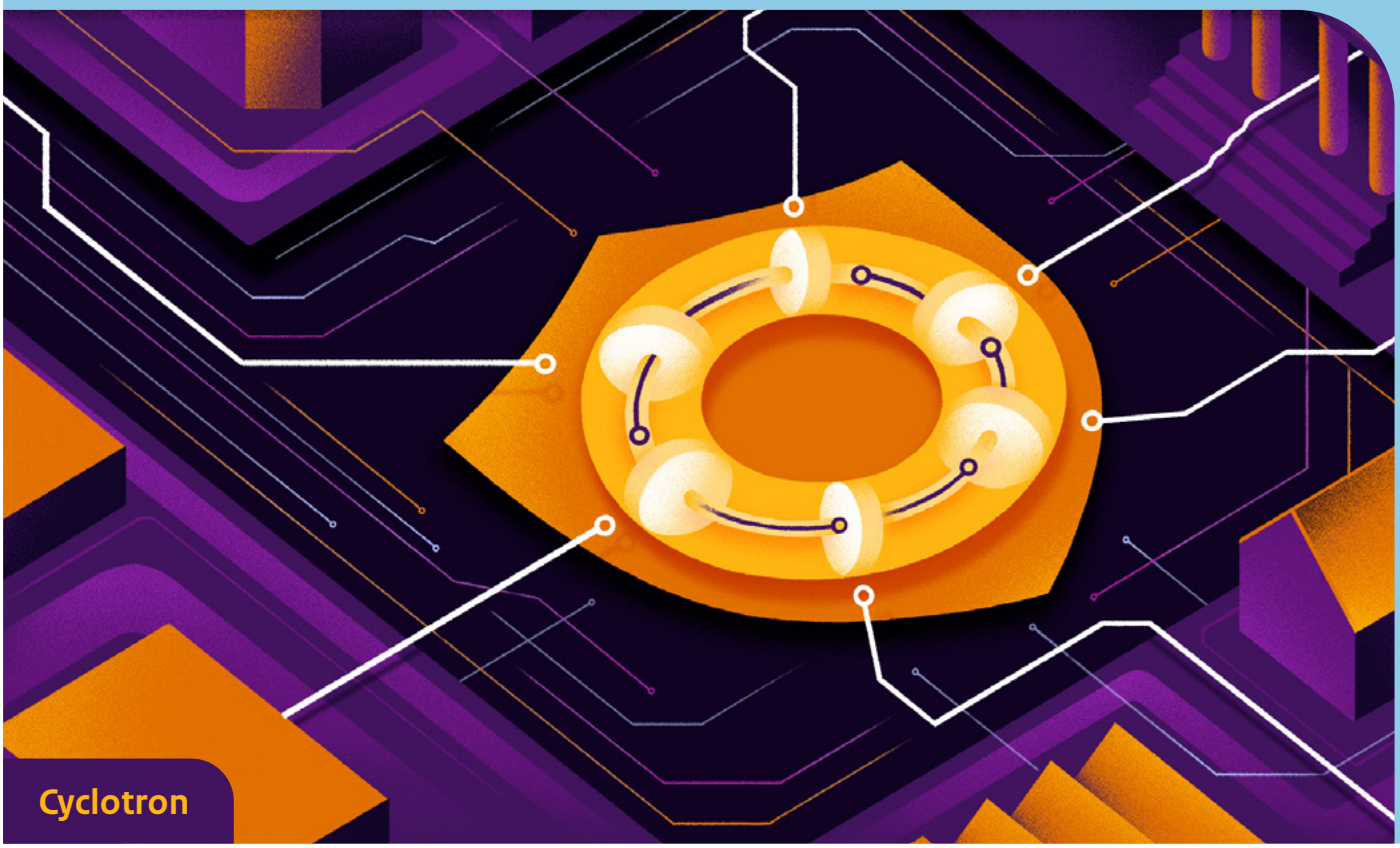
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Business E-mail Compromise (BEC)

Technisch advies

Versie: 1.0 (MITRE ATT&CK Structuur)



In samenwerking met:

ATTIC INVICTUS INCIDENT RESPONSE orange Cyberdefense TESORION

Inhoudsopgave

Introductie

Bij Business E-mail Compromise (BEC) doen criminelen zich voor als een persoon die binnen een organisatie wordt vertrouwd, vaak een directeur of leidinggevende. Deze vorm van oplichting is één van de grootste oorzaken van financiële schade en ontwrichting bij organisaties – tot en met een faillissement aan toe. Vooral het mkb blijkt kwetsbaar voor BEC-aanvallen. Dit technische advies is gebaseerd op het MITRE ATT&CK-raamwerk en bevat een uitgebreid maatregelenpakket tegen BEC. Deze publicatie is bedoeld voor jouw IT-dienstverlener of Managed Service Provider.

N.B. dit document heeft enkel betrekking op Microsoft 365 (Outlook). Dit is een technisch advies, dus de genoemde maatregelen zijn technisch van aard. Overige maatregelen zoals procedures rondom het doen van betalingen zijn hierin niet meegenomen.

Doelgroep

De inhoud van dit technische advies is primair bedoeld voor IT Security Specialisten, IT-dienstverleners en Managed Security Service Providers (MSSPs).

In samenwerking met

Deze publicatie is tot stand gekomen met Attic Security, Orange Cyberdefense, Invictus en Tesorion. Deze partners hebben hun expertise en praktijkervaring ingebracht om een actueel beeld te schetsen van Business E-mail Compromise incidenten in Nederland.

