Hulp bij een gecompromitteerd e-mail-account

Hulp bij een gecompromitteerd e-mail-account

Business Email Compromise (BEC) is een vorm van fraude waarbij een aanvaller misbruik maakt van e-mailcommunicatie of een gecompromitteerd account om vertrouwen, informatie of geld te verkrijgen.

Dit document bevat een praktisch stappenplan voor het analyseren, beperken, onderzoeken en herstellen van een BEC-incident. De volgorde van de acties onder elke stap is geprioriteerd: acties die verdere schade of verlies van bewijs kunnen voorkomen, staan eerder in het proces.

De stappen kunnen in de praktijk deels parallel lopen. Gebruik de volgorde daarom als uitgangspunt, maar wijk af wanneer de actuele dreiging of impact van het incident daar om vraagt.

Stappenplan

Stap 1. Identificatie en analyse

1.1 Incident valideren

Doel: Bevestigen dat sprake is van een (mogelijk) BEC-incident en bepalen of directe incidentrespons nodig is.

- Beoordeel de melding en controleer de verdachte e-mail of activiteit.
- Verifieer opvallende handelingen bij de betrokken gebruiker.
- Controleer of sprake is van ongeautoriseerde toegang, *spoofing* of frauduleuze communicatie.
- Leg de eerste feiten en het tijdstip van de melding vast.

1.2 Getroffen accounts en omvang vaststellen

Doel: Bepalen welke accounts, mailboxen, personen en diensten direct bij het incident betrokken zijn.

- Identificeer de getroffen gebruiker(s), mailbox(en) en e-mailadressen.
- Controleer of meerdere accounts vergelijkbare verdachte activiteit tonen.
- Breng interne en externe partijen in kaart die vanuit het account zijn benaderd.
- Controleer of gekoppelde diensten zoals Teams, OneDrive of SharePoint betrokken zijn.

1.3 Impact bepalen

Doel: Inschatten welke gevolgen het incident heeft voor gegevens, financiën, processen en betrokkenen.

- Controleer of frauduleuze betaalverzoeken of wijzigingen van betaalgegevens zijn verstuurd.
- Bepaal of vertrouwelijke informatie of persoonsgegevens mogelijk zijn ingezien of gedeeld.

- Stel vast welke bedrijfsprocessen of externe relaties zijn geraakt.
- Schat de financiële, operationele en reputatie-impact in.

1.4 Incident classificeren

Doel: De ernst en prioriteit bepalen zodat de juiste afhandelingsroute en escalatie worden gekozen.

- Classificeer het incident op basis van omvang, impact en actuele dreiging.
- Bepaal de prioriteit en benodigde responscapaciteit.
- Escaleer naar incidentcoördinatie, management of privacyfunctie indien vereist.
- Leg de gekozen classificatie en onderbouwing vast.
- Deel relevante informatie met School-CERT. Wij kunnen dit indien nodig sectorbreed delen.

1.5 Bewijsmateriaal veiligstellen

Doel: Relevante informatie bewaren zodat onderzoek mogelijk blijft en bewijs niet verloren gaat.

- Stel verdachte e-mails inclusief headers en bijlagen veilig.
- Bewaar relevante authenticatie-, audit- en mailboxlogs.
- Leg IOC's vast, zoals IP-adressen, domeinen, url's en gebruikte applicaties.
- Documenteer welke gegevens wanneer en door wie zijn veiliggesteld.

Stap 2. Schade beperken

2.1 Actieve ongeautoriseerde toegang beëindigen

Doel: De toegang van de aanvaller zo snel mogelijk stoppen voordat verdere acties worden uitgevoerd.

- Trek actieve sessies, refresh tokens en OAuth-tokens in.
- Verwijder ongeautoriseerde applicatietoestemmingen.
- Controleer en verwijder ongewenste gedelegeerde mailboxrechten.
- Blokkeer zo nodig tijdelijk het getroffen account.
- Documenteer alle acties die ondernomen worden voor het herstel.

2.2 Getroffen account beveiligen

Doel: Voorkomen dat de aanvaller opnieuw kan inloggen en de rechtmatige gebruiker veiligstellen.

- Reset het wachtwoord en controleer of het nieuwe wachtwoord uniek is.
- Herregistreer of forceer MFA wanneer daar aanleiding voor is.
- Controleer herstelgegevens en authenticatiemethoden op ongewenste wijzigingen.
- Laat de gebruiker pas opnieuw aanmelden nadat de actieve toegang is ingetrokken.

