Whitepaper

PHISHING

Inleiding

Phishing-aanvallen blijven een reële bedreiging voor bedrijven van elke omvang. Ondanks voorlichtingsinspanningen en beveiligingsmaatregelen kunnen medewerkers nog steeds het slachtoffer worden van deze misleidende praktijken. Het doel van deze whitepaper is om bedrijven te voorzien van richtlijnen voor het omgaan met het scenario waarin een medewerker zijn inloggegevens heeft verstrekt via een phishing-e-mail.

Wat te doen:

1. **Melding aan de IT-afdeling:** Als een medewerker vermoedt dat hij zijn inloggegevens heeft ingevuld op een phishing-website, moet hij onmiddellijk handelen. De medewerker moet de IT-afdeling onmiddellijk op de hoogte stellen van de situatie. IT kan verdere stappen ondernemen om de impact te beoordelen en eventuele beveiligingsmaatregelen te implementeren.

2. **Onmiddelijke actie:** Dit omvat het veranderen van zijn wachtwoord voor alle getroffen accounts en het resetten van de sessies. Andere accounts waar dit wachtwoord gebruikt wordt dienen ook te worden aangepast naar unieke wachtwoorden

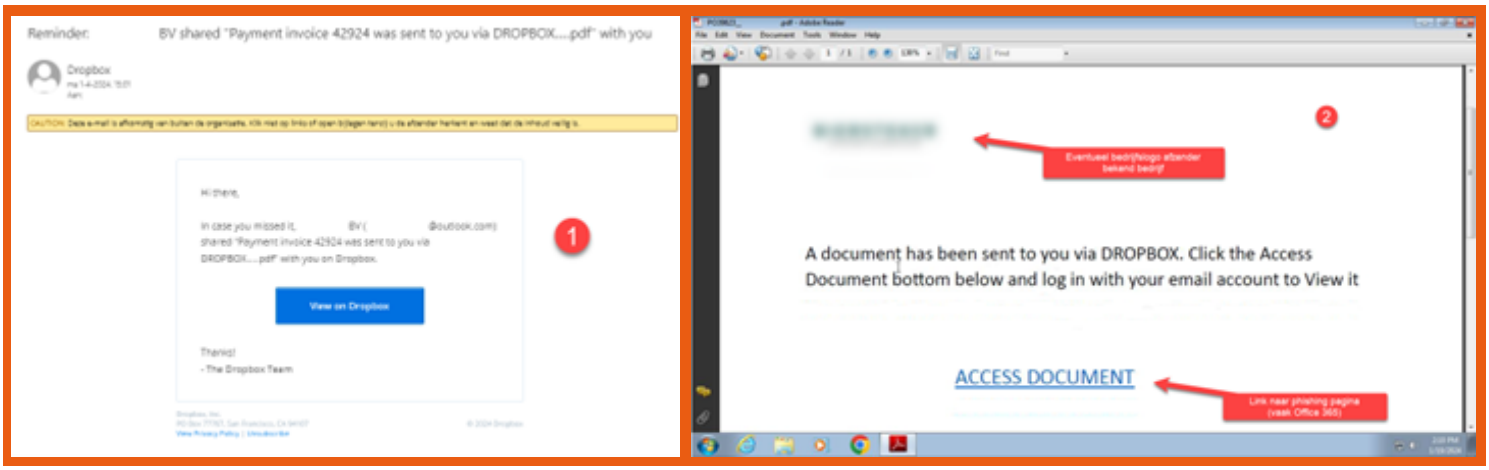
3. **Monitoring van accounts:** IT moet de getroffen accounts nauwlettend in de gaten houden op verdachte activiteiten. Dit kan onder meer ongebruikelijke inlogpogingen, ongeautoriseerde wijzigingen of verdachte e-mails omvatten

Waar op te letten

1. **Phishing-e-mailkenmerken:** Wijs medewerkers op de typische kenmerken van phishing-e-mails, zoals verdachte afzenderadressen, spelfouten, onlogische verzoeken en dreigingen

2. **Vergelijking van webadressen:** Moedig medewerkers aan om altijd de URL van de website te controleren voordat ze inloggegevens invoeren. Legitieme websites moeten een beveiligd HTTPS-protocol gebruiken en het juiste domein van het bedrijf weergeven

3. **Multifactor authenticatie:** Akkoordeer niet zomaar MFA-meldingen. Alleen als je zelf aanmeldt en de MFA-melding afkomstig is vanuit jouw locatie.



Gevolgen:

1. **Risico op gegevensdiefstal:** Het verstrekken van inloggegevens via phishing-e-mails kan leiden tot gegevensdiefstal, wat kan resulteren in financiële verliezen, reputatieschade en juridische gevolgen voor het bedrijf.

2. **Verlies van vertrouwen:** Het verlies van vertrouwen van klanten en zakelijke partners kan aanzienlijke langetermijneffecten hebben op het bedrijf, wat moeilijk te herstellen kan zijn.

Conclusie

Het is van cruciaal belang voor bedrijven om medewerkers bewust te maken van de gevaren van phishing-aanvallen en hen te voorzien van de juiste training en procedures om adequaat te reageren op verdachte e-mails. Door proactief te handelen en samen te werken met de IT-afdeling kunnen bedrijven de impact van phishing-aanvallen minimaliseren en de algehele beveiliging van hun systemen versterken. VTM Groep staat klaar om medewerkers te ondersteunen en de beveiliging van onze systemen voortdurend te verbeteren.

Vragen?

heb je na het lezen van deze whitepaper nog vragen over Phishing?

Twijfel dan niet en neem vrijblijvend contact op met jouw accountmanager of onze Security specialist Dolf Winterink. De gegevens zijn hieronder terug te vinden.

Dolf Winterink

Dolf.winterink@vtmgroep.nl

VTM Groep

Klantportal portal.vtmgroep.nl
Telefoon 0174 - 527 320
Adres Honderdland 190, 2676 LT Maasdijk
E-mail info@vtmgroep.nl