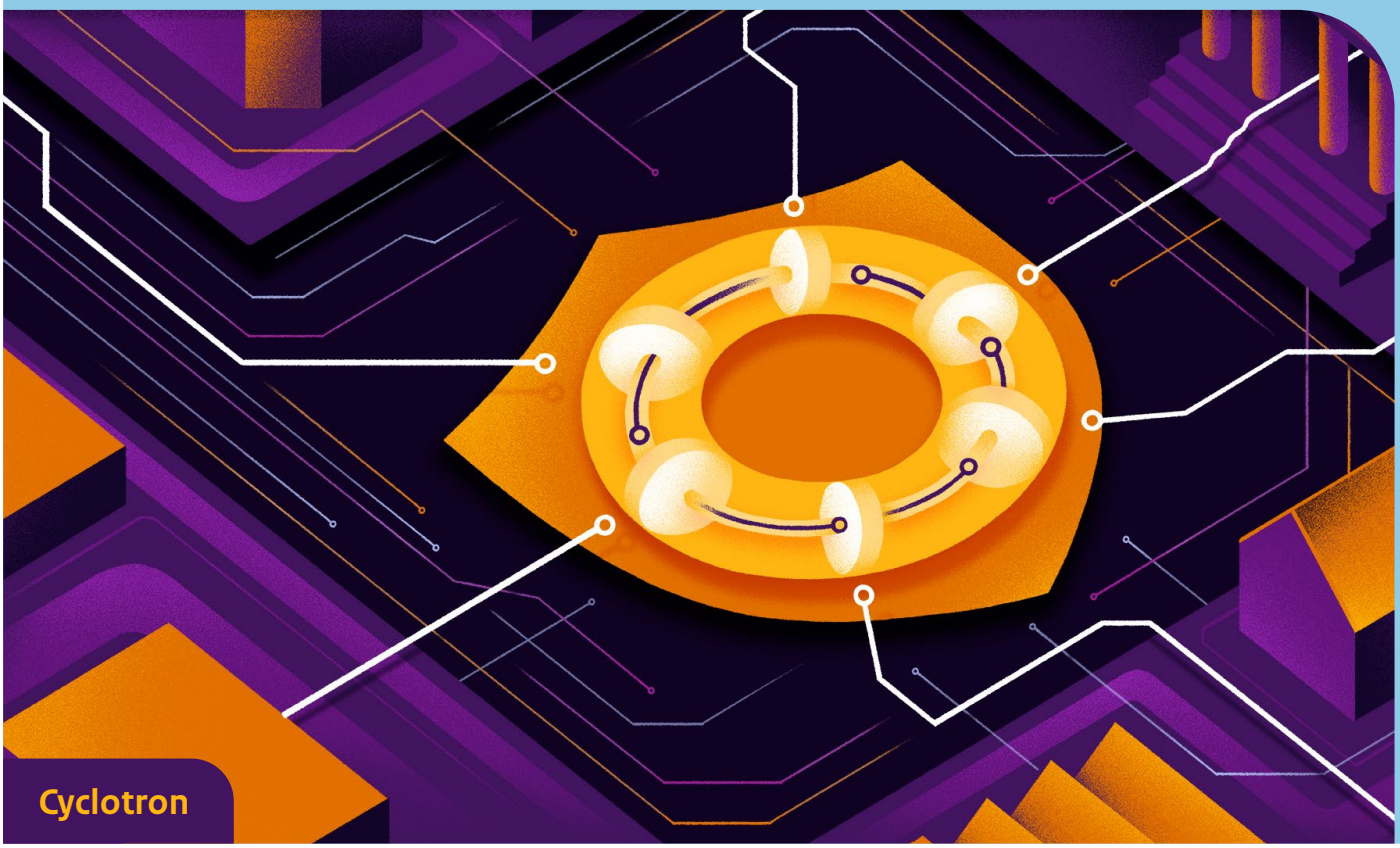
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Business E-mail Compromise (BEC)

Praktische handvatten voor het mkb

Versie: 1.0



In samenwerking met:

