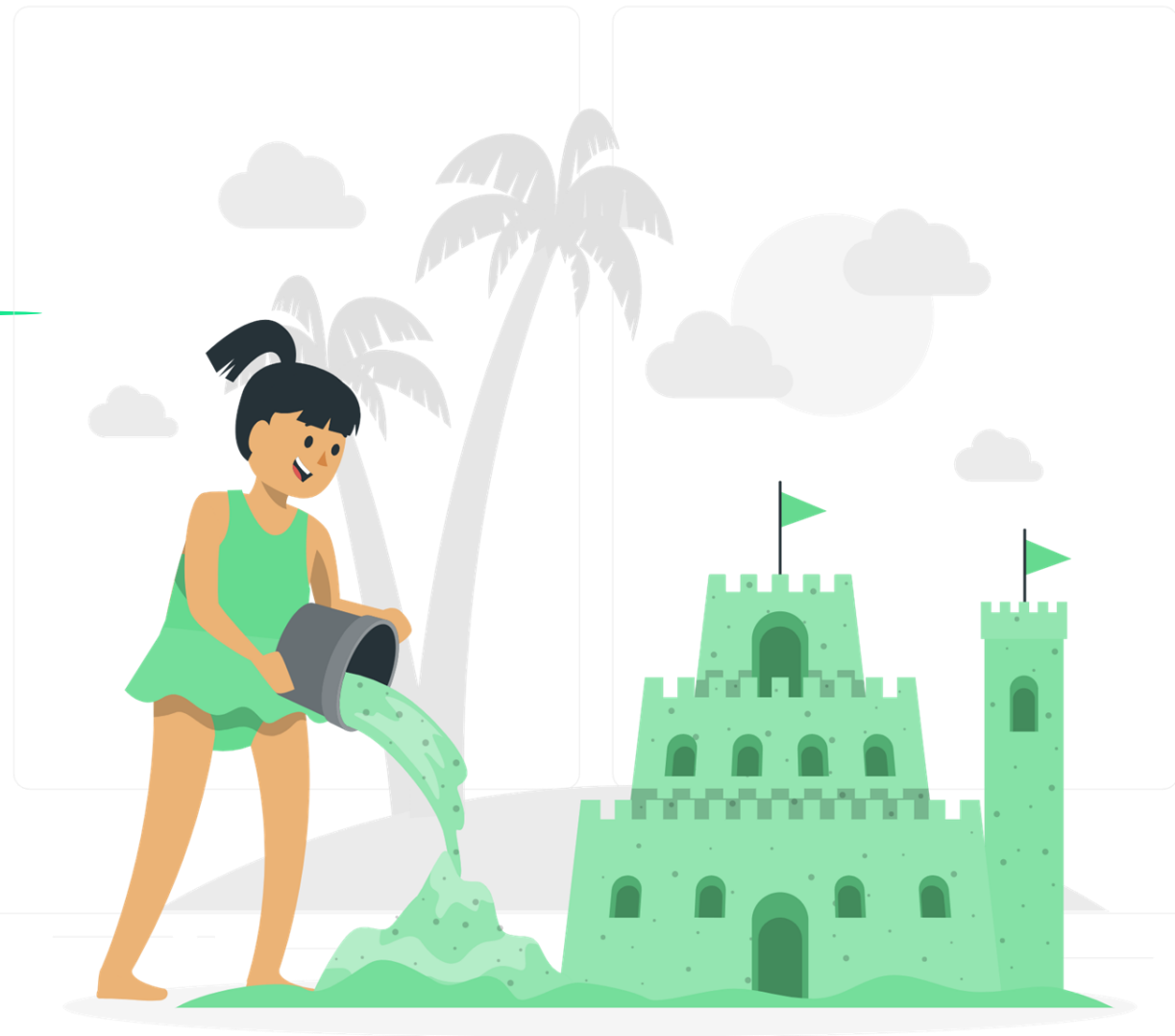


# Het Normenkader Informatiebeveiliging.

Samen met Edufort.