2.3 Kwaadaardige wijzigingen verwijderen

Doel: Persistentiemechanismen en ongewenste mailboxconfiguratie verwijderen.

- Verwijder verdachte inbox- en forwardingsregels.
- Controleer mailboxmachtigingen en gedelegeerde toegang.
- Verwijder onbekende gekoppelde applicaties of add-ins.
- Herstel andere ongewenste account- of mailboxinstellingen.

2.4 Verdachte communicatie blokkeren

Doel: Voorkomen dat dezelfde infrastructuur of berichten verder binnen de organisatie worden gebruikt.

- Blokkeer kwaadaardige afzenders, domeinen en url's.

- Zoek naar vergelijkbare phishingberichten in andere mailboxen en verwijder of zet deze in quarantaine.
- Werk relevante mailfilters en detectieregels bij.
- Deel relevante IOC's met School-CERT. Hiermee kunnen wij andere besturen faciliteren.

2.5 Directe schade beperken

Doel: Financiële, operationele en reputatieschade zo snel mogelijk minimaliseren.

- Controleer met Finance of verdachte betalingen of rekeningwijzigingen zijn aangevraagd.
- Probeer frauduleuze betalingen te blokkeren of terug te roepen.
- Waarschuw benaderde leveranciers, klanten of collega's wanneer zij risico lopen.
- Start verhoogde monitoring op het account en gerelateerde indicatoren.

Stap 3. Onderzoek

3.1 Activiteiten van de aanvaller analyseren

Doel: Vaststellen wat de aanvaller binnen het account en de omgeving heeft gedaan.

- Analyseer verdachte aanmeldingen, locaties, apparaten en IP-adressen.
- Onderzoek mailbox- en auditactiviteiten, inclusief geopende, verzonden en verwijderde berichten.
- Controleer wijzigingen aan regels, machtigingen, MFA en gekoppelde applicaties.
- Onderzoek aanwijzingen voor fraudevoorbereiding, zoals het volgen van betaal- of leverancierscommunicatie.

3.2 Verdere compromittering onderzoeken

Doel: Bepalen of het incident zich naar andere accounts, systemen of personen heeft uitgebreid.

- Controleer andere accounts op dezelfde IOC's of afwijkende aanmeldingen.
- Onderzoek of vanuit het gecompromitteerde account andere gebruikers zijn benaderd.
- Controleer gekoppelde diensten zoals Teams, OneDrive en SharePoint, of andere diensten waar dezelfde inloggegevens gebruikt worden.
- Onderzoek ongeautoriseerde applicaties, machtigingen of laterale toegang.

3.3 Gegevensimpact vaststellen

Doel: Bepalen welke informatie de aanvaller mogelijk heeft ingezien, gewijzigd, gekopieerd of gedeeld.

- Bepaal welke e-mails en mailboxmappen mogelijk zijn benaderd.
- Controleer of bestanden zijn geopend, gedownload of gedeeld.
- Onderzoek forwarding, export of andere vormen van mogelijke exfiltratie.
- Breng persoonsgegevens, vertrouwelijke informatie en financiële informatie in kaart.

3.4 Oorzaak vaststellen

Doel: Achterhalen hoe de aanvaller toegang heeft gekregen en waarom de aanval kon slagen.

- Onderzoek mogelijke phishing- of credential-theftmomenten.
- Controleer misbruik van MFA, sessietokens of OAuth-toestemmingen.
- Interview de betrokken gebruiker over verdachte e-mails, links of downloads.
- Bepaal welke beveiligingsmaatregelen ontbraken, faalden of zijn omzeild.

3.5 Tijdlijn reconstrueren

Doel: Alle bevindingen samenbrengen tot een chronologisch en controleerbaar beeld van het incident.

- Leg het eerste bekende moment van toegang of verdachte activiteit vast.
- Orden de belangrijkste acties van de aanvaller op datum en tijd.
- Voeg containment- en herstelacties toe aan dezelfde tijdlijn.
- Bepaal de vermoedelijke start, duur en beëindiging van het incident.

Stap 4. Herstel

4.1 Veilige toegang herstellen

Doel: De rechtmatige gebruiker gecontroleerd weer toegang geven nadat de aanval is gestopt.

- Deblokkeer het account wanneer de beveiligingscontroles zijn afgerond.
- Controleer wachtwoord, MFA en herstelmethoden voordat de gebruiker opnieuw inlogt.
- Laat de gebruiker de aanmelding testen vanaf een vertrouwd apparaat.
- Controleer kort na herstel opnieuw op verdachte sessies of aanmeldingen.

