

# VEILIG DIGITAAL MAGAZINE



In dit magazine zijn artikelen bijeengebracht welke onder andere in een eerder stadium zijn gepubliceerd op de website [veiligdigitaal.com](http://veiligdigitaal.com)

Dit magazine verschijnt met onregelmatige tussenpozen meerdere keren per jaar.



# Polymorfe Malware: De Veranderende Dreiging

Polymorfe malware is een type schadelijke software die zijn code of uiterlijk voortdurend verandert om detectie door traditionele antivirusprogramma's te ontwijken. Hoewel de kernfunctionaliteit van de malware hetzelfde blijft, maakt deze constante verandering het moeilijk voor beveiligingssoftware om de malware te herkennen en te blokkeren.

Deze geavanceerde vorm van malware gebruikt technieken zoals code-obfuscatie, encryptie en het herschikken van instructies om bij elke uitvoering of verspreiding een unieke vorm aan te nemen. Dit betekent dat traditionele beveiligingsoplossingen, die vaak vertrouwen op bekende handtekeningen of patronen, moeite hebben om deze malware te detecteren.

VEILIGDIGITAAL.COM





# Wat is Polymorfe Malware?



## Polymorfe Virussen

Deze veranderen hun code of uiterlijk bij elke infectie, waardoor ze moeilijk te herkennen zijn op basis van een statische handtekening.



## Polymorfe Wormen

Vergelijkbaar met virussen, maar wormen kunnen zich zelfstandig verspreiden zonder tussenkomst van de gebruiker.



## Polymorfe Trojaanse Paarden

Deze veranderen hun code of gedrag om detectie te vermijden en doen zich vaak voor als legitieme applicaties.



## Polymorfe Ransomware

Deze past zijn encryptie-algoritmen of communicatiemethoden aan om beveiligingsmaatregelen te omzeilen en succesvol gegevens van slachtoffers te versleutelen.



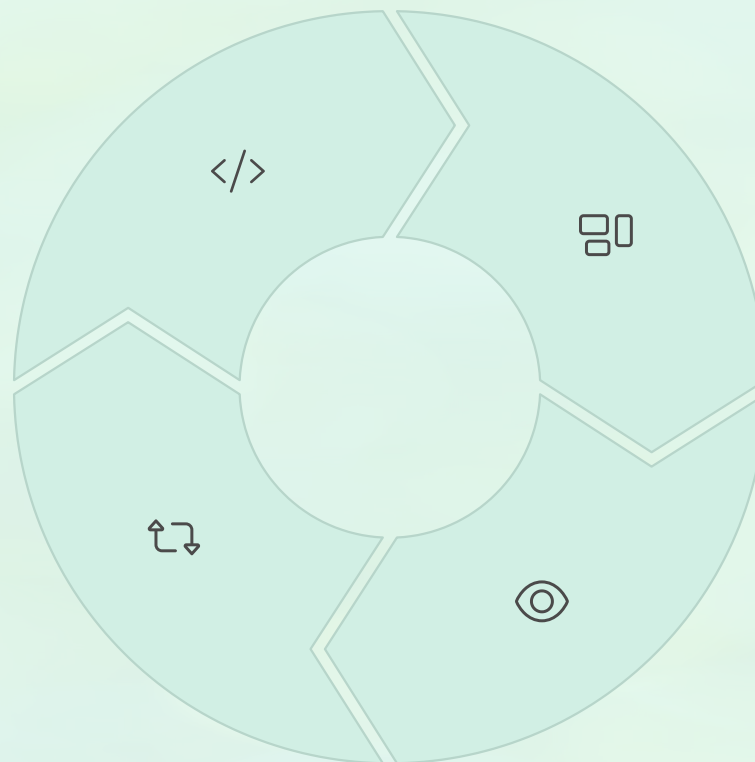
# Hoe Werkt Polymorfe Malware?

## Code-obfuscatie

De malware verbergt zijn schadelijke code door deze te verhullen of te versleutelen

## Herhaalde Aanvallen

De malware blijft zich aanpassen en nieuwe pogingen doen om systemen te infecteren



## Mutatie

Bij elke uitvoering verandert de code structuur terwijl de functionaliteit hetzelfde blijft

## Detectie Ontwijking

Door constant te veranderen ontwijkt de malware herkenning door beveiligingssoftware

Polymorfe malware gebruikt geavanceerde technieken om detectie te vermijden. Door zijn code voortdurend te veranderen, blijft de functionaliteit intact terwijl het uiterlijk wijzigt. Dit maakt traditionele detectiemethoden die op vaste handtekeningen vertrouwen grotendeels ineffectief tegen deze vorm van malware.



# Beschermingsstrategieën



## Geavanceerde Beveiligingssoftware

Kies voor antivirus- en antimalware-oplossingen die gedragsanalyse en heuristische detectie gebruiken, in plaats van alleen op handtekeningen te vertrouwen.



## Software Updates

Regelmatige updates van besturingssystemen en applicaties dichten beveiligingslekken die door malware kunnen worden misbruikt.



## E-mail Voorzichtigheid

Open geen verdachte bijlagen of klik niet op onbekende links, vooral als ze van onbekende afzenders komen.



## Netwerksegmentatie

Door je netwerk op te splitsen in segmenten, kun je de verspreiding van malware beperken als een deel van het netwerk wordt geïnfecteerd.



# Preventieve Maatregelen

## Regelmatige Back-ups

Zorg voor frequente back-ups van belangrijke gegevens, zodat je bij een infectie je gegevens kunt herstellen zonder losgeld te betalen. Bewaar back-ups op een veilige, offline locatie om te voorkomen dat ze ook worden geïnfecteerd.

## Educatie en Bewustwording

Train jezelf en anderen in het herkennen van phishingpogingen en andere veelvoorkomende aanvalsmethoden. Bewustwording is een van de sterkste verdedigingslinies tegen alle vormen van malware.

## Multi-factor Authenticatie

Implementeer waar mogelijk multi-factor authenticatie om een extra beveiligingslaag toe te voegen, zelfs als inloggegevens worden gecompromitteerd door malware-aanvallen.

Preventieve maatregelen vormen een essentieel onderdeel van een effectieve verdedigingsstrategie tegen polymorfe malware. Door proactief te handelen en deze maatregelen te implementeren, kun je het risico op succesvolle aanvallen aanzienlijk verminderen.

# Toekomst van Malwarebestrijding



De toekomst van malwarebestrijding ligt in het gebruik van geavanceerde technologieën zoals kunstmatige intelligentie en machine learning. Deze technologieën kunnen patronen herkennen en afwijkend gedrag detecteren, zelfs wanneer de malware zichzelf voortdurend verandert.

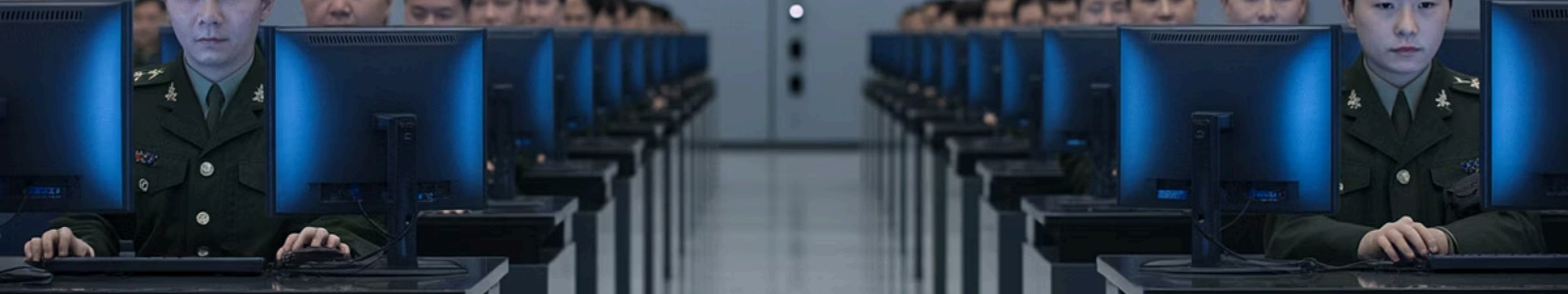
Door te focussen op gedragsanalyse in plaats van statische handtekeningen, kunnen beveiligingssystemen polymorfe malware effectiever bestrijden. Daarnaast wordt collectieve beveiliging steeds belangrijker, waarbij organisaties informatie over bedreigingen delen om samen sterker te staan tegen cyberdreigingen.

# In cybercriminaliteit speelt China op topniveau

China's groeiende rol in wereldwijde cyberdreigingen.