# Wie zijn we en wat doen we?

— Passie voor veilig onderwijs

## Michel van Melis

Beleidsadviseur DG en ICT

### Klant van Edufort

- o Werkt als beleidsadviseur DG en ICT voor zowel Stichting Nuwelijn en Muzerij als Stichting SKPOEL
- o Werkt daarnaast voor ISOMODE, een Brabants ICT samenwerkings- en netwerkgroep gericht op DG en I(C)T
- o Is tevreden klant van Edufort



## Joost Grunwald

Cybersecurity specialist

### Met passie voor cybersecurity

- o Master cybersecurity aan de radboud universiteit
- o Werkt als ethisch hacker, heeft kwetsbaarheden gevonden bij de overheid, Red Bull en NASA
- o Mede oprichter Edufort, helpt met informatiebeveiliging en werkt ook bij SURF



# Agenda.

- Stap voor stap door het Normenkader Informatiebeveiliging.

1.

**Introductie Edufort** en onze kernwaarden

2.

**Hoe helpt Edufort** besturen met IBP en het normenkader

3.

**Perspectief** van een klant van Edufort

4.

**Snelle test** met een ethisch hacker



# Edufort: onze normen en identiteit.



# Waarom Edufort?

Impact maken binnen digitale veiligheid

1.

## Huidige klanten helpen met nieuwe uitdagingen

Ik en mijn collega hebben al meerdere jaren expertise opgebouwd op het gebied van privacy en cybersecurity. We willen onze klanten ook kunnen ondersteunen met het Normenkader IBP.

2.

## Cybersecurity is nog onderbelicht

In alle bedrijfsbrede security scans die we hebben gedaan op schoolomgevingen hebben we minimaal 1 kritieke kwetsbaarheid gevonden.

3.

## We krijgen kriebels van normenkader sales

'Met A5 licenties voldoen aan het Normenkader' – Onzin  
'De pro Google licentie voor privacy risico's' – Relatief klein risico  
Er is geen peperdure software licentie die het normenkader of je technische security voor je gaat regelen



# Kernwaarden: waar Edufort voor staat

— Waar we als Edufort voor willen staan, wie we elke dag proberen te zijn

1

## **Customer Obsession**

Geobsedeerd zijn met zoveel mogelijk waarde leveren aan onze klanten, elke dag weer

2

## **Maatwerk**

We zien Edufort als het dynamische puzzelstuk, alleen hulp waar je dat nodig hebt.

3

## **Korte lijntjes**

We vinden korte en directe lijntjes essentieel

4

## **Digitaal weerbaar**

Helpen het Nederlands onderwijs daadwerkelijk veiliger te maken

2.

Hoe kan **Edufort** je helpen met IBP en normenkader?



# Het aanbod van Edufort

## — Onze puzzelstukjes

De 'papierwinkel'

### Beleid & Procedures



Nulmeting volledige normenkader om te kijken hoe je er voor staat momenteel.

Opstellen beleidsstukken en procedures en zorgen dat dit bij elkaar klopt.

De 'techniek'

### Technische security



Hackers uit team NL met ervaring binnen het onderwijs testen jouw technische cybersecurity

Verschillende soorten vormen:

- Bedrijfsbrede security scan
- Pentest op specifiek platform
- Red team, komen we binnen?

De 'regie'

### IBP-manager



Zet een van onze IBP managers weg bij jouw schoolbestuur, ze helpen vanaf 10 uur per maand met de regie en oppak rond het IBP normenkader.

Verschillende soorten vormen:

- Bedrijfsbrede security scan
- Pentest op specifiek platform
- Red team, komen we binnen?



# Het vrijblijvende aanbod van **Edufort**

—○— Onze gratis puzzelstukjes

De ‘vriendelijke hacker’

## Cybersecurity advies

Bel of mail me volledig vrijblijvend om te sparren over cybersecurity, als je een incident of dringende vraag hebt. Wij willen altijd helpen en meedenken, ook zonder daar rijk van te worden.



Het ‘inzicht’

## Wat ziet een ethisch hacker?

Laat gratis eens door een ethisch hacker naar jouw organisatie kijken, wat zien we vanaf het internet, ben je wel echt zo cyberveilig als je denkt?