4.2 Ongewenste wijzigingen herstellen

Doel: De account- en mailboxconfiguratie terugbrengen naar de gewenste en vertrouwde situatie.

- Herstel legitieme mailboxregels en instellingen waar nodig.
- Controleer en herstel machtigingen, aliassen en forwarding.
- Verwijder resterende ongeautoriseerde koppelingen of configuraties.
- Controleer of bedrijfsprocessen of contactgegevens door de aanval zijn gewijzigd.

4.3 Beveiliging versterken

Doel: Aanvullende maatregelen doorvoeren om herhaling van hetzelfde aanvalspad te verkleinen.

- Versterk MFA- en Conditional Access-beleid waar nodig.
- Verbeter detecties voor afwijkende aanmeldingen, mailboxregels en OAuth-toestemmingen.
- Beperk onnodige rechten en externe toegang.
- Voer gerichte bewustwordingsmaatregelen uit als menselijk handelen een rol speelde.

4.4 Herstel verifiëren

Doel: Bevestigen dat de omgeving schoon is en de genomen herstelmaatregelen effectief zijn.

- Controleer opnieuw op bekende IOC's en verdachte activiteit.
- Verifieer dat sessies, tokens, regels en machtigingen correct zijn.
- Bevestig dat monitoring geen nieuwe afwijkingen laat zien.
- Leg vast wie het herstel heeft gecontroleerd en wanneer.

4.5 Betrokkenen informeren

Doel: Zorgen dat betrokken gebruikers en stakeholders weten dat het herstel is uitgevoerd en welke acties nog volgen.

- Informeer de getroffen gebruiker over het herstel en aandachtspunten.
- Informeer interne stakeholders over status en resterende risico's.
- Stem communicatie af met leveranciers of klanten als zij geraakt zijn.
- Communiceer eventuele aanvullende monitoring of vervolgmaatregelen.

Stap 5. Evaluatie en rapportage

5.1 Incident en impact documenteren

Doel: Een volledige, feitelijke registratie maken van het incident, de impact en de uitgevoerde respons.

- Beschrijf aanleiding, scope, impact en belangrijkste bevindingen.
- Leg containment-, onderzoeks- en herstelmaatregelen vast.
- Neem de definitieve tijdlijn en relevante bewijsverwijzingen op.
- Documenteer openstaande risico's of onzekerheden.

5.2 Respons evalueren

Doel: Beoordelen hoe effectief en efficiënt het incident is gedetecteerd en afgehandeld.

- Evalueer detectiesnelheid, escalatie en besluitvorming.
- Beoordeel of containment snel genoeg en volledig was.
- Controleer of rollen, verantwoordelijkheden en communicatie duidelijk waren.
- Leg knelpunten in tooling, logging of procedures vast.

5.3 Lessen vastleggen

Doel: Concrete lessen formuleren die toekomstige BEC-incidenten beter voorkomen of sneller laten afhandelen.

- Bepaal welke signalen eerder herkend hadden kunnen worden.
- Leg verbeterpunten voor processen en draaiboeken vast.
- Bepaal of aanvullende training of awareness nodig is.
- Deel relevante lessen met teams die vergelijkbare risico's beheren.

5.4 Verbetermaatregelen bepalen

Doel: Lessen vertalen naar concrete acties met duidelijke verantwoordelijkheid en opvolging.

- Definieer technische en organisatorische verbetermaatregelen.
- Wijs per maatregel een eigenaar en gewenste opleverdatum toe.
- Prioriteer maatregelen op risico en uitvoerbaarheid.
- Plan een moment om de implementatie en effectiviteit te controleren.

5.5 Rapporteren aan stakeholders

Doel: De juiste stakeholders voorzien van een passende samenvatting, bevindingen en vervolgacties.

- Stel een eindrapport of managementsamenvatting op.
- Rapporteer aan management en relevante proceseigenaren.
- Betrek privacy, juridische of toezichthoudende functies indien van toepassing.
- Maak duidelijk welke verbetermaatregelen nog openstaan en wie eigenaar is.

Praktische notitie

Bij een BEC-incident kunnen meerdere fasen tegelijk actief zijn. Containment en onderzoek moeten elkaar ondersteunen: voorkom verdere schade, maar stel waar mogelijk eerst de informatie veilig die nodig is om het incident te reconstrueren.

Kennisnet

School CERT Laatst bijgewerkt 4 september 2026

Voor ondersteuning: cert@school-cert.nl of 0800 321 22 33

Voor vragen over School-CERT: info@school-cert.nl