# Het Chinese cyberleger

300K

Staatshackers

Actief in militaire eenheden

25+

Hackgroepen

Door overheid gesponsord

10+

Jaren actief

Groeiende invloed



# Doelwitten van Chinese hackers



## Westerse bedrijven

Diefstal intellectueel eigendom



## Onderzoeksinstellingen

Focus op innovatie en technologie



## Overheidsinstanties

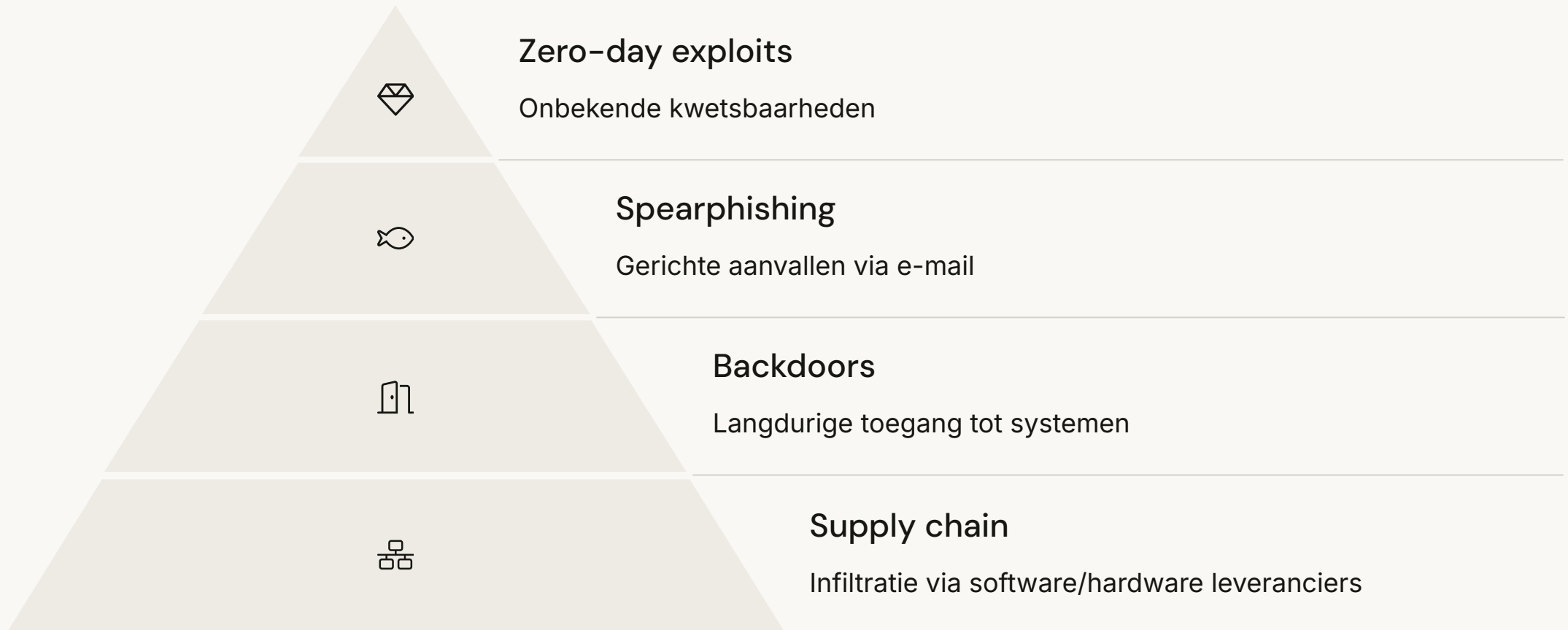
Inlichtingen en geopolitieke voordelen



## Dissidenten

Surveillancedoeleinden

# Strategie en tactieken





# Bekende Chinese hackgroepen



APT1 (Unit 61398)

Militaire eenheid gericht op westerse industrie



APT10 (Stone Panda)

Focus op cloudproviders en intellectueel eigendom

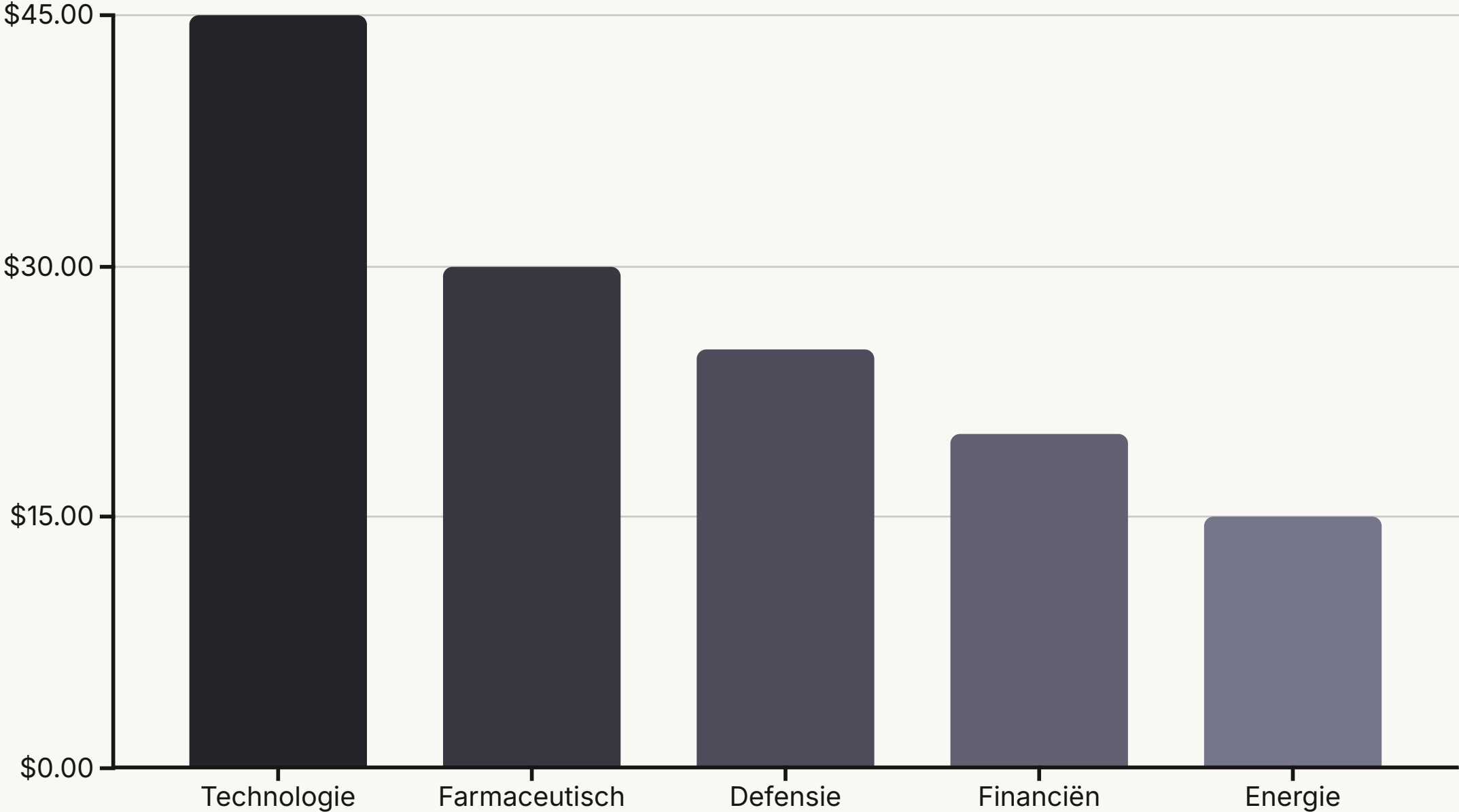


APT41

Combinatie van financiële motieven en spionage



# Economische impact



# Waarom doet China dit:



## Kostenbesparend onderzoek

Miljarden bespaard op R&D door intellectuele eigendomsdiefstal



## Technologische voorsprong

Versnelde ontwikkeling door gestolen innovaties



## Concurrentie voordeel

Chinese bedrijven krijgen voorsprong op internationale markten



## Geopolitieke macht

Toegang tot gevoelige informatie versterkt internationale positie



# Verdedigingsmaatregelen



# Internationale samenwerking

## Informatie-uitwisseling

Delen van threat intelligence tussen landen

## Gemeenschappelijke wetgeving

Harmonisatie van cyber-strafrecht

## Gezamenlijke operaties

Internationaal onderzoek naar aanvallen

## Diplomatieke druk

Sancties tegen Chinese cybercriminelen

# Global Cybersecure Summit.





# Malwaretrucs bij zipbestanden

Hackers ontwikkelen steeds slimmere technieken om malware te verspreiden via zipbestanden. Ze verbergen schadelijke code die vaak door beveiligingssoftware wordt gemist.

Hun trucs variëren van zip-concatenatie tot misleidende bestandsnamen. De gevolgen kunnen verwoestend zijn.

VEILIGDIGITAAL.COM

# Hoe hackers zipbestanden misbruiken



## Zip-concatenatie

Meerdere archieven samengevoegd met verborgen malware.



