Remcoh
Voordelig en compleet ICT-beheer

Beveiliging

Remcoh legt uit: wat is phishing?

White Paper

Middels deze white paper informeert en adviseert Remcoh u over hoe malafide praktijken van internetcriminelen voorkomen kunnen worden. In deze white paper behandelt Remcoh een veel gebruikte methode: Phishing

Cybercriminelen worden steeds handiger en brutaler

Beslist.nl verspreidt urenlang malware, vier gemeenten plat door virusbesmetting, Het Korps Landelijke Politiediensten waarschuwt voor valse e-mails, twee mannen aangehouden om witwassen na phishing, recordaantal phishingsites in 2012.

Cybercriminelen worden steeds handiger en brutaler als het gaat om hacken van websites, servers en werkstations, tablets en smartphones om aan bedrijfsgevoelige data te komen. Phishing, trojans, spoofing en pharming zijn een kleine greep uit de malafide praktijken van de internetcriminelen.

Wat is phishing

Internetcriminelen proberen per vervalste e-mails of websites, persoonlijke gegevens te bemachtigen: zoals inloggegevens, bankrekeningnummers, pincodes, BSN-nummer of creditcardgegevens. Met deze informatie krijgen internetcriminelen toegang tot en controle over uw betalingsverkeer.

Phishing e-mails en websites

Meestal ontvangt het slachtoffer een e-mail waarin gevraagd wordt, om in te loggen op de internet bankaccount, deze te controleren en te verifiëren.
Ook wordt er gebruikgemaakt van instant messaging (door middel van Twitter, X-chat, Windows Live Messenger, etc.) en wordt het slachtoffer soms telefonisch benaderd.
Phishing websites doen zich voor als legitieme websites en bootsen vaak bekende merken na van bijvoorbeeld financiële instellingen zoals o.a. ING, ABN AMRO en PayPal.

Hoe herken je een phishing e-mail

In een phishing-bericht vind je vaak de volgende elementen:

- De mail is vaak onpersoonlijk en begint met een algemene opening als "Geachte klant"
- Er wordt gevraag om inloggegevens of op een link te klikken en daar in te loggen
- Er wordt gesuggereerd dat uw account "geverifieerd" moet worden met uw
- Er wordt gedreigd met gevolgen als er niet onmiddellijk gehoor wordt gegeven aan de mail.

Phishing-methode: Keylogger

Een veelgebruikte methode is dat de fraudeur een e-mail stuurt met een bijlage, waarin een Keylogger zit verborgen.
Een keylogger is een programma of een stuk hardware waarmee men de toetsaanslagen tot zelfs de muisbewegingen van een computergebruiker kan registreren. De mail functioneert dan als een Trojaans paard.

Zodra de gebruiker de bijlage heeft geopend, wordt zonder dat de gebruiker het doorheeft de keylogger geactiveerd. Hierdoor kan de fraudeur via internet zien welke wachtwoorden de gebruiker gebruikt bij het inloggen bij zijn of haar bank.
Phishing mail heeft dus als doel om je ordinair te bestelen. Het is niet altijd even eenvoudig om deze van echt te onderscheiden, vandaar wat tips om phishing te voorkomen:

Tips van Remcoh om phishing te voorkomen

- Volg geen links welke per mail worden verstuurd voor zaken welke je niet bekend zijn.
- Indien je een link volgt, controleer dat het internetadres in de adresbalk hoort bij de onderneming, zeker voordat je een formulier of inlogvenster invult. Sommige websites lijken exacte kopieën van de echte website met een bijna gelijk webadres.
- Inloggen op websites wordt altijd over een secure connectie gedaan, dit is controleerbaar door de gegevens van het (SSL) certificaat op te vragen (adresbalk met slotje: https://) Controleer dit zeker wanneer je een meegestuurde link volgt.
- Als je weet dat het bericht onbetrouwbaar is, reageer niet op het bericht en volg geen links, maar verwijder het bericht direct. Op het moment dat je reageert middels mail of volgen van een link, weten ze van je bestaan en zal je een veelvoud van gelijksoortige berichten gaan ontvangen.
- Wees helemaal op je hoede wanneer er naar je betalingsgegevens wordt gevraagd.

Let op!

Een financiële instelling zal NOOIT vragen om per e-mail wachtwoorden of andere gevoelige informatie te controleren, te wijzigen, te versturen of aan te passen.

Voorkomen is beter én goedkoper dan genezen!

Over Remcoh

Remcoh is er voor ondernemers die hun systeembeheer, gebruikersondersteuning en bewaking gedeeltelijk of volledig willen uitbesteden, voor een vast en laag tarief per maand!

Remcoh is er voor iedereen: voor kleinzakelijke ondernemers én groter MKB.
Of u nu kiest om zelf te investeren in de centrale hardware of gebruik wilt maken van cloud diensten; Remcoh zal ervoor zorgen dat u zich kunt focussen op de kernactiviteiten van uw onderneming. Remcoh is onderdeel van Paradigit zakelijk.

Over Paradigit zakelijk

Als strategisch partner voor zakelijke relaties biedt Paradigit Zakelijk zorgeloos werken met Remcoh. Remcoh neemt alle zorgen op het gebied van automatisering én systeembeheer uit handen. Paradigit zakelijk is dé specialist in het opleveren van turnkey projecten, het leveren van deskundig advies en biedt tevens een ruim aanbod van computers, servers, storage- en netwerkapparatuur voor uw bedrijfsnetwerk.

Contact

Indien u vragen heeft kunt u contact opnemen met Remcoh.

Paradigit Zakelijk
Hooge Zijde 30
5626 DC Eindhoven
Tel: 040-7512100
Fax: 040-7512199

E-mail: info@remcoh.nl