om incidenten i syfte att minimera spridningen av skador: preliminära kontakter med myndigheter.
5. En mer omfattande utredning av transaktionskedjan utifrån loggdata; vad som har hänt, vem som har orsakat incidenten och när.
6. Städa eventuellt infekterade filer och motsvarande, arkivera loggdata med tanke på fortsättningen.
7. Kompletterande anmälningar till myndigheter.
8. Långsiktigt skydd mot motsvarande incidenter.

4.1 Utesluta en inloggad angripare

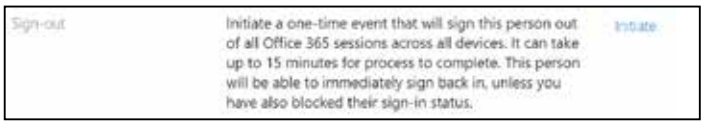
Om du känner till eller misstänker att en viss inloggningsuppgift har hamnat i orätta händer och att angriparen kan använda denna, kan åtkomsten med den röjda inloggningsuppgiften till olika Office 365-tjänster spärras. Det kan dock hända att tjänsterna en viss tid kommer ihåg gamla data för att den normala användningen ska gå fortare.

Av det ovannämnda följer att angriparen kan använda inloggningsuppgiften ännu en viss tid även efter att lösenordet bytts ut. Det innebär att du också behöver avbryta uppkopplingar som används för tillfället.

Avbrytandet börjar i Office 365-hanteringsportalen. I portalen öppnas uppgifterna om den röjda inloggningsuppgiften och sedan OneDrive-inställningarna. I inställningarna finns en funktion som visas på bilden nedan.



När du klickar på länken Initiate avbryts uppkopplingarna med inloggningsuppgiften från alla enheter inom de följande 15 minuterna. Nya inloggningar ska också förhindras för att angriparen inte genast därefter ska kunna logga in på nytt. I Sign in status i användaruppgifterna kan spärren aktiveras med en funktion som visas på bilden nedan.



När ändringen sparats visar rutan också ett förslag till byte av lösenord, vilket bör göras med detsamma.

Om målanvändaren har synkroniserats från en lokal Active Directory-katalog och om lösenordet byts i denna katalog, kan PowerShell-kommandot Get-MsolUser användas för att kontrollera att lösenordet har förmedlats till Azure AD-molnet. I så fall kontrolleras tidpunkterna LastDir-SyncTime och LastPasswordChangeTimestamp bland resultaten.

Dessutom går det att använda följande två PowerShell-kommandon för att avbryta uppkopplingar:

- Revoke-SPOUserSession är ett SharePoint Online-kommando som avbryter målanvändarens SharePoint-uppkopplingar.
- Revoke-AzureADUserAllRefreshToken on Azure är ett AD-kommando som avbryter en viss användares uppkopplingar till alla program som använder Azure AD.

Till sist är det bra att kontrollera om det finns delegater i målanvändarens postlåda. Om deras lösenord har hamnat i orätta händer, är det möjligt att med lösenorden få åtkomst till målanvändarens postlåda.

4.2 Triage/forensik/utredning av incidenter

Ensimmäinen askel hyökkäyksen tapahduttua on Det första steget efter en attack är att härda informationssäkerhetssystemet för hela hyresgästen genom att tvinga alla användare att använda tvåfaktorsautentisering.

Vid användning av Azure AD Premium eller AD FS ska användning utanför organisationen och med icke identifierade enheter också förhindras. Med dessa åtgärder kan en pågående attack avbrytas effektivt och ändå tillåta en kontinuerlig verksamhet i organisationen.

Nästa steg är att identifiera offren för attacken. Nedan beskrivna informationskällor och metoder kan användas vid identifieringen.

När offren för attacken har identifierats, förhindras sändning av offrens e-post till mottagarna med regler. På så sätt förhindras spridning av nya nätfiskemeddelanden och skräppost och därigenom även nya offer. Vid användning av Exhange Plan 2 bör offrens lådor genast aktiveras med ”hold” (Legal Hold) för att bevisen inte ska försvinna.

Informationskälla/metod	Vad ska utredas?
Auditlogg	Har det skett exceptionella incidenter, till exempel nya domäner har skapats eller ändringar har gjorts i identifieringsmetoden för en domän?
	Har ändringar gjorts i loggdata?
Inloggningsaktivitet	Visas det exceptionella inloggningstider och inloggningsställen?
Office 365-auditlogg	Har regler skapats för e-postadresser? Brottslingar kan lägga till en regel för att omdirigera e-postmeddelanden till sin egen e-postadress i syfte att följa en viss e-posttrafik.

När informationssäkerhetssystemet har härdats, tillvaratas alla tillgängliga loggar i syfte att lagra och analysera bevismaterialet.

