Artsen en apothekers roepen volgende regering op om te **investeren in cyberbeveiliging**

Uit onze grote enquête over cyberbeveiliging in de gezondheidszorg blijkt dat de meerderheid van artsen en apothekers (84%) meent dat het ondersteunen van professionals en instellingen in de gezondheidszorg op het gebied van cyberbeveiliging een prioriteit moet zijn voor de volgende regering. Ze vragen om een verhoging van het budget voor cyberbeveiliging voor ziekenhuizen, en cyberbeveiligingspremies voor niet-ziekenhuismedewerkers.

VINCENT CLAES

Eén op de vijf deelnemers (19%) aan onze grote enquête over cyberbeveiliging is de afgelopen zes jaar het slachtoffer geweest van een cybermisdrijf. Meer Franstaligen dan Nederlandstaligen melden dit (24% vs. 12%).

Met welke aanvallen hebben huisartsen, specialisten en apothekers te maken gehad (in dalende volgorde)?

- Phishing: pogingen om gegevens te stelen of toegang te krijgen tot bankrekeningen via een e-mail, sms of telefoontje: 55%.
- Hacking: ongeautoriseerde toegang tot computersystemen: 54%
- Computersabotage: vernietigen, blokkeren of wissen van computergegevens: 45%
- Ransomware: eisen van losgeld om gegevens te herstellen die door ransomware zijn geblokkeerd: 45%
- Cyberpesten: online lastigvallen via e-mail of berichten: 21%.

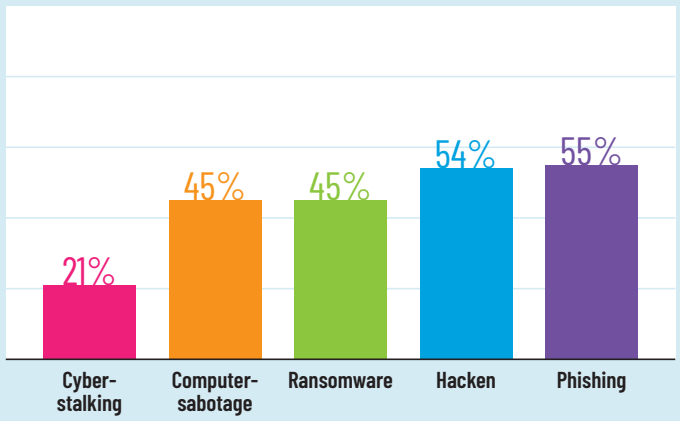
De helft van de artsen en apothekers maakt zich permanent zorgen over de IT-beveiliging van hun beroepsactiviteit. Een derde vindt echter dat "het een probleem is voor hun IT-afdeling en hun IT-specialist", niet voor henzelf. Apothekers zijn vaker deze mening toegedaan dan artsen (49% vs. 18%).

Verhoog het budget voor cyberbeveiliging

Acht van de tien respondenten zijn van mening dat het ondersteunen van professionals in de gezondheidszorg op het gebied van cyberbeveiliging een prioriteit moet zijn voor de volgende regering, die een concreet actieplan moet opstellen, en dat de federale overheid het budget voor cyberbeveiliging in ziekenhuizen moet verhogen.

Tegen 2023 had de federale regering een budget van 15 miljoen euro voorzien voor alle ziekenhuizen. Dat verbleekt bij de €130 miljoen die de NRZV (Nationale Raad voor Ziekenhuisvoorzieningen) aanbeveelt om structureel te investeren. Eind april kwam Frank Vandenbroucke met een niet-structureel budget van 39,5 miljoen euro om ziekenhuizen beter te beveiligen tegen cyberaanvallen. "Ziekenhuizen zijn steeds vaker het doelwit van cyberaanvallen, zoals het afgelopen jaar opnieuw is gebleken. Investeren in cyberbeveiliging om patiëntgegevens zo goed mogelijk te beschermen en de beschikbaarheid van zorg te garanderen is essentieel", aldus de minister van Volksgezondheid.

