Hands on ICT
De phishingtest

Test de alertheid van je medewerkers

Powered by Hands on ICT

your365

www.handsonict.nl

De phishingtest

Test de alertheid van je medewerkers

Om de kennis en alertheid van je medewerkers te testen, kun je een phishingtest (ook wel phishingsimulatie genoemd) uitvoeren. Door middel van een phishingtest simuleer je een levensecht scenario waarbij je de kennis en alertheid van je medewerkers controleert aangaande IT-beveiliging en risico's die op de loer liggen.

Phishing is een aanvalstechniek die door kwaadwillende wordt gebruikt om gevoelige gegevens te ontfutselen aan een individu of organisatie. Een phishing simulatie geeft inzicht in hoeverre medewerkers phishingmails openen, doorklikken op links of zelfs inloggegevens verstrekken. Daarnaast is een phishing simulatie een perfect middel om bewustwording te creëren.

De risico's van een phishing-aanval

Phishing wordt uitgevoerd via meerdere kanalen zoals mobiel of social media waarbij e-mail de meest gebruikte tool is. Bij een phishingmail wordt vaak een bekend persoon als afzender geïmiteerd. Zo denkt de ontvanger (het slachtoffer) dat het bericht legitiem is. Denk hierbij aan berichtjes vanuit de baas of een bedrijf waar je zaken mee doet. Doordat de aanvallers vaak actuele onderwerpen gebruiken, zijn mensen sneller geneigd om op de linkjes te klikken. Bij het klikken op die link kan gevaarlijke ransomware of andere schadelijke software binnen je organisatie geïnstalleerd worden. Het risico is dus heel groot.

De zwakste schakel in IT-beveiliging

Binnen een organisatie zijn de medewerkers vaak de zwakste schakel. Een van de belangrijkste oorzaken van alle lekken en hacks is namelijk het menselijk handelen. Vaak is dit een gevolg van een gebrek aan kennis over online veiligheid bij medewerkers van een organisatie. Het onjuiste gedrag en de onwetendheid van medewerkers vergroot hiermee de kans op een beveiligingslek in je ICT-omgeving. Het kan als organisatie daarom van belang zijn om de kennis over online veiligheid bij medewerkers te testen. Dit kan door middel van een phishingtest.

Wat is een phishingtest

Een phishingtest is een simulatie, opgezet door ons als externe organisatie, om erachter te komen hoe weerbaar en bewust jouw medewerkers zijn bij dit soort cyberaanvallen. Bij deze test ontvangen alle medewerkers een email, precies zoals deze door hackers normaliter worden opgezet. Met een betrouwbaar ogende afzender en een link om op te klikken. Bijvoorbeeld een mail waarin gevraagd wordt om de inloggegevens te wijzigen van het Microsoft-account of van een andere dienst. Door op de link te klikken ontvangen de medewerkers een inlogscherm waar het username en wachtwoord kan worden ingevuld. Als een medewerker dit doet tijdens de test worden uiteraard de inloggegevens niet opgeslagen en komt de informatie niet bij kwaadwillende terecht.

Met onze monitoringstools kunnen wij exact zien welke medewerkers in deze mail zijn getrapt en wie naar aanleiding van het klikken op de link informatie heeft achtergelaten. Dit geeft een wereld aan inzichten over hoe bewust je medewerkers zijn voor dergelijke aanvallen. Met deze data kun je een security awareness training aanbieden aan de betreffende medewerkers.

Wat kom je te weten met een phishingtest

Met onze monitoringstools kunnen we heel veel data ophalen na het verzenden van de phishingtest. Hiermee kun je als onderneming actie ondernemen om je organisatie nog beter te beveiligen. Daarnaast kun je met de door ons geleverde rapporten je organisatie informeren over de test en de uitkomsten hierin delen om meer bewustwording rondom cybersecurity te benadrukken.

- Hoeveel % van je medewerkers klikken op de link?
- Wat is de incident respons, hoeveel collega's rapporteren de phishingmail bij je ICT-afdeling?
- Met welke systemen zoals browser of OS hebben mensen op de link geklikt?