ATTIC INVICTUS INCIDENT RESPONSE orange Cyberdefense TESORION

Inhoudsopgave

Introductie 3

Deel 1: Achtergrond 4

De fraude die zich voordoet als jouw eigen mensen 4

Hoe werkt een BEC-aanval? 5

De verstrekkende gevolgen van een geslaagde BEC-aanval 6

MITRE ATT&CK: Een raamwerk voor bescherming 9

De nieuwe dreiging: AI maakt BEC gevaarlijker 9

Hoe herken je AI-gegenereerde fraude? 11

Bescherming tegen AI-versterkte BEC 11

Waarom BEC ook jouw bedrijf kan treffen 12

Deel 2: Praktische handvatten 13

Simpele tips die je vandaag nog kunt toepassen 13

Stel deze vragen aan jouw IT-dienstverlener 13

Tot slot: bewustzijn is de beste verdediging 15

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. In deze publicatie lees je hoe een BEC-incident zich typisch ontwikkelt, welke organisatorische en procesmatige factoren een rol spelen en waar je als manager daadwerkelijk op kunt sturen.

BEC is geen technische hack. Criminelen misbruiken vertrouwen, autoriteit en tijdsdruk om jouw medewerkers te verleiden tot betalingen of het delen van vertrouwelijke informatie. Met gebruik van AI worden die aanvallen bovendien razendsnel professioneler: in perfecte taal, met nagebootste stemmen en zelfs gesimuleerde videogesprekken. De traditionele signalen om fraude te herkennen werken niet meer. Wat wél werkt, lees je in deze publicatie.

**In aanvulling op deze publicatie is een technisch advies opgesteld met een volledig uitgewerkt maatregelenpakket dat je kunt delen met jouw Managed Security Service Provider (MSSP).*

Doelgroep

Deze publicatie is primair voor ondernemers, managers en bestuurders van organisaties die onder het mkb vallen. De inhoud is bewust praktisch en niet technisch zodat je ook zonder IT-achtergrond direct aan de slag kunt.

De technische bijlage is bedoeld voor jouw IT-dienstverlener of Manager Security Service Provider (MSSP)

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.

Deel 1: Achtergrond

De fraude die zich voordoet als jouw eigen mensen

Business E-mail Compromise (BEC) is een van de snelst groeiende vormen van digitale oplichting in Nederland. Bij BEC doen criminelen zich voor als iemand die je vertrouwt: bijvoorbeeld de directeur, een collega, een vaste leverancier of zelfs een klant. Via e-mail of telefoon proberen ze je te verleiden tot betalingen of het delen van vertrouwelijke informatie.

Het gevaarlijke aan BEC is dat het niet gaat om ingewikkelde technische aanvallen. Criminelen maken gebruik van **vertrouwen en menselijk gedrag**. Ze creëren urgentie, benadrukken vertrouwelijkheid en imiteren geloofwaardig de manier waarop de directeur of leverancier normaliter communiceert.

Dit kan ieder bedrijf overkomen

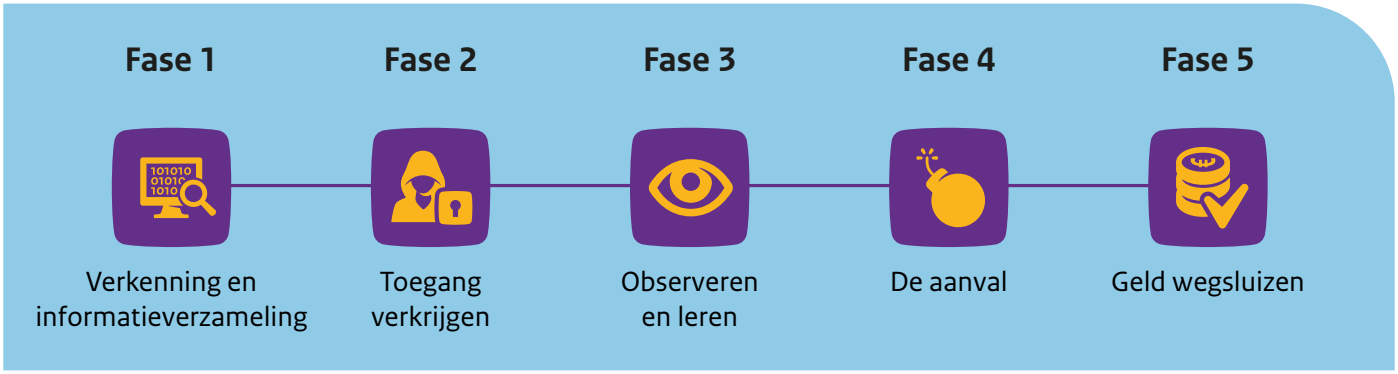
Een voorbeeld uit de praktijk:
Een medewerker van een middelgroot bedrijf ontvangt een e-mail van de directeur met het verzoek om een betaling van €45.000 uit te voeren. Alles klopt: de toon, de timing en verwijzingen naar lopende projecten. Pas dagen later blijkt dat de directeur het bericht nooit heeft verstuurd. Aanvallers hebben zich eerder toegang verschaft tot de mailbox en kunnen zo meelezen met interne communicatie. Het geld is naar het buitenland weggesluisd.