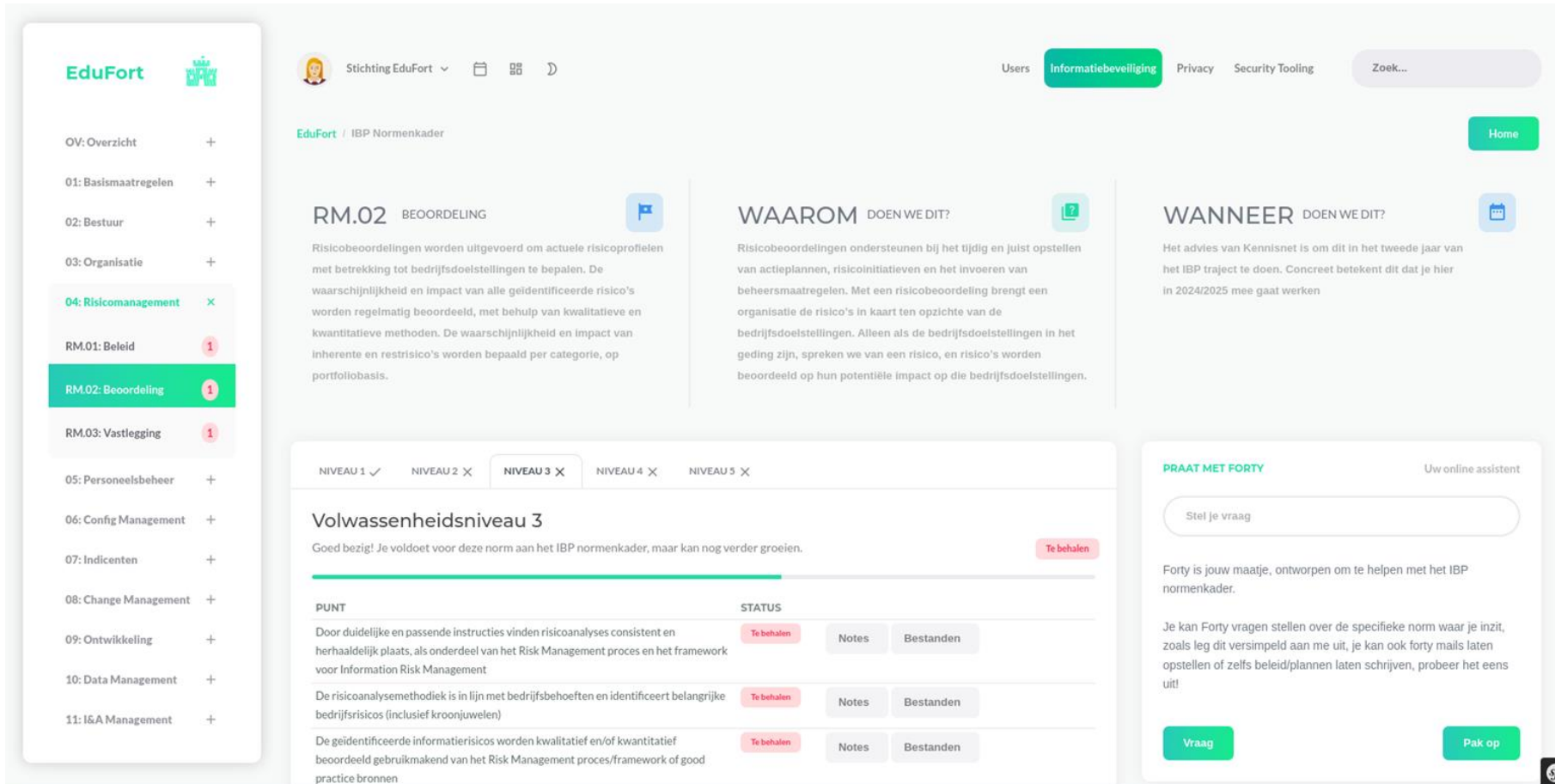
Het ‘overzicht’