Deze organisaties zijn ook onderdeel van Cyclotron: een samenwerkingsverband van hoog-volwassen publieke en private partijen die actuele dreigingsinformatie over cyberveiligheid uitwisselen. Deze samenwerking helpt om cyberdreigingen beter in kaart te brengen, te doorgronden en sneller (en effectiever!) te kunnen reageren. Cyclotron is onderdeel van de

Nederlandse Cybersecuritystrategie 2022-2028.

Over MITRE ATT&CK

MITRE ATT&CK staat voor Adversarial Tactics, Techniques, and Common Knowledge en is een universeel raamwerk dat het gedrag van cyberaanvallers categoriseert op basis van praktijkobservaties. Het klinkt misschien abstract en intimiderend, maar het is een heel praktisch hulpmiddel om grip te krijgen op cyberrisico's. Je kunt het zien als een database waarin wereldwijd het gedrag van hackers wordt bijgehouden, gecategoriseerd en vertaald naar begrijpelijke stappen. Het raamwerk kijkt naar het 'waarom' (de tactiek van de hacker), het 'hoe' (de techniek die ze gebruiken, zoals phishing) en de concrete uitvoering (de procedure). Door deze stappen te begrijpen, zie je sneller waar je beveiliging nog tekortschiet en kun je gerichte keuzes maken om je bedrijf beter te beschermen, zonder dat je hoeft te verdrinken in technische details.

Bijlage

Hieronder vind je een overzicht van alle MITRE-technieken, tactieken en procedures (TTPs) die bij BEC-aanvallen worden gebruikt en de maatregelen die je moet nemen. In deze tabel is ook aangegeven wat de prioriteit is en is een inschatting gemaakt van hoeveel impact de maatregel heeft op jouw bedrijf. Ook is aangegeven wat de inspanningen zijn om de maatregel te realiseren.

ID	MITRE TTP	Beschrijving	Prioriteit	Impact	Inspanning
001	T1598	Security Awareness op OSINT	Midden	Midden	Laag
002	T1672	SPF, DKIM en DMARC correct configureren	Midden	Hoog	Midden
003	T1672	Direct Send-functie uitschakelen	Hoog	Hoog	Midden
004	T1110.003 / T1539 / T1557 / T1566.002 / T1621	Phishing-resistente multifactorauthenticatie (MFA)	Hoog	Hoog	Hoog
005	T1110.003 / T1539 / T1557 / T1566.002 / T1621	Microsoft Defender for Microsoft 365	Midden	Hoog	Laag
006	T1078.004	Voorwaardelijk toegangsbeleid	Hoog	Hoog	Midden
007	T1078.004	Monitoring van verdachte inlogpogingen	Hoog	Hoog	Midden
008	T1059 / T1204	Blokkeren van riskante extensies	Hoog	Midden	Laag
009	T1098.001 / T1556.006 / T1671	OAuth-app consent beperken of uitschakelen	Hoog	Hoog	Laag
010	T1068	Least Privilege-principe & PIM	Midden	Midden	Midden
011	T1562.001 / T1564.008	Security alerts doorsturen	Hoog	Hoog	Laag
012	T1562.001 / T1564.008	Unified Audit Log (UAL) inschakelen	Hoog	Hoog	Midden
013	T1562.001 / T1564.008	Monitoring op configuratie drift	Hoog	Hoog	Midden
014	T1538	Beperk toegang tot Microsoft Entra	Midden	Laag	Laag
015	T1534 / T1537 / T1566.003	Interne en uitgaande phishing detectie	Midden	Hoog	Midden
016	T1114.002 / T1114.003 / T1530 / T1078	Blokkering van automatische e-mailforwarding	Hoog	Hoog	Midden
017	T1114.002 / T1114.003 / T1530 / T1078	Teams & SharePoint-collaboration beperken	Midden	Midden	Midden
018	T1567	Access Reviews	Midden	Midden	Midden
019	T1656 / T1657	Administratieve verificatie van betalingen	Hoog	Hoog	Midden

01. Reconnaissance

Aanvallers verzamelen informatie om hun aanval zo geloofwaardig mogelijk te maken.

Security Awareness op OSINT (Open Source Intelligence) richt zich op het trainen van medewerkers over de risico's van informatie die zij onbewust publiekelijk delen. Dit omvat gegevens op zakelijke en persoonlijke socialemediaprofielen, zoals LinkedIn, maar ook informatie op de bedrijfswebsite.

Waarom is dit belangrijk?
Bij BEC-aanvallen is geloofwaardigheid essentieel. Hoe meer details over functies, hiërarchieën en zakelijke relaties publiekelijk bekend zijn, hoe makkelijker een aanvaller een overtuigend scenario kan opstellen om een medewerker te misleiden. Het 'oogsten' van deze informatie is vaak de eerste stap om een doelwit te selecteren en een aanval op maat te maken.

Effectieve aanpak
- Train medewerkers op de risico's van 'oversharing' en leer hen kritisch te kijken naar welke organisatie-informatie zij online plaatsen. Een goed social media beleid kan hierbij helpen.
- Stel richtlijnen op voor het publiceren van gevoelige informatie, zoals directe e-mailadressen van sleutelfiguren of gedetailleerde projectinformatie op de website.
- Stimuleer een cultuur waarin medewerkers ongebruikelijke verzoeken (zelfs als deze gebaseerd lijken op publieke feiten) altijd via een tweede kanaal verifiëren.

Geobserveerde Technieken

T1598 | Phishing for Information
Criminelen verzamelen informatie over de organisatie via LinkedIn, de website en sociale media.

Maatregelen

ID: 001 | Security Awareness op OSINT
Prioriteit: Midden
Impact: Midden
Inspanning: Laag

02. Resource Development

Het voorbereiden van de infrastructuur om de aanval technisch te ondersteunen.