Nederlandse bedrijven hard getroffen

BEC-fraude treft bedrijven van alle groottes. Hieronder enkele recente voorbeelden[1] uit Nederland:

Bedrijf	Schade	Methode
Pathé Nederland	€ 19,2 miljoen	CEO-fraude via e-mail
Jewometaal Rotterdam	€ 11,4 miljoen	CEO-fraude telefoon + e-mail
Rijksmuseum Twenthe	€ 2,85 miljoen	Factuurfraude via onderschepte e-mails
Financieel dienstverlener	€ 1,5 miljoen	Wijziging rekeningnummer

1 Eye Security waarschuwt: Toename van BEC-incidenten in 2024 drijft verzekeringskosten op.



Hoe werkt een BEC-aanval?

BEC-aanvallen volgen meestal een vast patroon. Door te begrijpen hoe criminelen te werk gaan, kun je je beter wapenen. Een typische aanval verloopt in vijf fasen:

Fase 1: Verkenning en informatieverzameling

Criminelen beginnen met het verzamelen van informatie over jouw organisatie. Ze zoeken op:

- **LinkedIn**: Wie zijn de beslissers? Wie werkt op de financiële afdeling?
- **Bedrijfswebsite**: Lopende projecten, klanten, leveranciers
- **Persberichten**: Overnames, partnerships, expansieplannen
- **Datalekken**: E-mailadressen en wachtwoorden van medewerkers

Deze fase kan weken tot maanden duren. Criminelen investeren tijd om geloofwaardig over te komen.

Fase 2: Toegang verkrijgen

Nu proberen criminelen toegang te krijgen tot jouw systemen:

- **Phishing-mail** met een nep-inlogpagina voor bijvoorbeeld Microsoft 365 of andere systemen
- **Omzeilen MFA** waardoor multifactorauthenticatie onvoldoende bescherming biedt
- **Gestolen inloggegevens** gekocht op het darkweb (vaak hergebruikte wachtwoorden)
- **Malware** via valse facturen of documenten in e-mailbijlagen.

Eenmaal binnen kunnen ze meelezen met e-mailverkeer en interne communicatie observeren.

Fase 3: Observeren en leren

Met toegang tot een mailbox gaan criminelen **geduldig observeren**:

- Hoe communiceren leidinggevenden intern?
- Welke projecten lopen er? Met welke leveranciers?
- Wie heeft bevoegdheid om betalingen goed te keuren?
- Wat zijn de interne procedures en gewoontes?
- Welke grote facturen worden binnenkort verstuurd?

In een gedocumenteerd geval observeerden criminelen 72 dagen lang voordat ze toesloegen. Ze kenden alle details van lopende transacties.

Fase 4: De aanval

Op het perfecte moment slaan ze toe. Dit kan zijn:
- **CEO-fraude**: Een urgent verzoek van de 'directeur' voor een vertrouwelijke betaling
- **Factuurfraude**: Een 'correctie' op een lopende factuur met nieuw rekeningnummer
- **Leveranciersfraude**: Een melding dat bankgegevens zijn gewijzigd

De timing is cruciaal: vaak vlak voor een vakantie, tijdens een drukke periode, of als een beslisser afwezig is.

Fase 5: Geld wegsluizen

Zodra het geld is overgemaakt, werken criminelen razendsnel:
- Het geld wordt via verschillende rekeningen verspreid
- Vaak via meerdere landen om de sporen uit te wissen
- Binnen enkele uren kan het geld onvindbaar zijn
- Uiteindelijk wordt het omgezet in cryptovaluta of contant geld

De verstrekkende gevolgen van een geslaagde BEC-aanval

Tijd is van cruciaal belang: Hoe sneller je een frauduleuze betaling ontdekt en jouw bank waarschuwt, hoe groter de kans op herstel.

Een succesvolle BEC-aanval is meer dan een financiële tegenslag, het kan het voortbestaan van je bedrijf bedreigen. De impact reikt veel verder dan het overgeschreven bedrag en treft organisaties op meerdere vlakken tegelijk.

