Social Engineering

Criminelen gebruiken vaak social engineering om toegang te krijgen tot systemen. Zij ‘hacken mensen’ om aan gevoelige informatie te komen. Als uw medewerkers zich hiervan bewust zijn, verkleint u de kans op ernstige cyber-incidenten. Wij kunnen helpen met phishingsimulaties en andere diesnten.

Deze Social Engineering Diensten geven u:

Inzicht in kwetsbaarheden

Deze diensten laten u zien hoe weerbaar uw medewerkers zijn tegen social engineering.

Bewuste medewerkers

Door uw medewerkers te laten ervaren hoe social engineers te werk gaan verhoogt u hun bewustzijn.

Een partner met expertise

Onze ethisch social engineers hebben ruime ervaring en gaan zorgvuldig te werk, bijvoorbeeld tijdens de debrief.

Waarom Social Engineering Diensten?

De technische beveiliging van systemen wordt steeds beter. Om toch toegang te krijgen tot uw netwerken en systemen, gebruiken cybercriminelen **social engineering**. Zij doen zich voor als iemand anders en manipuleren medewerkers om gevoelige gegevens af te staan. De bekendste vorm is e-mailphishing, maar socoial engineering kan ook via de telefoon of fysiek. Het is belangrijk dat uw medewerkers op de hoogte zijn van de werkwijze van dit soort criminelen.

Het eerste doel van deze Social Engineering Diensten is om te testen welke bedrijfsinformatie een kwaadwillende social engineer kan achterhalen. Daarvoor kunnen wij meerdere middelen inzetten, van fysieke of telefonische social engineering, tot een e-mailphishing-simulatie. Het tweede doel is om uw medewerkers bewust te maken van de risico’s van social engineering. Hogere awareness verkleint de kans op een ernstig security incident voor uw organisatie.

De Social Engineering Diensten die wij bieden:

E-mailphishing simulatie	Telefonische phishing	Phishing Specials (smishing etc)	Mystery Guest onderzoek

E-mailphishing simulatie

E-mailphishing is de meest gebruikte manier van cybercriminelen om de eerste toegang tot een netwerk te krijgen. Om uw medewerkers alert te maken op dit soort nepmails, voeren wij een e-mailphishing simulatie uit. Het doel van een phishingcampagne is altijd het positief beïnvloeden van bewustzijn, houding en handelen van medewerkers.

In nauw overleg met u zetten we een e-mailphishingcampagne op. Tijdens een afgesproken periode **versturen we gesimuleerde phishingmails** en meten we de respons van medewerkers: klikken mensen op de link in de e-mail? Melden zij de phishingmail bij het aangewezen meldpunt?

Na afloop van de campagne ontvangt u alle **metingen in een rapport**. Wij geven u concrete aanbevelingen, zodat u actie kunt ondernemen om uw weerbaarheid tegen e-mailphishing te vergroten.

Telefonische phishing (vishing)

Bij voice phishing, of 'vishing', doen criminelen zich aan de telefoon voor als bijvoorbeeld een IT-heldeskmedewerker om mensen gevoelige gegevens te ontfutselen. Tijdens een telefonisch phishingonderzoek bellen onze social engineers met een aantal van uw medewerkers, om te controleren hoe weerbaar uw organisatie is tegen dit soort aanvallen. U ontvangt geanonimiseerd videomateriaal van het onderzoek dat u kunt gebruiken om andere medewerkers te trainen. Dit is een effectieve leermethode.

Telefonische phishing in cijfers

1	In gemiddeld **x van de x gevallen** geven medewerkers via de telefoon hun inloggevens aan onze social engineers.
2	In 2023 belden onze social engineers met **zo'n xxx medewerkers** van uiteenlopende klanten. Ieder gesprek duurde **gemiddeld x minuten**.
3	Onze telefonische phishing opdrachten leiden tot een duidelijke toename in awareness. Gemiddeld steeg die **met x procent**.

Phishing Specials

Cybercriminelen gebruiken naast e-mailphishing en telefonische phishing ook andere vormen van misleiding, bijvoorbeeld phishing via SMS, of 'smishing.' U kunt onze social engineers inzetten voor de volgende tactieken om uw weerbaarheid te testen:

Bij **USB-phishing** laten aanvallers een USB-stick met malware erop achter, of geven deze weg. Als iemand de USB in een computer steekt, kan de aanvaller toegang krijgen.