## Misleidende bestandsnamen

"Invoice.zip" of "rapport.pdf.exe.zip" lokken slachtoffers.



## Wachtwoordbeveiliging

Omzeilt antivirussoftware door scannen te blokkeren.



## Archive bombs

Crasht systemen met extreem grote uitgepakte bestanden.





# Hoe kun jij je beschermen tegen zip-malware

Effectieve verdediging begint met waakzaamheid en goede gewoonten.



## Let op de bron

Download alleen bestanden van vertrouwde websites.  
Wees kritisch bij e-mailbijlagen.



## Houd software up-to-date

Werk je antivirusprogramma en besturingssysteem regelmatig bij voor optimale bescherming.



## Scan voor opening

Controleer zipbestanden altijd met beveiligingssoftware voordat je ze opent.



## Wees voorzichtig met wachtwoorden

Open nooit wachtwoordbeveiligde zipbestanden van onbekende afzenders.



# Welke nieuwe archiefaanvallen verwachten we?

De toekomst brengt geavanceerde bedreigingen die onze huidige verdediging omzeilen.

## AI-gestuurde exploits

Kunstmatige intelligentie helpt hackers kwetsbaarheden automatisch te ontdekken in archiveringsformaten.

## Polymorfe archiefmalware

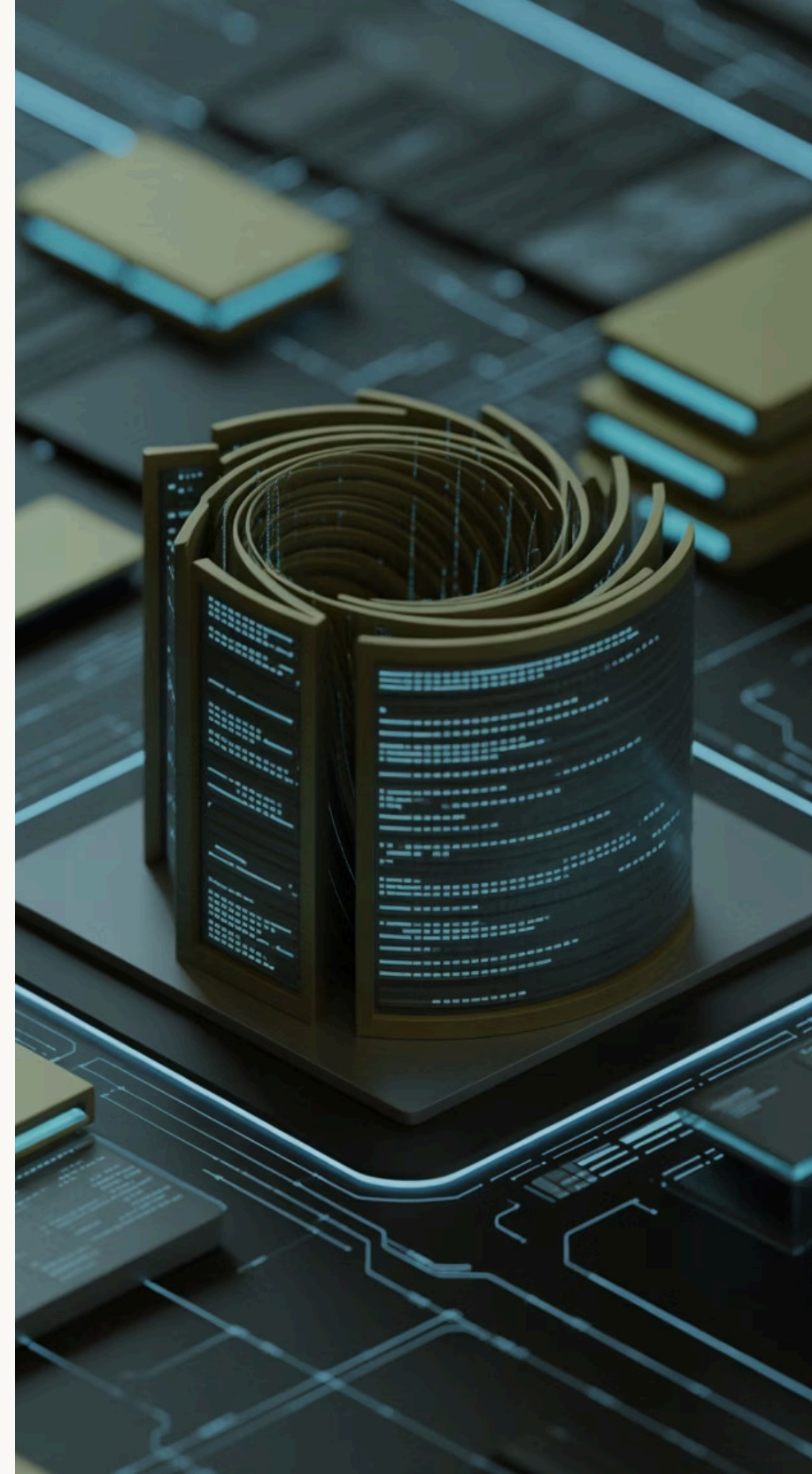
Bestanden die zichzelf aanpassen na detectie om beveiliging te omzeilen.

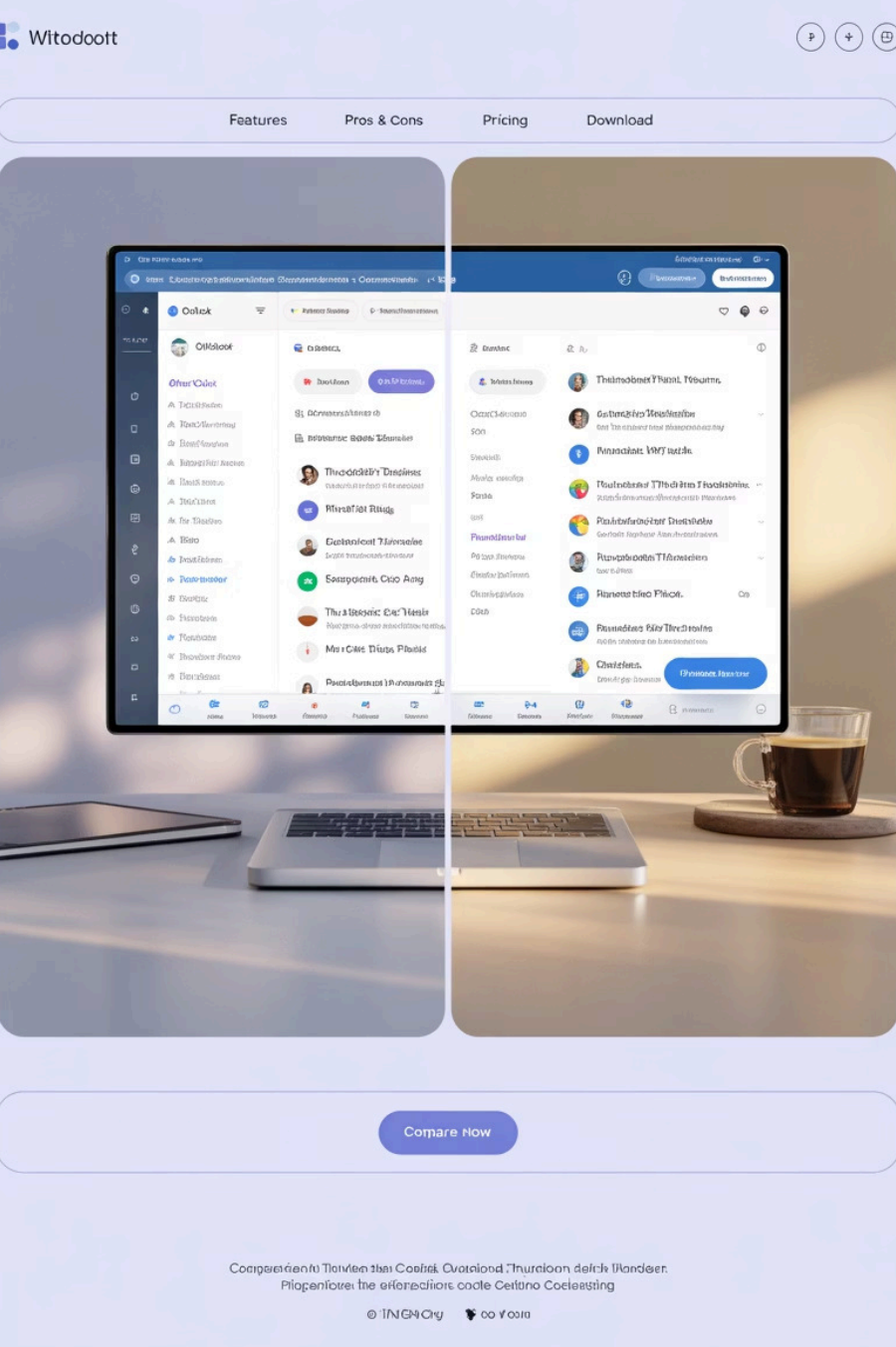
## Hybride encryptieaanvallen

Combinatie van legitieme en kwaadaardige encryptie maakt detectie bijna onmogelijk.