In november 2018 hacken criminelen de e-mailadressen van zowel de Italiaanse CEO als een medewerker op de financiële administratie in Nederland van elektronicafabrikant Elco (Helmond/Aarle-Rixtel). Met vervalste maar nauwelijks van echt te onderscheiden e-mailadressen sturen ze namens de CEO betalingsopdrachten. € 223.000 verdwijnt naar China, € 548.760 naar Roemenië. In totaal wordt € 771.760 overgemaakt. Voor Elco, al jaren bezig met een reorganisatie, is dit verlies de genadeslag. Het Italiaanse moederbedrijf vraagt faillissement aan. Elco Netherlands gaat failliet[2], het familiebedrijf verdwijnt door één geslaagde aanval.

> *Het was een flinke hap uit de broek.*
> *De fraude greep fors in op de liquiditeitspositie.*
>
> *Curator Geurt te Biesebeek*

2 Elektronicafabrikant Elco failliet door CEO Fraude/Nieuws CEO Fraude/CEO fraude/Cybercrime/Menu Onderwijs & Ontwikkeling | Cybercrimeinfo.nl

Naast het directe financiële verlies stapelen de kosten zich bij een aanval op:

Forensisch onderzoek en juridische kosten
Je moet uitzoeken hoe de aanval precies is verlopen, welke systemen zijn gecompromitteerd en welke data zijn ingezien. IT-forensisch onderzoek kost al snel € 10.000 – € 50.000. Juridische advisering over aansprakelijkheid, contractbreuk en AVG-meldingen voegt daar nog eens € 5.000 – € 25.000 aan toe.

Productiviteitsverlies
Het IT-team, de financiële afdeling en de directie besteden weken aan de nasleep in plaats van hun eigenlijke werk. Bij een mkb met 50 medewerkers betekent dit al snel honderden uren verloren productiviteit; omgerekend tienduizenden euro's.

Terwijl je met de nasleep bezig bent, loopt de normale bedrijfsvoering vertraging op. Offertes blijven liggen, projecten lopen vast, klanten worden niet op tijd bediend. Voor mkb'ers die afhankelijk zijn van persoonlijke relaties en snelle levering kan deze verstoring klanten permanent doen vertrekken.

Systeemherstel en beveiligingsupgrades
Gecompromitteerde accounts moeten worden opgeschoond, beveiligingsmaatregelen aangescherpt, systemen geüpgraded. Budgetten: € 15.000 – € 100.000 afhankelijk van de ernst.

Contractbreuk en aansprakelijkheid
Als klantgegevens zijn gecompromitteerd, kunnen klanten jou aansprakelijk stellen voor schade. Dit leidt tot juridische procedures, schikkingen en mogelijk zelfs tot schadeclaims.

Verzekeringsproblemen
Veel cyberverzekeringen dekken BEC-aanvallen niet of slechts gedeeltelijk, zeker als basismaatregelen zoals multifactorauthenticatie (MFA) ontbraken. Na een incident stijgen de premies fors of wordt dekking geweigerd.

Naast het financiële verlies en de kosten, kan er ook sprake zijn van reputatieschade en een impact op de organisatie.

Klanten trekken zich terug
Een softwarebedrijf dat slachtoffer werd van BEC verloor drie grote klanten binnen twee maanden na het incident. De klanten twijfelden aan de beveiliging van hun gegevens: "Als jullie je eigen mailboxen niet kunnen beveiligen, hoe staat het dan met onze data?"

Leveranciers eisen vooruitbetaling
Leveranciers die horen van de fraude stellen strengere betalingsvoorwaarden. Het bedrijf moet plots vooruitbetalen of een bankgarantie stellen, wat cashflow verder onder druk zet.

Moeilijker nieuwe klanten werven
In sectoren waar compliance en beveiliging cruciaal zijn (zorg, financiële dienstverlening, overheidsopdrachten) kan een datalek of fraudegeschiedenis het binnenhalen van nieuwe opdrachten jaren blijven bemoeilijken

De betrokken medewerker
De financieel medewerker die het geld overschreef, wordt overweldigd door schuldgevoelens. "Ik heb het bedrijf deze schade bezorgd. Ik had het moeten zien." Stress, slapeloosheid, burn-out symptomen. In sommige gevallen leidt dit tot langdurig ziekteverzuim of zelfs ontslag waarbij de medewerker zelf het slachtoffer is van professionele criminelen.