Artsen en apothekers die de afgelopen 10 jaar slachtoffer zijn geweest van cybercriminaliteit en zijn geconfronteerd met daden van:



- **cyberstalking:** online lastigvallen via e-mail of berichten
- **computersabotage :** vernietigen, blokkeren, wissen van computergegevens
- **ransomware:** losgeld eisen om gegevens die geblokkeerd zijn door ransomware te herstellen
- **hacken:** ongeoorloofde toegang tot een computersysteem
- **phishing:** pogingen om gegevens te stelen of toegang te krijgen tot bankrekeningen via een e-mail, sms of telefoontje

GEEN CRISIS-MANAGEMENTPLAN

Zijn artsen en apothekers voorbereid op een cyberaanval? Op papier lijkt dit niet het geval te zijn. Slechts weinigen van hen (minder dan 15%) hebben crisismanagement-, communicatie-, herstel- en bedrijfscontinuïteitsplannen opgesteld. Toegegeven, het zijn over het algemeen de grotere organisaties die de middelen hebben om deze gestructureerde processen preventief te ontwikkelen.

61% **van de deelnemers aan onze enquête weet wie ze kunnen contacteren binnen hun professionele structuur (ziekenhuis, groepspraktijk, apotheek, enz.) als ze het slachtoffer zijn van een cyberaanval. De meesten hebben de contactgegevens (telefoon, e-mail) van deze persoon. Artsen en apothekers zijn echter minder goed in staat om de persoon te identificeren die verantwoordelijk is voor het IT-continuïteitsplan in geval van een aanval of brand. Slechts 45% van de Nederlandstaligen en 27% van de Franstaligen weet wie deze persoon is.**

MS15227AN

BETERE BESCHERMING VAN GEZONDHEIDSPROFESSIONALS TEGEN KWAADAARDIGE OPMERKINGEN

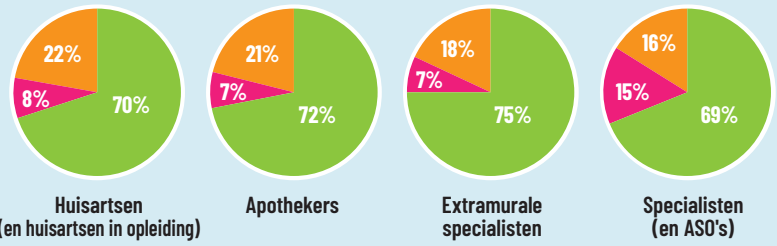
75% van de deelnemers aan onze enquête wil dat de overheid specifieke regels invoert om professionals in de gezondheidszorg te beschermen tegen kwaadaardige commentaren op sociale netwerken en verwijzingssites voor zorgverleners. Specialisten in ziekenhuizen - die meer worden blootgesteld aan commentaar op sociale netwerken - vragen vaker om deze maatregel (77%) dan huisartsen (73%) of apothekers (68%).
In onze columns hebben een aantal artsen al hun ergernis geuit over negatieve recensies over hen die op websites zijn gepubliceerd.

De meerderheid van de artsen en apothekers (79%) vindt dat de federale overheid een cyberbeveiligingspremie moet toekennen aan extramurale artsen huisartsen (70%), extramurale specialisten (75%) en apothekers (72%) om zorggegevens beter te beschermen. Franstaligen en specialisten in opleiding zijn meer voorstander van deze steun dan Nederlandstaligen (83% vs. 73%), net als een verhoging van het federale budget voor cyberbeveiliging (89% vs. 64%).

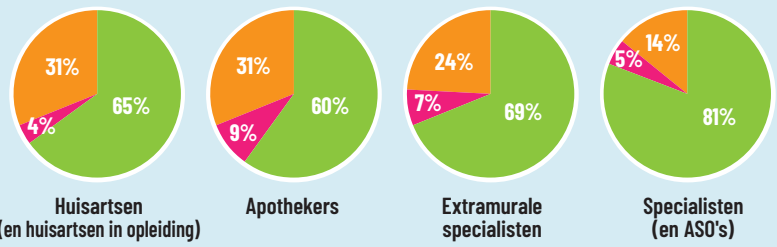
Niet verrassend denkt één op twee respondenten dat artsen of apothekers niet verantwoordelijk kunnen worden gesteld voor een inbreuk op de beveiliging van de gegevens van hun patiënten. Iets meer apothekers dan huisartsen (56% vs. 46%) zijn tegen een dergelijke aansprakelijkheid. Over het geheel genomen is echter 30% van de respondenten bereid om deze verantwoordelijkheid op zich te nemen.

