HODARI
PRIVACY COMPLIANCE SECURITY GOVERNANCE

Herkennen en voorkomen van business email compromise

M.T.A. (Marcel) Klaver en L. (Lodewijk) Benjaminse
juni 2020

OPENBAAR

Introductie

1

1. Inleiding
2. Herkennen en voorkomen
3. Bronvermelding

Inleiding
De ernst van de zaak

Business email compromise (BEC), ook wel CEO-fraude genoemd, is een vorm van *phishing* en komt helaas nog steeds regelmatig voor. *Phishing* en *ransomware* zijn met het toenemend gebruik van social media in opkomst en zullen naar verwachting de komende jaren sterk toenemen.[1] De kosten door *phishing* tussen 2013 en 2018 voor bedrijven worden geschat op USD 12,5 miljard wereldwijd. In Nederland is bij de Fraudehelpdesk van januari 2017 tot oktober 2019 voor EUR 4,5 miljoen aan schade als gevolg van CEO-fraude gemeld.[3]

Enkele voorbeelden op zowel internationaal als nationaal niveau van *phishing* en *business email compromise*:

- 6 januari 2015: Xoom Corporation maakt USD 30,8 miljoen over naar overzeese bankrekeningen[4];
- 10 november 2018: CEO-fraude kost Pathé EUR 19 miljoen[5];
- 30 augustus 2019: fraudeurs gebruiken AI en bootsen stem van Duitse CEO na om zo EUR 220.000 buit te maken[6];
- 4 december 2019: man in noord Nederland bijna EUR 1 miljoen kwijt via bankpas oplichting[7];
- 19 januari 2020: jeu-de-boules vereniging verliest EUR 78.000 na delen van bankgegevens van de club na nepmailtje[8];
- 30 maart 2020: COVID-19 oplichting, zoals het aanbieden van speciale ‘Corona antivirus software’, verkoop van mondkapjes of gratis Netflix accounts om de isolatie periode te doorbreken[9].

Interessante feiten:

- Het blijkt dat *phishing* het begin is van 78% van alle cyberaanvallen en 32% van alle datalekken.[10] Dit maakt duidelijk hoe belangrijk de menselijke factor is in het afslaan van aanvallen op de IT-infrastructuur, continuïteit van de dienstverlening en vertrouwelijkheid van kostbare data binnen organisaties.
- Om detectie tegen te gaan, bestaan *phishing* websites gemiddeld slechts 15 uur.
- Elke maand worden er ongeveer 400.000 *phishing* websites gemaakt.
- *Phishing* websites zijn veelal onderdeel van een onschuldige website, waarbij een subpagina gecompromitteerd is en vervangen door een malicieuze website om zo meer vertrouwen te scheppen.[11]