Het hele team
Het moreel daalt. Collega's vragen zich af: "Hadden wij het kunnen voorkomen? Kunnen we onze leidinggevenden nog wel vertrouwen?" Het onderlinge vertrouwen, essentieel in kleinere organisaties, krijgt een deuk.

De directie
Naast het financiële verlies komen persoonlijke gevoelens van falen, schaamte en boosheid. Bij Pathé Nederland kostte het incident beide directeuren hun baan. Ook bij LEONI AG werd de directeur ontslagen na een verlies van € 40 miljoen.

De nieuwe dreiging: AI maakt BEC gevaarlijker

De spelregels zijn veranderd. Tot voor kort kon je een fraudepoging vaak herkennen aan slechte taal, vreemde zinnen of opvallende spelfouten. Die tijd is voorbij. Kunstmatige intelligentie (AI) heeft criminelen een wapen gegeven waarmee zij in enkele seconden perfect Nederlands schrijven, je stem kunnen nabootsen en zelfs videogesprekken met de directeur kunnen simuleren.

Criminelen gebruiken AI om honderden e-mails te genereren die elk specifiek zijn afgestemd op de ontvanger. De e-mail naar de financiële administratie verwijst naar een echte leverancier, gebruikt jouw interne terminologie en sluit aan bij lopende projecten, allemaal geautomatiseerd verzameld uit publieke bronnen, social media en eerdere datalekken.

Naast perfect Nederlands wordt AI ook ingezet om berichten zo gericht mogelijk op te stellen. Hierbij wordt openbare informatie over jouw bedrijf en over de ontvanger gebruikt als input voor AI. Voorheen was dit handmatig werk dat veel tijd kostte. Tegenwoordig is een BEC aanval sneller en geautomatiseerd uit te voeren.

Generatieve AI is een technologie die realistische en overtuigende content kan creëren, zoals afbeeldingen, video's, audio of tekst, op basis van een simpele opdracht of data-invoer (prompt). Waar deze technologie bedoeld is om werk te verlichten en creativiteit te stimuleren, misbruiken criminelen dezelfde tools voor steeds overtuigender aanvallen.

Vier manieren waarop criminelen AI inzetten

1. Perfecte phishing-mails in elke taal
ChatGPT en vergelijkbare AI-tools kunnen in seconden overtuigende e-mails schrijven die:

- Geen spel- of grammaticafouten bevatten
- De schrijfstijl van jouw directeur perfect imiteren
- Natuurlijk en professioneel overkomen
- Zijn aangepast aan de Nederlandse zakelijke cultuur
- Specifiek gericht zijn op de ontvanger

Uit onderzoek[3] [4] [5] blijkt dat **40% van alle BEC-phishingmails nu AI-gegenereerd is**. Na de introductie van ChatGPT steeg het aantal social engineering-aanvallen met **135%.**

2. Voice deepfakes: De stem van jouw CEO
Met slechts enkele seconden geluidsmateriaal (bijvoorbeeld van een bedrijfsvideo op YouTube) kunnen criminelen de stem van de directeur namaken. Het klinkt identiek en kan live worden gebruikt tijdens een telefoongesprek.

Een voorbeeld uit de praktijk:
Een medewerker van Jewometaal Rotterdam werd telefonisch benaderd door wat leek de Duitse CEO. Elf betalingen werden uitgevoerd voor totaal € 11,4 miljoen. Pas bij dreiging met ontslag was er twijfel ontstaan.

3 www.hipaajournal.com/bec-increase-20pc-ai-40pc
4 www.darktrace.com/news/darktrace-email-defends-organizations-against-evolving-cyber-threat-landscape
5 SlashNext-The-State-of-Phishing-Report-2023.pdf

3. Video deepfakes: Videogesprekken met jouw CFO
De meest geavanceerde vorm: criminelen kunnen nu live videogesprekken voeren waarbij je jouw leidinggevende ziet en hoort.

Recente cases
Hong Kong (februari 2024): Een medewerker nam deel aan een videovergadering met wat leek de CFO en collega's. Iedereen was een deepfake. Schade: € 23,7 miljoen.

Nederland (2024): Bunq werd doelwit van deepfake CEO-fraude via video.
De aanval werd tijdig ontdekt door getrainde medewerkers.

4. Geautomatiseerde spear-phishing campagnes
AI kan automatisch duizenden gepersonaliseerde phishing-mails genereren door:
- LinkedIn-profielen te analyseren
- Recente bedrijfsnieuws te verwerken
- Voor elke ontvanger een unieke, relevante boodschap te creëren
- De perfecte timing te kiezen (na werkuren, tijdens vakanties).