Het inzetten van SPF, DKIM en DMARC betreft een maatregel voor het zoveel mogelijk borgen van legitiem emailverkeer, waardoor het risico van misbruik door middel van jouw e-maildomein verlaagd wordt.

Waarom is dit belangrijk?
Deze protocollen werk en samen om spoofing, phishing en ongeautoriseerd gebruik van het bedrijfsdomein te voorkomen. Dit wordt gedaan op basis van DNS-based e-mailauthenticatie. Deze protocollen verzorgen controles zoals: wie mag e-mails verzenden vanuit dat domein, is tijdens transport de integriteit van de mail geraakt en wat er gedaan moet worden als de controles falen. Meer informatie over de verschillende protocollen en een test van het e-maildomein zijn te vinden op NCSC.nl en internet.nl.

Effectieve aanpak
- Publiceer een correct SPF-record dat alleen geautoriseerde mailservers toestaat
- Activeer DKIM voor digitale ondertekening van uitgaande e-mail.
- Implementeer een DMARC-policy met p=quarantine of p=reject, waarbij DKIM en SPF een pass moeten hebben.

De Direct Send-functie in Exchange Online maakt het mogelijk om e-mails te versturen via Microsoft 365 zonder dat daarvoor actieve authenticatie (inloggen) nodig is. Deze functie is vaak nog actief voor oudere apparaten zoals printers, scanners of legacy-applicaties die geen moderne SMTP-authenticatie ondersteunen.

Waarom is dit belangrijk?
Omdat er bij Direct Send geen identiteitscontrole plaatsvindt, kan iedereen die verbinding kan maken met deze interface e-mails versturen die voor de ontvanger lijken te komen van een interne afzender. Voor een aanvaller is dit extreem waardevol; het stelt hen in staat om perfect gespoofte interne e-mails te verzenden voor phishing of impersonatie (zoals een betaalverzoek van de directie) die nagenoeg niet van echt te onderscheiden zijn en veel security-filters omzeilen

Effectieve aanpak
- Schakel Direct Send volledig uit binnen de tenant, tenzij er een aantoonbare technische noodzaak is voor specifieke bedrijfsprocessen.
- Indien gebruik onvermijdelijk is, beperk de toegang dan strikt tot een vooraf gedefinieerde set van vertrouwde en statische IP-adressen.
- Sta uitsluitend verzending toe vanaf specifiek geautoriseerde afzenderdomeinen om misbruik van andere adressen te voorkomen.
- Monitor het volume van verstuurde e-mail vanaf deze vertrouwde IP-adressen actief op afwijkingen die kunnen duiden op misbruik voor een grootschalige phishing-campagne.

Geobserveerde Technieken

T1672 | E-mail-spoofing
Het manipuleren van e-mail-infrastructuur zodat het lijkt of een mail van een legitieme bron komt.

Maatregelen

ID: 002 | SPF, DKIM en DMARC correct configureren
Prioriteit: Midden
Impact: Hoog
Inspanning: Midden

ID: 003 | Direct Send-functie uitschakelen
Prioriteit: Hoog
Impact: Hoog
Inspanning: Midden

03. Credential Access

De fase waarin de aanvaller geldige inloggegevens probeert te verkrijgen.

Phishing-resistente MFA verwijst naar moderne verificatiemethoden die bestand zijn tegen technieken waarbij aanvallers gebruikers misleiden om hun MFA-code of goedkeuring af te staan. Traditionele methoden zoals SMS-codes, telefoongesprekken of standaard pushmeldingen kunnen relatief eenvoudig worden onderschept of misbruikt via onder andere phishingkits, MFA-fatigue en man-in-the-middle-aanvallen.

Waarom is dit belangrijk?
Bij BEC richten aanvallers zich steeds vaker op het omzeilen van MFA. Wanneer een organisatie gebruikmaakt van zwakkere MFA-methoden, kan een aanvaller alsnog toegang verkrijgen tot Microsoft 365 door gebruikers te misleiden of pushmeldingen te forceren. Phishing-resistente varianten, zoals FIDO2 of Windows Hello for Business, voorkomen dat authenticatiegegevens kunnen worden doorgegeven of onderschept, waardoor de aanvalskans aanzienlijk wordt verkleind. Robuuste MFA is één van de meest effectieve maatregelen om ongeautoriseerde toegang te blokkeren.

Effectieve aanpak

- Implementeer phishing-resistente MFA, zoals FIDO2 security keys of Windows Hello for Business.
- Blokkeer het gebruik van SMS-, e-mail- of telefoongebaseerde MFA.
- Combineer MFA met Conditional Access policies om toegang te beperken op basis van locatie, apparaat, risico en context.

Microsoft Defender for Office 365 biedt geavanceerde bescherming tegen phishing, schadelijke links, malware en spoofing. Het breidt de standaardbeveiliging van Exchange Online uit met realtime analyse, sandboxing en URL-controlemechanismen die helpen om moderne e-maildreigingen te detecteren en blokkeren voordat gebruikers worden misleid.

Waarom is dit belangrijk?
E-mail blijft een van de meest gebruikte aanvalsvectoren binnen BEC. Aanvallers gebruiken vaak kwaadaardige links, geïnfecteerde bijlagen of overtuigende phishingpagina's om inloggegevens te stelen of malware te plaatsen.
Defender for Office 365 voorkomt dat gebruikers schadelijke links openen, blokkeert risicovolle bijlagen automatisch en biedt gedetailleerde detecties die helpen om BEC-pogingen vroegtijdig te identificeren.

Geobserveerde Technieken

T1110.003 | Password Spraying
Het proberen van één veelvoorkomend wachtwoord op een grote lijst met gebruikersnamen.

T1539 | Steal Web Session Cookie
Het direct buitmaken van actieve sessie-tokens om MFA te passeren zonder inloggegevens.