## Software als schakel



# Demo Normenkader IBP tool

De enige tool **gebouwd voor het normenkader IBP**



The screenshot displays the Edufort Normenkader IBP tool interface. On the left is a navigation sidebar with a tree view of categories: OV: Overzicht, 01: Basismaatregelen, 02: Bestuur, 03: Organisatie, 04: Risicomanagement (selected), 05: Personeelsbeheer, 06: Config Management, 07: Incidenten, 08: Change Management, 09: Ontwikkeling, 10: Data Management, and 11: I&A Management. The main content area is titled 'RM.02 BEOORDELING' and contains three columns: 'WAAROM DOEN WE DIT?' and 'WANNEER DOEN WE DIT?'. Below these is a section for 'Volwassenheidsniveau 3' with a progress bar and a table of criteria. The table has columns for 'PUNT' and 'STATUS'. The criteria are: 1. Door duidelijke en passende instructies vinden risicoanalyses consistent en herhaaldelijk plaats, als onderdeel van het Risk Management proces en het framework voor Information Risk Management (Status: Te behalen). 2. De risicoanalysemethodiek is in lijn met bedrijfsbehoeften en identificeert belangrijke bedrijfsrisicos (inclusief kroonjuwelen) (Status: Te behalen). 3. De geïdentificeerde informatierisicos worden kwalitatief en/of kwantitatief beoordeeld gebruikmakend van het Risk Management proces/framework of good practice bronnen (Status: Te behalen). On the right, there is a 'PRAAT MET FORTY' chatbot section with a search bar and a 'Pak op' button. The top navigation bar includes 'Users', 'Informatiebeveiliging', 'Privacy', 'Security Tooling', and a search bar.

3.

Het perspectief van  
een klant.



4.

Hoe veilig zijn  
jullie?