Waar een crimineel vroeger één bedrijf per keer kon aanvallen, kan hij nu met AI **honderden bedrijven tegelijk benaderen** met op maat gemaakte berichten.

Hoe herken je AI-gegenereerde fraude?

AI maakt detectie lastiger, maar niet onmogelijk. Let op deze signalen:

Bij e-mail:
- **Te perfect**: Ongewoon formele taal terwijl jouw directeur normaal informeel communiceert
- **Generiek**: De boodschap zou naar iedereen kunnen zijn gestuurd
- **Timing**: E-mail verstuurd op ongebruikelijk tijdstip
- **Context**: De e-mail past niet bij lopende gesprekken of projecten.

Vooral de context is zeer belangrijk. Is het te verwachten dat een bepaalde handeling gevraagd wordt uit te voeren en specifiek nu?

Bij voice deepfakes:
- **Onnatuurlijke pauzes** of robotachtige intonatie
- **Ruis of haperingen** in het geluid
- **Vermijden van specifieke vragen** over recente gebeurtenissen
- **Druk om snel te handelen** zonder mogelijkheid tot terugbellen.

Bij video deepfakes:
- **Vreemde lipsynchronisatie** – mond beweegt niet perfect met geluid mee
- **Inconsistente belichting** op gezicht
- **Plotselinge beeldkwaliteit wijzigingen**
- **Onnatuurlijke (oog)bewegingen** of knipperen, afwijkingen in het uiterlijk
- **Slechte verbinding** als excuus voor beeldstoring.

Bescherming tegen AI-versterkte BEC

De komst van AI betekent dat jouw verdediging moet verschuiven van “herken de fout” naar “verifieer de legitimiteit”:

✗ Werkt niet meer	✓ Werkt wel
Vertrouwen op spelfouten	**Altijd terugbellen via bekend nummer**
Vertrouwen op taalgebruik	**Vier-ogen principe bij betalingen**
Alleen e-mailverificatie	**(Phishing resistente) Multifactorauthenticatie**
Vertrouwen op stemherkenning	**Vraag persoonlijke details die alleen zij weten**

Extra bescherming:

- **Afgesproken codewoord**: Spreek met jouw directie een geheim woord af dat bij urgente betaalverzoeken moet worden genoemd
- **Verificatievragen**: Stel vragen over recente gesprekken die alleen de echte persoon kan beantwoorden
- **Alternatief kanaal**: Bij twijfel over een (video)gesprek: neem via een ander kanaal contact op
- **Training en bewustwording**: Laat medewerkers voorbeelden van AI-deepfakes zien zodat ze weten wat mogelijk is
- **AI-detectietools**: Vraag je MSP naar tools die AI-gegenereerde content kunnen herkennen.

De boodschap is duidelijk: In het AI-tijdperk kun je niet meer vertrouwen op eerste gezicht of gehoor. Verificatie via onafhankelijke kanalen is essentieel.

Waarom BEC ook jouw bedrijf kan treffen

Veel mkb’ers denken: “Wij zijn te klein, criminelen hebben geen interesse in ons.” Niets is minder waar.

Onderzoek[6] toont aan dat **70% van het mkb** op wekelijkse basis te maken kan krijgen met BEC-pogingen. Juist kleinere bedrijven zijn aantrekkelijk voor criminelen omdat:

- **Kortere communicatielijnen** – Medewerkers kennen elkaar goed en vertrouwen elkaar sneller
- **Informele besluitvorming** – Minder strikte procedures voor goedkeuring van betalingen
- **Beperkte IT-beveiliging** – Vaak geen geavanceerde beveiligingssystemen
- **Drukke medewerkers** – Weinig tijd om verdachte signalen te checken.

De gemiddelde schade per BEC-incident bedraagt € 118.000[7]. Voor veel mkb’ers een existentiële bedreiging. Bovendien vergoedt de bank dit type fraude niet, omdat je zelf de betaling hebt goedgekeurd.

6 https://abnormal.ai/blog/bec-vec-attacks
7 www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Herken de signalen van BEC

De meeste BEC-pogingen vertonen herkenbare patronen. Door alert te blijven op deze signalen, kun je fraude voorkomen.