T1557 | AitM
Een proxy-aanval waarbij inloggegevens en sessie-tokens in real-time worden onderschept.

T1566.002 | Spearphishing Link
Gerichte e-mails met malafide links naar valse inlogpagina's.

T1621 | MFA Request Generation
Het overspoelen van de gebruiker met MFA-verzoeken (MFA Fatigue) in de hoop op een onbedoelde goedkeuring.

Maatregelen

ID: 004 | Phishing-resistente multifactorauthenticatie (MFA)
Prioriteit: Hoog
Impact: Hoog
Inspanning: Hoog

ID: 005 | Microsoft Defender for Office 365
Prioriteit: Midden
Impact: Hoog
Inspanning: Laag

Effectieve aanpak

- Activeer Safe Links om kwaadaardige URL's automatisch te herschrijven en realtime te controleren.
- Gebruik Safe Attachments zodat bijlagen eerst in een sandbox-omgeving worden geopend en geanalyseerd.
- Blokkeer .html-bijlagen in e-mail, omdat deze vaak worden misbruikt voor phishingpagina's of credential harvesting.
- Schakel anti-phishingbeleid in voor alle gebruikers (met name finance, directie en beheeraccounts)

04. Initial Access

De fase waarin de aanvaller met verkregen inloggegevens toegang krijgt tot de cloudomgeving.

Voorwaardelijke Toegang (ofwel: Conditional Access) is een essentieel onderdeel van Microsoft Entra ID dat op basis van specifieke signalen bepaalt of een gebruiker toegang krijgt tot Microsoft 365 resources. Het systeem evalueert factoren zoals de geografische locatie van de gebruiker, de status van het gebruikte apparaat en de specifieke gebruikersrol voordat toegang wordt verleend.

Waarom is dit belangrijk?
BEC-aanvallen maken veelvuldig gebruik van gestolen inloggegevens. Zonder aanvullende toegangsvoorwaarden kan een aanvaller met enkel een buitgemaakt wachtwoord al toegang krijgen tot mailboxen of bedrijfsbestanden. Conditional Access fungeert als een slimme bewaker die kijkt naar de context van de inlogpoging, waardoor gestolen gegevens alleen bruikbaar zijn als de aanvaller ook voldoet aan alle andere strenge veiligheidseisen van de organisatie.

Effectieve aanpak

- Stel een basisregel in waarbij iedere aanmelding multifactorauthentication (MFA) vereist.
- Configureer beleid om aanmeldingen vanuit risicovolle landen of locaties waar de organisatie niet actief is direct te blokkeren.
- Pas apparaat- en compliancecontroles toe, zodat alleen goedgekeurde en up-to-date apparaten toegang krijgen tot gevoelige data.
- Maak gebruik van risicogebaseerde policies waarbij de toegang automatisch wordt geblokkeerd of herauthenticatie wordt afgedwongen bij een gedetecteerd hoog aanmeldrisico.

Monitoring van verdachte inlogpogingen richt zich op de actieve bewaking van aanmeldingsactiviteiten binnen Microsoft Entra ID. Hierbij wordt gebruikgemaakt van geavanceerde signalen en algoritmen om inlogpogingen met een verhoogd risicoprofiel te identificeren, zoals aanmeldingen vanaf beruchte malafide IP-adressen of patronen van ‘impossible travel’.

Waarom is dit belangrijk?
Zelfs wanneer preventieve maatregelen zoals MFA aanwezig zijn, kunnen aanvallers soms de beveiliging passeren via technieken zoals sessie-diefstal of AitM-phishing. In dergelijke gevallen is detectie de laatste verdedigingslinie. Door in real-time verdachte patronen te herkennen, kan een organisatie direct ingrijpen voordat een aanvaller de kans krijgt om facturen te manipuleren of gevoelige bedrijfsdata te verzamelen.

Geobserveerde Technieken

T1078.004 | Cloud Accounts
Gebruik van gestolen of gekochte inloggegevens van cloudomgevingen.

Maatregelen

ID: 006 | Voorwaardelijk toegangsbeleid
Prioriteit: Hoog
Impact: Hoog
Inspanning: Midden

ID: 007 | Monitoring van verdachte inlogpogingen
Prioriteit: Hoog
Impact: Hoog
Inspanning: Midden

Effectieve aanpak

- Activeer actieve monitoring binnen Microsoft Entra om inlogpogingen met een hoog risico automatisch te detecteren.
- Implementeer policies die bij detectie van een hoog risico de toegang direct blokkeren of de gebruiker dwingen tot een veilig wachtwoordherstel via self-service password reset.
- Monitor specifiek op aanmeldingen vanuit ongebruikelijke geografische locaties of via anonimiseringsdiensten zoals VPN's en het Tor-netwerk.
- Zorg dat alerts voor kritieke aanmeldrisico's direct worden doorgezet naar de juiste beheerder of een Security Operations Center (SOC) voor verdere opvolging.

05. Execution

Het moment waarop de gebruiker wordt verleid tot een handeling die de aanval activeert.

Deze maatregel betreft het technisch blokkeren van specifieke e-mailbijlagen met extensies die een hoog risico vormen voor de veiligheid van de organisatie. De nadruk ligt hierbij op bestandstypen zoals .html, .htm, .js, en .vbs, die kunnen worden gebruikt om schadelijke scripts uit te voeren of phishingpagina's lokaal te laden.

Waarom is dit belangrijk?
E-mailbijlagen blijven een van de meest gebruikte methoden voor het verspreiden van malware en het opzetten van phishing-aanvallen binnen BEC-scenario's. Vooral .html-bijlagen worden misbruikt om gebruikers te verleiden tot het invoeren van inloggegevens op lokaal uitgevoerde, nagemaakte inlogpagina's. Omdat deze pagina's niet op een externe webserver staan, worden ze vaak niet herkend door standaard URL-scanners, waardoor ze een effectieve methode vormen voor credential harvesting.

