



CYBERSECURITY

Grootkeuken Nederland
Ramon Dooijewaard
FME Cyberweerbaarheid

WAT ALS...

Wat als alle gegevens van jouw organisatie openbaar worden?

Wat als alle IT-systemen drie weken niet gebruikt kunnen worden?

Wat als er losgeld betaald moet worden ter grootte van 2-5% van de jaaromzet?

NIEUWS

Tandartsenketen betaalt twee miljoen euro losgeld om 'gegijzelde' patiëntgegevens terug te krijgen

Tandartsenketen Colosseum Dental heeft meer dan twee miljoen euro losgeld betaald aan de criminele groepering die de systemen had gegijzeld. De tandartsenorganisatie, die meer dan 130 vestigingen in Nederland, België en Luxemburg heeft, was platgelegd met LV ransomware, bevestigen betrokkenen aan *de Volkskrant*.

CYBERSECURITY, URGENT?

- Cybercriminaliteit is uitgegroeid tot de **grootste bedreiging** voor bedrijven.

Bedrijven geraakt door brand: 1 op de 8.000

Bedrijven geraakt door inbraak: 1 op de 250

Bedrijven geraakt door een cyberaanval: 1 op de 5

(bron: Rabobank)

- Onderzoek toont zelfs aan dat de technologische industrie in 2021 voor het eerst meer werd aangevallen dan enige andere sector. We zijn target #1
- 41% van de aanvallen maakt gebruik van phishing mails (en 1 op de 5 medewerkers trapt hier in!)
- Bedrijven zijn volop aan de slag met digitalisering, wat inhoudt dat het aantal kanalen via welke een hacker binnen kan komen enorm toeneemt en er weinig zicht is op verbonden apparaten (aanvalsoppervlakte groeit, zowel IT als OT)
- Hackers zetten meest moderne technieken in om binnen te komen (het is een industrie met veel specialisten op verschillende vlakken), het is lucratief!
- Complexiteit van een IT-omgeving zorgt ervoor dat reageren lastig wordt voor management

WETGEVING GAAT VERANDEREN

De Europese NIB-richtlijn is herzien en heeft een **breder reikwijdte**. Dit leidt tot **extra verplichtingen** voor de middelgrote industrie (minimaal 50 FTE en een jaarmzet van 10 miljoen EUR).

Deze verplichtingen gaan niet alleen over jouw eigen bedrijf, maar betreft **ketenverantwoordelijkheid**.

Nederland heeft **tot eind 2023** om deze richtlijn te vertalen in wetgeving en te implementeren. Dit doen ze door de **Wet beveiliging netwerk- en informatiesystemen (Wbni)** aan te passen.

Voor de zomer verwachten we de eerste concept-teksten.

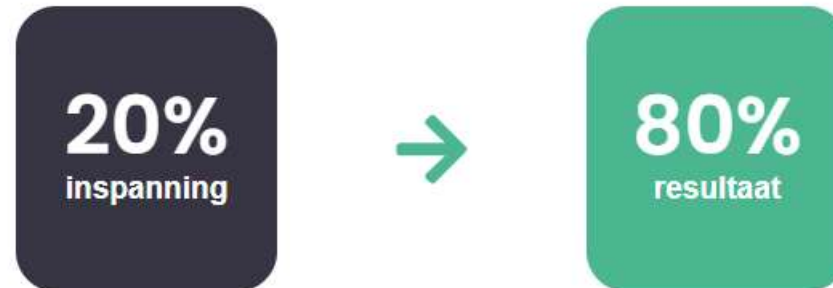


Samen Digitaal Veilig

INITIATIEF VAN



KLEINE INSPANNING, GROOT RESULTAAT



Kleine inspanning,
groot resultaat

De 20-80 regel geldt ook voor digitale veiligheid. Als je 20% veiligheid toevoegt aan je bedrijf, ben je in de regel al 80% veiliger. Het zijn namelijk de kleine, dagelijkse dingen die het verschil maken. Met Samen Digitaal Veilig weet jij precies wat die dingen zijn. En het belangrijkste: iedereen doet mee: jij als ondernemer, je medewerkers en ook je IT-leveranciers.

DE KRACHT VAN SAMEN

Samen Digitaal Veilig doe je niet alleen!

Een onderneming is zo veilig als de zwakste schakel. Daarom is het ook zo belangrijk dat iedereen samenwerkt; de ondernemer, haar medewerkers en de eigen IT-leverancier(s).

Die samenwerking wordt geactiveerd en gemonitord door het platform Samen Digitaal Veilig.



STAP 1

SAMEN DIGITAAL VEILIG



In meer dan 50% van de gevallen is het een gebruiker of medewerker die zelf een veiligheidsissue veroorzaakt (phising mails, zwakke wachtwoorden, USB-sticks, etc.)