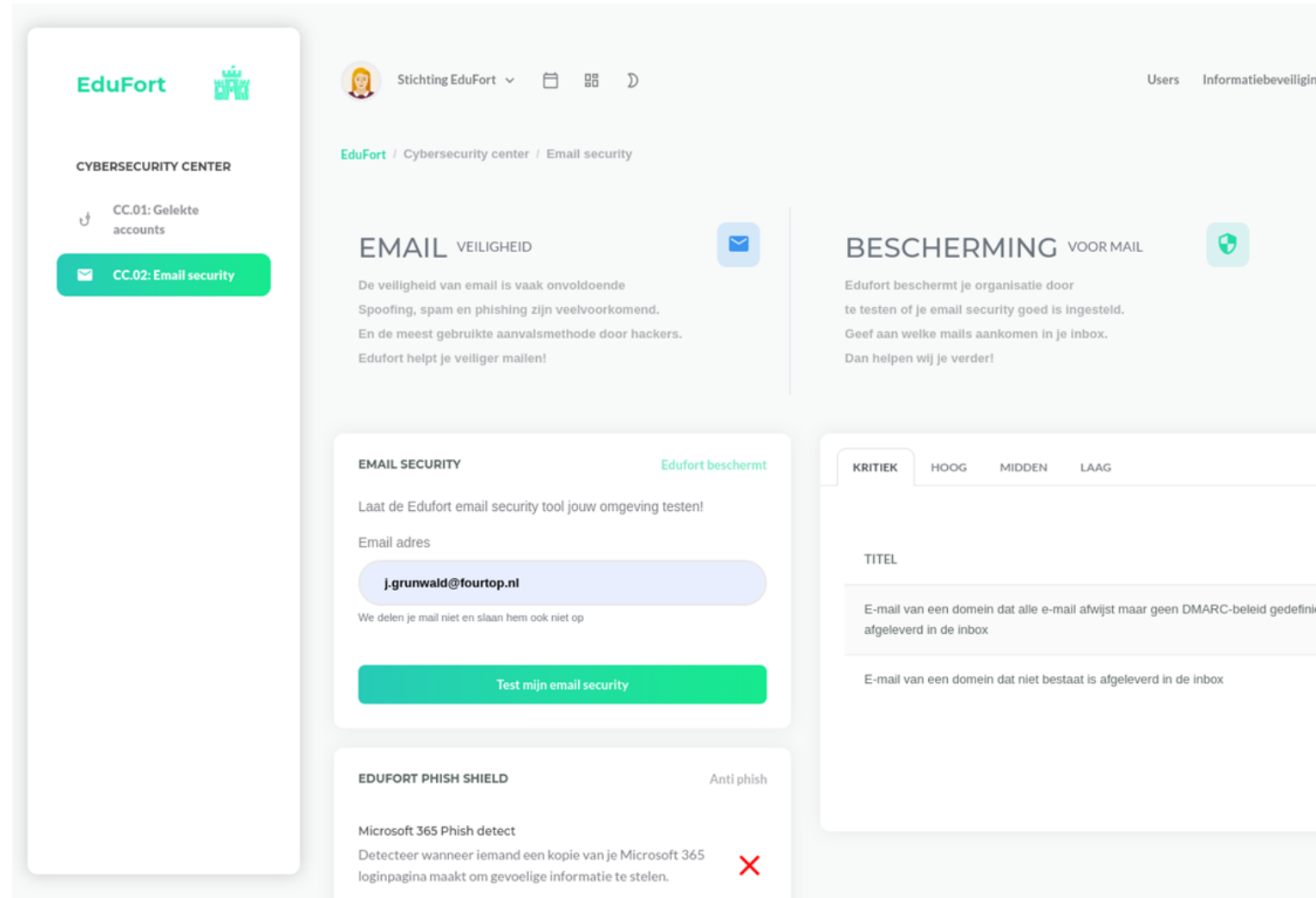


# Hoe is jullie Email security?

— Zoals in de Edufort tool

Ga naar

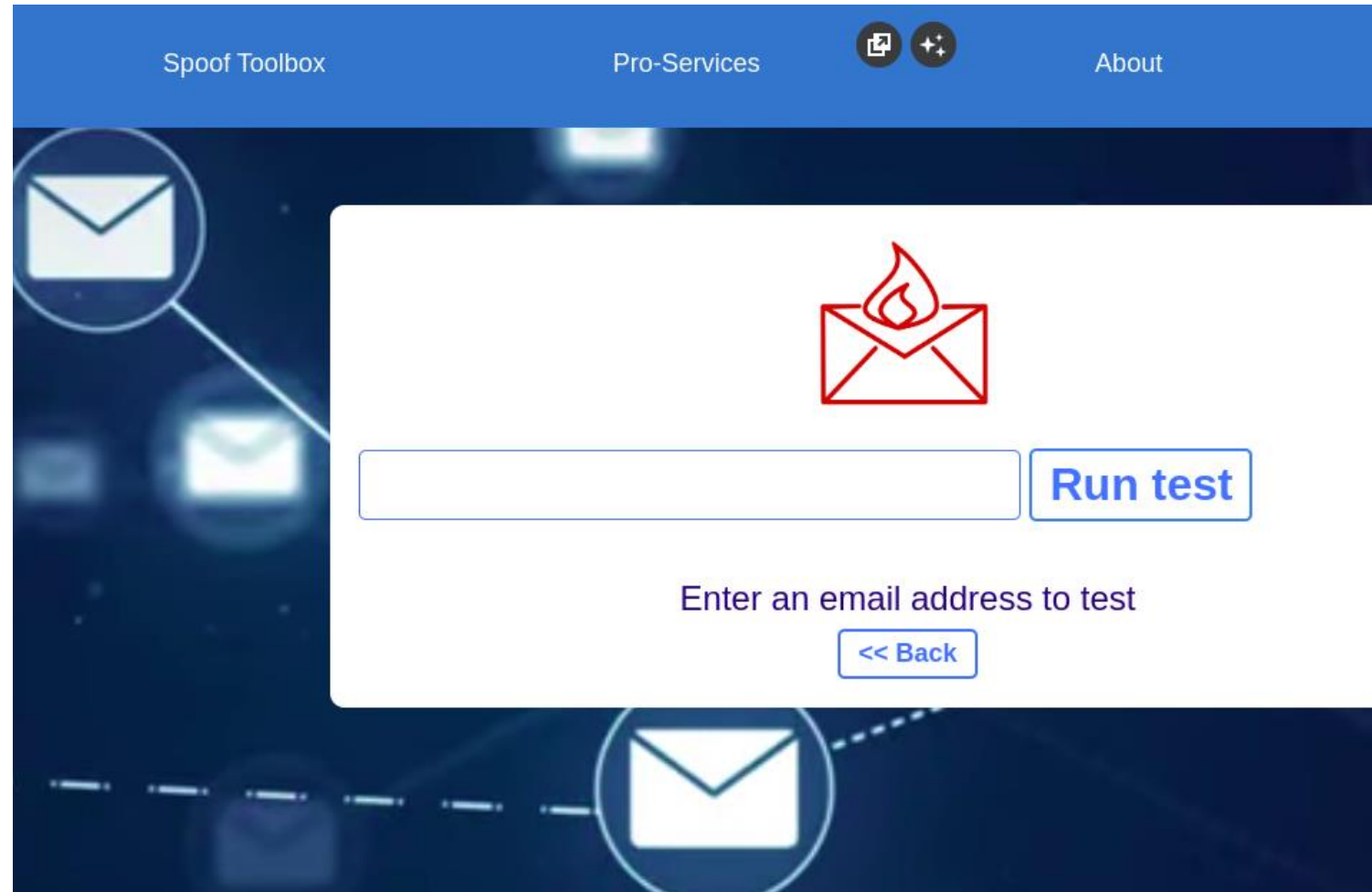
<https://emailspooftest.com>



The screenshot displays the Edufort Cybersecurity Center interface. On the left, a sidebar shows navigation options: 'CYBERSECURITY CENTER', 'CC.01: Gelekte accounts', and 'CC.02: Email security' (highlighted in green). The main content area is titled 'EMAIL VEILIGHEID' and includes a blue envelope icon. Below this, there is a section for 'EMAIL SECURITY' with the status 'Edufort beschermt'. It prompts the user to 'Laat de Edufort email security tool jouw omgeving testen!' and provides an input field for an email address, which contains 'j.grunwald@fourtop.nl'. A green button labeled 'Test mijn email security' is positioned below the input field. To the right, a 'BESCHERMING VOOR MAIL' section explains that Edufort tests email security and provides a list of email titles under the 'KRITIEK' tab, including 'E-mail van een domein dat alle e-mail afwijst maar geen DMARC-beleid gedefinieerd' and 'E-mail van een domein dat niet bestaat is afgeleverd in de inbox'. At the bottom, the 'EDUFORT PHISH SHIELD' section is visible, featuring a red 'X' icon and the text 'Microsoft 365 Phish detect' and 'Detecteer wanneer iemand een kopie van je Microsoft 365 loginpagina maakt om gevoelige informatie te stelen.'

# Hoe is jullie Email security?

- Vul je eigen mail adres in  
En kijk met me mee



# De email security test

— Wat kwam er binnen?

## E9

Iedereen kan uit jouw naam en domeinnaam mail versturen, ook naar jouw medewerkers