Ur Centralkriminalpolisens synvinkel är utmaningen med utredningen av dataintrången i Office 365 att det är svårt att få information. Av denna anledning är det högst viktigt att lagring av loggdata införs i Office 365-programvaran.

Utifrån de aktuella Office 365-auditloggarna är det möjligt att upptäcka obehöriga inloggningar, att undersöka inloggarnas IP-adresser och att upptäcka minst en del av de åtgärder som har vidtagits i systemet obehörigt. Utan loggdata är det nästan omöjligt att utreda denna information och att bevisa dataintrånget.

I förebyggande syfte rekommenderas det därför att kunderna kontrollerar om de använder lagring av loggdata, varifrån loggarna är tillgängliga och hur lång tid.

Vid dataintrång rekommenderar vi att du så fort som möjligt gör en brottsanmälan (eller skickar ett Nättips) för att loggdata fortfarande ska vara tillgängliga en tillräckligt lång tid.

4.3 Kontakt med Cybersäkerhetscentret

Cybersäkerhetscentret är intresserat av nätfiskemeddelanden gällande programvaran Office 365 och gjorda dataintrång i programvaran. Vi använder informationen för att skapa en nationell lägesbild och till exempel för att skicka begäranden om att koppla bort nätfiskewebbplatser.

Anmälan till Cybersäkerhetscentret kan skickas per e-post på cert@traficom.fi eller på blanketten Anmäl kränkningar på https://www.kyberturvallisuuskeskus.fi/sv.

4.4 Kontakt med polisen

Intrång i användarkonton och obehörig användning av konton uppfyller rekvisiten för dataintrång. Incidenten kan även omfattas av andra brottsbeteckningar som framkommer eller preciseras under utredningen och polisens brottsutredning. Brottsanmälan kan göras till den lokala polisinrättningen antingen per telefon, genom att besöka inrättningen eller på Internet på https://www.poliisi.fi/brott/elektronisk_brottsanmalan.

Om en händelse endast förblir ett försök eller om organisationen av någon anledning inte vill göra en brottsanmälan, är det ändå bra att lämna ett Nättips om händelsen till polisen. Alla ytterligare upplysningar om transaktionskedjor eller aktörer kan bidra till att utreda något annat brott eller till att skapa en helhets-

bild av mer omfattande brottshärvor. Nättips kan lämnas på Internet på https://www.poliisi.fi/nattips.

4.5 Anmälan till dataombudsmannens byrå

Nästan alltid handlar dataintrång i Office 365 i organisationer också om personuppgifter.

En anmälan om personuppgiftsincident ska göras till dataombudsmannens byrå och, om incidenten har medfört en hög risk för de registrade, även till de drabbade.

Efter att personuppgiftsansvariga har anmält en personuppgiftsincident till dataombudsmannens byrå, kan de få rådgivning om skyddet av personuppgifter. Dessutom hjälper anmälan organisationens ledning att skapa en lägesbild. Vid behov kan dataombudsmannen ålägga organisationen att iaktta skyldigheter i enlighet med dataskyddsförordningen.

Vid intrång i Office 365 är processen efter anmälan om säkerhetsincident följande:

1. Kontrollera att attacken inte pågår längre.
2. Utreda attackens omfattning i fråga om personuppgifter.
3. Utreda mängden och kvaliteten på de personuppgifter som läckt ut.
4. Göra en riskbedömning av om incidenten har medfört en hög risk för personerna.
5. Vid behov kan organisationen åläggas att iaktta skyldigheter i enlighet med dataskyddsförordningen.
6. Dokumentation och ytterligare anvisningar om sådana behövs. Vid attacker mot Office 365 begärs vanligen tilläggsutredningarna nedan. Informationen fungerar även som dokumentation om säkerhetsincidenter. Vid behov begärs dessutom till exempel mera loggdata.

Tilläggsuppgifter för anmälan om säkerhetsincident vid intrång i Office 365:

1. Är det fråga om en Office 365-miljö eller en OWA-miljö?
2. Har organisationen kontrollerat att otillåtna omsändningsregler inte har skapats för kontona?
3. Om ja, till vilken e-postadress?
4. Har organisationen kontrollerat att ingen obehörigt har loggat in på kontot under denna tid? (t.ex. auditlogg för en Azure AD-kod)
5. Om ja, har organisationen kontrollerat om e-postmeddelanden har laddats ned? (t.ex. loggar för Office 365 Exchange)
6. Har OneDrive eller SharePoint-tjänster använts för kontot?
7. Innehåller e-postmeddelanden som finns på kontona, OneDrive eller SharePoint-tjänster personuppgifter?
8. Om ja, hur många personers uppgifter och vilka kategorier av personuppgifter? (t.ex. namn, personbeteckning, e-postadress, adress)
9. Har organisationen övervägt multifaktorsautentisering (MFA)?
10. Lämna Azure AD:s Sign-Ins-logg över de koder som läckte ut under attacken i csv-format till dataombudsmannens byrå.

