CBV FACTSHEET

Najaar 2024

Aanpak verzekeringsfraude leidt tot 86 miljoen besparing

Verzekeraars hebben in 2023 in totaal **7.976** keer verzekeringsfraude vastgesteld. Het gaat dan om fraude bij zowel het aanvragen van verzekeringen als bij claims. Dat is fors minder dan het aantal bewezen verzekeringsfraudes in 2022. Wel zijn de financiële gevolgen per geval het afgelopen jaar groter geweest. De gerealiseerde besparing door fraudebestrijding door de verzekeraars is met **7% gestegen naar ruim 86 miljoen euro**.

Een deel van de daling van het totaal aantal vastgestelde fraudes komt door een iets andere manier waarop de fraudecijfers zijn vastgelegd. Het Centrum Bestrijding Verzekeringscriminaliteit (CBV) constateert hoe dan ook voor het tweede jaar op rij een afname van het totaal aan gedetecteerde incidenten. Procentueel is het aantal claims dat op fraude is onderzocht gelijk gebleven. Er is minder vaak gefraudeerd maar wel met hogere bedragen.

Als een fraude is onderzocht en aangetoond, zijn er meerdere maatregelen mogelijk. De claim afwijzen, de polis beëindigen, de onderzoekskosten terugvorderen en aangifte doen bij de politie. Verzekeraars kunnen er ook voor kiezen de gegevens van de fraudeur op te nemen in het gezamenlijke waarschuwingssysteem. Verzekeraars hebben vorig jaar 3.177 keer iemands gegevens in dit systeem geregistreerd. Dat is **15% minder** dan in 2022. Voor zes op de tien fraudeurs blijft het bij één of meer andere maatregelen.

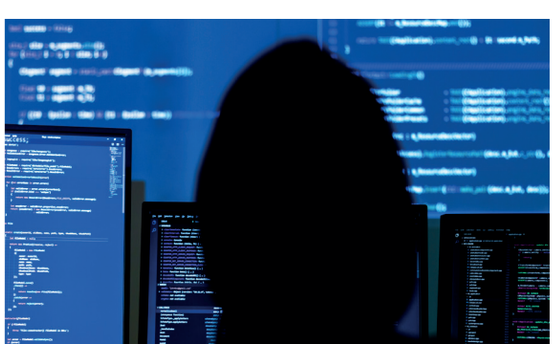
Volgens het uitsprakenregister heeft de Geschillencommissie Financiële Dienstverlening van klachteninstituut Kifid in 2023 in **4 gevallen** bepaald dat de registratie door verzekeraars uit het externe waarschuwingssysteem moest worden verwijderd. In 4 andere gevallen is de duur van de registratie ingekort.

Nieuwe bril?

Verzekerde is naar eigen zeggen beroofd van een deel van haar ruimbagage op weg naar haar zonvakantie. Juist toen had ze die dure designzonnebril zo hard nodig. Bij het onderzoek naar de claim verschijnen op social media haar vakantiefoto's met een hoofdrol voor die 'gestolen' zonnebril. Mevrouw biecht op dat ze teveel heeft geclaimd. Het aandikken van haar claim betekent echter dat alles wordt afgewezen.

Private opsporing verzekeringsfraude

Eind 2017 zijn het Openbaar Ministerie (OM), de politie en het Verbond van Verzekeraars samen een onderzoek (Proeftuin Private Opsporing Verzekeringsfraude) gestart om de opsporing en vervolging te verbeteren. Dankzij jurisprudentie die is voortgekomen uit dit onderzoek, zijn inmiddels de voorwaarden vastgesteld waaronder privaat verricht onderzoek kan dienen als de basis van een strafrechtelijk opsporingsonderzoek. Onder strikte condities – zoals hantering van een onderzoeksprotocol door de private partijen, beoordeling van het onderzoeksresultaat en verhoor van de verdachte door een opsporingsambtenaar – wordt het mogelijk incidentonderzoeken van verzekeraars maximaal te benutten. OM, politie en het Verbond gaan met elkaar in gesprek over hoe deze werkwijze landelijk gebruikt kan worden.