## Cross-format exploits

Malware die tussen verschillende archiefformaten kan springen en samenwerken.





# Microsoft Outlook vs Mozilla Thunderbird

E-mailclients zijn essentieel voor zowel particulieren als bedrijven. Ze verschillen op belangrijke punten.

Dit artikel vergelijkt de meest gebruikte opties: Microsoft Outlook en Mozilla Thunderbird.

We kijken naar functionaliteit, gebruiksgemak en kosten. Zo kunt u een weloverwogen keuze maken.

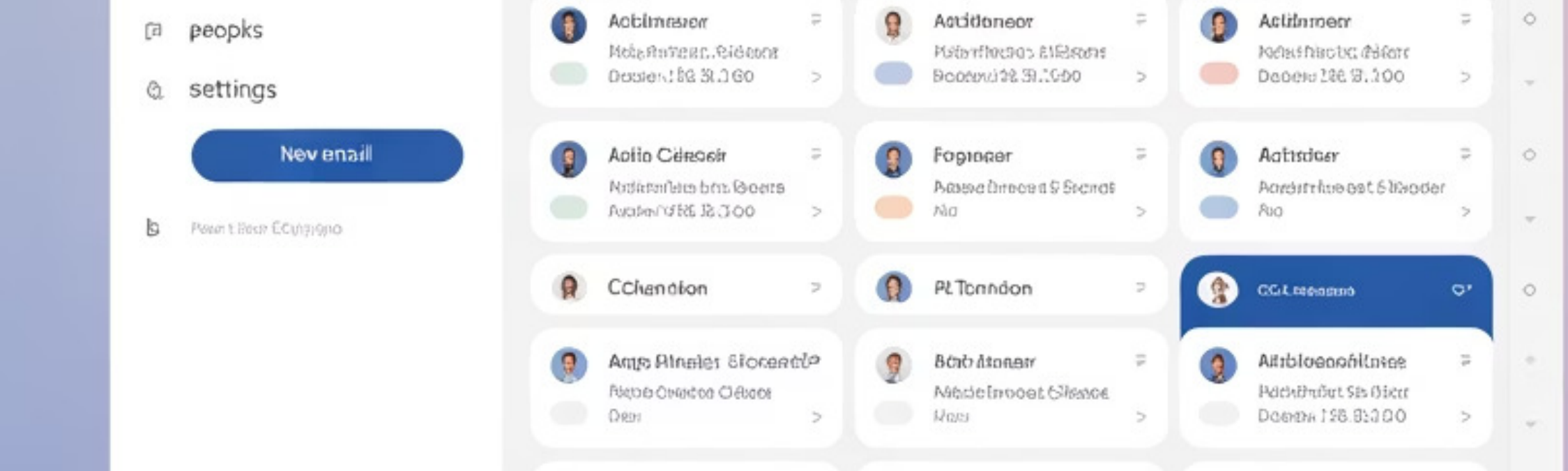
VEILIGDIGITAAL.COM

Compare Now

Copyright © 2019 Veilig Digitaal. All rights reserved. Privacy Policy

© INGENIUM





# Overzicht: Microsoft Outlook

## Integratie

Naadloos verbonden met Office 365 en Microsoft Exchange. Werkt perfect samen binnen het ecosysteem.

## Platformen

Beschikbaar op Windows, macOS, iOS en Android. Consistente ervaring op alle apparaten.

## Functionaliteit

Uitgebreide agenda, taakbeheer en contactpersonen. Alles-in-één oplossing voor productiviteit.



# Overzicht: Mozilla Thunderbird



## Open-source

Gratis en transparante code. Gedreven door community-ontwikkelaars.



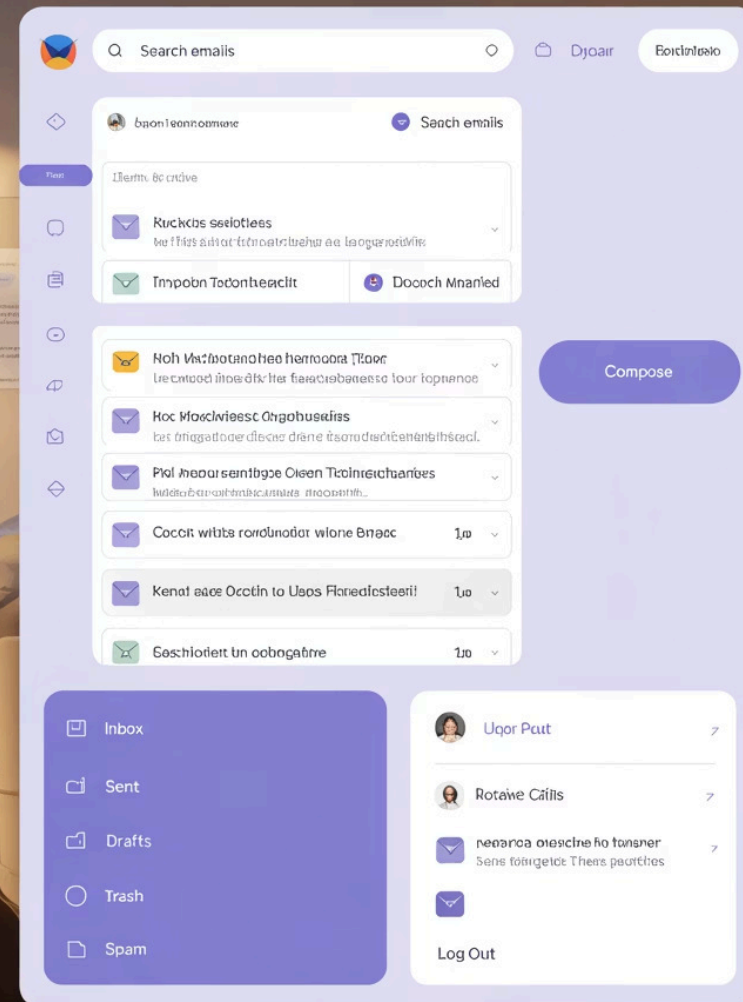
## Multi-platform

Werkt op Windows, macOS en Linux. Flexibel voor verschillende gebruikers.



## Uitbreidbaar

Eenvoudig aan te passen met add-ons. Personaliseer naar eigen wensen.



# Belangrijkste Verschillen

## Microsoft Outlook

- Betaalde software
- Moderne interface
- Ingebouwde agenda
- Global Address List

## Mozilla Thunderbird

- Gratis te gebruiken
- Klassieke interface
- Beperkte agendafunctie
- Standaard e-mailprotocollen



# Voordelen van Microsoft Outlook



## Geavanceerde beveiliging

Robuuste spamfilters, firewall-integratie en antivirusbescherming houden uw inbox veilig.



## Microsoft-integratie

Werkt naadloos samen met Word, Excel, Teams en andere Microsoft-apps.



## Offline toegang

Cached Exchange Mode zorgt voor toegang tot e-mails, zelfs zonder internetverbinding.



# Voordelen van Mozilla Thunderbird



## Kostenbesparing

Volledig gratis en open-source. Geen licentiekosten of abonnementen nodig.



## Aanpasbaarheid

Uitgebreide collectie add-ons en thema's. Pas de client aan naar wens.



## Lichtgewicht

Snelle opstartijd en lage systeemeisen. Werkt ook op oudere computers.

