AUDIT
VLAANDEREN

BESCHRIJVING VAN DE PHISHING-TEST 2017 GEORGANISEERD DOOR AUDIT VLAANDEREN

Dit document beschrijft het verloop en de aanpak van de phishing-test die Audit Vlaanderen in 2017 organiseerde voor gemeenten, OCMW's en provincies. Een weergave van de overkoepelende resultaten van deze phishing-test is te vinden in een afzonderlijk document. De deelnemende lokale besturen ontvingen daarnaast elk ook een individueel rapport met de (geanonimiseerde) resultaten op het niveau van het bestuur. Alle overkoepelende resultaten kunnen ook worden geconsulteerd op de website www.auditvlaanderen.be.

Wat is een phishing-test en wat is het doel?

Phishing is een vorm van computercriminaliteit waarbij oplichters nietsvermoedende personen proberen te misleiden via een phishing-mail. Met zo'n phishing-mail proberen computercriminelen op listige wijze aan persoonlijke informatie of bankgegevens te komen of de computers van hun doelwit te besmetten met kwaadaardige software (zoals een virus, ransomware, keylogger).

Een phishing-test simuleert deze vorm van internetfraude op een veilige manier om te testen hoe gebruikers omgaan met verdachte e-mail. De resultaten van een phishing-test kunnen een organisatie helpen om het bewustzijn hieromtrent nog te verhogen en een aanleiding zijn om de kwetsbaarheid inzake informatiebeveiliging te evalueren.

VERLOOP VAN DE PHISHING-TEST

Audit Vlaanderen voert in 2017 een thema-audit informatiebeveiliging uit bij de lokale besturen. Meer info hierover kan u vinden op de website www.auditvlaanderen.be . Het globale rapport met overkoepelende resultaten wordt in de eerste helft van 2018 verwacht.

In de marge van deze thema-audit konden alle gemeenten, OCMW's en provincies inschrijven voor een vrijwillige en kosteloze phishing-test. Alle provincies, 72 % van de gemeenten en 64 % van de OCMW's in Vlaanderen schreven zich hier ook effectief voor in.

Eind 2016 werd het aanbod van de door Audit Vlaanderen georganiseerde phishing-test kenbaar gemaakt via diverse kanalen. In januari 2017 konden de geïnteresseerde besturen via de secretaris/griffier hun inschrijving regelen.

In de loop van februari 2017 werden de e-mailadressen van de deelnemende besturen verzameld via een beveiligde methode. Audit Vlaanderen schoonde de bezorgde informatie op, waarbij alleen de persoonlijke e-mailadressen werden weerhouden. Ook bij de verdere technische verwerking werden o.a. dubbel opgegeven adressen uit de verzendlijst gehaald.
Het spreekt voor zich dat de verzamelde gegevens voor geen andere doeleinden werden en worden gebruikt en na afloop van de test en rapportage zullen worden vernietigd.

In de periode maart-april 2017 werden uiteindelijk drie phishing-mails uitgestuurd naar de ingeschreven e-mailadressen (zie hieronder). Voor de technische uitvoering hiervan liet Audit

Vlaanderen zich ondersteunen via het perceel IT-audit van het raamcontract Audit Vlaanderen 2015-02.

Audit Vlaanderen koos er voor om drie “scenario’s” te testen:

- Phishing-mail 1 was een zeer goed verzorgde e-mail;
- Phishing-mail 2 was een e-mail die makkelijk herkenbaar was als verdacht aanbod;
- Phishing-mail 3 wees op het feit dat adequate maatregelen tegen malafide e-mails soms moeilijk combineerbaar zijn met de noodzaak om te communiceren.

De keuze van deze scenario’s gebeurde volledig autonoom door Audit Vlaanderen. In de mate dat werd gealludeerd op bestaande organisaties, werd kort voor de verspreiding van de betrokken mail contact opgenomen met deze organisaties teneinde afspraken te maken over de omgang met eventuele reacties.

De drie phishing-mails zijn enkel gestuurd naar de e-mailadressen die de ingeschreven besturen zelf aan Audit Vlaanderen bezorgden ten behoeve van deze phishing-test. voor deze test bezorgde e-mailadressen. Deze mails werden bewust uitgestuurd om na te gaan hoeveel personen potentieel onveilige handelingen zouden stellen. Doordat de bewuste mails en de betrokken websites geen malafide code bevatten, was deze test volstrekt onschadelijk.

De eerste phishing-mail werd uitgestuurd in de week van 17 april. De tweede phishing-mail in de week van 24 april. Om technische redenen verliep de verzending telkens over meerdere dagen. Een derde phishing-mail die enkel gericht werd aan de secretarissen van de ingeschreven gemeenten en OCMW’s, werd uitgestuurd vanaf 26 april.