Effectieve aanpak

- Configureer Exchange Online transportregels om inkomende e-mails met bijlagen zoals .html, .htm en andere script-gerelateerde extensies automatisch te blokkeren of in quarantaine te plaatsen.
- Activeer Microsoft Defender for Office 365 'Safe Attachments' om bijlagen die niet direct geblokkeerd worden eerst in een sandbox-omgeving te controleren op schadelijke eigenschappen.
- Stel voor specifieke zakelijke behoeften een uitzonderingsproces in (whitelist), maar zorg dat deze bijlagen altijd aan extra inspectie worden onderworpen.

Geobserveerde Technieken

T1059 | Execution via Malicious Scripts
Gebruik van scripts om acties uit te voeren binnen de browser of het systeem.

T1204 | User Execution
De gebruiker voert onbewust een schadelijke actie uit, zoals het klikken op een link.

Maatregelen

ID: 008 | Blokkeren van riskante extensies
Prioriteit: Hoog
Impact: Midden
Inspanning: Laag

06. Persistence

Zorgen dat de toegang behouden blijft, zelfs als het wachtwoord wordt gewijzigd.

OAuth-app consent bepaalt of gebruikers zelf applicaties toestemming mogen geven om toegang te krijgen tot Microsoft 365 resources zoals e-mail en bestanden. Kwaadwillende misbruiken deze functionaliteit door een malafide applicatie te laten autoriseren. Hierdoor krijgt de aanvaller langdurige en directe toegang, zonder wachtwoorden te stelen of MFA te omzeilen.

Waarom is dit belangrijk?
Wanneer een gebruiker onbedoeld toestemming geeft aan een malafide applicatie, krijgt die applicatie toegang tot mailboxen en data. Deze toegang blijft doorgaans actief, zelfs na een wachtwoordwijziging of het inschakelen van MFA. Omdat dit proces op de achtergrond plaatsvindt en vaak onopgemerkt blijft, kunnen aanvallers langdurig informatie verzamelen en voorbereidingen treffen voor een gerichte BEC-aanval.

Effectieve aanpak

- Schakel user consent uit of beperk het tot een vooraf goedgekeurde lijst van veilige applicaties.
- Gebruik de Admin Consent Workflow in Entra ID zodat alleen beheerders applicaties kunnen autoriseren.
- Controleer regelmatig alle Enterprise Applications en verwijder ongebruikte of verdachte apps.

Geobserveerde Technieken

T1098.001 | Account Manipulation
Additional Cloud Credentials: Het toevoegen van extra geheimen of certificaten aan cloud-accounts of apps.

T1556.006 | Modify Authentication Process
Het toevoegen van een eigen MFA-methode aan het account van het slachtoffer.

T1671 | Illicit Consent Grant
Gebruikers misleiden om een malafide OAuth-app toegang te geven tot mailboxen en data.

Maatregelen

ID: 009 | OAuth-app consent beperken of uitschakelen
Prioriteit: Hoog
Impact: Hoog
Inspanning: Laag

07. Privilege Escalation

De aanvaller probeert meer rechten te krijgen om de hele tenant te controleren.

Het Least Privilege-principe houdt in dat gebruikers en beheerders toegang krijgen tot, of uitsluitend de rechten krijgen die noodzakelijk zijn voor hun functie of taak. Dit vermindert het risico dat accounts per ongeluk of door misbruik toegang bieden tot gevoelige data of kritieke configuraties.

Waarom is dit belangrijk?
Bij BEC geldt: hoe meer rechten een gecompromitteerd account heeft, hoe groter de schade. Te ruime of permanente beheerrechten geven aanvallers de mogelijkheid om rechten aan te passen, nieuwe accounts te maken of beveiligingsinstellingen uit te schakelen. Door rechten te beperken en alleen tijdelijk toe te kennen, verklein je het aanvalsoppervlak en verhoog je de detectiekans bij misbruik. Daarnaast is het voor auditing en forensisch onderzoek essentieel dat beheeracties altijd herleidbaar zijn tot een specifiek persoon. Dit is alleen mogelijk wanneer beheertaken worden uitgevoerd met persoonsgebonden accounts.

Hoe verkom je het?
- Geef gebruikers en beheerders uitsluitend de minimaal noodzakelijke rechten.
- Maak gebruik van Privileged Identity Management (PIM) voor tijdelijke en goedgekeurde toewijzing van beheerrollen.
- Gebruik geen permanente Global Administrator-accounts. Beheer moet plaatsvinden via persoonsgebonden accounts met just-in-time-rechten.
- Houd één of twee break-glass accounts aan voor noodsituaties. Deze accounts worden uitsluitend voor incidenten gebruikt en zijn beschermd met sterke wachtwoorden en robuuste monitoring.

Geobserveerde Technieken

T1068 | Exploitation for Privilege Escalation
Het misbruiken van configuratiefouten om beheerrechten te verkrijgen.

Maatregelen

ID: 010 | Least Privilege-principe & PIM
Prioriteit: Midden
Impact: Midden
Inspanning: Midden

08. Defense Evasion

Het omzeilen van beveiligingsmaatregelen en het verbergen van sporen.

Microsoft Exchange genereert automatische security alerts over risicovolle activiteiten, zoals het aanmaken van forwardingregels, wijzigen van mailboxrechten of privilege escalatie. Deze meldingen worden onder andere verzonden vanaf het adres Office365Alerts@microsoft.com en zijn terug te vinden in de Compliance Alerts binnen het Microsoft Purview admin center.

