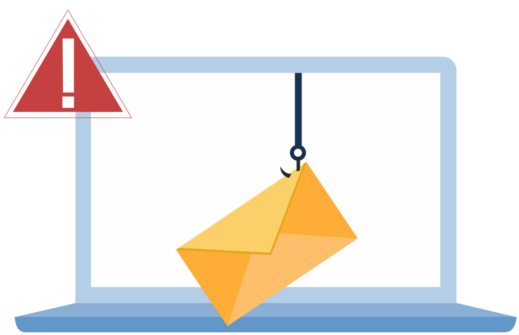
De evolutie van phishing

Van doorzichtige e-mails tot geavanceerde fraude

Introductie

Phishing is een van de meest voorkomende en tegelijkertijd gevaarlijkste vormen van cybercriminaliteit. Sinds het internet bestaat, zijn criminelen voortdurend bezig met het ontwikkelen van nieuwe methodes waarmee gevoelige informatie van zowel particulieren als organisaties ontfutseld kan worden.

Om een goed beeld te krijgen van de omvang en impact van phishing vandaag de dag, zoomen we uit en kijken we naar de oorsprong en ontwikkelingen in de afgelopen decennia.



C-SOC
A MASERO COMPANY

Inhoud

De oorsprong van Phishing

Met phishing wordt bedoeld dat een aanvaller zich voordoet als een legitieme entiteit om gevoelige informatie binnen te hengelen zoals inlog- en betalingsgegevens. Meestal gebeurt dit via e-mails maar het kan ook gebeuren via een telefoongesprek, sms of zelfs sociale media.

De term phishing werd voor het eerst gebruikt in de jaren ‘90 maar het concept van mensen misleiden om persoonlijke informatie los te krijgen is natuurlijk al veel ouder. Een van de eerst bekende gevallen van phishing vond plaats in 1996 waarbij hackers valse AOL mails verstuurden om inloggegevens te verkrijgen.

In de beginjaren van phishing waren de aanvallen vaak eenvoudig en gemakkelijk te herkennen. Cybercriminelen stuurden massaal een e-mail rond die zogenaamd afkomstig was van een legitiem bedrijf, waarin gevraagd werd persoonlijke informatie te delen ter bevestiging. Ondertussen heeft deze vorm van internetfraude een ware evolutie doorgemaakt.

Moderne phishing methodes

Waar een phishing mailtje voorheen nog makkelijk te herkennen was aan gebrekkig taalgebruik, rare zinsopbouw of slechte opmaak zijn de methodes ondertussen veel geavanceerder. Naarmate internetgebruikers beter geïnformeerd raakten, werd het noodzakelijk voor cybercriminelen om hun technieken en methodes te verbeteren.

Social engineering

Door middel van psychologische manipulatie proberen cybercriminelen hun slachtoffer te misleiden zodat vertrouwelijke informatie wordt vrijgegeven, of bepaalde acties worden ondernomen die de beveiliging van de persoon zelf of de hele organisatie compromitteert. Door zich te richten op de menselijke factor en gebruik te maken van sociale interacties wordt ingespeeld op angst, nieuwsgierigheid en hebzucht.

Spear phishing

In tegenstelling tot algemene phishing aanvallen, die op grote schaal worden uitgevoerd, zijn spear phishing aanvallen gericht op specifieke personen of organisaties. Deze vorm van phishing is vaak heel overtuigend en lastig te detecteren, omdat er gebruik wordt gemaakt van persoonlijke informatie van het doelwit.

Moderne phishing methodes

Whaling

Een specifieke vorm van spear phishing is whaling, waarbij de aanvaller zich richt op hooggeplaatste doelwitten binnen een organisatie. Een succesvolle whaling aanval kan op financieel- en operationeel vlak enorme schade aanrichten.

Clone phishing

Door het klonen van een legitieme, eerder verzonden e-mail kan ongemerkt een kwaadaardige link of bijlage worden verzonden. Ontvangers zijn in dit geval vaak niet op hun hoede en zijn zo eerder geneigd op de link te klikken of de bijlage te openen, met alle gevolgen van dien.

Mobiele phishing

Via onze mobiele telefoon kunnen we gemakkelijk om de tuin worden geleid door criminelen. Door zich met een sms-bericht voor te doen als een bekende halen criminelen hun slachtoffer over om bijvoorbeeld geld over te maken of persoonlijke informatie te delen (smishing). Ook wordt speciale opnametechnologie gebruikt om een voicemail te creëren die afkomstig lijkt te zijn van banken of andere betrouwbare bronnen, waarmee slachtoffers onder druk gezet worden (vishing).

Een case: de 2020 Twitter Hack

Het gevaar van phishing technieken die worden gebruikt om toegang te krijgen tot social media accounts, blijkt uit deze case waarbij invloedrijke personen en bedrijven werden gehackt in een gecoördineerde aanval.

Op 15 juli 2020 werden de Twitter accounts van o.a. Elon Musk, Bill Gates, Barack Obama maar ook bedrijven zoals Apple en Uber gehackt. Via deze accounts werden berichten geplaatst die lezers opriepen om Bitcoins over te schrijven naar specifieke wallets, met de belofte dat hun inleg verdubbeld zou worden.

