

Altijd een stap voor op phishing- en cyberaanvallen

Als organisatie met **meerdere netwerk-gebruikers** ben je steeds op zoek naar de meest doeltreffende manier om dat netwerk te beschermen, toch?

Jammer genoeg is het niet langer voldoende om alleen een firewall en anti-malware te installeren. Om vindingrijke hackers geen voet tussen de deur te bieden, heb je extra bescherming nodig.

- De belangrijkste tekortkoming van standaard cybersecurityoplossingen, is dat ze niet snel genoeg zijn in het herkennen en blokkeren van **nieuwe bedreigingen**. Ze detecteren de dreiging namelijk pas op het ogenblik dat deze al is binnengekomen op het netwerk.

- Daardoor blijft je netwerk – en dus je bedrijfsgegevens – onbeveiligd tegen bedreigingen die nog maar nét bestaan, maar die je bedrijf aanzienlijk kunnen schaden. Daarnaast is er ook nog de kans op reputatieschade, of dat uw bedrijf tijdelijk niet bereikbaar is door de gevolgen van een aanval op uw netwerk.

Het is dus een kwestie van die **nieuwe gevaren altijd een stap voor** te zijn. Met een extra laag bovenop je bestaande pakket reduceer je mogelijke schade binnen je netwerk tot een minimum. En nu kan dat met een toegankelijke en onmiddellijk geïnstalleerde oplossing van Belgische bodem: Secutec SecureDNS.



We zochten eigenlijk geen extra tool omdat we ons niet bewust waren van het probleem. Na een korte en effectieve test met Secutec SecureDNS, hebben wij ervoor gekozen om deze extra beveiligingslaag aan te brengen.”

Philippe Maquoi, operational security team leader SPW

Welke risico's loop je ondanks je huidige cybersecurity oplossingen?

Cybercrime blijft toenemen en vooral phishing, een 'truc' om data te stelen via malware, wint aan populariteit. Ook het aantal gevallen van ransomware, waarbij cybercriminelen het netwerk van een bedrijf gijzelen in ruil voor losgeld, blijft sterk toenemen. Deze vorm van cybercriminaliteit is heel winstgevend voor hackers, aangezien hier vaak grote sommen losgeld mee gepaard gaan en het risico om gepakt te worden klein is.

De beste oplossing om je netwerk te beveiligen tegen cybercriminaliteit is om het langs de buitenkant te laten monitoren. Een hacker gaat op zoek naar de zogenaamde sweet spots; de grootste zwakheden van buitenaf.

Maar liefst 91% van alle malware gebruikt onbeveiligde DNS-verbindingen. Door deze uit te sluiten, sluit je dus ook meteen een groot deel van de risico's af. En dat is exact wat Secutec SecureDNS doet. Een erg snelle reputatiecheck van websites die worden opgevraagd door medewerkers.

Secutec SecureDNS zorgt dus voor een extra beschermingslaag. Zo loop je beduidend minder risico op:

- Kosten door een onderbreking van je werking door het uitvallen van je server,
- Omvangrijke en zorgwekkende datalekken,
- Verlies van klanten die hun vertrouwen in je organisatie verliezen.

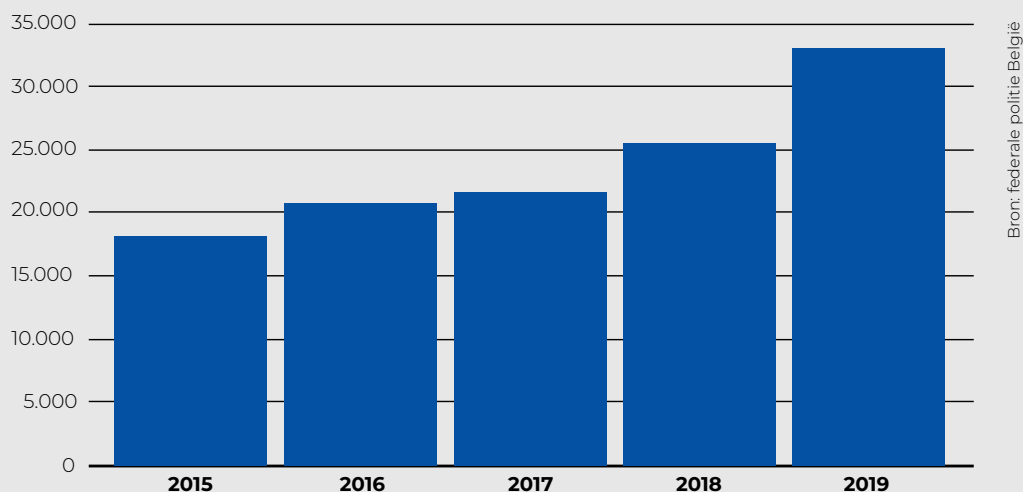


Door de wekelijkse rapportage van Secutec SecureDNS, zagen wij een enorme toename van phishingwebsites die inspeelde op het nieuws rondom corona. Allemaal onveilige verbindingen die Secutec SecureDNS verhinderde.”