Moet de federale overheid: Ja Nee Geen antwoord

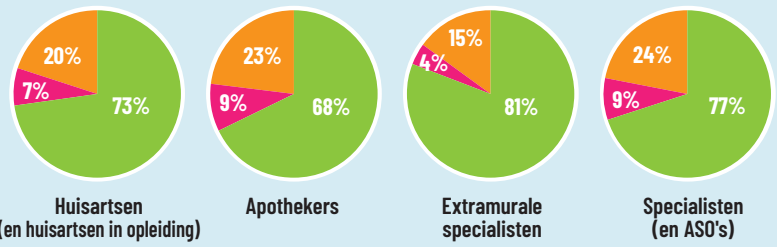
Een cyberbeveiligingspremie toekennen aan niet-ziekenhuisartsen?



Budget ziekenhuizen voor cyberbeveiliging verhogen?

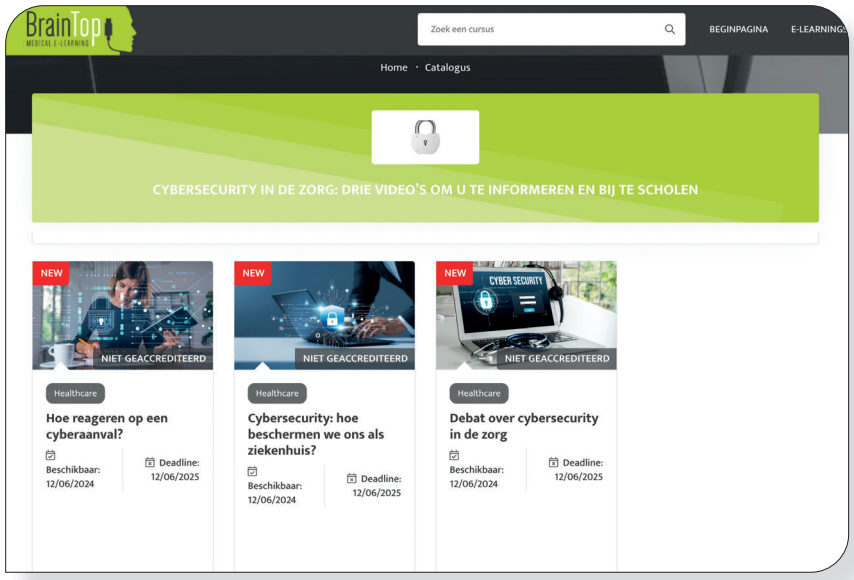


Specifieke regelgeving invoeren om zorgverleners te beschermen tegen kwaadaardige commentaren op sociale netwerken en referentiesites?

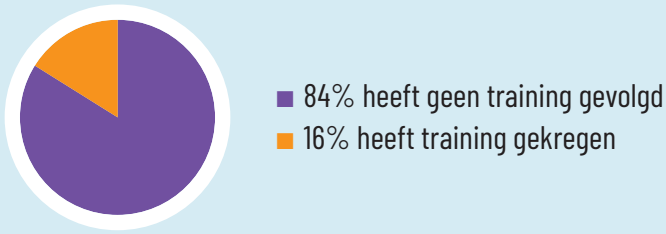


Duidelijke behoefte aan training in cyberbeveiliging

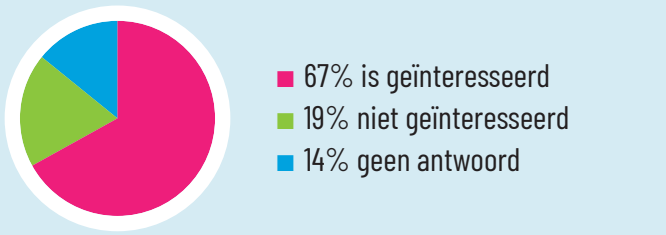
67% van de respondenten in onze enquête wil een opleiding in cyberbeveiliging volgen. Om aan deze duidelijke vraag te voldoen, bieden we informatie en trainingsvideo's over cyberbeveiliging aan op onze BrainTop-website.



Hoeveel artsen en apothekers volgden een opleiding in cyberbeveiliging in de afgelopen 5 jaar?



Hoeveel artsen en apothekers zouden een opleiding willen volgen in cyberbeveiligingstraining?



