Crowe

ACA IT-Solutions, onderdeel van Crowe

Whitepaper:

Phishing

Voorkom oplichting door cybercriminelen.

ACA IT-Solutions, onderdeel van Crowe

Phishing voorkomen

Phishing is de meest gebruikte aanvalsmethode onder cybercriminelen. Het is een geavanceerde vorm van oplichting. Meer dan 90% van alle cyberaanvallen en beveiligingsincidenten begint met een phishing-aanval. Bescherm je organisatie tegen deze aanvallen en voorkom enorme schade.

Waarom is deze methodiek zo populair? Simpelweg omdat de aanval relatief eenvoudig, lucratief en uitermate succesvol is. We zien vaak dat het eenlingen zijn of kleine groepen cybercriminelen die de aanval uitvoeren. Hierdoor blijven ze gemakkelijk onder de radar en richten ze enorme schade aan bij hun slachtoffers, zowel financieel als technisch.

Cybercriminaliteit bereikt volwassen fase
Phishing heeft enorme naamsbekendheid gekregen door de e-mailberichten die vaak in gebrekkig Engels werden geschreven. Iedereen kent deze berichten nog wel. Daarin werden vreemde (vaak ongeloofwaardige) verzoeken gedaan. Zo werd bijvoorbeeld verzocht om het bankrekeningnummer, zodat er een erfenis gestort kon worden. Daar trapt inmiddels niemand meer in. De cybercriminelen werken tegenwoordig zeer professioneel. De phishing-aanvallen zijn nauwelijks nog van legitieme berichten te onderscheiden. Met vele slachtoffers als gevolg!

Cybercriminaliteit heeft een volwassen fase bereikt. Dat is zorgwekkend. Zowel nationaal als internationaal luidt men de noodklok om consumenten en het bedrijfsleven te attenderen op deze oplichtingspraktijken die een spoor van ellende achterlaten en jaarlijks vele miljarden aan financiële schade veroorzaken. Ook worden ICT-omgevingen op grote schaal ontwricht en worden belangrijke bedrijfsgegevens onbruikbaar en/of gestolen.

Aanvalsmethodes
Phishing wordt tegenwoordig niet alleen meer per e-mail gedaan. Cybercriminelen zoeken steeds naar nieuwe methodieken om de potentiële slachtoffers te verrassen op een onachtzaam moment.

- E-mail
- Malafide bijlages
- Malafide URL’s
- Smishing (SMS / Whatsapp)
- Vishing (telefonisch)
- Spear Phishing

ACA IT-Solutions, onderdeel van Crowe

> *Praktijkonderzoek wijst uit dat tot wel 4 op de 10 medewerkers op phishingmails klikt.*
> *Hoe is dat in jouw organisatie?*

David Ruijs, IT Business Professional ACA IT-Solutions

De ‘succesfactor’

Waarom is phishing nou zo succesvol? Omdat de succesfactor hoog is. Cybercriminelen gaan zeer inventief te werk. Ze spelen in op de zwakke plekken die ieder mens heeft. Hierdoor is men eerder genegen om snel op de link te klikken of de bijlage te openen. Eén verkeerde klik van een medewerker is funest. Enkele voorbeelden van veel gebruikte berichten:

- **Je hebt een snelheidsboete**
- **Je creditcard verloopt bijna**
- **De levering van je pakketje is vertraagd**
- **Laatste aanmaning telefoonrekening**
- **Je zakelijke mailbox heeft de maximale capaciteit bereikt**

De gevolgen van een succesvolle phishing aanval zijn enorm. Het is een middel om het ‘hogere doel’ te bereiken. Dit kan zijn het plunderen van een bankrekening, het activeren van een cryptolocker, het stelen van waardevolle gegevens zoals gebruikersnamen/wachtwoorden of bijvoorbeeld patenten.

ACA IT-Solutions, onderdeel van Crowe

Hoe kwetsbaar is jouw organisatie en hoe pareer je phishing-aanvallen?
Een goede beveiliging van jouw organisatie vraagt om een gedegen aanpak op basis van drie pijlers: Beleid, Techniek, Gedrag. Op basis hiervan adviseren wij een meervoudige werkwijze:

1. Maak beleid
Kies voor een beleidsmatige aanpak van IT-Security. Door je huidige situatie te reviewen (bijvoorbeeld door een IT-Security Audit), een meerjarenplan, het opstellen van procedures en het trainen van medewerkers creëer je een veilige werkomgeving en dat geeft rust.