## E10

Iedereen kan vanuit niet bestaande e mailadressen mail naar jou versturen. Bijvoorbeeld Sivon.eu, of kennis.net



# Risico: Phishing

— Cybercriminelen komen vaak binnen met phishing

Risico's Voeg risico toe

REF.	RISICO	KANS	IMPACT	EIGENAAR	CONTROLS
29	parnassys export gedeeld met @home adres	very high	very high	Joost Grunwald	
30	<p><b>Titel:</b> Phishing</p> <p><b>Uitleg:</b></p> <p>Met (slimme) phishing wachtwoorden stelen en binnenkomen binnen onze stichting en gevoelige leerlinggegevens stel</p> <p><b>Events:</b></p> <p><b>Oorzaken:</b></p> <p>Voor mensen is het erg moeilijk om phishing door te hebben, vooral met overvullende mailboxes, phishing is nooit een menselijke fout, maar een technische</p> <p><b>Consequenties:</b></p> <p>Het lekken van onze gevoelige data</p> <p><b>Risico inschattingen:</b></p> <div style="display: flex; align-items: center; gap: 5px;"> <div style="width: 20px; height: 10px; background-color: #28a745; border: 1px solid black; border-radius: 5px; display: flex; align-items: center; justify-content: center;">4</div> <div style="width: 20px; height: 10px; background-color: #ffc107; border: 1px solid black; border-radius: 5px; display: flex; align-items: center; justify-content: center;">16</div> <div style="width: 20px; height: 10px; background-color: #dc3545; border: 1px solid black; border-radius: 5px; display: flex; align-items: center; justify-content: center;">20</div> </div>	very high	high	Joost Grunwald	<p><b>MFA</b> <span style="float: right; background-color: #dc3545; color: white; padding: 2px 5px; border-radius: 3px;">high</span></p> <p>Het inzetten van MFA om phishing moeilijker te maken</p> <p style="text-align: center;"></p>