Waarom is dit belangrijk?
Security alerts vormen vaak de eerste aanwijzing dat een aanvaller actief is binnen de omgeving. In veel organisaties worden deze meldingen echter slechts naar één beheerder verzonden, waardoor het risico ontstaat dat waarschuwingen over het hoofd worden gezien of niet tijdig worden opgevolgd. Door alerts breder te distribueren, bijvoorbeeld naar IT-beheer, SOC en securityverantwoordelijken wordt de kans op tijdige detectie en actie aanzienlijk vergroot.

Effectieve aanpak

- Richt een speciale distributiegroep of dedicated mailbox in voor alle beveiligingsmeldingen.
- Voeg relevante teams toe (zoals, SOC, IT-beheer, CISO, security officer).
- Controleer regelmatig of alle kritieke Microsoft 365-, Exchange- en Purview-alerts correct worden afgeleverd en opgevolgd.

De Unified Audit Log (UAL) is de centrale bron van waarheid binnen Microsoft 365. Het legt een breed scala aan activiteiten vast, van gebruikersaanmeldingen tot wijzigingen in mailboxrechten en configuraties door beheerders. Door deze logging te combineren met logforwarding naar een SIEM-oplossing (zoals Microsoft Sentinel), worden deze gegevens centraal geanalyseerd en beveiligd opgeslagen.

Waarom is dit belangrijk?
Volledige zichtbaarheid is essentieel om verdachte activiteiten tijdig te detecteren en te begrijpen. Zonder actieve auditlogging is een organisatie blind na een inbreuk; het is dan onmogelijk om vast te stellen welke data een aanvaller heeft ingezien of welke frauduleuze acties er zijn verricht. Bovendien proberen aanvallers vaak logging uit te schakelen of sporen te wissen om onopgemerkt te blijven; externe logforwarding en actieve monitoring op de status van de UAL voorkomen dat deze blinde vlek ontstaat.

Geobserveerde Technieken

T1562.001 | Impair Defenses
Disable or Modify Tools: Het uitschakelen van logging of alerts door de aanvaller.

T1564.008 | Email Hiding Rules
Het instellen van regels om inkomende mails van de bank of IT direct te verplaatsen naar onopvallende mappen.

Maatregelen

ID: 011 | Security alerts doorsturen
Prioriteit: Hoog
Impact: Hoog
Inspanning: Laag

ID: 012 | Unified Audit Log (UAL) inschakelen
Prioriteit: Hoog
Impact: Hoog
Inspanning: Midden

ID: 013 | Monitoring op configuratiedrift
Prioriteit: Hoog
Impact: Hoog
Inspanning: Midden

Effectieve aanpak
- Controleer en waarborg dat de Unified Audit Log is geactiveerd binnen Microsoft Purview.
- Configureer logforwarding naar een SIEM-oplossing voor gecentraliseerde analyse en langdurige retentie van gegevens.
- Stel actieve alerts in voor risicovolle gebeurtenissen zoals aanmeldingen vanaf ongewone locaties, externe mailboxregels of wijzigingen in beheerderstaken.

Monitoring op configuratiedrift betreft de continue en actieve bewaking van de vastgestelde beveiligingsinstellingen (de security baseline) binnen de Microsoft 365 omgeving. Deze maatregel is erop gericht om onbedoelde of ongeautoriseerde wijzigingen in kritieke beveiligingsconfiguraties direct te identificeren.

Waarom is dit belangrijk?
Zodra aanvallers toegang hebben verkregen tot een omgeving, proberen zij vaak de aanwezige verdedigingsmechanismen stapsgewijs te verzwakken of uit te schakelen om onzichtbaar te blijven. Door bijvoorbeeld auditlogging uit te zetten of MFA-uitzonderingen voor specifieke accounts toe te voegen, creëren zij een blinde vlek waarin zij ongehinderd fraude kunnen plegen. Zonder actieve monitoring op deze afwijkingen (drift) kan een omgeving ongemerkt fundamenteel onveilig worden gemaakt, zelfs als de initiële inrichting correct was.

Effectieve aanpak
- Implementeer actieve monitoring die wijzigingen in de security baseline van de organisatie realtime detecteert.
- Stel directe alerts in die afgaan wanneer kritieke functies zoals de Unified Audit Log (UAL) worden uitgeschakeld.
- Monitor specifiek op het toevoegen van MFA-uitzonderingen in Conditional Access policies of het registreren van nieuwe MFA-methodes voor bevoorrechte accounts.
- Zorg voor een proces waarbij elke gedetecteerde afwijking van de standaardconfiguratie direct wordt geëvalueerd en, indien ongeautoriseerd, onmiddellijk wordt hersteld.

09. Discovery

De aanvaller verkent de omgeving om waardevolle informatie en doelwitten te vinden.

Deze maatregel betreft het technisch beperken van de toegang tot het Microsoft Entra (voorheen Azure AD) beheerportaal voor reguliere gebruikers die geen beheerrol hebben. In de standaardconfiguratie van Microsoft 365 hebben namelijk alle gebruikers binnen de organisatie een bepaalde mate van leesrechten in de directory. Door deze toegang expliciet te blokkeren, wordt de zichtbaarheid van de volledige organisatiestructuur beperkt tot geautoriseerde beheerders.

Waarom is dit belangrijk?
In de Discovery-fase van een BEC-aanval probeert een aanvaller de organisatie in kaart te brengen. Wanneer een aanvaller toegang heeft tot een standaard gebruikersaccount, kan hij via het Entra-portaal eenvoudig een lijst ophalen van alle medewerkers, hun specifieke rollen (zoals wie de Global Admin of CFO is) en de gebruikte bedrijfsapplicaties. Deze informatie is cruciaal voor het voorbereiden van zeer gerichte en geloofwaardige vervolgstappen, zoals spearphishing of impersonatie van sleutelfiguren.