De uitgestuurde phishing-mails beoogden de reële kwetsbaarheid van de ingeschreven besturen te testen.
Dit leidde er toe dat bij verschillende besturen werd vastgesteld dat de aanwezige beheersmaatregelen deze besturen toelieten één of meerdere van de phishing-mails tegen te houden nog vóór dat deze in de mailboxen van de bestemmelingen belandden. Bij de besturen waar geen reactie werd geregistreerd op phishing-mail 1, werd deze phishing-mail een week later nogmaals naar de betrokken e-mailadressen gestuurd.
Aan besturen bij wie zowel voor mail 1 als voor mail 2 geen enkele reactie werd geregistreerd, kon geen zinvolle individuele rapportering worden bezorgd. Deze besturen kregen daarom aansluitend de mogelijkheid nog een bijkomende phishing-mail bewust door te laten naar de mailboxen van de individuele gebruikers teneinde naast de technische weerbaarheid ook het bewustzijn van hun medewerkers te kunnen meten.

Over de resultaten werd teruggekoppeld aan de respectievelijke secretaris/griffier via een overkoepelend rapport voor alle gemeenten en OCMW’s, via een overkoepelend rapport voor de provincies en via een individueel rapport voor elk deelnemend individueel lokaal bestuur. De overkoepelende rapporten werden actief openbaar gemaakt via o.a. de website van Audit Vlaanderen. Een overkoepelend resultaat wordt ook meegenomen in het globale rapport over de thema-audit informatiebeveiliging.

Hebt u nog vragen over onveilige mails en websites? Dan kunnen we u o.a. verwijzen naar de websites https://overheid.vlaanderen.be/nieuws/hou-het-veilig-op-het-internet en https://www.safeonweb.be/nl.

Hieronder vindt u nog een beschrijving van elk van de phishing-mails.

PHISHING-MAIL 1: SPORTIEF VLAANDEREN / SPORTIEF OP HET WERK

De eerste phishing-mail was een verzorgde e-mail die opriep om meer te bewegen op het werk en doorverwees naar een betrouwbaar ogende wedstrijd waar zogezegd een sporthorloge te winnen viel voor allen die hun gebruikersnaam en wachtwoord ingaven. De verdachte aard van deze actie kon o.a. worden gedetecteerd doordat "Sportief Vlaanderen" geen bestaande organisatie is, de hyperlink maskeerde waarheen die leidde en de website waarop gevraagd werd gebruikersgegevens in te geven niet beveiligd was (wel http:// en geen https://, in vele browsers ook getoond met een slotje met een streep door).

De gevaren die met deze mail werden getest waren:

- Door te klikken op een mogelijks malafide link kan de computer van de gebruiker worden besmet met kwaadaardige code (zoals malware / cryptoware / ransomware / keylogger / …).
- Door op een onbekende en onveilige website gebruikersgegevens in te geven, kunnen de mensen achter deze website uw gebruikersgegevens misbruiken om zich toegang te verschaffen tot uw gegevens (hetzij uw mail-account, hetzij de gegevens in de ICT-

omgeving van uw werkgever, hetzij uw facebook-account) of om in uw naam handelingen te stellen (bijvoorbeeld dure bestellingen te plaatsen).

Het mag duidelijk zijn dat niemand een horloge won.

Deze actie was geïnspireerd op een actueel initiatief van Sport Vlaanderen (voorheen Bloso). Ondanks het feit dat niemand kans maakt op het winnen van een horloge, blijft het belangrijk om voldoende te bewegen en te sporten, ook op het werk. Voor meer informatie hierover, surft u (veilig) naar de enige 'juiste' website: https://www.sport.vlaanderen/sportophetwerk . Maakt ook van uw bestuur een sportieve organisatie!

PHISHING-MAIL 2: SMARTPHONE PROMO WSG

De tweede phishing-mail was een slordig bericht dat een hyperlink bevatte naar een website met een ongeloofwaardig commercieel aanbod waar enkel kon op worden ingegaan mits een gebruikersnaam en wachtwoord werd opgegeven. De verdachte aard van deze actie kon op verschillende manieren worden gedetecteerd. Zo is "WSG" geen bestaande organisatie en oogden de e-mail en de website erg onbetrouwbaar en amateuristisch, zowel qua formuleringen als qua uitzicht.

De gevaren die met deze mail werden getest, waren gelijkaardig aan deze van phishing-mail 1.

Het mag duidelijk zijn dat niemand effectief tot aankoop kon overgaan.

PHISHING-MAIL 3: KLACHT AAN SECRETARIS

Als derde phishing-mail stuurde Audit Vlaanderen een klacht van een fictieve persoon ("Johan Debruykere") naar het e-mailadres van de secretaris. Deze e-mail werd verstuurd vanuit een gratis e-mailadres, bevatte geen adres of telefoonnummer maar drong wel aan op een snelle behandeling. Voor concrete details verwees het bericht naar een html-bestand dat in bijlage werd meegestuurd. Audit Vlaanderen gaf in die bijlage aan dat het niet om een klacht maar om een phishing-test ging. Met deze mail wilde Audit Vlaanderen er vooral op wijzen dat openbare besturen misschien wel maatregelen kunnen nemen tegen malafide e-mails maar dat soms communicatie toch moeilijk

of niet vermijdbaar is. Bij deze mail bestond het gevaar dat de bijlage kwaadaardige code bevatte of doorverwees naar een website met kwaadaardige code. In dit geval kon het risico wel worden beheerst door de html-bijlage te openen met een puur tekstprogramma waarbinnen eventuele code niet wordt uitgevoerd.