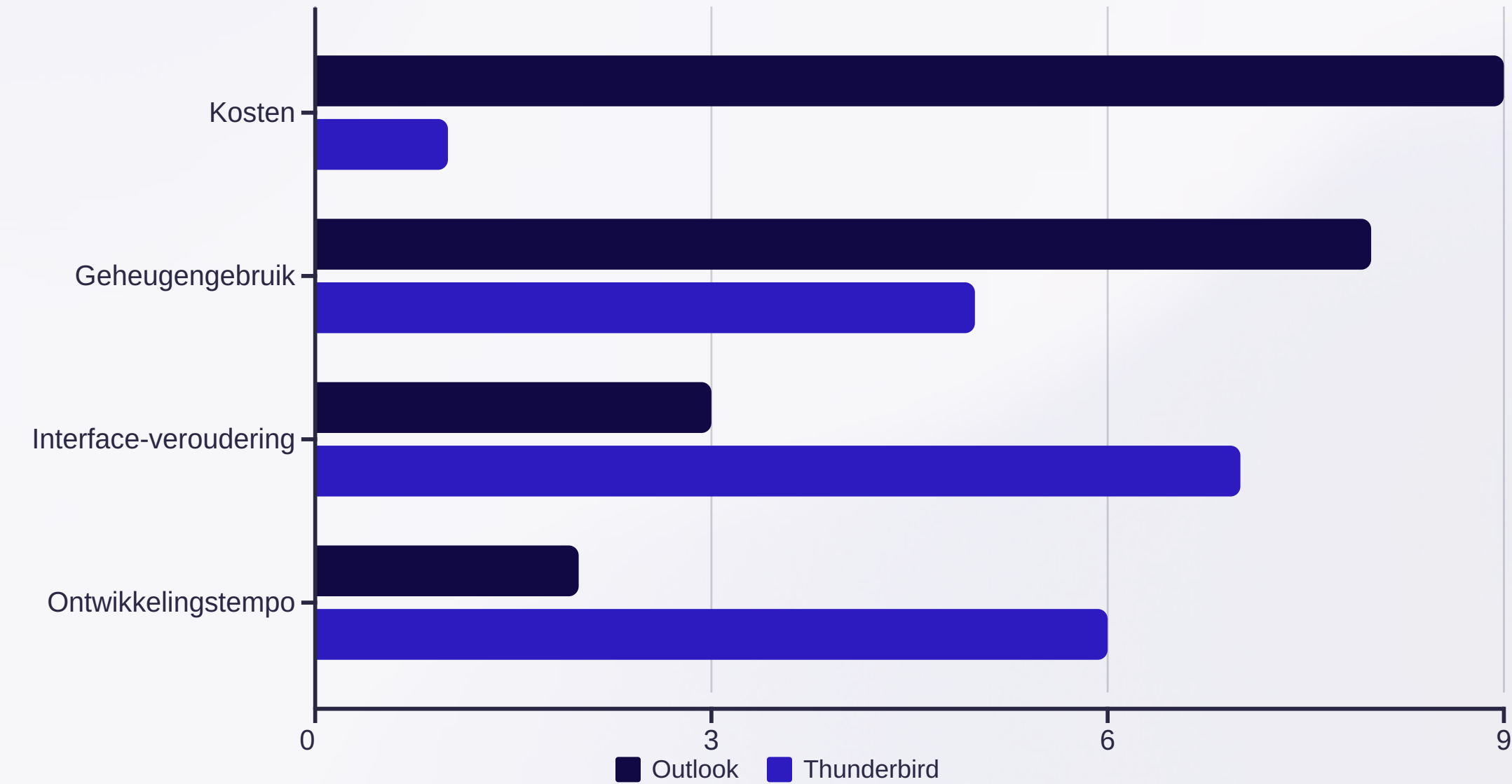


## Multi-account beheer

Eenvoudig beheer van meerdere e-mailaccounts in één overzicht.



# Nadelen van Beide Clients



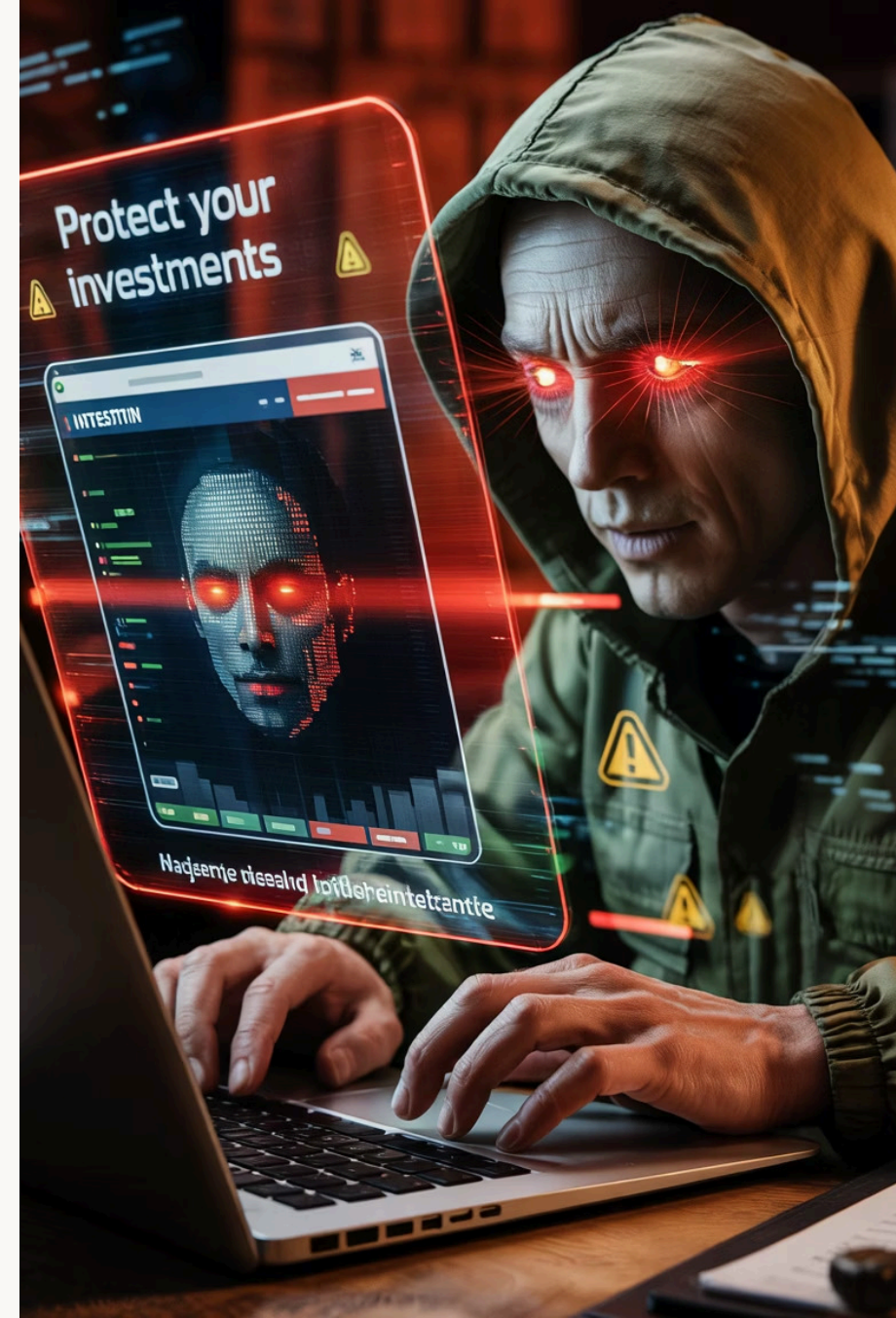
# Conclusie en Aanbevelingen



# Online Investeringsfraude: Een Alarmerend Onderzoek

Nieuwe inzichten tonen aan hoe cybercriminelen geavanceerde technieken gebruiken om nietsvermoedende internetgebruikers op te lichten.

Het recente onderzoek van Infoblox Threat Intel laat zien dat beide criminele netwerken gebruikmaken van zogenaamde Registered Domain Generation Algoritmes (RDGA). Deze technologie stelt hen in staat razendsnel duizenden domeinen te registreren, wat het bijzonder moeilijk maakt voor securitysystemen om alle frauduleuze websites te blokkeren.



# De Harde Cijfers

## 5.7 miljard 2

Dollar Verloren

Alleen al in de VS in 2024

Criminele Netwerken

Reckless en Ruthless Rabbit

## 1000+

Valse Domeinen

Dagelijks geregistreerd

De slachtoffers zijn vaak geen onvoorzichtige mensen. Ze zoeken juist naar financiële zekerheid voor hun toekomst.







# De Reckless Rabbit Methode



## Facebook Advertenties

Gerichte misleidende advertenties lokken potentiële slachtoffers.



## Misbruik van Beroemdheden

Vervalste aanbevelingen wekken vertrouwen bij slachtoffers.



## Internationale Aanpak

Lokale taal en context maken oplichting geloofwaardiger.



## Detectie Vermijden

Wildcard DNS-responsen maken subdomeinen moeilijk traceerbaar.

# De Ruthless Rabbit Technieken

## Cloaking-dienst

Filtert securityonderzoekers om  
onder de radar te blijven

## Dynamische URL's

Constant veranderende webadres-  
paden bemoeilijken opsporing



## Nabootsen van websites

Lokale nieuwssites en bekende  
merken worden geïmiteerd

## Oost-Europese focus

Gerichte aanvallen op specifieke  
landen

# Bescherm Jezelf

Your digital safety, simplified.



## Bescherm Jezelf



### Controleer altijd

Zoek onafhankelijke informatie over investeringsplatforms. Vertrouw niet op één bron.



### Wees voorzichtig met urgentie

Criminelen creëren tijdsdruk. Neem altijd de tijd om na te denken.



### Te mooi om waar te zijn?

Onrealistische rendementen zijn vaak een waarschuwingsteken. Wees realistisch.



### Meld verdachte activiteiten

Help anderen door fraude te melden bij de Fraudehelpdesk.