Effectieve aanpak
- Activeer de instelling Toegang tot Microsoft Entra-beheerportal beperken (Restrict access to Microsoft Entra administration portal) binnen de gebruikersinstellingen van Microsoft Entra ID.
- Zorg dat het principe van *Least Privilege* wordt nageleefd, zodat alleen gebruikers met een noodzakelijke en persoonsgebonden beheerrol toegang behouden tot de administratieve omgeving.
- Monitor regelmatig op wijzigingen in de toegangsinstellingen van het beheerportaal om te voorkomen dat deze beperking onbedoeld wordt opgeheven (configuratiedrift).

Geobserveerde Technieken

T1538 | Cloud Service Dashboard
Navigeren door het Microsoft 365 dashboard om rollen, applicaties en gebruikers te inventariseren.

Maatregelen

ID: 014 | Beperk toegang tot Microsoft Entra
Prioriteit: Midden
Impact: Laag
Inspanning: Laag

10. Lateral Movement

Het uitbreiden van de aanval naar andere gebruikers of systemen binnen de organisatie.

Deze maatregel betreft het configureren van beveiligingsmechanismen binnen Microsoft 365 om niet alleen inkomende e-mail van buiten de organisatie te controleren, maar ook al het interne en uitgaande e-mailverkeer actief te scannen op phishing-kenmerken. Hierbij wordt gebruikgemaakt van Microsoft Defender for Office 365 om berichten te analyseren op schadelijke links, bijlagen en impersonatiepogingen.

Waarom is dit belangrijk?
Veel standaardbeveiligingsinstellingen zijn primair gericht op de perimeters, waardoor intern verkeer vaak onvoldoende wordt gecontroleerd. In een BEC-scenario is dit een groot risico; wanneer een aanvaller eenmaal toegang heeft tot een mailbox, kan hij dat gecompromitteerde account gebruiken om geloofwaardige 'interne' phishing-mails naar collega's te sturen om de aanval verder uit te breiden (Lateral Movement). Omdat medewerkers e-mails van hun eigen collega's sneller vertrouwen, is de kans op een succesvolle vervolginbreuk zonder deze interne detectie aanzienlijk groter.

Effectieve aanpak

- Configureer Microsoft Defender for Office 365 om ook intern en uitgaand e-mailverkeer actief te scannen op phishing-kenmerken.
- Zorg dat beveiligingsfuncties zoals Safe Links en Safe Attachments consistent worden toegepast op alle mailstromen binnen de tenant, ongeacht de bron of bestemming.
- Activeer automatische meldingen voor beheerders bij de detectie van uitgaande spam of phishing, aangezien dit vaak een directe indicator is van een account dat door een aanvaller wordt misbruikt.

Geobserveerde Technieken

T1534 | Internal Spearphishing
Het versturen van phishing-mails vanaf een gecompromitteerd account naar collega's.

T1537 | Transfer Data to Cloud Account
Het verplaatsen van data tussen verschillende cloudresources.

T1566.003 | Spearphishing via Service
Gebruik van legitieme cloudservices (zoals gedeelde documenten) om interne targets te bereiken.

Maatregelen

ID: 015 | Interne en uitgaande phishingdetectie
Prioriteit: Midden
Impact: Hoog
Inspanning: Midden

11. Collection

Het verzamelen van de data die nodig is om de fraude te plegen.

Automatische e-mailforwarding maakt het mogelijk om inkomende e-mail direct door te sturen naar een ander adres. Aanvallers die toegang hebben verkregen tot een mailbox gebruiken deze functie vaak om berichten onopvallend te kopiëren naar een extern e-mailaccount. Hierdoor kunnen zij lopende communicatie volgen zonder verdere interactie of zichtbare sporen achter te laten.

Waarom is dit belangrijk?
Bij BEC is inzicht in zakelijke communicatie essentieel voor het voorbereiden van frauduleuze betaalverzoeken of het manipuleren van facturen. Door forwardingregels in te stellen kunnen aanvallers:

- vertrouwelijke informatie monitoren,
- betalingsprocessen en interne besluitvorming volgen, en
- langdurig toegang houden, zelfs nadat het wachtwoord is gewijzigd of de aanvaller is uitgelogd.

Omdat forwardingregels vaak stil en op de achtergrond werken, vormen zij een van de meest gebruikte en meest effectieve methoden binnen BEC.

Effectieve aanpak

- Blokkeer externe automatische forwarding via Exchange Online transportregels of outbound spam policies.
- Sta automatische forwarding uitsluitend toe voor vooraf goedgekeurde use-cases, bijvoorbeeld door te werken met een whitelist van vertrouwde domeinen of specifieke mailboxen.
- Controleer periodiek alle mailboxen op ongewenste of verdachte regels.
- Configureer alerts voor nieuwe of gewijzigde mailboxregels die forwarding of redirect-acties bevatten.

Microsoft Teams en SharePoint maken samenwerking met externe partijen mogelijk via gasttoegang, gedeelde bestanden en externe links. Hoewel dit de samenwerking vergemakkelijkt, introduceert het ook risico's. Aanvallers kunnen misbruik maken van gastaccounts, verkeerd geconfigureerde deelinstellingen of anonieme links om toegang te krijgen tot gevoelige informatie.

Waarom is dit belangrijk?
Bij BEC richten aanvallers zich niet alleen op e-mail, maar ook op samenwerkingsplatformen waar bedrijfsdocumenten, contracten, financiële informatie en operationele data worden gedeeld. Wanneer externe samenwerking onvoldoende wordt beperkt, kunnen aanvallers misbruik maken van gastaccounts, onjuist geconfigureerde deelinstellingen of anonieme links om toegang te krijgen tot gevoelige informatie.

