# 7 maatregelen om je bedrijf te beschermen tegen cybercriminelen

Whitepaper

digital trust center.

PVO / Midden-Nederland

# Waar begin je?

Elk bedrijf is anders. Maar elk bedrijf dient beschermd te worden tegen cyberaanvallen. Hoe bescherm je jouw bedrijf? Waar begin je mee?

Samen met Digital Trust Center hebben wij deze whitepaper geschreven. Pas deze 7 maatregelen toe en zorg ervoor dat de kans op een cyberaanval aanzienlijk wordt verkleind.

PVO Midden-Nederland

# MAATREGEL 1

## Maak een back-up van je belangrijkste bestanden

Een reservekopie kan een laatste redmiddel zijn als je bedrijf is aangevallen. Zorg daarom voor één of meerdere kopieën van je bedrijfsgegevens, zoals je klantdata en dossiers. Zo'n kopie heet ook wel een back-up. Kopieer de belangrijkste bestanden naar een externe harde schijf, koppel deze vervolgens los en berg deze op een veilige plaats op. En bewaar minimaal één back-up op een andere locatie.

Werk je in de cloud? Let dan op, dit betekent niet dat er automatisch een back-up van je gegevens wordt gemaakt.

**Meer weten?**

# MAATREGEL 2

## Stel inloggen in twee stappen in

Met multifactorauthenticatie (MFA) voeg je aan het inloggen met een wachtwoord een extra inlogvereiste toe. Dit heet ook wel inloggen in twee stappen of tweestapsverificatie. Hierdoor bevestig je op meer dan één manier dat jij het bent die wil inloggen. Een voorbeeld van een extra stap is dat er een sms naar je smartphone wordt gestuurd. Hier staat dan een toegangscode in. Of je ontgrendelt je account met een code van een authenticatieapp of via je vingerafdruk.

Stel multifactorauthenticatie op zoveel mogelijk plekken in, in ieder geval bij je zakelijke e-mailaccount en de belangrijke applicaties of systemen voor je bedrijf.