De phishingtest in 4 stappen

We voeren de phishingtest uit in ongeveer een maand tijd. Hierbij maken we een verschil in configuratie, implementatie en rapportage. Elke stap hebben we hieronder verder uitgelegd.

STAP 1 - Intake & configuratie

De eerste stap die gezet moet worden is de intake met de ICT-verantwoordelijke van jullie organisatie. Hierin wordt besproken hoe de simulatie wordt opgezet. Details die besproken worden zijn onder andere:

- Vanuit welk domein moet de mailsimulatie verstuurd worden?
- Wat moet de boodschap van de e-mail zijn?
- Welk format/design gaan we gebruiken?
- Wanneer moeten de phishing e-mails verzonden worden?
- Naar welke users moet de phishingtest verstuurd worden?

Hiermee gaan onze IT Consultants aan de slag en zorgen dat de simulatie helemaal klaargezet wordt.

STAP 2 - Livegang simulatie

Bij het nabootsen van de spam mail is het belangrijk om de mailing vanuit een safe mailadres te sturen. Daarmee kun je de mail als veilige afzender toekennen. Dit alles om te zorgen dat de email niet in de spambox van de users belanden en het effect van de phishingtest zo groot mogelijk is. De vooraf geconfigureerde e-mails worden vervolgens gefaseerd naar de usergroep gestuurd. Als een email naar alle gebruikers tegelijk wordt gestuurd, worden gebruikers argwanend en zullen de resultaten worden beïnvloed. Hierna zullen de eerste resultaten worden geregistreerd.

STAP 3 - Rapportage & advies

Nadat de mails zijn verstuurd, kan gekeken worden naar de belangrijkste resultaten:

- Hoeveel en specifiek welke medewerkers op de link hebben geklikt?
- Hoeveel en specifiek welke medewerkers hun inloggegevens hebben achtergelaten?

Deze resultaten worden gedeeld door middel van een rapportage en vervolgens besproken met de ICT-verantwoordelijke van jullie organisatie.

STAP 4 - Security Awareness videotraining

De security awareness training is een zeer belangrijke aanvulling op deze simulatie. Waarom? Uit de test is gebleken welke users vatbaar zijn voor phishing en daardoor een actieve bedreiging vormen voor je IT-beveiliging. Het is zaak om hiermee aan de slag te gaan. Met de gekoppelde awareness videotraining kun je je medewerkers leren hoe ze security bedreigingen kunnen herkennen waardoor je medewerkers als een extra laag in je IT-security gaan fungeren.

De phishingtest en bijbehorende trainingen kunnen herhaaldelijk worden uitgevoerd. Zo weet je of de training effect heeft gehad of dat er een nieuw vervolg aan gegeven moet worden.

IT-security als topprioriteit

Het goed inrichten van je IT-security is vandaag belangrijker dan ooit. Met YourSecurity bieden wij een scala aan diensten en producten om ervoor te zorgen dat je altijd en overal veilig aan het werk bent en dat je waardevolle bedrijfsdata goed geborgd is. Met YourSecurity zorgen we voor continu inzicht in de kwaliteit van jouw IT-security en helpen we je met de juiste diensten en producten je ICT-omgeving waterdicht en gebruiksvriendelijk te houden. Vraag nu een offerte aan voor YourSecurity of vraag meer informatie aan.

Vraag offerte aan

Contactgegevens
Hands on ICT
Nesland 5a
1382 MZ Weesp
+31(0)88 - 181 1300

info@handsonict.nl
www.handsonict.nl

yoursecurity

Veiligheid boven alles

Iedere ICT-omgeving staat dag in dag uit bloot aan gevaren van buitenaf. Cybercriminelen bedenken steeds slimmere manieren om door digitale muren te breken. En vaak met succes. Dit kan grote impact hebben op jouw organisatie. Met YourSecurity zorgen we voor continu inzicht in de kwaliteit van jouw IT-security en helpen we je met de juiste diensten en producten je ICT-omgeving waterdicht en gebruiksvriendelijk te houden.

Meer informatie

www.handsonict.nl

Powered by Hands on ICT

your365