Het succes van deze fraudevormen is een combinatie van chaos en vertrouwen. In tijden van economische onzekerheid zijn mensen vatbaarder voor de belofte van snelle financiële winst. De criminelen spelen hier handig op in door een gevoel van urgentie te creëren en tegelijkertijd vertrouwen te wekken via bekende gezichten en merken.



# Passkeys: De Toekomst van Inloggen

Passkeys vervangen traditionele wachtwoorden met veiligere cryptografische sleutels. Ze zijn ontwikkeld door grote techbedrijven als reactie op inlogproblemen.

Maar liefst 62% van de volwassenen ervaart regelmatig problemen met hun wachtwoorden.

VEILIGDIGITAAL.COM





# Wat zijn Passkeys?



## **Cryptografische Sleutels**

Ze vervangen traditionele wachtwoorden met een sterker alternatief.



## **Biometrische Toegang**

Inloggen via vingerafdruk of gezichtsherkenning in plaats van typen.



## **Asymmetrische Cryptografie**

Gebaseerd op publieke en privé sleutelparen voor optimale beveiliging.



# Hoe Werken Passkeys?



## **Sleutelgeneratie**

Bij aanmaken worden twee cryptografische sleutels gegenereerd.

2

## **Verificatie**

Authenticatie via biometrische gegevens van je apparaat.



## **Beveiliging**

Unieke sleutels worden gebruikt voor elke inlogpoging.



## **Synchronisatie**

Automatische synchronisatie tussen je apparaten.

# Voordelen van Passkeys



## **Superieure Beveiliging**

Bescherming tegen phishing, hacking en keyloggers.



## **Anti-Social Engineering**

Beschermd tegen manipulatieve aanvallen.



## **Niets Onthouden**

Geen wachtwoorden om te beheren of te vergeten.



## **Snelle Toegang**

Eenvoudige en razendsnel inloggen op websites en apps.

UniTouch



# Nadelen van Passkeys

## **Beperkte Ondersteuning**

Nog niet door alle websites en diensten ondersteund.  
Adoptie groeit langzaam.

## **Apparaatafhankelijkheid**

Werkt alleen op compatibele apparaten. Oude systemen blijven buiten bereik.

## **Herstelproblemen**

Uitdagingen bij verlies of defect van je primaire apparaat.

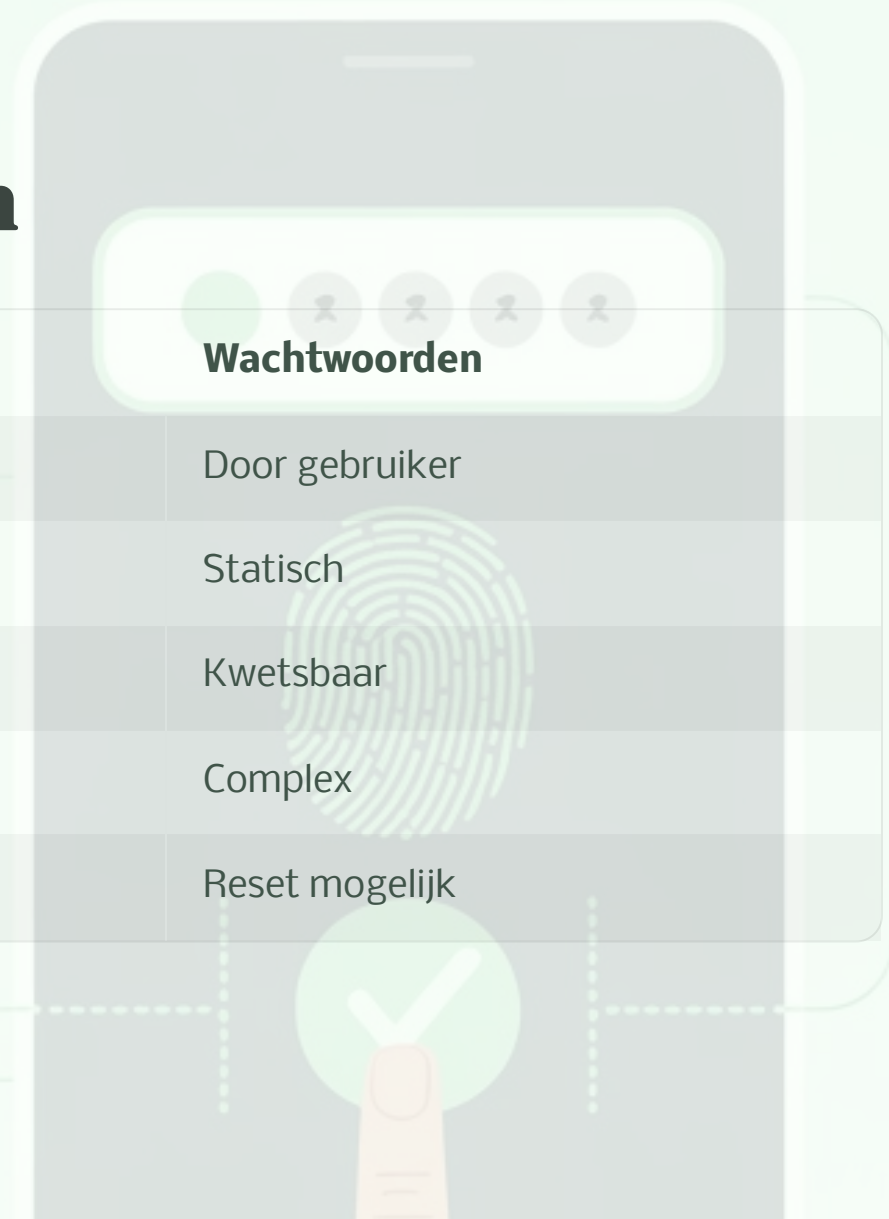
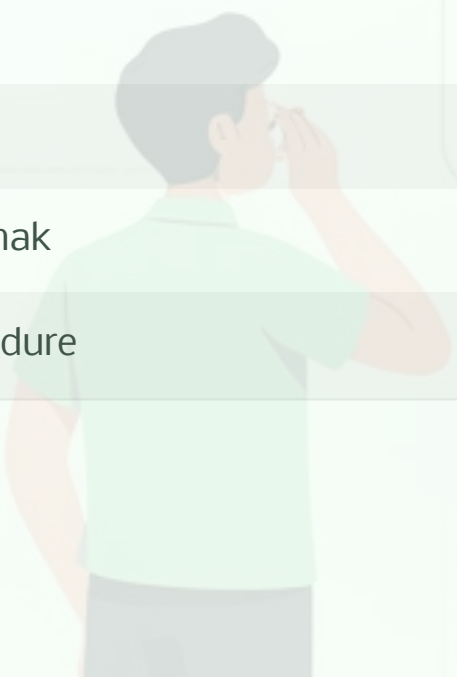
## **Overgangsuitdagingen**

Lastige periode waarin beide systemen naast elkaar bestaan.



# Passkeys vs. Wachtwoorden

| Aspect           | Passkeys         | Wachtwoorden   |
|------------------|------------------|----------------|
| Generatie        | Automatisch      | Door gebruiker |
| Aard             | Cryptografisch   | Statisch       |
| Phishing         | Bestand tegen    | Kwetsbaar      |
| Gebruiksgemak    | Eenvoudig        | Complex        |
| Herstelprocedure | Apparaatgebonden | Reset mogelijk |



# Hoe Implementeer Je Passkeys?



## **Controleer compatibiliteit**

Verifieer of je apparaten en browsers passkeys ondersteunen.

---



## **Kies ondersteunende diensten**

Gebruik diensten van Google, Apple of Microsoft.

---

3

## **Activeer biometrische authenticatie**

Stel vingerafdruk of gezichtsherkenning in.

---



## **Migreer stapsgewijs**

Schakel geleidelijk over van wachtwoorden naar passkeys.

# De Toekomst van Authenticatie

## Groeiende Adoptie

Steeds meer websites en diensten implementeren passkeys.

## Integratie

Combinatie met andere authenticatiemethoden.



## Gebruiksgemak

Vereenvoudigde toegang zonder wachtwoordstress.

## Verbeterde Beveiliging

Minder kwetsbaar voor datalekage en hacks.