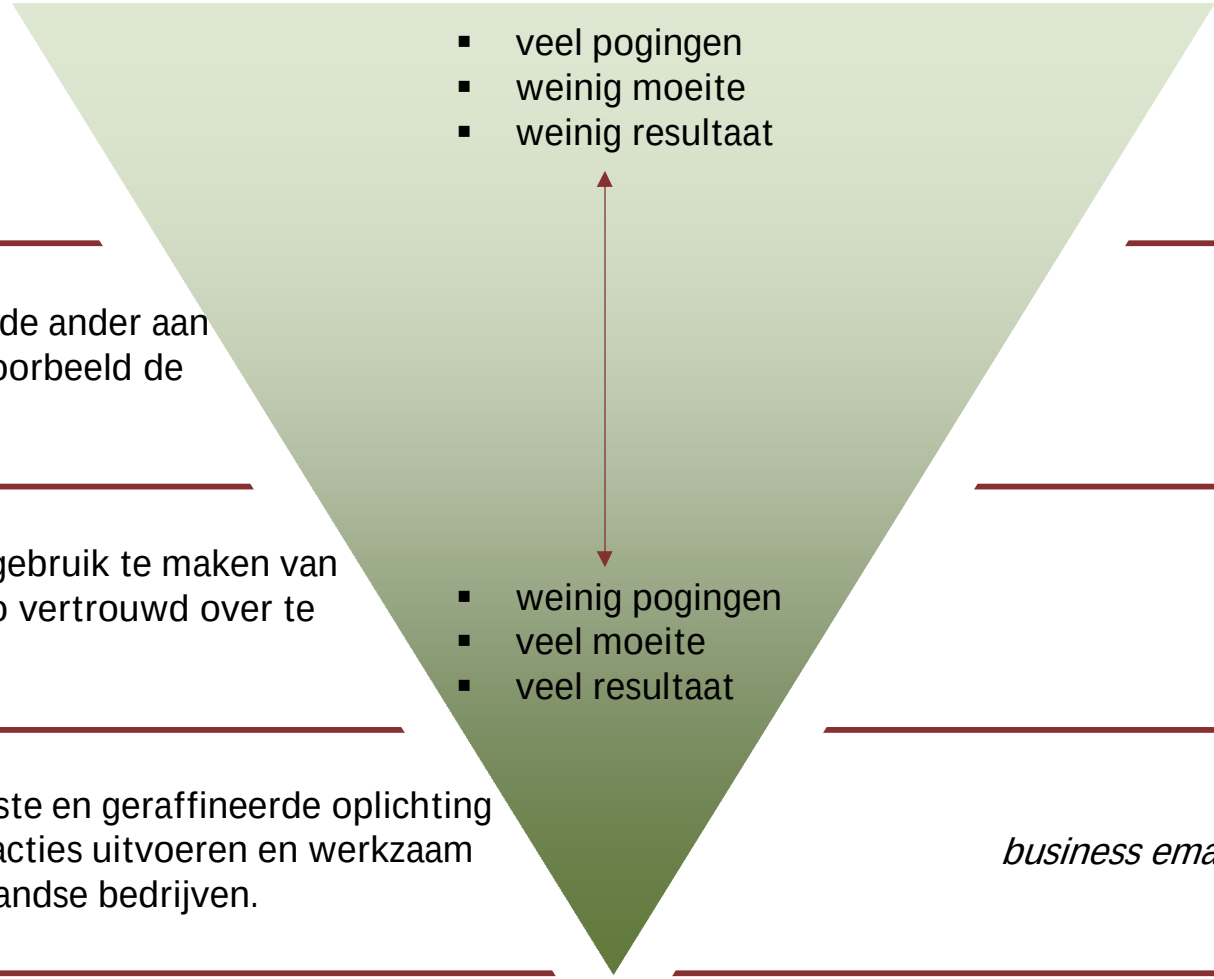
Inleiding
Begrippen

Spam (ofwel *sending people annoying messages*) is het ongevraagd sturen van commerciële en/of marketing mails.

Phishing is het versturen van ongewenste mails met als doel de ander aan te zetten tot het delen van gevoelige informatie of geld, bijvoorbeeld de ‘Nigeriaanse prins’ (ook wel voorschotfraude).

Spear phishing is het gericht sturen van *phishing* mails door gebruik te maken van bijvoorbeeld je naam, functie of persoonlijke gegevens om zo vertrouwd over te komen.

Business email compromise is gedefinieerd als een toegespitste en geraffineerde oplichting met als doelwit de individuen die regelmatig financiële transacties uitvoeren en werkzaam zijn bij (grote) organisaties die zaken doen met veelal buitenlandse bedrijven.



spam

phishing

spear phishing

business email compromise

Herkennen en voorkomen

2

1. Inleiding
2. Herkennen en voorkomen
3. Bronvermelding

Herkennen en voorkomen
Maatregelen tegen *phishing* en *business email compromise*

Wat kan er nu gedaan worden om *phishing* en *business email compromise* te voorkomen? Hier onder benoemen wij een aantal maatregelen die zijn gefocust op: *people*, *process* en *technique*.