# Risico: Phishing

— Cybercriminelen komen vaak binnen met phishing

Risico's Voeg risico toe

REF.	RISICO	KANS	IMPACT	EIGENAAR	CONTROLS
29	parnassys export gedeeld met @home adres	very high	very high	Joost Grunwald	
30	<p><b>Titel:</b> Phishing</p> <p><b>Uitleg:</b> Met (slimme) phishing wachtwoorden stelen en binnenkomen binnen onze stichting en gevoelige leerlinggegevens stel</p> <p><b>Events:</b></p> <p><b>Oorzaken:</b> Voor mensen is het erg moeilijk om phishing door te hebben, vooral met overvullende mailboxen, phishing is nooit een menselijke fout, maar een technische</p> <p><b>Consequenties:</b> Het lekken van onze gevoelige data</p> <p><b>Risico inschattingen:</b></p> <div style="display: flex; align-items: center; gap: 5px;"> <div style="width: 20px; height: 15px; background-color: #00ff00; border: 1px solid black; border-radius: 5px; display: flex; align-items: center; justify-content: center;">4</div> <div style="width: 20px; height: 15px; background-color: #ffff00; border: 1px solid black; border-radius: 5px; display: flex; align-items: center; justify-content: center;">16</div> <div style="width: 20px; height: 15px; background-color: #ffa500; border: 1px solid black; border-radius: 5px; display: flex; align-items: center; justify-content: center;">20</div> <div style="width: 20px; height: 15px; background-color: #ff0000; border: 1px solid black; border-radius: 5px; display: flex; align-items: center; justify-content: center;">20</div> </div>	very high	high	Joost Grunwald	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><b>MFA</b> <span style="float: right; background-color: #ff0000; color: white; border-radius: 10px; padding: 2px 5px;">high</span></p> <p>Het inzetten van MFA om phishing moeilijker te maken</p> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p><b>Phishing resistente MFA</b> <span style="float: right; background-color: #ffa500; color: white; border-radius: 10px; padding: 2px 5px;">medium</span></p> <p>Het gebruik van MFA die slimme phishing kan tegenhouden</p> </div> <p style="text-align: center;"></p>

# Risico: Phishing

— Cybercriminelen komen vaak binnen met phishing

Risico's [Voeg risico toe](#)

REF.	RISICO	KANS	IMPACT	EIGENAAR	CONTROLS
29	parnassys export gedeeld met @home adres	very high	very high	Joost Grunwald	
30	<p><b>Titel:</b> Phishing</p> <p><b>Uitleg:</b></p> <p>Met (slimme) phishing wachtwoorden stelen en binnenkomen binnen onze stichting en gevoelige leerlinggegevens stel</p> <p><b>Events:</b></p> <p><b>Oorzaken:</b></p> <p>Voor mensen is het erg moeilijk om phishing door te hebben, vooral met overvullende mailboxen, phishing is nooit een menselijke fout, maar een technische</p> <p><b>Consequenties:</b></p> <p>Het lekken van onze gevoelige data</p> <p><b>Risico inschattingen:</b></p>	very high	high	Joost Grunwald	<p><b>MFA</b> <span>high</span></p> <p>Het inzetten van MFA om phishing moeilijker te maken</p> <p><b>Phishing resistente MFA</b> <span>medium</span></p> <p>Het gebruik van MFA die slimme phishing kan tegenhouden</p> <p><b>SSO Parnassys, passkeys AFAS</b> <span>low</span></p> <p>Voor AFAS gebruik je passkeys, voor Parnassys gebruik je SSO</p> <p><b>Spoofing voorkomen</b> <span>very low</span></p> <p>Voorkom spoofing door SPF, DKIM, DMARC te gebruiken</p> <p></p>



**Joost Grunwald**

[joostgrunwald@edufort.nl](mailto:joostgrunwald@edufort.nl)

06 – 31 52 72 20

**Gerald Rutten**

[geraldrutten@edufort.nl](mailto:geraldrutten@edufort.nl)

06 – 57 33 47 17

# Discussie:

## Cyber dreigingen

- Wie denkt dat hij een A5 licentie of duur Google abonnement nodig heeft om veilig te zijn of aan het normenkader te voldoen?

Wie denkt dat zijn/haar bestuurder onvoldoende kennis heeft van informatiebeveiliging en de risico's?

Wie vind het lastig om naast Beleidsmedewerker ICT ook nog half verantwoordelijk te zijn voor privacy, informatiebeveiliging tot aan defecte laptops?

# Discussie:

## Cyber dreigingen

—○ Wie denkt dat cybercriminelen bij hem/haar niet binnenkomen?

Wie heeft persoonlijk of op zijn werk ervaring met een hack?

Wie vind het normenkader terecht?

# Discussie:

## Cyber dreigingen

—○ Wie vind het normenkader moeilijk qua papierwinkel (beleid en dergelijke)?

Wie vind hun technische veiligheid moeilijk?

Wie vind iets anders nog een grote uitdaging?