**Meer weten?**

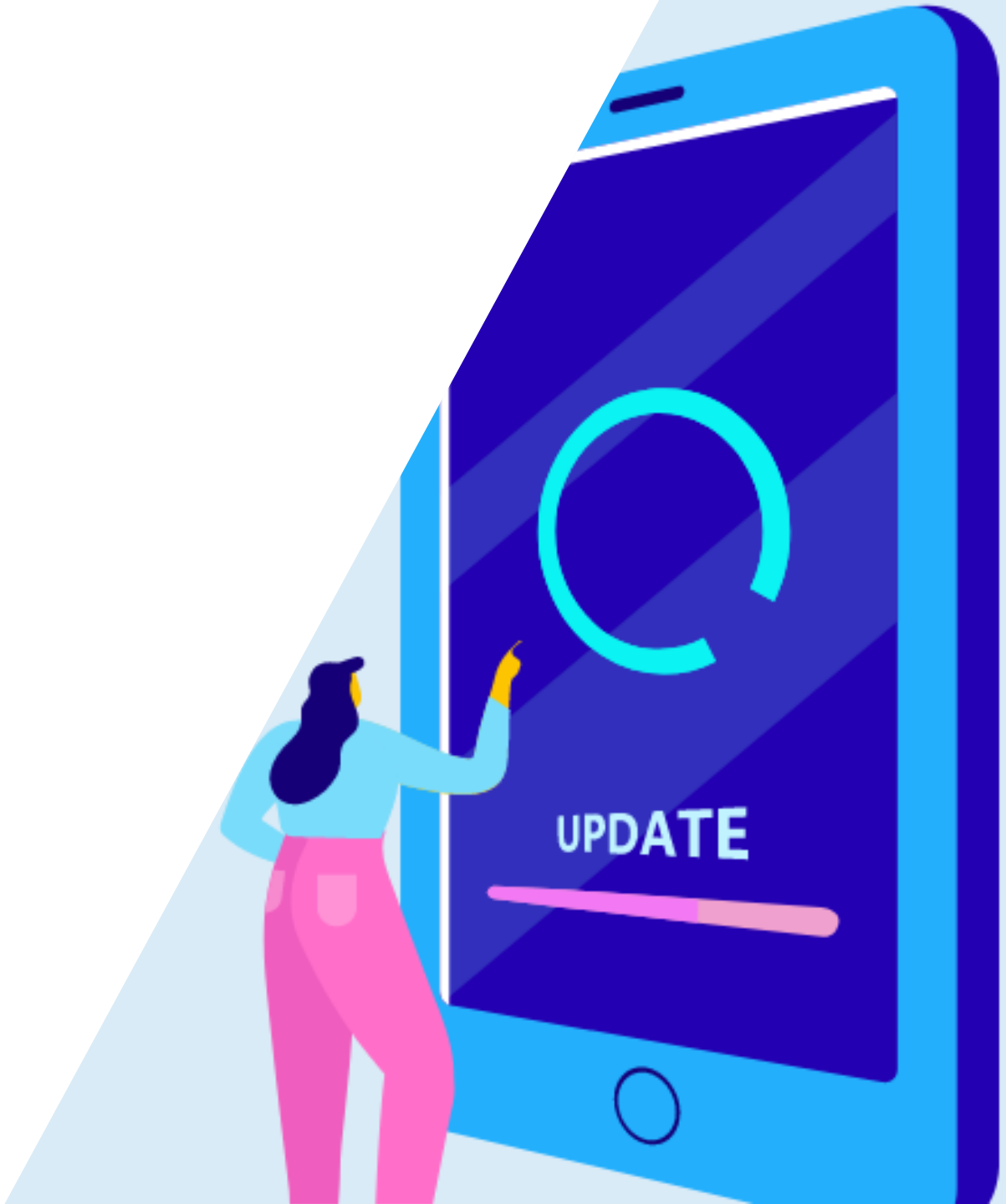
# MAATREGEL 3

## Zet automatische updates aan

Software-updates bevatten vaak verbeteringen voor de gebruiker. Ook bevatten ze vaak beveiligingsupdates. Voer je een update niet of later uit, dan kan je beveiliging kwetsbaar worden. Zo kan er bijvoorbeeld een beveiligingslek ontstaan. Kwaadwillenden zoeken actief naar manieren om binnen te dringen via zo'n lek.

Wacht daarom niet met het updaten van apparaten die met het internet verbonden zijn. Zet bij voorkeur ‘automatisch updaten’ aan. Denk hierbij niet alleen aan je computer of smartphone, maar ook aan je printer, slimme deurbel, website, server en router.

**Meer weten?**



# MAATREGEL 4

## Gebruik antivirussoftware

Een antivirusprogramma of antivirussoftware die je beschermt tegen internetvirussen en ‘malware’ is op veel apparaten inmiddels standaard aanwezig. Soms kun je ook zelf een antivirusproduct kiezen.

Installeer een antivirusprogramma en zorg dat deze software up-to-date blijft. Doe dit op alle computers, telefoons en servers binnen je bedrijf. Zo loop je minder risico op schade door virussen en andere malware.

**Meer weten?**

# MAATREGEL 5

## Controleer de beveiligingsstandaarden van je e-mail

Via internet.nl controleer je de beveiliging van je e-mailadres en domeinen. De website vertelt of je e-mailadres en/of domeinnaam voldoet aan moderne beveiligingsstandaarden. Zo krijg je een beeld van hoe jouw website en e-maildomeinen ervoor staan qua veiligheid.

Wat is mijn domeinnaam? Je domeinnaam is het gedeelte achter de ‘@’ bij je e-mailadres.

**Meer weten?**

# MAATREGEL 6

## Leer phishing herkennen

Maak jezelf en je medewerkers alert en zorg ervoor dat jullie phishing kunnen herkennen. Oefenen kan hierbij helpen. Doe de phishingquiz of speel de phishingbingo van het Digital Trust Center. Ook de 'eerst checken dan klikken'-tool kan helpen phishing te leren herkennen. Je kunt eventueel ook een phishingtest starten in samenwerking met een IT-dienstverlener.

**Meer weten?**

# MAATREGEL 7

## Print een bellijst voor noodsituaties

Heb je door een cyberaanval geen toegang meer tot je informatiesystemen? Dan is er sprake van een noodgeval. Zorg er daarom voor dat de contactgegevens van je IT-dienstverlener, softwareleverancier of securitybedrijf uitgeprint klaarliggen. Bekijk een voorbeeld van zo'n bellijst.

Heb je belangrijke klanten en (keten)partners? Zorg er dan ook voor dat jouw IT-dienstverlener bij hen geregistreerd staat als contactpersoon.

