



Presentatie Cybersecurity

Door Riemer Brouwer, CISO, december 2025



VOEDSELBANKEN.NL

Oog voor voedsel • Hart voor mensen

Cybersecurity wordt steeds belangrijker omdat hackers steeds gevaarlijker worden

VOORBEELDEN

- Food for the Poor: 50.000 gegevens van klanten en donateurs gestolen (mei 2025)
- San Francisco Food Bank: 60.000 klantgegevens gestolen (feb 2025)
- Central Pennsylvania Food Bank: 20 GB aan data gestolen (okt 2024)

Et cetera

Cybersecurity is geen IT-thema, maar missie-continuïteit:

Systemen niet beschikbaar → Geen uitgifte

Voedselbanken zijn, helaas, een gemakkelijke prooi

1

We zijn allemaal vrijwilliger, waardoor kennis en kunde t.a.v. cybersecurity niet altijd voorhanden is

2

Het IT landschap is versnipperd met veel lokaal gebouwde applicaties die steeds meer in de cloud worden geplaatst

3

Onze systemen bevatten veel privacy gegevens, bijv. van cliënten

4

“Ach, wie zou ons nu willen aanvallen?”

Ruwweg zijn er 4 belangrijke manieren waarop hackers ons kunnen aanvallen

Malware

Combinatie van 'malicious' (kwaadaardig) en software. Bijv. computervirussen



Phishing

Het slachtoffer wordt benaderd via e-mail, sms, instant messaging, sociale media of telefoon om gegevens te stelen



Ransomware

Ransomware versleutelt databestanden van gebruikers, met als doel om deze later te ontsleutelen in ruil voor losgeld



Social Engineering

Het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, of angst



Hackers gaan over het algemeen niet specifiek naar ons op zoek, we zijn helaas 'slechts' bijvangst

Ransomware

Ransomware versleutelt databestanden van gebruikers, met als doel om deze later te ontsleutelen in ruil voor losgeld



Hacker begint met hacken

Geheel automatisch

IP adres 1, dan adres 2, dan adres 3....enz.

De hacker stuit op een onbeschermd systeem!

Dan start een volgend programma om daadwerkelijk binnen te komen



Zo ja

Pas dan komt de hacker zelf kijken

Het gaat bij ransomware aanvallen om geld: hoe kun je slachtoffers het meest 'efficiënt' afpersen



Ransomware versleutelt databestanden van gebruikers, met als doel om deze later te ontsleutelen in ruil voor losgeld



Twee scenario's:

1. De hacker versleutelt je gegevens en je moet betalen om weer bij je gegevens te kunnen
 - Bij grote organisaties erg effectief want die kunnen niet snel alles weer terugzetten.
 - Bij de gemiddelde voedselbank niet een probleem want je zet gewoon je backup terug
2. De hacker steelt je gegevens en dreigt met publicatie
 - Dit scenario ligt meer voor de hand bij Voedselbanken: de hacker speelt in op schaamte van onze cliënten en bescheidenheid van donoren

Cybersecurity beschermt onze missie: uitgiftezekerheid en vertrouwen staan centraal

Als één lokale Voedselbank wordt gehacked, straalt dat af op alle voedselbanken

Drie zaken zijn daarom in ons ecosysteem van wezenlijk belang om te beschermen:

- De uitgifte van voedsel
- De privacy van onze cliënten
- De privacy van onze donoren

Onze kerntaken en afhankelijkheden maken duidelijk wat we écht moeten beschermen



Geen NIS2-plicht, wél NIS2-inspiratie: zo versterken we onze basis

NIS2 samengevat

1

Zorg voor een informatiebeveiligingsbeleid en heb de cybergovernance op orde

2

Heb je leveranciers en ketenrisico's in beeld en onder controle

3

Detecteer incidenten tijdig en acteer snel volgens een draaiboek

1. Gebruik veilige wachtwoorden

- Probeer lange wachtwoorden te gebruiken: hoe langer een wachtwoord, hoe moeilijker hackers dit kunnen raden.
- Een simpele truc is om een zin te nemen als wachtwoord, bijv.
Spruitjeszijnlekker!
- Deze zin is gemakkelijk te onthouden, maar erg lastig om te raden voor hackers.
- Zorg ook dat je verschillende wachtwoorden gebruikt voor verschillende applicaties.
- Vaak kan je wachtwoorden opslaan op je computer. Erg gemakkelijk en aan te raden...maar let op: doe dit alleen als je de computer niet deelt met anderen.



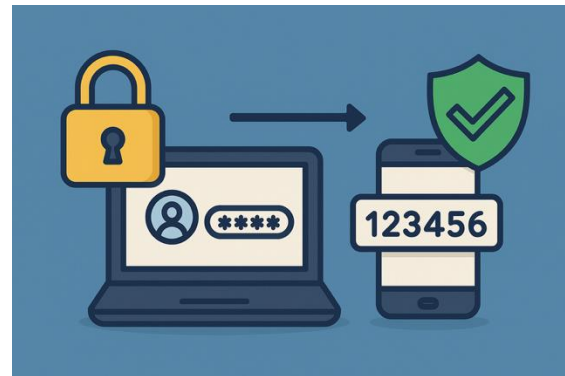
2. Maak regelmatig backups

- Bewaar documenten van de Voedselbank niet alleen op je eigen PC.
- Want stel dat je PC het begeeft, dan ben je al je documenten kwijt.
- Zorg dus voor backups.
- Je kunt backups op verschillende manieren maken:
 - op een USB stick of USB harde schijf
 - een kopie neerzetten in je Google Drive of Microsoft Drive
 - In sommige gevallen: door een kopie op te slaan op de systemen van je voedselbank. Check bij de IT beheerder of dit van toepassing is bij jouw voedselbank



3. Gebruik Twee-Factor Authenticatie

- Twee-Factor Authenticatie (2FA, ook wel MFA genoemd) houdt in dat je bijv. een code krijgt die je extra moet invullen naast je wachtwoord.
- Tegenwoordig ontvang je deze code meestal via een app op je telefoon. Microsoft Authenticator is een bekende app die hiervoor wordt gebruikt: je logt in met je gebruikersnaam en wachtwoord, opent vervolgens de app en vult de code in.
- Dit beschermt je tegen hackers, want als die proberen in te loggen dan komen ze niet verder omdat de code alleen naar jou wordt gestuurd.