Gijzelacties voorkomen

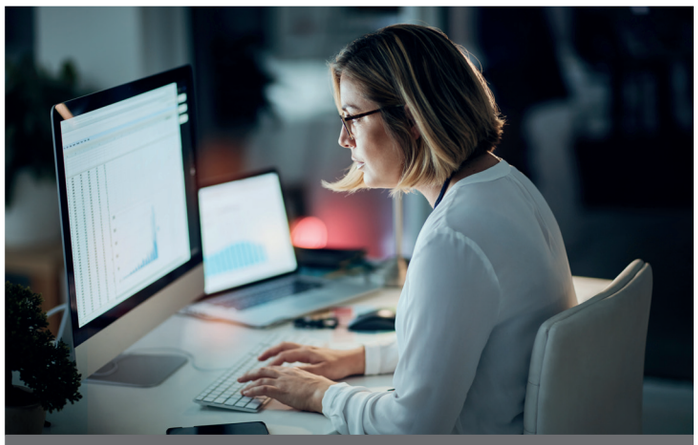
Bij een wereldwijde politieoperatie wordt de infrastructuur van een beruchte groep ransomwarecriminelen ontmanteld. Tijdens het onderzoek worden veel gestolen inloggegevens aangetroffen, ook van medewerkers van Nederlandse bedrijven. Vermoedelijk zijn de gegevens buitgemaakt via malware die op hun systemen is geplaatst. Het gezamenlijk cybersecurity team van de verzekeraars (**i-CERT**) ontvangt hierover relevante informatie vanuit de overheid, die wijst op een hoge dreiging voor specifieke partijen in de sector. Deze informatie is door het CBV direct met deze partijen gedeeld. Zij hebben hierdoor hun systemen gericht kunnen onderzoeken op verdachte activiteit en maatregelen kunnen nemen om (verdere) inbreuken te voorkomen.

Een koud kunstje?

Tijdens afwezigheid van verzekerde gaat de vriezer kapot en verzekerde claimt de bedorven inhoud van de vriezer. Verzekerde stuurt als bewijs foto's van de verloren gegane inhoud toe, maar onderzoek wijst uit dat deze beschimmelde beelden van internet zijn geplukt. Verzekerde erkent dat het de verkeerde foto's zijn en stuurt direct de 'juiste' foto's op. Helaas voor de verzekerde wordt duidelijk dat die foto's diezelfde dag zijn gemaakt en dat alle etenswaar keurig bevroren is. Wel blijkt dat op de foto's een filter is geplaatst waardoor de inhoud van de vriezer toch bedorven lijkt. De claim wordt afgewezen en verzekerde kan voorlopig even afkoelen.

Zure Apple van de groenteboer

Na inbraak in de woning claimt verzekerde diverse goederen, waaronder een laptop en een drone. De aanschaf van deze goederen wordt onderbouwd met facturen van één en dezelfde winkel. Onderzoek naar het adres van de winkel leidt naar een groente- en tabakswinkel. De expert van de verzekeraar bezoekt de locatie en stelt vast dat de geclaimde goederen daar niet kunnen zijn aangeschaft. De claim van de verzekerde van ruim 15.000 euro gaat in rook op en de gegevens van deze 'rotte appel' worden in het Externe Verwijzingsregister vastgelegd.



Dienstverlening

Verzekeraars leveren veel informatie aan bij het fraudeloket van het CBV en het loket van het i-CERT, dat ook bij het CBV is ondergebracht. Het delen en centraal samenbrengen van kennis en informatie is immers essentieel om fraude en (cyber) criminaliteit te voorkomen én aan te pakken. Zo helpen verzekeraars elkaar in het belang van de samenleving en de eerlijke premiebetaler. Ook overheidsinstanties en personen weten het CBV te vinden. In 2023 heeft het CBV via de diverse kanalen:

- ✓ **225** adviezen over relevante cyberincidenten en -dreigingen met de sector gedeeld.
- ✓ **2.654** incidentmeldingen van verzekeraars ontvangen met dossierinformatie over onderzoeken naar mogelijke fraude.
- ✓ **213** informatievragen van politie en justitie afgehandeld.
- ✓ **87** anonieme tips over mogelijke verzekeringsfraude ontvangen van bezorgde burgers.
- ✓ **5** sectorbrede waarschuwingen over opvallende of nieuwe fraudevormen uitgegeven.

Direct digitaal uitdeuken

Analisten van het i-CERT signaleren op een site van cybercriminelen een omvangrijke dataset waarin gegevens staan die van meerdere verzekeraars afkomstig lijken. De gegevens blijken gestolen bij een vlak daarvoor gehackte schadehersteller. Deze wordt door de cybercriminelen ook nog eens afgeperst met gijzelsoftware. De belanghebbende verzekeraars, die nog van niets weten, worden direct gewaarschuwd. Zij ontvangen van het i-CERT adviezen met een nadere analyse van de situatie en handelingsperspectieven om de gevolgen voor alle betrokkenen zo goed mogelijk te beheersen.

Deze factsheet is een uitgave van het Centrum Bestrijding Verzekeringscriminaliteit (CBV), onderdeel van het Verbond van Verzekeraars.
Het CBV helpt verzekeraars bij het aanpakken en voorkomen van verzekeringsfraude en -criminaliteit en hun eigen cyber security.
Het CBV doet dit door zowel beleidsontwikkeling voor de sector als operationele dienstverlening aan verzekeraars.

Contact
Tips of vragen? Mail dan naar: **cbv@verzekeraars.nl** of kijk op **verzekeraars.nl/branche/verzekeringscriminaliteit**