PRODUCTSHEET | AWARENESS

SMISHING

SPEEL IN OP DE LAATSTE DREIGINGEN VAN HACKERS

Schade voor organisaties door phishing stijgt ieder jaar, en is het afgelopen jaar zelfs verviervoudigd! De nieuwste variant die hackers gebruiken is het vissen naar informatie via sms. Smishing staat dan ook voor SMS phishing. Net zoals bij phishing krijgt de gebruiker een berichtje dat op een urgente manier vraagt om actie te ondernemen. Bij smishing wordt een tekstbericht verzonden naar de telefoon van de gebruiker, in plaats van naar het e-mailaccount. Het bericht vraagt de gebruiker doorgaans om onmiddellijk actie te ondernemen door een telefoonnummer te bellen of naar een bepaalde website te surfen. Het telefoontje wordt vaak beantwoord door een automatisch antwoordsysteem dat vraagt om persoonlijke informatie zoals wachtwoorden of creditcardinformatie te verstrekken.

WAAROM IS HET BELANGRIJK

Voor organisaties wordt er vaak een gerichte actie op touw gezet: een zogenaamde spearsmishing aanval. Op deze manier worden bedrijfsgegevens of informatie van personen buitgemaakt. Dit leidt tot enorme schade; niet alleen financieel, maar ook imagoschade en schade voor de feitelijke slachtoffers. Daarom is het belangrijk medewerkers bewust te maken van de bedreigingen van smishing, hoe hacker te werk gaan en ook de weerbaarheid van medewerkers te testen.

HOE LOSSEN WIJ DAT OP?

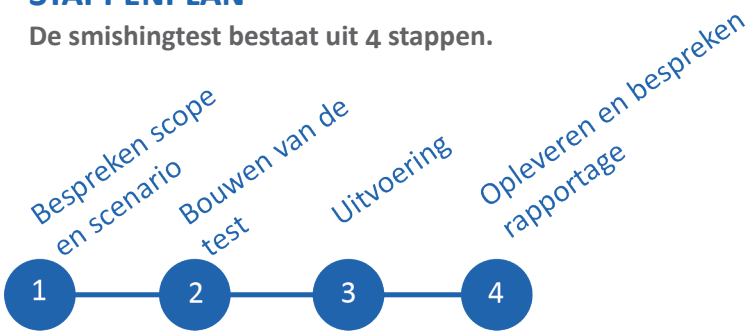
De smishingtest van Auditrail helpt op drie vlakken: ten eerste wordt door middel van een realistisch scenario objectief gemeten hoeveel medewerkers op de link in de sms klikken, en hoe veel medewerkers actie ondernemen naar aanleiding van het bericht. Ook nemen we een aantal technische zaken mee zoals operating systems en browserversies. Daarnaast testen we met deze smishing de incident response: hoe lang duurt het voor de sms gemeld wordt en wat zijn de acties van de IT-afdeling? Als derde is het aspect van bewustzijn enorm belangrijk. Daarom helpen wij om de uitkomsten van de test op een goede manier voor het voetlicht te krijgen bij organisaties.

VOORDELEN

- Simulatie van een reële dreiging;
- Ultieme test van weerbaarheid tegen smishing;
- Check op technische componenten;
- Test van incident response;
- Grote bijdrage aan awareness medewerkers;
- Gericht actieplan met verbetervoorstellen.

STAPPENPLAN

De smishingtest bestaat uit 4 stappen.



Auditrail
information security | privacy | quality | grc
Leiderdorp | Groningen

071 - 747 17 17
koffie@audittrail.nl
www.audittrail.nl