17 mrt 2026 -09:53

Nieuw overheidsprotocol moet Belgische internetgebruikers beter beschermen tegen cybercriminaliteit

De Federale Gerechtelijke Politie (FGP), het Centrum voor Cybersecurity België (CCB) en de Belgische cyberbeveiliger Secutec slaan de handen in elkaar om phishing een halt toe te roepen. Het '*Nationaal Protocol voor Detectie en Disruptie van Phishingdreigingen*' moet nieuwe, kwaadaardige websites automatisch detecteren en de internetgebruiker waarschuwen voor phishingpogingen. Phishing wordt almaar meer aangestuurd door artificiële intelligentie en is een ware plaag voor de maatschappij. In 2025 ontving het CCB ongeveer 10 miljoen meldingen via verdacht@safeonweb.be. Het heeft ertoe geleid dat kwaadaardige websites zo'n 200 miljoen keer zijn vermeden.

Het overheidsprotocol vloeit voort uit Phish Nemo, een project en toepassing van de Federale Gerechtelijke Politie van Limburg, waarmee ze sinds 2022 phishingdomeinnamen opspoort en blokkeert. Binnen het kader van de samenwerking die vandaag werd bekrachtigd, zal de FGP de Phish Nemo-applicatie overdragen aan het CCB. Zo willen de partners de toepassing op grotere schaal en binnen het Belgische cybersecurity-ecosysteem implementeren, met de steun van Secutec.

Secutec zal Phish Nemo nauwer integreren met de BAPS-phishingdatabank (*Belgian Anti-Phishing Shield*) van het CCB, voor onmiddellijke updates. Tot vandaag scande Secutec de veiligheidscertificaten van dubieuze websites, om vervolgens frauduleuze adressen manueel toe te voegen aan de BAPS-databank. Naast Phish Nemo werkt het CCB nog met andere *trusted partners* om de lijst continu te actualiseren.

De databank staat ter beschikking van telecombedrijven, zodat zij hun internetgebruikers automatisch kunnen doorverwijzen naar een waarschuwingspagina wanneer ze een frauduleuze of kwaadaardige website bezoeken. Dat proces kon enkele uren tot verschillende dagen in beslag nemen. De fijnmazige integratie zal dus een onmiddellijke en fundamentele impact hebben op de cyberveiligheid in ons land.

Ten slotte formaliseert het protocol ook het delen van gegevens met betrekking tot kwaadaardige sites. Zo willen de drie partners phishingcriminelen eenvoudiger in kaart brengen, analyseren en een halt toeroepen.

Samenwerking als de sleutel tot succes

Met dit protocol maken de drie partners een duidelijke keuze om phishing proactief te bestrijden, en frauduleuze campagnes te stoppen vooraleer ze slachtoffers maken. Zo neemt de druk op politie en aanklagers af, en kunnen er meer middelen worden ingezet om criminele netwerken structureel te ontmantelen.

Door de expertise van de Federale Gerechtelijke Politie, het CCB en Secutec te bundelen, is een sterke aanpak mogelijk die detectie, data-analyse, blokkering en gerechtelijk onderzoek met elkaar integreert. De Federale Politie is ervan overtuigd dat nationale samenwerking met partners de effectieve bestrijding van

online criminaliteit versterkt.

Noot voor de redactie:

Het Nationaal Protocol voor Detectie en Disruptie van Phishingdreigingen (Phish Nemo) werd vandaag ondertekend door de directeurs-generaal Miguel De Bruycker (het Centrum voor Cybersecurity België) en Laurent Blondiau (Federale Gerechtelijke Politie), en door Secutec-CEO Geert Baudewijns (zie foto).

Over Phish Nemo
Het Phish Nemo-project is in 2022 opgestart door het Datalab-team van de Federale Gerechtelijke Politie van Limburg. Hun doel was duidelijk: phishing voorkomen door kwaadaardige sites te detecteren bij de creatie, terwijl onderzoeken daarvoor pas konden beginnen na een formele klacht. Vandaag worden de verzamelde gegevens gebruikt om de cybercriminelen of frauduleuze netwerken sneller te identificeren. Sinds 2022 zijn 1.600 kwaadaardige sites dankzij Phish Nemo in een vroeg stadium geblokkeerd, zijn ruim 120.000 potentiële slachtoffers gevrijwaard en leidde de informatie tot verschillende concrete gerechtelijke onderzoeken en arrestaties.
Voor zijn innovatieve aanpak ontving Phish Nemo in 2024 de Best Innovative Project Award bij de Circle of Police Leadership (CPL) en in 2025 de prijs voor Best Innovative Proposal van Europol EC3.

Centrum voor Cyber Security België
Wetstraat 18
1000 Brussel
België
http://www.ccb.belgium.be

Katrien Eggers
Woordvoerder(NL/FR/E)
+32 485 76 53 36
katrien.eggers@ccb.belgium.be

Michele Rignanese
Woordvoerder(NL/FR/E)
+32 (0)477 38 87 50
michele.rignanese@ccb.belgium.be