4. Gebruik versleuteling indien mogelijk

- Versleuteling, ook wel encryptie genoemd, helpt om de gegevens te beschermen.
- Werk je bijv. op je eigen PC, dan kun je BitLocker activeren. Hiermee versleutelt Microsoft de gehele harde schijf zonder dat je er last van hebt.
- Mocht een hacker onverhoopt bij de PC kunnen, dan is de data versleuteld en dus onbruikbaar.
- Ook de applicaties die je gebruikt voor je Voedselbank, bijv. een financieel pakket, hebben meestal opties om versleuteling aan te zetten. De IT beheerder kan je daarbij helpen.



5. Let op de privacy

- De AVG is voor Voedselbanken van groot belang omdat we vaak veel persoonlijke gegevens hebben van onze cliënten en sponsors.
- Voedselbanken Nederland is bezig om een Handreiking AVG op te stellen.
- Zodra deze gereed is, zal de Handreiking worden verspreid onder de Voedselbanken
- Tot het zover is, kun je alvast nadenken over hoe je omgaat met persoonlijke gegevens: zijn deze goed beschermd zodat onbevoegden geen toegang hebben?



6. Stel een calamiteitenplan op

- Stel, je raakt toch je gegevens kwijt of ze worden publiekelijk bekend, wat dan?
- Een calamiteitenplan kan hierbij helpen.
- Het Plan bevat stappen en acties die je kunt nemen om de schade te beperken.
- Daarnaast maakt het Plan duidelijk wie welke acties dient te nemen.
- Voedselbanken Nederland zal een voorbeeld opstellen van een Calamiteitenplan dat je kunt aanpassen aan de situatie van jouw Voedselbank.



7. Zorg dat oude gegevens veilig worden verwijderd

- Bepaal hoe lang je gegevens van bijv. voormalige cliënten wilt bewaren.
- Immers, niet alles hoeft tot in het oneindige in het systeem te zijn vastgelegd.
- Het is daarom goed om hierover met elkaar afspraken te maken: vanaf wanneer worden oude en verouderde gegevens verwijderd uit de systemen?
- Vanuit de AVG is dit overigens ook vereist.



8. Schenk aandacht aan de fysieke beveiliging

- De fysieke beveiliging heeft betrekking op zaken als prints die je maakt.
- Voedselbanken gebruiken soms uitgeprinte overzichten met cliëntgegevens tijdens de uitdeling van voedsel.
- Let er op dat je dergelijke prints zorgvuldig vernietigt en niet zomaar bij het oud papier legt.
- Hetzelfde geldt voor uitgeprinte notulen, financiële overzichten, et cetera.



9. Draag kennis en ervaring over aan anderen

- Cybersecurity heeft betrekking op het beschermen van informatie.
- Veel van die informatie bestaat uit kennis en opgedane ervaring.
- Zorg dat je Voedselbank-collega's jouw taken kunnen overnemen in een noodgeval, bijv. ziekte of een ongeluk.
- Deel informatie en documenten met elkaar.
- Wat helpt is het aanmaken van zogeheten functionele accounts op de systemen.
- Dus bijv. een e-mail adres als 'secretaris@voedselbank.nl' in plaats van je privé email, en waarvan bijv. de voorzitter ook het wachtwoord weet.
- Mocht je dan toch onverhoopt niet beschikbaar zijn, dan kan een ander je taken overnemen.



Naast cybersecurity is privacy ook steeds belangrijker aan het worden met de AVG als wetgevende norm

Rechten van betrokkenen

Organisaties moeten leden informeren over hun rechten met betrekking tot hun persoonlijke gegevens, zoals het recht op toegang tot hun gegevens, het recht om gegevens te corrigeren of te verwijderen

Gegevensbescherming

Organisaties moeten zorgen voor adequate beveiligingsmaatregelen om persoonlijke gegevens te beschermen tegen ongeautoriseerde toegang, verlies, diefstal of misbruik.

Privacy Beleid

Doelbeperking

Organisaties mogen persoonlijke gegevens alleen verzamelen en gebruiken voor specifieke, gerechtvaardigde doeleinden die aan de leden zijn gecommuniceerd.

Toestemming en transparantie

Organisaties moeten de privacy-rechten van hun leden respecteren. Ze moeten duidelijk communiceren welke persoonlijke gegevens worden verzameld, waarvoor ze worden gebruikt en met wie ze kunnen worden gedeeld.

Gegevensuitwisseling

Als Organisaties persoonlijke gegevens delen met derde partijen, moeten ze ervoor zorgen dat deze partijen voldoen aan de privacywetgeving en passende beveiligingsmaatregelen treffen om de gegevens te beschermen.

Voedselbanken NL zoekt naar manieren om de lokale organisaties te ondersteunen met security en privacy

Advisering

- Webinars en lezingen
- “Help Desk” voor het beantwoorden van ad hoc vragen
- Trainingsprogramma voor medewerkers

Documentatie

- Cybersecuritybeleid
- Cybersecurity policies
- Incidentresponsplan
- Privacy beleid



20