Pieter Verheyden, senior system engineer VAB

Cyberveiligheid vandaag

In 2019 werden er bijna 33.000 gevallen van cybercriminaliteit gerapporteerd. Dat is een stijging van 30% t.o.v. het jaar voordien. E-commerce heeft een belangrijk aandeel in deze groei. Nu meer mensen online bestellen, stijgen de kansen voor hackers om toe te slaan en ook het groeiend aantal werknemers die van thuis werkt, vormt een uitdaging voor de veiligheid van organisaties.



De meeste 'cyberdreiging' zit onopvallend verborgen in schijnbaar betrouwbare en legitieme documenten, e-mails, apps en websites.

[Adviesbureau BDO](#) analyseerde 15.000 websites en concludeerde dat 1 tot 5 overheids- en bedrijfswebsites in België een gemakkelijk doelwit vormen voor hackers.

Volgens anti-phishingplatform Phished liep [in 2020 wel 22% van de ontvangers van phishing-berichten in de val](#). Die trend zal zich blijven voortzetten dus je moet actief je medewerkers aanmanen tot **waakzaamheid**.

Maar reken niet alleen daarop: phishers zijn slim en een extra bescherm laag is geen overbodige luxe. Zeker omdat er wordt 'gehengeld' met **actualiteitsgebonden berichten** over onzekere en belangwekkende onderwerpen, zoals het coronavaccin.

Een extra bescherm laag: waarom is die zo belangrijk?

De extra bescherm laag van Secutec SecureDNS beveiligt de DNS-verbindingen die je gebruikers maken.



Wat is een DNS-verbinding?

Een **DNS** of **Domain Name Server** matcht het IP-adres van je medewerker of netwerkgebruiker aan de **website-naam of URL** die de gebruiker probeert te bereiken – door hem in zijn browser te typen of door op een link te klikken.

Een DNS is dus eigenlijk het **‘telefoonboek van het internet’**, een virtuele verzameling van alle gebruikers en hun IP-adressen.

Wat maakt een DNS-verbinding zo kwetsbaar?

In tegenstelling tot IP-adressen blijven DNS-verbindingen **vaak onbeveiligd**. Hackers met slechte bedoelingen weten dat ook: meer dan 91% van alle malware gebruikt DNS om verbinding te maken met je server en daar gegevens te stelen of het verkeer om te leiden naar schadelijke websites.

Een extra toevoeging aan je huidige bescherming

Voor de duidelijkheid: Secutec SecureDNS is geen vervanging voor je huidige beschermingspakket, maar voegt er iets aan toe. Je bestaande cybersecuritypakket is de deur van je huis, met Secutec SecureDNS draai je het slot dicht.

Secutec SecureDNS helpt u met een gerust hart te ondernemen doordat u inzicht krijgt in de digitale veiligheid van uw organisatie, zonder onnodige technische details.

De grootste voordelen van Secutec SecureDNS

- Secutec SecureDNS **blokkeert meer dreigingen, en sneller** dan andere beschermingssoftware.
- Er is **geen server-reboot** of -pauze nodig voor de opstart.
- Onze specialist implementeert SecureDNS in **minder dan een uur**, via een efficiënte remote call.
- SecureDNS werkt onafhankelijk van systeem, netwerk of beveiliging en is dus voor **iedereen toegankelijk**.
- Heb je **telewerkers** die een ander netwerk gebruiken? Ook hun verkeer wordt automatisch omgeleid en gecontroleerd via de Secutec SecureDNS server.
- Je ontvangt regelmatig **gedetailleerde en gepersonaliseerde rapporten**: wat werd er geblokkeerd en wie probeerde verdachte sites te bereiken?
- Elke installatie is **op maat** van jouw bedrijf.
- Je krijgt onmiddellijk een **melding** als we een dreiging identificeren.
- Je voelt je **continu ondersteund** dankzij de support van onze experts.
- **We houden alle apparaten veilig**, dus ook die waarover u geen controle heeft, denk hierbij bijvoorbeeld aan educatieve instellingen met een gastnetwerk voor studenten.



Secutec SecureDNS is belachelijk gemakkelijk te implementeren. Het neemt bij wijze van spreken 30 seconden in beslag.”

Pieter Verheyden, senior system engineer VAB



CYBERSECURITYTM
MADE IN EUROPE

Bereikbaar en Belgisch, maar op internationaal niveau

Secutec is een **Belgische securityspecialist** die staat voor hoge kwaliteit, snelle reactie en duurzame, professionele relaties.

Wij beschermen grote en internationale bedrijven en organisaties maar zijn lokaal verankerd in België, waardoor we dus perfect op jouw noden kunnen inspelen.

Wij gebruiken zowel lokale informatie als informatie van gerenommeerde internationale leveranciers van beveiligingsoplossingen.

Je kan
Secutec
SecureDNS
nu **4 weken**
gratis uit-
proberen.

Verlies dus geen tijd en bescherm je kostbare data tegen digitale aanvallen.

Contacteer ons op sales@secutec.be
of +32 3 877 82 93