Rode vlaggen bij e-mail en telefoon

Urgentie en druk – “Dit moet vandaag nog”, “Ik zit in een vergadering, geen tijd om te bellen”

Verzoek tot geheimhouding – “Vertrouwelijk, deel dit met niemand”, “Dit is een gevoelige overname”

Ongebruikelijke verzoeken – Betalingen naar nieuwe rekeningen, wijziging betalingsgegevens

Afwijkend taalgebruik – Iets andere schrijfstijl dan normaal, ongebruikelijke begroeting

Verdacht e-mailadres – Kleine variaties: bedrijf-naam.nl i.p.v. bedrijfnaam.nl

Tijdens drukke periodes – Criminelen slaan toe bij vakanties, jaarafsluiting, drukke projecten

Vertrouw niet op het telefoonnummer – Criminelen kunnen het laten lijken dat ze vanaf een bekend nummer bellen (spoofing)

Deel 2: Praktische handvatten

Simpele tips die je vandaag nog kunt toepassen

Het goede nieuws: met eenvoudige maatregelen verklein je het risico aanzienlijk. Deze tips zijn praktisch toepasbaar, kosten weinig tijd en bieden direct bescherming.

Basismaatregel 1: Het vier-ogen principe

Laat betalingen altijd door minimaal twee personen goedkeuren. Dit voorkomt dat één medewerker onder druk schadelijke beslissingen kan nemen. Leg dit formeel vast in bedrijfsprocedures.

Basismaatregel 2: Verificatie via bekend nummer

Bij elk betaalverzoek of wijziging van rekeningnummers: bel ALTIJD terug naar een nummer uit jouw eigen administratie. Gebruik NOOIT het nummer uit het verdachte bericht. Een telefoontje van 30 seconden kan €50.000 schade voorkomen.

Basismaatregel 3: Vaste procedures voor wijzigingen

Spreek af dat bankgegevens van leveranciers alleen worden gewijzigd na telefonische bevestiging.
Maak dit onderdeel van jouw inkoopproces.

Verdere bescherming

- **Train jouw team** – Bespreek BEC in teamvergaderingen, deel voorbeelden
- **Creëer een meldcultuur** – Medewerkers moeten zich veilig voelen om twijfels te delen
- **Controleer rekeningnummers** – Vergelijk altijd met jouw eigen administratie
- **Wees extra alert bij urgentie** – Hoe groter de druk, hoe grondiger de controle
- **Gebruik sterke wachtwoorden** – En schakel multifactorauthenticatie in voor e-mail
- **Technische controle** – Meld het indien onverwachte inlogmeldingen via multifactoraleauthenticatie komen.

Stel deze vragen aan jouw IT-dienstverlener

Veel mkb'ers vertrouwen op een Managed Service Provider (MSP) voor hun IT-beveiliging. Dat is slim, maar het is belangrijk om gerichte vragen te stellen over BEC-bescherming:

1. **"Hoe bescherm jij ons tegen phishing en BEC-aanvallen?"**
   Vraag naar e-mailfilters, impersonatiebescherming en anti-spoofingmaatregelen.
2. **"Monitoren jullie verdachte inlogpogingen?"**
   Controleer of er melding komt bij ongebruikelijke inlogactiviteiten.
3. **"Is multifactorauthenticatie ingeschakeld voor alle accounts?"**
   Dit maakt het veel moeilijker voor criminelen om accounts over te nemen.
4. **"Hoe snel worden wij gewaarschuwd bij een incident?"**
   Bij BEC telt elke minuut. Vraag naar incidentmeldingsprocedures.
5. **"Kunnen jullie ons helpen met awareness training?"**
   Vraag of zij testmails kunnen versturen of trainingen kunnen verzorgen.

Directe actie (binnen 1 uur)

1. **Bel direct je bank** – Vraag om de betaling te stoppen of terug te halen
2. **Doe aangifte bij de politie** – Online via politie.nl of telefonisch 0900-8844
3. **Meld bij je IT-dienstverlener** – Laat mailboxen en de email server/Microsoft 365 controleren op inbraak en schakel een forensisch expert in.
4. **Wijzig wachtwoorden** – Van alle betrokken accounts
5. **Informeer ontvangers** – Indien criminelen e-mailberichten verzonden hebben uit jouw e-mailaccount

Meldplicht bij datalekken

Heeft een aanvaller toegang gekregen tot mailboxen of persoonsgegevens? Dan ben je **wettelijk verplicht dit binnen 72 uur te melden bij de Autoriteit Persoonsgegevens**. Deze meldplicht is er niet voor niets: jouw melding helpt andere organisaties te waarschuwen, patronen in cybercriminaliteit te herkennen en toekomstige slachtoffers te voorkomen. Door te melden draag je direct bij aan de digitale veiligheid van Nederland en bescherm je niet alleen jouw eigen organisatie, maar ook die van anderen.