# Sidechannel-Attack

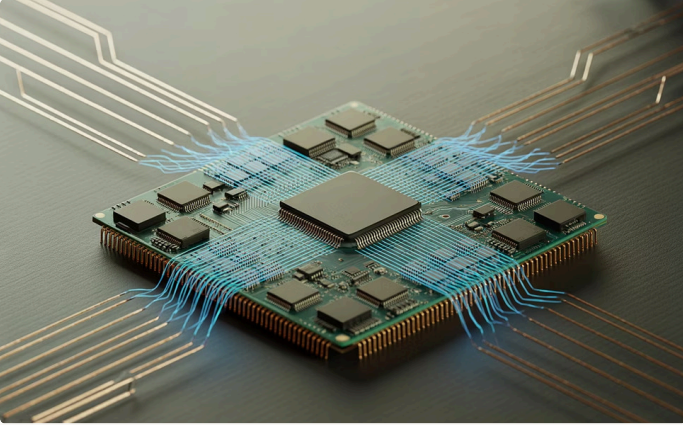
Een sidechannel-attack is een geavanceerde aanvalstechniek die gebruik maakt van onbedoelde informatiekkanalen. Deze techniek richt zich op lekken via fysieke kenmerken, niet via traditionele softwarehacks.

Aanvallers analyseren signalen zoals timing en energieverbruik om gevoelige informatie te onthullen. Dit vormt een groeiende bedreiging voor moderne beveiligingssystemen.

VEILIGDIGITAAL.COM



# Hoe Werken Sidechannel-Aanvallen?



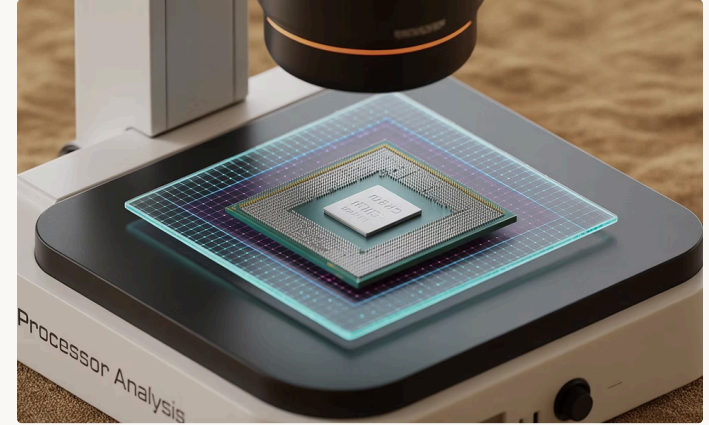
## Analyse van Signalen

Aanvallers bestuderen zorgvuldig externe signalen zoals timing, stroomverbruik en elektromagnetische straling. Deze signalen lekken onbedoeld informatie.



## Indirecte Benadering

Deze aanvallen omzeilen traditionele beveiligingsmaatregelen. Ze breken niet direct in op software of netwerken, wat ze moeilijk detecteerbaar maakt.



## Micro-observatie

Door minuscule gedrag patronen van hardware en software te observeren, kunnen gevoelige gegevens worden gereconstrueerd. Dit vereist geduld en precisie.

# Typen Sidechannel-Aanvallen



## Timing Attacks

Hackers meten minuscule tijdsverschillen in computerprocessen. Deze variaties verraden geheime informatie zoals cryptografische sleutels.



## Power Analysis

Door stroomverbruik van apparaten te analyseren, kunnen aanvallers cryptografische sleutels achterhalen. Populair bij het kraken van betaalkaarten.



## Electromagnetic Attacks

Gevoelige apparatuur vangt elektromagnetische straling op. Hieruit worden datapatronen gereconstrueerd, zelfs op afstand.





# Praktische Voorbeelden

## Spectre & Meltdown (2018)

Deze kwetsbaarheden in moderne CPU's maakten het mogelijk om via timing-kanalen gevoelige gegevens te stelen uit andere programma's. Miljarden apparaten waren getroffen.

## Smartcard Exploits

Aanvallers analyseren het stroomverbruik van betaalkaarten. Ze kunnen zo PIN-codes en encryptiesleutels achterhalen tijdens transacties.

## Router-aanvallen

Door elektromagnetische signalen van routers te onderscheppen, kunnen hackers RSA-sleutels reconstrueren en vertrouwelijke netwerkverkeer ontcijferen.

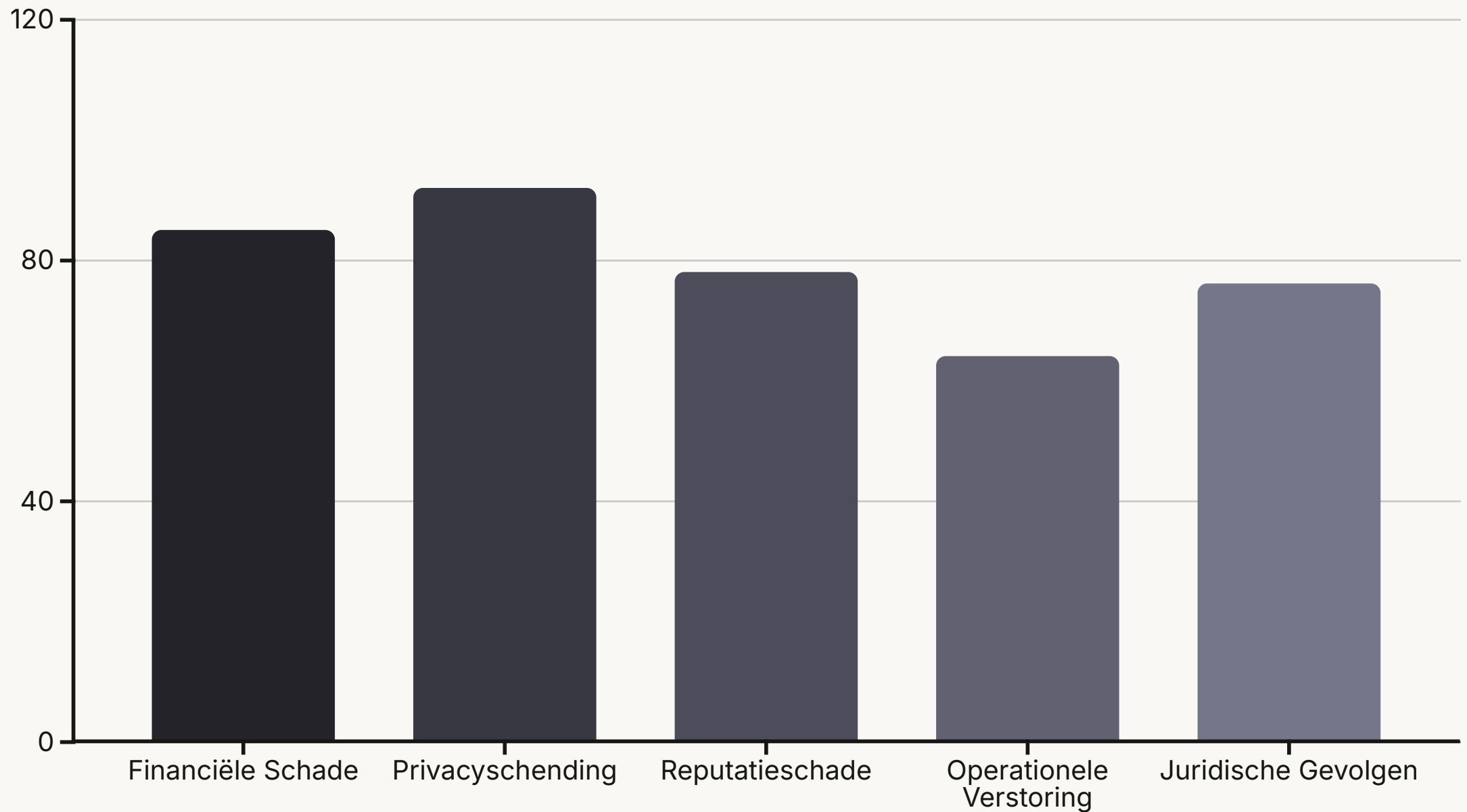


# Zijn Sidechannel-Aanvallen Gevaarlijk?



Het grootste gevaar van sidechannel-aanvallen is hun onzichtbaarheid. Ze exploiteren fysieke eigenschappen die niet worden bewaakt door standaard beveiligingsmaatregelen.

# Risico's voor Organisaties



Sidechannel-aanvallen vormen een ernstige bedreiging voor bedrijven. Ze kunnen leiden tot datalekken, schendingen van de AVG en aanzienlijke imagoschade.



# Recente Incidenten & Onderzoek



## 2022: 'Cacheout' Aanval

Intel-processoren getroffen door nieuwe variant van speculative execution attack. Miljoenen computers potentieel kwetsbaar voor data-extractie.



## 2019: BLEURT Aanval

Onderzoekers van TU Eindhoven ontdekten kwetsbaarheden in IoT-apparaten. Aanvallers konden via elektromagnetische lekken encryptiesleutels stelen.



## 2023: Cloud Risico's

Google publiceerde onderzoeksresultaten over sidechannel-kwetsbaarheden in gedeelde cloud-infrastructuur. Co-tenant aanvallen werden gedemonstreerd.

# Detectie van Sidechannel-Aanvallen



Detectie is uitdagend omdat sidechannel-aanvallen geen traditionele digitale sporen achterlaten. Gespecialiseerde monitoring van hardwaregedrag is essentieel.