Geobserveerde Technieken

T1114.002 | Remote Email Collection
Het op afstand uitlezen van mailboxen.

T1114.003 | Email Forwarding Rule
Automatisch doorsturen van mail naar een extern adres om communicatie ongemerkt te volgen.

T1530 | Data from Cloud Storage
Het doorzoeken van SharePoint of OneDrive op facturen en contracten.

T1078 | Valid Accounts (Guest Accounts Misuse)
Misbruik van gastaccounts om toegang te krijgen tot gedeelde bestanden.

Maatregelen

ID: 016 | Blokkering van automatische e-mailforwarding
Prioriteit: Hoog
Impact: Hoog
Inspanning: Midden

ID: 017 | Teams & SharePoint collaboration beperken
Prioriteit: Midden
Impact: Midden
Inspanning: Midden

Risico's ontstaan onder andere wanneer ongecontroleerde externe toegang wordt toegestaan, gedeelde links openbaar beschikbaar zijn, oude gastaccounts actief blijven of samenwerkingen met onbekende of onbetrouwbare domeinen mogelijk zijn. Het beperken van samenwerking tot vertrouwde domeinen verkleint deze risico's en helpt datalekken te voorkomen.

Effectieve aanpak

- Configureer een allowlist van vertrouwde domeinen waarmee externe samenwerking is toegestaan.
- Schakel anonieme toegang tot gedeelde links uit of beperk deze tot view-only waar strikt noodzakelijk.
- Controleer regelmatig gedeelde mappen op ongewenste of verlopen externe toegang.
- Controleer regelmatig Teams-kanalen op ongewenste of verlopen externe toegang.
- Controleer regelmatig bestaande externe gebruikers op ongewenste of verlopen toegang.
- Automatiseer het intrekken van toegang voor inactieve of verlopen gastaccounts, bijvoorbeeld op basis van inactiviteit of access reviews via Entra ID.

12. Exfiltration

Het daadwerkelijk naar buiten brengen van de verzamelde data.

Access Reviews (toegangsbeoordelingen) is een gestructureerd proces waarbij periodiek wordt gecontroleerd of gebruikers, gasten en beheerders nog steeds de rechten en toegang nodig hebben die aan hen zijn toegewezen. Dit richt zich specifiek op het evalueren van de toegang tot Teams-kanalen, SharePoint-mappen en bevoorrechte rollen binnen de Microsoft Entra-omgeving.

Waarom is dit belangrijk?
Bij BEC-incidenten maken aanvallers vaak misbruik van 'vergeten' toegang, zoals oude gastaccounts die niet meer in gebruik zijn of onnodig ruime rechten op mappen met gevoelige financiële informatie. Wanneer externe samenwerking niet regelmatig wordt opgeschoond, blijven er kwetsbare ingangen openstaan die een aanvaller kan gebruiken om ongemerkt data te verzamelen of te exfiltreren. Door deze toegang systematisch in te trekken, wordt het aanvalsoppervlak verkleind en het risico op datalekken aanzienlijk verlaagd.

Effectieve aanpak
- Controleer regelmatig Teams-kanalen en gedeelde mappen op ongewenste of verlopen externe toegang.
- Beoordeel periodiek alle bestaande externe gebruikers en verwijder accounts waarvan de noodzaak voor samenwerking is vervallen.
- Automatiseer, waar mogelijk, het intrekken van toegang voor inactieve of verlopen gastaccounts via de Access Reviews-functionaliteit in Microsoft Entra ID.
- Dwing een proces af waarbij eigenaren van data en Teams-omgevingen verantwoordelijk zijn voor de periodieke goedkeuring van de aanwezige gebruikerslijsten.

Geobserveerde Technieken

T1567 | Exfiltration Over Web Services
Het buitmaken van data via legale webdiensten of gedeelde links.

Maatregelen

ID: 018 | Access Reviews
Prioriteit: Midden
Impact: Midden
Inspanning: Midden

13. Impact

Het uiteindelijke doel van de aanvaller: de financiële diefstal.

In de Impact-fase zijn technische barrières vaak al gepasseerd. De verdediging verschuift hier van techniek naar strikte administratieve procedures, waarbij het vier-ogen-principe en handmatige verificatie van betaalinstructies centraal staan.

Waarom is dit belangrijk?
Dit is de laatste 'vangrail' om daadwerkelijke financiële diefstal (T1657) te voork omen. Zelfs als een aanvaller via impersonatie (T1656) een technisch perfecte vervalste factuur aanbiedt, kan een procedurele controle de transactie op het laatste moment stoppen.

Effectieve aanpak

- Hanteer een strikt vier-ogen-principe: elke betaling moet door minimaal twee personen worden geaccordeerd.
- Valideer wijzigingen in bankgegevens of ongebruikelijke spoedbetalingen altijd telefonisch via een bekend en vertrouwd nummer.
- Leg deze procedures vast in een protocol waar ook voor de directie geen uitzonderingen op mogelijk zijn.
- Stimuleer het vragenstellen aan de andere goedkeurder om te bepalen of dit mogelijk fraude zou kunnen zijn.

Geobserveerde Technieken

T1656 | Impersonation (impersonatie)
Zich voordoen als een vertrouwde persoon (CEO, leverancier) om betalingen los te krijgen.

T1657 | Financial Theft (financiële diefstal)
De daadwerkelijke diefstal van geld door manipulatie van betaalverzoeken.

Maatregelen

ID: 019 | Administratieve verificatie van betalingen
Prioriteit: Hoog
Impact: Hoog
Inspanning: Midden

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

April 2026