Bij **SMS-phishing**, of smishing, sturen oplichters valse SMS- of chatberichten. Ze zetten mensen mensen onder druk met berichten die dringend lijken en vragen dan om op een link te klikken of persoonlijke gegevens te delen.

QR phishing, of quishing, maakt gebruik van QR-codes die na het scannen naar een schadelijke website leidt. Oplichters proberen mensen te misleiden om deze QR-code te scannen, met als doel persoonlijke informatie te stelen of malware te installeren.

Mystery Guest onderzoek

Tijdens een Mystery Guest onderzoek proberen onze ethische social engineers fysieke toegang te krijgen tot uw kantoren en panden. Op die manier proberen zij informatie te verzamelen die aanwezig is op bureaus en werkplekken, in documenten, archieven en op het interne bedrijfsnetwerk, via werkplekken, printers of netwerkaansluitingen.

De social engineers werken op basis van een uitgedacht scenario dat zij in overleg met u bepalen. Dit maakt het onderzoek **zo realistisch mogelijk**.

Met de uitkomsten van het onderzoek kunt u uw fysieke locaties **beter beschermen** tegen ongewenste bezoekers en uw medewerkers trainen.

Wat onze klanten zeggen

"Ik ga hier nooit meer intrappen"

"Eerlijk gezegd hadden wij niet verwacht dat onze medewerkers via de telefoon zoveel wachtwoorden aan de social engineers zouden geven. Wij krijgen terug van medewerkers: 'Ik ben wel geschrokken, maar wat goed dat jullie dit doen. Ik ga hier nooit meer intrappen.'"

Gerelateerde diensten

OSINT onderzoek

OSINT staat voor ‘Open Source Intelligence’: het is informatie uit openbare bronnen zoals sociale media en nieuwswebsites. Tijdens dit onderzoek controleren wij welke informatie over uw organisatie publiekelijk toegankelijk is online, zodat u zichzelf kunt beschermen.

Cybersecurity e-Learning

Wilt u cybersecuritykennis overdragen aan u uw medewerkers? In samenwerking met ARDA bieden wij laagdrempelige en interactieve Cybersecurity e-Learning modules aan, voor effectieve kennisoverdracht.

SAFE Awareness Programma

De kloof tussen security awareness en veilig gedrag is groot. Daarom richt het SAFE Awareness Programma zich op daadwerkelijke gedragsverandering. Tijdens dit meerjarige programma krijgen uw medewerkers trainingen, interventies en tools om zich veiliger te gedragen, zodat uw oragisatie beter beschermd is tegen aanvallen.

Voorbeeld | Social Engineering

Welk probleem had de klant?

Een Nederlandse gemeente wilde weten hoe hun medewerkers zouden reageren op telefonische phishing. Terwijl wij bezig waren met dit onderzoek, werd de gemeente aangevallen via een echte phishingmail.

Resultaat

Wij combineerden de resultaten van het telefonische phishing onderzoek met bevindingen en advies over de echte phishingaanval. We filmden een interview met de CISO’s en de ethisch social engineers. Dit filmpje kreeg grote aandacht van medewerkers, waardoor de gemeente de awareness echt verhoogde.

Secura
A BUREAU VERITAS COMPANY

Over Secura / Bureau Veritas

Secura is een toonaangevend cybersecuritybedrijf. Ons doel is om uw cyberweerbaarheid te vergroten. Onze klanten variëren van overheid en zorg tot financiën en industrie. Secura biedt technische diensten aan, zoals vulnerability assessments, penetratietesten en red teaming. We bieden ook audits, forensische diensten en awarenesstrainingen aan.

Secura is onderdeel van Bureau Veritas (BV), een beurs-genoteerde onderneming die gespecialiseerd is in testen, inspecteren en certificeren. BV is opgericht in 1828, heeft ruim 80.000 medewerkers en is actief in 140 landen.

BUREAU VERITAS 1828

Meer weten?

Neem contact met ons op om uw cyberweerbaarheid te verhogen.

info@secura.com

+31 (0) 88 888 3100

secura.com