De aanvalsmethode

Door middel van een spear phishing campagne lukte het de aanvallers om een aantal Twitter medewerkers in de val te lokken. Door zich voor te doen als collega's van de IT-afdeling (social engineering) haalden de criminelen de medewerkers over hun inloggegevens te delen en zo toegang te verschaffen tot interne tools. Ook maakten ze gebruik van vishing waardoor de aanval persoonlijker en overtuigender was dan traditionele phishing via e-mail.

De impact

Hoewel er geen hoge bedragen zijn buitgemaakt via deze Bitcoin fraude, veroorzaakte de aanval aanzienlijke schade.

Een recente case: de 2020 Twitter Hack

Zo had de aanval een vergaande impact op de reputatie van Twitter, omdat het vertrouwen in de veiligheid van het platform ernstig werd beschadigd. Er werden meerdere onderzoeken in het leven geroepen en de FBI dwong Twitter om hun beveiligingsprotocollen te herzien en te verbeteren.

De harde les

Deze geslaagde phishing aanval benadrukt het belang van robuuste maatregelen tegen deze vorm van internetfraude. De leerpunten die we uit deze case kunnen halen:

- **Multifactor Authenticatie** - door MFA bij alle medewerkers te implementeren, kunnen we voorkomen dat kwaadwillende personen toegang krijgen tot gevoelige systemen.
- **Bewustwording en training** - op de hoogte blijven van de ontwikkelingen en gevaren helpt u en uw medewerkers om verdachte berichten te herkennen.
- **Beperkte toegang** - door ervoor te zorgen dat niet iedereen zomaar toegang heeft tot interne systemen, verkleint u het risico op een geslaagde hack.
- **Monitoring en response** - laat uw netwerken en systemen monitoren door een betrouwbare cybersecurity partner die direct kan ingrijpen bij verdachte activiteiten.

De toekomst van phishing

Phishing technieken zullen zich blijven ontwikkelen en er zal constant gezocht worden naar nieuwe methodes om mensen digitaal te misleiden. Daarom moeten organisaties continu op de hoogte blijven van de laatste trends en ontwikkelingen op het gebied van cybercriminaliteit. Daarom blikken we vast vooruit op de toekomst van phishing.

AI en Machine Learning

Door de razendsnelle opkomst van Artificial Intelligence zijn cybercriminelen in staat hun phishing technieken nog overtuigender te maken en zeer geloofwaardige berichten te creëren, door natuurlijke taalverwerkingstechnieken toe te passen. Doordat AI-gedreven systemen binnen no-time grote hoeveelheden data kunnen analyseren, kan een phishing aanval in real-time worden aangepast aan de reactie van het slachtoffer. Zo wordt een aanval dynamischer en moeilijk detecteerbaar.

Deepfake

Een indrukwekkende maar tegelijkertijd angstaanjagende ontwikkeling is de deepfake technologie. Hierbij wordt gebruik gemaakt van AI om video en audio materiaal te manipuleren waardoor cybercriminelen zich kunnen voordoen als een betrouwbaar of leidinggevend persoon.

De toekomst van phishing

IoT apparaten

Het Internet of Things groeit snel en omvat alles van slimme apparaten binnenshuis tot gigantische industriële systemen. Het belang van een solide beveiliging op deze apparaten wordt nog altijd onderschat, wat ze kwetsbaar maakt voor phishing. Wanneer een IoT apparaat wordt gehackt, kan deze worden gebruikt om toegang te krijgen tot bredere netwerken wat tot een grootschalige beveiligingsinbreuk kan leiden.

Social Engineering

De kans dat deze vorm van phishing in de toekomst verder verfijnd wordt en daarmee doelgerichter kan worden ingezet, is zeer groot. Door social engineering in te zetten met andere vectoren zoals mal- of ransomware, vergroot de crimineel de effectiviteit van zijn aanval.

Crypto currencies

We kennen er ondertussen veel; crypto currencies zoals Bitcoin. Deze wereld wordt steeds groter en we zien dan ook een toename in aanvallen gericht op crypto gebruikers en -beurzen.

Conclusie

We hopen niet dat de moed u na het lezen van deze informatie in de schoenen is gezonken. Door het treffen van de juiste maatregelen kunt u zich namelijk goed voorbereiden op de toekomst en beschermen tegen nieuwe phishing technieken.

Naast de acties die u zelf kunt ondernemen om uw informatiebeveiliging te versterken, doet u er goed aan om de juiste cybersecurity partner in te schakelen die u niet alleen voorziet van concrete adviezen maar ook 24/7 uw netwerken en systemen monitort. Zo worden dreigingen direct opgepikt en kunt u zich met een gerust hart focussen op uw eigen core business.

Bent u nieuwsgierig geworden naar wat C-SOC voor u kan betekenen?

We komen graag in contact om de vele mogelijkheden en voordelen te bespreken in een vrijblijvend adviesgesprek!

www.c-soc.nl | verkoop@c-soc.nl

C-SOC
A MASERO COMPANY