Wanneer er sprake is geweest van ongeautoriseerde toegang tot mailboxen of persoonsgegevens dat mogelijk heeft geleid tot data-exfiltratie en/of geldfraude:

- Beoordeel of een melding bij de Autoriteit Persoonsgegevens verplicht is.
- Meld het incident wanneer dat vereist is volgens de wetgeving.

Snelle melding helpt om nieuwe aanvallen te herkennen en te stoppen. Melden draagt bij aan beter inzicht in digitale dreigingen in Nederland.

- Het NCSC komt daarom graag in contact met organisaties die misbruik hebben waargenomen. Daarnaast ontvangt het NCSC graag informatie over (pogingen tot) misbruik. Hiervoor neem je contact op met het NCSC via cert@ncsc.nl. Eventuele technische details zullen hierbij helpen.
- Organisaties die binnen de doelgroepen van het NCSC vallen, kunnen zich via samenwerken@ncsc.nl aanmelden om geautomatiseerde berichten te ontvangen over malware-infecties. Heb je dat al gedaan, dan adviseren we om regelmatig aangeleverde informatie over netwerkinfrastructuur (IP-adressen, ASnummers en domeinnamen) te updaten.

Wat doet de AP met een melding?
De Autoriteit Persoonsgegevens (AP) beoordeelt of jouw maatregelen passend zijn en of betrokkenen geïnformeerd moeten worden. Indien nodig kan de AP aanvullende maatregelen of communicatie met slachtoffers eisen.

Het informeren van slachtoffers helpt hen zich te beschermen tegen gevolgen van phishing, zoals identiteitsfraude en oplichting. Phishing verspreidt zich vaak verder via buitgemaakte mailadressen naar klanten of leveranciers, waardoor meer schade kan worden aangericht.

Wat zijn de meest gemaakte fouten die de AP ziet?

- Gevoelige persoonsgegevens (bijv. kopieën van ID-bewijzen) worden via e-mail verwerkt in plaats van via een veilige applicatie.
- Er wordt geen onderzoek gedaan naar de gehackte mailbox, waardoor het risico voor betrokkenen niet goed wordt ingeschat.
- Alleen ontvangers van een phishinglink worden geïnformeerd, terwijl ook andere personen van wie gegevens in de mailbox staan risico kunnen lopen.
- Onvoldoende beveiliging, zoals zwakke of hergebruikte wachtwoorden, geen MFA en het ontbreken van maatregelen zoals het opschonen van oude e-mails/contacten of het beperken van externe toegang (bijv. via VPN, IP-whitelisting of vertrouwde apparaten).

Technische maatregelen die uw MSP kan nemen

- SPF, DKIM en DMARC configureren (voorkomt e-mailspoofing)
- Impersonation protection inschakelen in Microsoft 365
- Legacy authentication uitschakelen
- Verdachte OAuth-apps monitoren en blokkeren
- E-mailbanners voor externe berichten
- Alleen inloggen vanaf bedrijfstoestellen of door het bedrijf beheerd (MDM).

In het technisch advies staan aanvullende maatregelen.

Leer en deel

Een BEC-incident is geen reden voor schaamte. Gebruik het als leerkans:

- Bespreek het incident met het team
- Evalueer welke procedures beter kunnen
- Deel je ervaring met branchegenoten (anoniem)
- Versterk je beveiligingsmaatregelen.
- Het NCSC biedt een aantal publicaties die je kunnen helpen: Incidentresponse en forensic readiness.

Tot slot: bewustzijn is de beste verdediging

BEC-fraude is een reële bedreiging voor elk bedrijf. De aanvallen worden steeds professioneler en door AI-technologie ook steeds overtuigender. Maar met de juiste bewustwording en simpele maatregelen ben je veel beter beschermd dan je denkt.

De kern van bescherming tegen BEC zit ‘m niet in technologie, maar in mensen (menselijk gedrag). Medewerkers die weten waar ze op moeten letten, procedures die een extra controle inbouwen en een cultuur waarin twijfelen mag en vragen stellen wordt aangemoedigd.

Belangrijke contactgegevens
Aangifte online fraude: www.politie.nl
Melden datalek: www.autoriteitpersoonsgegevens.nl
Melden fraude: www.fraudehelpdesk.nl

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