2. Beveilig 'de voor- en achterdeur'
Door een gedegen IT-Security omgeving zorg je ervoor dat cybercriminelen meer moeite moeten doen om binnen te komen. Hierdoor is de kans groter dat criminelen aan je voorbij gaan. Vergeet hierbij echter niet je digitale achterdeur ook te sluiten.

3. Train de medewerkers
Weet een cybercrimineel toch jouw medewerkers te bereiken? Zorg er dan voor dat zij mogelijke gevaren kunnen signaleren en weten hoe te handelen. Om het klikgedrag te meten in jouw organisatie starten we meestal met een phishing simulatie. We analyseren de resultaten en je ontvangt een uitgebreid adviesrapport met praktische aanbevelingen van onze specialisten.

4. Bescherm uw waardevolle eigendommen
Heeft een medewerker onverhoopt op een onveilige link geklikt? Je kunt enorme schade voorkomen door ervoor te zorgen dat de cybercrimineel niet kan doordringen tot de waardevolle eigendommen van jouw organisatie.

5. Minimaliseer de tijd om de schade te herstellen
Een grote kostenpost die vaak over het hoofd wordt gezien is de schade die cybercriminelen aan de ICT-omgeving of het wissen/blokkeren (cryptolocker) van applicaties en/of bedrijfsgegevens. Een goede Back-up & Recovery-oplossing is essentieel. Zo weet je zeker dat jouw ICT-omgeving, applicaties en gegevens veilig zijn en kunnen worden hersteld. Belangrijk element in deze is de RTO- en RPO-tijd. Ofwel: hoe lang geleden is de laatste back-up gemaakt en hoe snel ben je weer up-and-running?

Advies & ondersteuning

Bij ACA IT-Solutions, onderdeel van Crowe, draait alles om de drie-eenheid Beleid, Techniek en Mens. Elk vraagstuk is een samenspel van deze elementen. Dat leidt tot innovatieve IT-bedrijfsoplossingen, waarbij continuïteit, beschikbaarheid en veiligheid essentieel zijn. Daarmee bereiken onze klanten een onderscheidend resultaat.

Contact
Wil je meer informatie of een afspraak maken? Neem dan contact met ons op via onderstaande contactgegevens.

Adresgegevens
ACA IT-Solutions, onderdeel van Crowe
Beukenlaan 40-50
5651 CD Eindhoven

Contactgegevens
040 - 8 800 100
info@aca-it.nl
www.aca-it.nl

ACA IT-Solutions, onderdeel van Crowe

Cybercriminaliteit in cijfers

Wereldwijde schade cybercriminaliteit
> 5 biljoen dollar
($5.000.000.000.000)

Schade in Nederland:
Ruim 10 miljard
(€ 10.000.000.000)

Eigen medewerkers
Zij veroorzaken
> 70% incidenten door onjuist handelen

Iedereen kan hacker worden
Beperkte technische kennis nodig

Te koop op het DarkWeb:
Ransomware toolkit:
$ 200 - 300

Schade bij een succesvolle phishingaanval

Vervangen apparatuur
€ 10.000 – 1.000.000

Boetes
Maximaal € 20 miljoen / 4% van omzet wereldwijd

Onderhoud & herstel
€ 5.000 – 50.000

Improductiviteit
Gemiddeld € 264,- per medewerker per dag

Financiële impact per organisatiegrootte

Impact van ransomware op klein bedrijf
25 medewerkers
€ 6.600,-

Impact van ransomware op MKB-bedrijf
150 medewerkers
€ 39.600,-

Impact van ransomware op Groot-bedrijf
500 medewerkers
€ 132.000,-

Impact van ransomware Enterprise organisaties
1000 medewerkers
€ 264.000,-

Reputatieschade door cybercrime

Verminderd vertrouwen van relaties

Negatieve klantperceptie

Dalende verkoop en omzet

Verslechtering bedrijfspositie