- *people*:
  - herkennen van een *phishing* en *business email compromise* (awareness), zie slide 7 tot en met 9 voor toelichting.
- *process*:
  - zorg dat er een beveiligingsbewuste cultuur ontstaat in uw organisatie en dit top-down wordt gedragen;
  - stel duidelijke procedures vast voor het doen van grote betalingen en wijk daar niet van af, denk aan een vier-ogen-principe.
- *technique*:
  - voorkom *mail spoofing* door bijvoorbeeld *sender policy framework* (*SPF*) toe te passen en in verdere mate *domainkeys indentified mail* (*DKIM*) en *domain-based message authentication, reporting and conformance* (*DMARC*). *Spoofing* is het vervalsen van het adres van de afzender, waardoor het lijkt alsof de afzender te vertrouwen is. Bovenstaande technieken kunnen *spoofing* voorkomen;
  - *flags* toevoegen wanneer de 'sender' en 'return sender' niet hetzelfde zijn;
  - *spam* filters toepassen en up-to-date houden: *spam* dan wel markeren (zodat het opvalt bij de eindgebruiker) of geheel blokkeren (afhankelijk van privacy wetgeving in land);
  - functiescheiding logisch inrichten en technisch afdwingen.

- Er is een verband te zien tussen thuiswerken en succesvolle *phishing* pogingen. Het flexibele werken op welke locatie dan ook, hetzij thuis of op een publieke plek, kan invloed hebben op de vatbaarheid voor *phishing* en/of *business email compromise*.
- De wereld heeft op dit moment te maken met het COVID-19 virus en bijbehorende maatregelen, met als resultaat dat velen thuis werken. Naast de toegespitste *phishing* mails met betrekking tot het virus zelf (zie pagina 3), is het belangrijk dat de juiste processen om betalingen te doen te allen tijde worden toegepast bij het vele thuiswerken. Doordat collega's elkaar niet meer persoonlijk zien, is het moeilijker (ter controle) een collega te vragen mee te kijken, waardoor er mogelijk sneller met vertrouwen op een mail wordt gereageerd zonder de afzender te verifiëren.

Herkennen en voorkomen
Veilig gedrag is meer dan alleen bewustwording

Er vinden nog steeds veel succesvolle cyberaanvallen plaats door (onbewuste) fouten van interne medewerkers, ook al worden zij door middel van bewustwordingsprogramma's geïnformeerd over de risico's. Echte security awareness betekent een verandering in het gedrag van medewerkers en een aanpassing van de cultuur binnen een organisatie.[13]

Helaas betekent een veiligheidsbewuste cultuur nog niet dat elke medewerker ook veiligheidsbewust gedrag vertoont en initiatieven moeten verder reiken dan alleen het bewust maken van medewerkers.[15] MacInnis, Moorman en Jaworski[16] stellen dat gedrag bestaat uit motivatie, capaciteit en gelegenheid. Dit betekent het willen, kunnen en de kans krijgen om het gewenste gedrag te vertonen. Een voorbeeld: *business email compromise* komt nog steeds veel voor[17] , maar als medewerker wordt gevraagd of deze geld zal overmaken naar een onbekende rekening of het vier-ogen-principe niet zal toepassen, zal deze 'nee' antwoorden.

Gedrag wordt onder andere bepaald door de cultuur en het voorbeeld gedrag vanuit het management. De zes culturele dimensies van Hofstede geven inzicht in de cultuur van de organisatie en voorspellen factoren waardoor een organisatie kwetsbaarder is voor *business email compromise*. Deze zijn rechts weergegeven. Inzicht in de culturele dimensies van de eigen organisatie helpt bij het vinden van kwetsbaarheden, waarop specifieke maatregelen genomen kunnen worden.

Onderstaand overzicht geeft de zes culturele dimensies weer die Hofstede onderkent. Deze dimensies hebben invloed op de kans dat *business email compromise* slaagt.

Links staan de aspecten die de kans vergroten dat *business email compromise* slaagt in een organisatie. Rechts staan aspecten die de kans op succes verkleinen.

resultaatgericht	procesgericht
werkgericht	mensgericht
organisatie gebonden	professioneel
gesloten	open
losse controle	strakke controle
pragmatisch ingesteld	normatief ingesteld

