Aanvallen met ransomware of phishingmails zijn serieuze bedreigingen voor bedrijven. En hoe goed je wellicht je it-systemen hebt beveiligd, een 'ongeval' zit in een klein hoekje. Een moment van onoplettendheid bij een medewerker die op een verkeerde link klikt en daar zijn wachtwoord invult. Of hackers die een opening hebben gevonden in een computer waar niet op tijd de nieuwste virusscanner is geïnstalleerd.
Hoe dan te handelen? Dit infoblad vertelt je welke EERSTE stappen je zou moeten nemen. Hang het ergens op waar alle medewerkers het kunnen zien, zodat ook als de systemen plat liggen iedereen weet hoe te handelen. Oefen het noodplan ook periodiek.

DE TWEE BELANGRIJKE STAPPEN BIJ EEN CYBERINCIDENT:
1. BLIJF KALM
2. ZOEK HULP EN BEL JOUW ICT-ER OF IT DIENSTVERLENER (ZIE LIJST ONDERAAN MET BELANGRIJKE TELEFOONNUMMERS)

ER ZIJN TWEE BELANGRIJKE CYBERINCIDENTEN, DIE IEDER EEN EIGEN AANPAK VRAGEN.

WAT MOET IK DOEN BIJ EEN RANSOMWARE AANVAL?

1. BETAAL GEEN LOSGELD
Betalen lost het probleem nooit direct op en stimuleert computercriminelen om meer aanvallen uit te voeren.

2. DOCUMENTEER HET BERICHT VAN DE AANVALLER
Documenteer berichten van de aanvaller. Zie je een melding op het beeldscherm? Noteer datum, tijdstip en activiteit en maak hiervan een foto, screenshot of schrijf het bericht over. Dit is ook van belang voor de aangifte bij de politie.

3. ISOLEER DE GEÏNFECTEERDE COMPUTER(S) DOOR DEZE LOS TE KOPPELEN VAN HET NETWERK
Voorkom verdere verspreiding van de infectie over meer apparaten. Isoleer de geïnfecteerde computer(s) door deze los te koppelen van het netwerk of zet de wifi uit als je op een draadloos netwerk werkt.
Let op: schakel de stroom niet uit, tenzij je de apparaten NIET kunt loskoppelen. Zonder stroom verlies je mogelijk nuttig bewijsmateriaal.

4. MELD HET VOORVAL ZO SPOEDIG MOGELIJK ZOWEL INTERN ALS EXTERN
Breng relevante medewerkers en managers op de hoogte en zorg dat zij weten waar ze op moeten letten. Neem ook (telefonisch) contact op met een of meer van de instanties die onderaan dit infoblad staan.

Kijk (eventueel met een derde partij of via computers die niet aan het netwerk hebben gehangen en niet besmet kunnen zijn) of er al een sleutel bestaat om het digitale slot te openen op No More Ransom.

Met behulp van derden kun je een computer in 'veilige modus' zetten:
Windows **Apple**

Kijk of je de ransomware kunt verwijderen met hulp van de gratis proefversie van het programma HitmanPro van Sophos.

Als daar behoefte aan is kan er altijd contact opgenomen worden met de **Vertrouwenslijn Afpersing (tel: 0800-2800 200)**, voor ondernemers die slachtoffer zijn van bedreiging of (digitale) afpersing. De Vertrouwenslijn biedt een luisterend oor, geeft advies, ondersteuning en een handelingsperspectief.

VNO NCW MKB Nederland

CYBERNOODPLAN
EERSTE STAPPEN NA EEN CYBERAANVAL

WAT MOET IK DOEN ALS IK (OF EEN MEDEWERKER) OP EEN PHISHINGMAIL HEB (HEEFT) GEKLIKT?

1. KOPPEL HET APPARAAT LOS VAN HET INTERNET
Zoek je wifi-instellingen en verbreek de verbinding met het netwerk, of koppel de internetkabel los van het betreffende apparaat. Zo verklein je het risico dat malware zich door het netwerk verspreidt.

2. WIJZIG WACHTWOORDEN
Belandde je / de medewerker op een valse website? Wijzig het wachtwoord! Wordt het wachtwoord ook gebruikt voor andere accounts? Wijzig deze dan ook daar, bij voorkeur samen met wachtwoordhints en beveiligingsvragen. Laat de beheerder ook alle lopende sessies intrekken, omdat onbevoegden al ingelogd kunnen zijn met het wachtwoord. Indien mogelijk: voer een bedrijfsbrede wachtwoord-reset uit om extra voorzichtig te zijn.

3. MELD HET VOORVAL ZO SPOEDIG MOGELIJK ZOWEL INTERN ALS EXTERN
Breng relevant personeel inclusief managers op de hoogte en zorg dat zij weten waar ze op moeten letten. Neem ook contact op met een of meer van de onderstaande nummers.
Voer eventueel met hulp van een deskundige een virusscan uit om je computer te laten nalopen op virussen en laat deze door de virusscanner verwijderen. Zorg er altijd voor dat je de laatste versie van de virusscanner hebt gedownload zodat de nieuwste bedreigingen worden herkend.

WAAR KAN IK TERECHT NA EEN CYBERINCIDENT?

Doe aangifte bij de **politie,** online of op het politiebureau.
Tel: 0800-8844

Rapporteer een datalek bij de **Autoriteit Persoonsgegevens**
Tel: 088-180 52 55

Meld fraude bij de **Fraudehelpdesk**
Tel: 088-786 73 72

Vind algemene informatie bij het **Digital Trust Center**

NOTEER HIER BELANGRIJKE EIGEN TELEFOONNUMMERS:

1. IT-afdeling

2. IT-leverancier

3. (cyber-)verzekeraar

4. (cyber) security specialist

5. ……..

6. ……..

7. ……..