4.6 Ekonomiavdelningens kontroller

Hackade konton har använts bland annat för att skapa och/eller skicka förfalskade fakturor. Företag ska beakta detta hot i den egna processen för fakturabetalning eller när kontouppgifter läggs till eller redigeras.

Cybersäkerhetscentret har fått kännedom om flera incidenter där angriparna först har hackat e-postkonton och sedan med ovan nämnda omsändningsregler och postarkivering påverkat e-postdiskussioner mellan olika organisationer. Dessutom har angriparna redigerat befintliga fakturor och kontomeddelanden. Då kan en valid faktura ha blivit skickad till en kund eller samarbetspartner, men angriparen har dessemellan redigerat uppgifterna och betalningen dirigeras till helt fel ställe. Vid förfalskade fakturor gäller problemet särskilt fakturor i pdf-format. E-fakturor har än så länge inte hackats.

Därför ska organisationer föra en intern diskussion om hur uppgifterna på fakturor som ska betalas kontrolleras, hur organisationerna själva förmedlar fakturorna till sina kunder och hur ändringar i samarbetspartnernas och kundernas kontouppgifter kontrolleras.

4.7 Information till intressenter

Det är inte ovanligt att bli föremål för dataintrång och missbruk. Därför bör organisationen i förväg planera en informationsmodell och informationspolicy enligt olika scenarior. I vissa situationer är det också möjligt att en incident väcker uppmärksamhet i medier och tas upp i offentligheten. Därför är det bra att i förväg tänka på hur sådana situationer kan hanteras.

Om skräppost eller nätfiskemeddelanden har skickats från offrets konto, är det mycket sannolikt att det leder till meddelanden och kommentarer från mottagarna och deras organisationer. Dessutom är det sannolikt att det orsakar nya offer i andra organisationer. Därför är det önskvärt att proaktivt informera om incidenten när denna har upptäckts.

Särskilt uppmärksamhet ska läggas på organisationens interna kommunikation. I väldigt många situationer har skadliga meddelanden skickats från det första offrets konto till andra anställda i samma organisation. Efter detta har angriparen kunnat ta över ett allt större antal användarkonton i organisationen. Därför bör en intern kommunikation ske snabbt och med låg tolerans så att mängden skador kan hållas så liten som möjligt.

Ytterligare information:

tietosuoja(at)om.fi
Personuppgiftsincidenter:
https://tietosuoja.fi/sv/personuppgiftsincidenter
Anmälan om personuppgiftsincident:
https://tietosuoja.fi/sv/anmalan-om-personuppgiftsincident

Bilagor

Bilaga 1. Exempel på Conditional Access-regler

Två grupper har skapats i exemplet: sg_CA Excluded Cloud och sg_CA Excluded On-prem. Medlemmarna i grupperna är användarnamn och tjänstekoder som man inte vill att Conditional Access-reglerna ska påverka.

Namn	**Users and Groups**		**Villkor (Assignments)**		**Åtkomstkontroll (Access controls)**	
	Include	**Exclude**	**Device Platforms**	**Client apps**	**Block access**	**Grant access**
Allow modern authn from AADHJ or compliant devices - Clients	All Employees	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require device to be marked as compliant OR Require Hybrid AD joined device
Allow modern authn from AADHJ or compliant devices - Browser	All Employees	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Browser		Require device to be marked as compliant OR Require Hybrid AD joined device
Require MFA for admins - Clients	Admin groups	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require multi-factor authentication
Require MFA for admins - Browser	Admin groups	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Browser		Require multi-factor authentication
Require MFA for Guests - Clients	All guest users	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require multi-factor authentication
Require MFA for Guests - Browser	All guest users	sg_CA Excluded Cloud sg_CA Excluded On-prem	Android iOS Windows macOS	Browser		Require multi-factor authentication
Require MFA for All other Users - Clients	All users	sg_CA Excluded Cloud sg_CA Excluded On-prem All Employees Admin groups All guest user	Android iOS Windows macOS	Mobile apps and desktop clients > Modern authn clients		Require multi-factor authentication
Require MFA for All other Users - Browser	All users	sg_CA Excluded Cloud sg_CA Excluded On-prem All Employees Admin groups All guest users	Android iOS Windows macOS	Browser		Require multi-factor authentication
Block ActiveSync	Cloud apps > Office 365 Exchange Online			Mobile apps and desktop cllients Exchange ActiveSync clients > Apply policy to supported platforms	Block	
Block legacy authn				Mobile apps and desktop clients > Other clients	Block	

Transport- och kommunikationsverket
Traficom
Cybersäkerhetscentret
PB 320, 00059 TRAFICOM
tfn 029 534 5000
traficom.fi

TRAFICOM
Transport- och kommunikationsverket
Cybersäkerhetscentret