**Meer weten?**

# Wil jij aan de slag met het verbeteren van je cyberweerbaarheid?

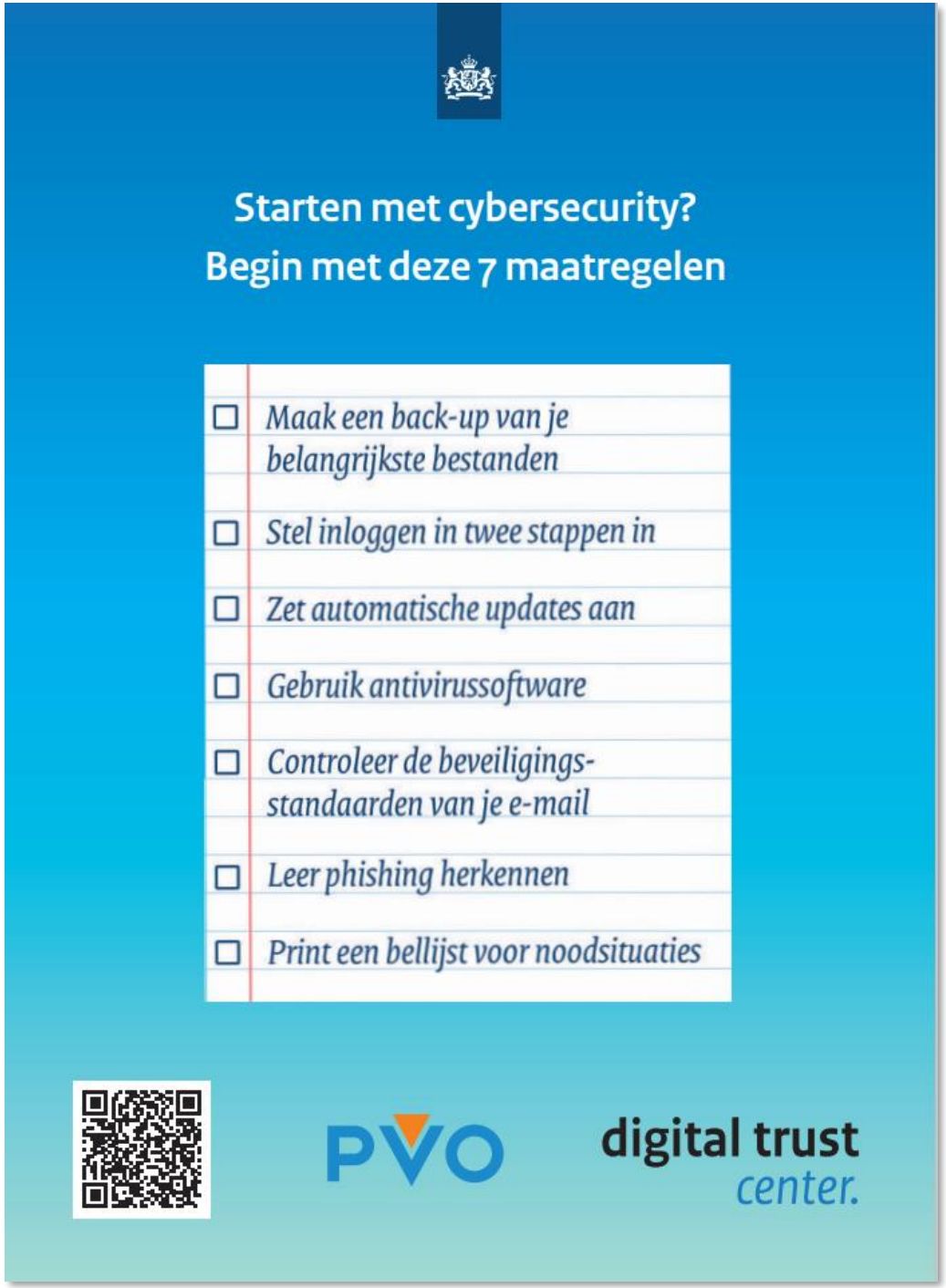
## Begin met deze 7 maatregelen

Wil je weten wat je nog meer kan doen om de cyberweerbaarheid van je bedrijf te vergroten? Kijk dan op de website van het Digital Trust Center. Doe bijvoorbeeld de basisscan en ontdek hoe het staat met jou cyberweerbaarheid.

**Wil je weten wat wij voor je kunnen betekenen?**

Neem dan contact op met een van onze themaspecialisten:

Over ons - PVO Midden-Nederland (pvo-middennederland.nl)



# Samen Veilig Ondernemen

## Daar maken we ons sterk voor.

PVO Midden-Nederland

Kroonstraat 25
3503 RH Utrecht
pvo-middennederland.nl

info@pvo-mn.nl

PVO Midden-Nederland

PVO Midden-Nederland zet zich in voor veilig ondernemen in de regio. We werken samen met overheid en bedrijfsleven om ondernemers bewust te maken van en te beschermen tegen criminaliteit, zowel fysiek als online. Ons doel is om de veiligheid in en rondom bedrijven te verbeteren en ondernemers weerbaarder te maken, zodat ze met vertrouwen kunnen blijven groeien in Midden-Nederland.