# Mitigerende Maatregelen



## Hardware Bescherming

- Elektromagnetische afscherming toepassen
- Randomisatie van timing implementeren
- Energieverbruik homogeniseren



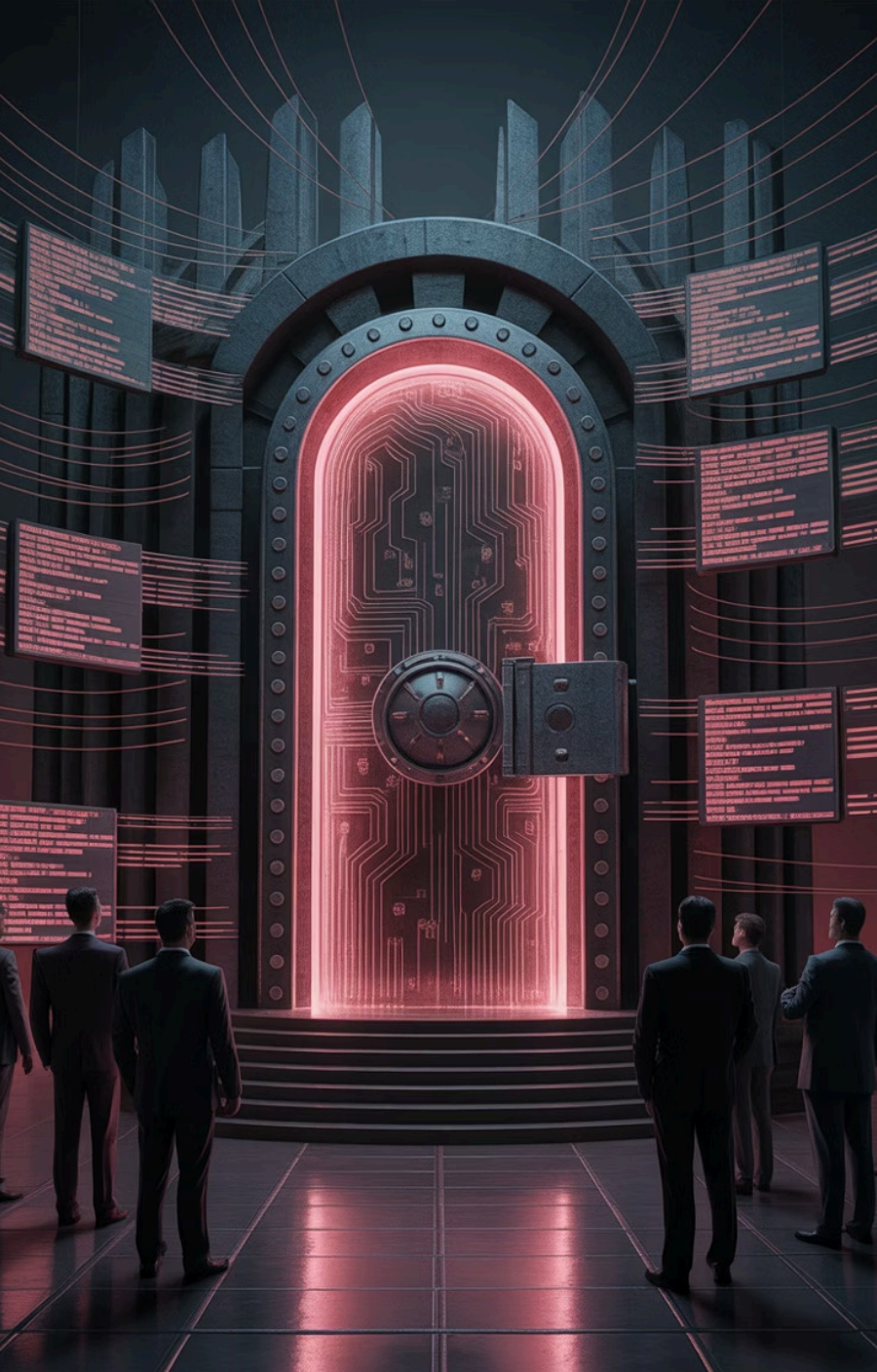
## Software Beveiliging

- Constant-time algoritmes gebruiken
- Generieke foutmeldingen implementeren
- Regelmatige code-audits uitvoeren



## Organisatorische Maatregelen

- Personeel trainen in herkenning
- Beveiligingsbeleid actualiseren
- Incident response plan ontwikkelen



# Conclusie & Aanbevelingen

## Erken de Dreiging

Sidechannel-aanvallen zijn een reëel en groeiend gevaar.  
Onderschat de risico's niet, zelfs als ze technisch complex lijken.

## Implementeer Bescherming

Combineer technische en organisatorische maatregelen. Update hardware en software regelmatig met beveiligingspatches die sidechannel-kwetsbaarheden adresseren.

## Blijf Voorbereid

Investeer in onderzoek, educatie en monitoring. De technieken van aanvallers evolueren voortdurend, dus uw verdediging moet meegroeien.







# Slimme apparaten moet je ook updaten

Het updaten van je slimme apparaten is super belangrijk voor hun werking en veiligheid. Denk aan je router, beveiligingscamera's en slimme verlichting.

Deze apparaten zijn vaak online en kunnen het doelwit worden van cybercriminelen als je ze niet bijhoudt.



# Hou je slimme apparaten slim



## Betere beveiliging

Updates geven je niet alleen nieuwe functies, maar vaak ook betere beveiliging.



## Optimale werking

Zonder updates kunnen je apparaten trager worden of minder goed werken.



## Veilig huis

Regelmatig updaten houdt je huis veilig tegen cyberdreigingen.





# Wat zijn slimme apparaten?

## Wifi-verbinding

Een apparaat is slim als het verbonden is met wifi.

## Risico's

Zonder goede instellingen kunnen cybercriminelen toegang krijgen tot opgeslagen informatie.

## Controle verliezen

Hackers kunnen apparaten op afstand bedienen als ze niet beveiligd zijn.



# Mogelijke gevaren



## Meekijken

Ongewenste toegang tot je webcam of babyfoon.



## Manipulatie

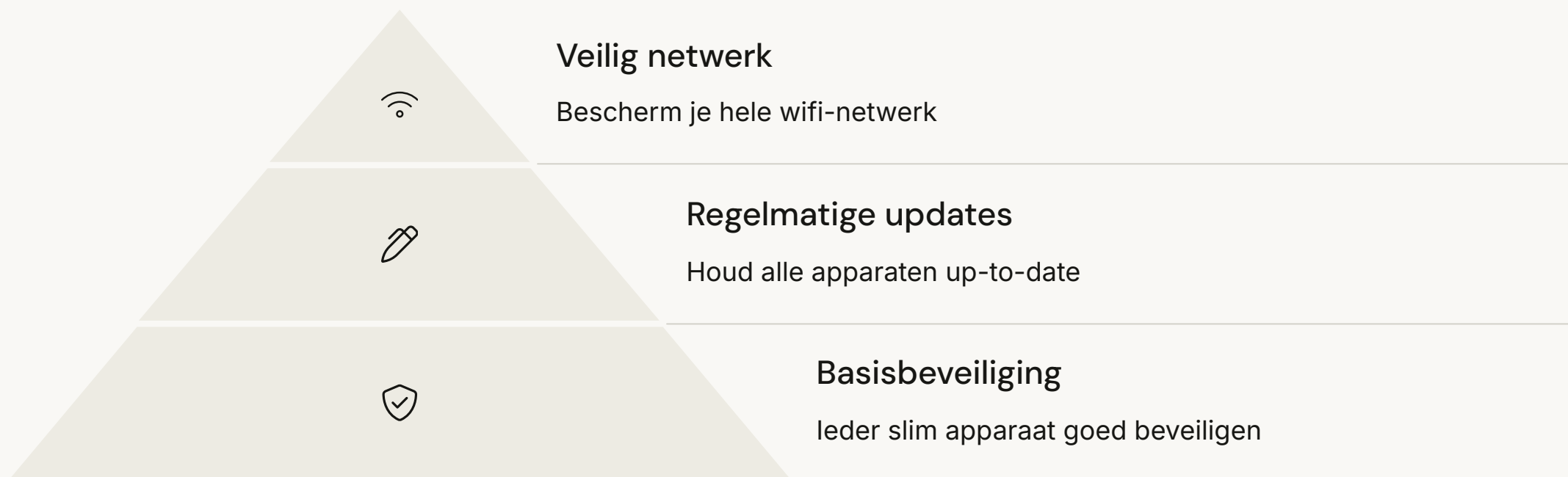
Thermostaat steeds warmer of kouder instellen.



## Ongewenst gebruik

Je wasmachine zomaar aanzetten.

# Netwerk beschermen



Ieder slim apparaat dat verbonden is met het internet moet je goed beveiligen met de laatste updates.