Herkennen en voorkomen
Phishing mails

De ontwikkelingen met betrekking tot *phishing* en met name *business email compromise* staan niet stil. Criminelen passen steeds geavanceerdere technieken toe. Een gevaarlijke ontwikkeling is bijvoorbeeld *deepfake* ofwel het digitaal nabootsen van mensen in beeld of geluid. Er zijn voorbeelden van CEO-fraude bekend waarbij fraudeurs een nagemaakte stem inzetten, zoals het voorbeeld gegeven op de eerste slide bij een Britse energiemaatschappij. Hierbij kreeg de Britse CEO zogenaamd een telefoontje van de baas van het moederbedrijf in Duitsland met het verzoek met spoed geld over te maken naar een Hongaarse leverancier.[6] Maar ondanks deze geavanceerde technieken kun je *phishing* herkennen aan een aantal algemene kenmerken. Hieronder wordt op mail gefocust, maar ook voor andere varianten gelden een aantal van dezelfde kenmerken.

Herkennen van *phishing* mails[14]:

- vaak zijn de *phishing* mails slecht geschreven, let hierbij vooral op grammaticale fouten in plaats van spelling;
- de mail komt van een publiek domein (zoals gmail.com of hotmail.com), de afzender doet zich voor als iemand anders i.e. *spoofing*) of het domein is verkeerd gespeld (i.e. *typosquatting*);
- er zijn verdachte bijlagen of links toegevoegd aan de mail;
- de mail zet toe tot actie (dit kan het delen van informatie of het overmaken van geld zijn, dan wel het klikken op een link of downloaden van een bestand);
- er wordt een gevoel van urgentie en tijdsdruk gecreëerd (als je nu niet reageert is de kans verkeken, gaat de deal niet door of lukken de betalingen niet);
- de afzender is uit op geld of persoonlijke informatie zoals bankgegevens of wachtwoorden.

Phishing is niet beperkt tot het versturen van verdachte mails. Denk bijvoorbeeld ook aan:

- *smishing:* via sms;
- *vishing*: via telefoon/VoIP;
- *pharming:* DNS cache poisoning[12].

Herkennen en voorkomen
Herkennen van specifiek *business email compromise*

Business email compromise of CEO-fraude wordt minder vaak gestuurd dan bijvoorbeeld *spam*, omdat het aanzienlijk meer moeite voor de fraudeurs kost om deze te personaliseren. Het te behalen resultaat is wel vele malen groter. Doordat er meer tijd geïnvesteerd is in het legitimeren van dit type *phishing*, kan het nog lastiger zijn om ze te herkennen.

Herkennen:
- de nadruk bij *business email compromise* wordt vaak gelegd op de gezagsverhouding: het betaalverzoek wordt als een opdracht van een leidinggevende gegeven;
- de zogenaamde CEO benadrukt dat vertrouwelijkheid van groot belang is: de opdracht mag niet gedeeld worden met collega's;
- de medewerker wordt geprezen en belangrijk gemaakt: hij is uitgekozen om de opdracht uit te voeren vanwege zijn uitzonderlijke kwaliteiten;
- de druk wordt verhoogd: het slagen van een transactie wordt op de schouders van een bepaalde medewerker gelegd;
- de valse mails die deze nep-CEO's sturen zijn meestal ook te herkennen aan het gebruik van een vals mailadres: heel vaak lijkt deze wel van het domein van het bedrijf te komen, maar zijn één of meer tekens vervangen die erg op elkaar lijken (*typosquatting*), bijvoorbeeld de (kleine) letter l en de (hoofdletter) I;
- vaak wordt een gevoel van tijdsdruk gegeven: het geld moet snel worden overgemaakt.

Voorkomen:
- maak medewerkers attent op het bestaan van CEO-fraude;
- train medewerkers erop om niet te antwoorden op een mail (zeker wanneer het gevoelige informatie betreft), maar het mailadres te selecteren uit de contactenlijst van het bedrijf of de medewerker zelf;
- maak werknemers bewust van het feit dat een stem niet per se echt hoeft te zijn maar door criminelen kan zijn gemanipuleerd;
- laat werknemers na een telefonisch ontvangen verzoek een betaling te doen bellen met de veronderstelde leidinggevende via de intern bekende telefoonnummers;
- bekijk de website en profielen op social media van de organisatie en medewerkers kritisch; is het nodig de namen, functies en contactgegevens van medewerkers openbaar te maken?[3]