Stap 1: Video's voor medewerkers:

- 8 korte video's over online veiligheid en beantwoorden van vragen

STAP 2

SAMEN DIGITAAL VEILIG



Alles start met het in kaart brengen van de huidige systemen (wat is er geïmplementeerd, wat is gekoppeld en wat is extern te benaderen) en werkwijze

Stap 2: scan voor de veiligheid van interne systemen

- Vragenlijst die de ondernemer (samen met de interne IT-verantwoordelijke) in kan vullen.

STAP 3

SAMEN DIGITAAL VEILIG



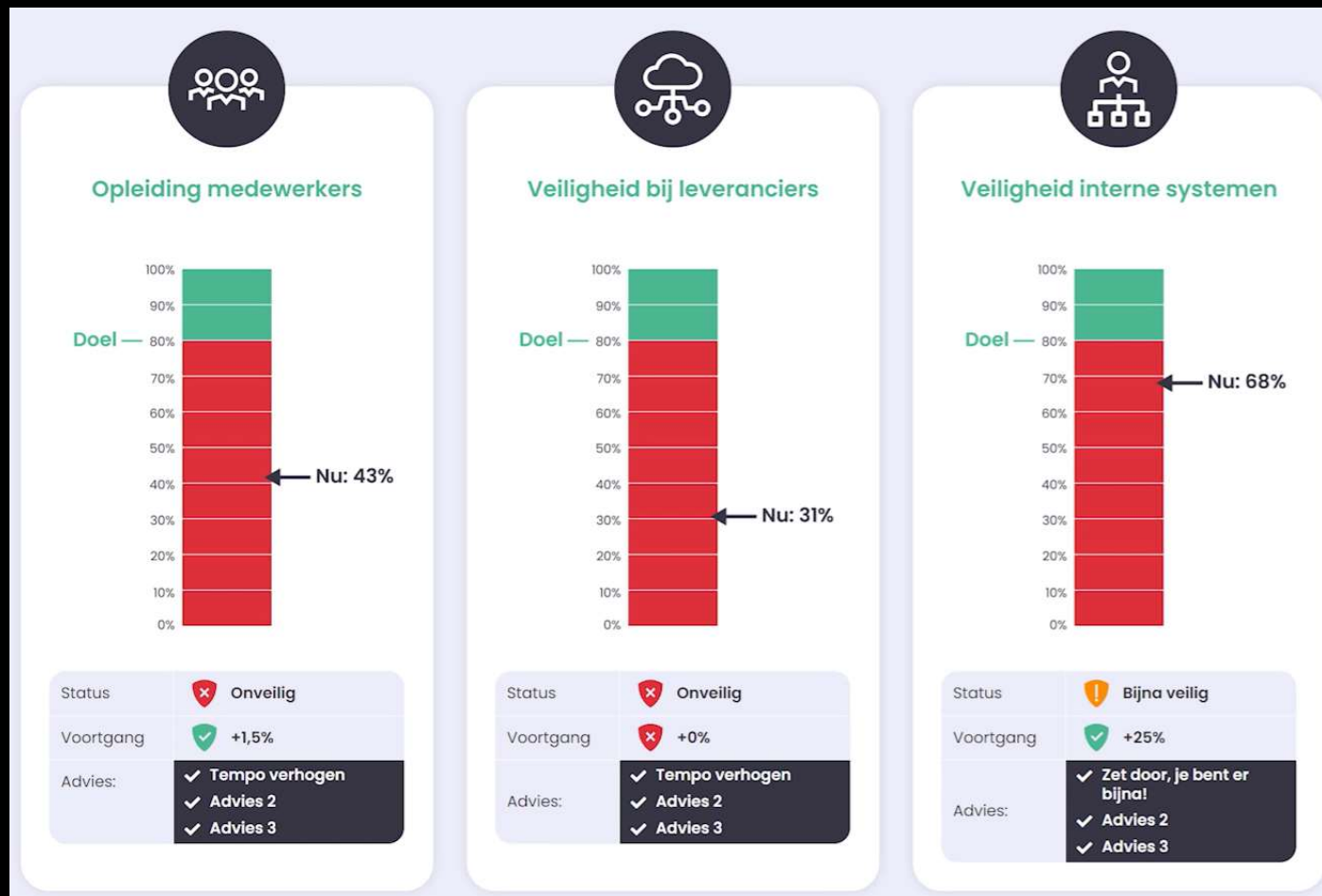
“Ik heb toch een anti-viruspakket/IT-leverancier”
“Mijn netwerkleverancier regelt dat”
“Mijn software zit in de cloud”
“Ze zullen zich toch niet op ons bedrijf richten”

Digitale veiligheid is complex en dat zal alleen maar meer worden. Veel ondernemers weten onvoldoende wat de dienstverlening vanuit hun IT-leverancier inhoudt.

Stap 3: vragenlijst IT-leverancier

- Nodig je externe IT-leverancier uit om eenvoudig een vragenlijst in te vullen die de digitale veiligheid van het bedrijf in kaart brengt.
- Check je gevoel van veiligheid

VEILIGHEIDSDASHBOARD



AANMELDEN

WWW.SAMENDIGITAALVEILIG.NL/FME

(www.samendigitaalveilig.nl/grootkeukenNL)