NOODKAART

PHISHING

Najaar 2022

Cyber Weerbaarheidscentrum
BRAINPORT
Voor hightech- & maakindustrie in NL

1 > KOPPEL UW APPARAAT LOS VAN INTERNET

Zoek uw wifi-instellingen en verbreek de verbinding met het netwerk of koppel de internetkabel los van uw apparaat. Zo verkleint u het risico dat malware zich door het netwerk verspreidt. Iets kwaadaardigs geïnstalleerd of geopend? Koppel uw apparaat los van internet.

2 > WIJZIG UW WACHTWOORDEN

Belandde u op een valse website? Ga naar de echte website en wijzig uw wachtwoord. Gebruikt u het wachtwoord voor andere accounts? Wijzig deze dan ook, bij voorkeur samen met wachtwoordhints en beveiligingsvragen. Laat de beheerder ook alle lopende sessies intrekken, omdat onbevoegden al ingelogd kunnen zijn met uw wachtwoord. Indien mogelijk: voer een bedrijfsbrede wachtwoord-reset uit om extra voorzichtig te zijn.

3 > MELD HET VOORVAL INTERN OF SCHAKEL INCIDENT RESPONSE HULP IN

Denk aan uw IT-leverancier, (cyber)verzekeraar of een derde partij met 24/7 noodnummer, bijvoorbeeld: Eye Security: **088-6444800** ; IP4Sure: **040-2095020** ; BDO: **088-2364899**

Heeft uw organisatie voldoende kennis in huis om
dit zelf op te pakken? Volg onderstaande stappen.

4 > SCAN HET VOLLEDIGE NETWERK OP MALWARE

Antivirus is niet onfeilbaar. Scan uw netwerk op malware, inclusief alle apparaten, bestanden, applicaties, servers, etcetera.

5 > CONTROLEER INLOGPOGINGEN

Controleer alle relevante accounts binnen de organisatie op inlogpogingen.
Heeft u bewijs welke accounts (mogelijk) zijn getroffen, kunt u heel gericht inlogpogingen onderzoeken.

6 > CONTROLEER UW ACCOUNT OP WIJZIGINGEN

Als er toegang is geweest tot een account, controleer dan of er geen wijzigingen in zijn aangebracht, bijvoorbeeld om uw email door te sturen of onzichtbaar te maken of om valse apparaten te registreren.

7 > VOER EEN FORENSISCHE ANALYSE UIT

Onderzoek alle relevante logboeken op tekenen van een eventuele inlogpoging, inbraak en/of misbruik. Denk aan firewalllogboeken, logboeken van uw e-mailserver en DNS-logboeken. Dit geeft een volledig beeld van de eventuele verspreiding van de phishing aanval.

8 > COMMUNICEER

Breng al het relevante personeel, inclusief managers, op de hoogte en zorg dat ze weten waar ze op moeten letten.

i

Meer informatie over dit onderwerp deelt Cyber Weerbaarheidscentrum Brainport met haar participanten. Ook lid worden van deze stichting zonder winstoogmerk? Bezoek www.cwbrainport.nl of mail naar info@cwbrainport.nl.

Met dank aan

BRAINPORT EINDHOVEN
METROPOOL REGIO EINDHOVEN
Provincie Noord-Brabant
Ministerie van Economische Zaken en Klimaat