Bronvermelding

3

1. Inleiding
2. Herkennen en voorkomen
3. Bronvermelding

Bronvermelding

1. "*Komende tijd forse groei verwacht van phishing en ransomware*", A. Huiskes, 19 januari 2020, https://www.customertalk.nl/artikelen/onderzoek/komende-tijd-forse-groei-verwacht-van-phishing-en-ransomware
2. "*I-050417-PSA: Business E-mail Compromise*", FBI, 4 mei 2017, https://www.ic3.gov/media/2017/170504.aspx#fn3
3. "*Campagne CEO-fraude*", Fraudehelpdesk, 15 oktober 2019, https://www.fraudehelpdesk.nl/campagnes/campagne-ceo-fraude
4. "*Xoom says $30.8 mln transferred fraudulently to overseas accounts*", Reuters, 6 jan 2015, https://www.cnbc.com/2015/01/06/xoom-says-308-mln-transferred-fraudulently-to-overseas-accounts.html
5. "*Ceo-fraude kostte Pathé 19 miljoen euro*", M. van Ast, 10 november 2018, https://www.parool.nl/nieuws/ceo-fraude-kostte-pathe-19-miljoen-euro~b8ae182c
6. "*Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*", C. Stupp, 30 augustus 2019, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
7. "*Enorme phishingzaak slachtoffer bijna miljoen euro kwijtgeraakt*", RTV Noord, 4 december 2019, https://nos.nl/artikel/2313241-enorme-phishingzaak-slachtoffer-bijna-miljoen-euro-kwijtgeraakt
8. "*78.000 euro weg na phishing, bankrekening Rijswijkse jeu-de-boulesclub leeggetrokken*", Omroep West, 19 januari 2020, https://www.omroepwest.nl/nieuws/3988107/78-000-euro-weg-na-phishing-bankrekening-Rijswijkse-jeu-de-boulesclub-leeggetrokken
9. "*COVID-19 Scam Roundup – March 30, 2020*", D. Bisson, 30 maart 2020, https://www.tripwire.com/state-of-security/security-awareness/covid-19-scam-roundup-week-of-3-23-20
10. "*2019 Data Breach Investigations Report*", Verizon, januari 2020, https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
11. "*4 eye opening facts about phishing*", M. Samarati, 24 juni 2019, https://www.itgovernance.co.uk/blog/4-eye-opening-facts-about-phishing
12. "*6 Common Phishing Attacks and How to Protect Against Them*", D. Bisson, 7 oktober 2019, https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them

Bronvermelding

13. "*A Primer on Risk and Security Awareness*", L. Spitzner, 27 januari 2016, https://www.sans.org/security-awareness-training/blog/primer-risk-and-security-awareness
14. "*5 ways to detect a phishing email*", L. Irwin, 6 juni 2019, https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email
15. "*Een psychologische benadering van awareness in cybersecurity: Medewerkers geven hun wachtwoord niet weg via de telefoon, toch?*", 2019, I.M. Wetzer en E. Weijkamp, InformatieBeveiliging
16. "*Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads*", D.J. MacInnis, C. Moorman en B.J. Jaworski, 1991, Journal of Marketing
17. "*Psychologie over CEO-fraude: En waarom awareness niet voldoende is*", I.M. Wetzer en E. Weijkamp, 2020, InformatieBeveiliging

HODARI draagt bij aan betere informatiebeveiliging en privacy. Wij helpen organisaties aantoonbaar grip te krijgen op informatiebeveiliging en privacy door vraagstukken op het gebied van governance, risk en compliance op te lossen.

Wij bieden kwalitatief hoogwaardige oplossingen waarbij de meest complexe vraagstukken tot in detail zijn opgelost. Wij hebben ruime ervaring opgedaan binnen verschillende sectoren, zoals de financiële sector, energiesector, retail, (rijks)overheid, advocatuur en IT-dienstverleners. Regelmatig handelen wij binnen projecten naar aanleiding van fusies en overnames, reorganisaties, bevindingen van accountants of opmerkingen van toezichthouders.

HODARI B.V.

071-2032385
hodari.nl

L. (Lodewijk) Benjaminse
lodewijk.benjaminse@hodari.nl