Volgen artsen en apothekers specifieke opleidingen om de risico's van cybercriminaliteit te voorkomen? Op dit moment is dat nog zeldzaam. Acht op de tien respondenten heeft dat in de afgelopen vijf jaar niet gedaan. Dit is geen bewijs van gebrek aan interesse, want 67% van de respondenten zegt bereid te zijn om een training te volgen.

Uit dat enthousiasme blijkt de waarde van ons initiatief om trainings- en informatievideo's en artikelen over cyberbeveiliging te publiceren op onze BrainTop-site en op onze mediasites.

Ons redactieteam heeft video's gemaakt om u meer te leren over digitale bescherming:

- **Cybersecurity: hoe bescherm je jezelf in het ziekenhuis?**

Een interview met Sabrina Cristofano, voorzitter van de Gibbis Cybersecurity Group en Chief Information Security Officer en Data Protection Officer bij Brugmann University Hospital.

- **Een videodebat over cyberbeveiliging** in de gezondheidszorg met Dieter Goemaere (Gibbis), Peter Fontaine (Europaziekenhuizen), Mathieu Lardinois (SkyForce) en Nina Hasratyan (Agence du numérique).

U vindt op onze website ook een presentatie van de Cybersecurity Toolkit voor kleine en middelgrote ondernemingen geproduceerd door de Global Cyber Alliance (GCA).

Deze video's kunnen worden bekeken op ons BrainTop-platform.

Ontdek onze opleidingen
https://tinyurl.com/y5c8k42c3

Met de steun van

Cyberwal by digital wallonia

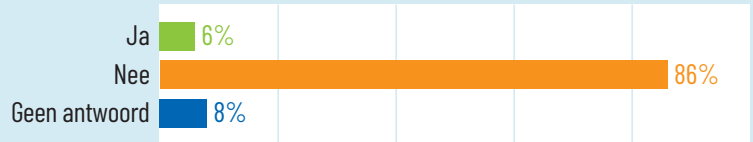
Wallonie Relance

SKYFORCE CYBER SECURITY

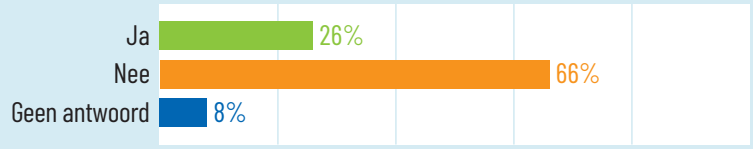
TOENAME VAN PERSOONLIJKE INVESTERINGEN

Welke maatregelen namen artsen en apothekers de afgelopen 5 jaar om zich te beschermen tegen cyberaanvallen?

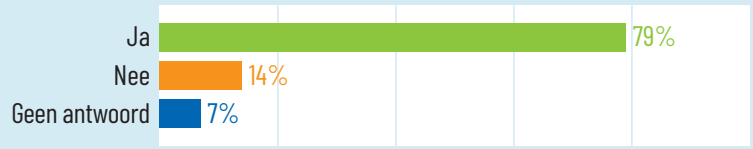
Een specifieke cyberbeveiligingsverzekering afsluiten:



Een expert inschakelen om hen te adviseren:



Krachtige antivirussoftware installeren:



Een op de twee respondenten heeft de afgelopen vijf jaar geïnvesteerd in IT-oplossingen en apparatuur om hun bedrijf beter te beschermen tegen cyberaanvallen. Deze artsen en apothekers hebben dus de hand op de knip moeten houden om zich uit te rusten. In 2004 verhoogde 83% van de respondenten hun budget voor cyberbescherming met 0% tot 50%, en 13% met 51% tot 100%.

Welke praktische maatregelen nemen artsen en apothekers om zich te beschermen tegen cybercriminaliteit? In de afgelopen 5 jaar heeft 79% van de respondenten effectieve antivirussoftware geïnstalleerd. Veel minder echter (26% in FR en 41% in NL) hebben een expert/bedrijf gevraagd hen te adviseren over hoe ze hun IT-systeem zo doeltreffend mogelijk kunnen beschermen.

Artsen en apothekers zijn nog niet gewend om zich specifiek te verzekeren tegen de gevolgen van een cyberaanval. Slechts 6% van de respondenten heeft dit recent gedaan.

Een derde van de deelnemers aan ons onderzoek (33% aan NL zijde en 42% aan FR zijde) maakt gebruik van een *virtual private network* (VPN) om te communiceren. Bijna acht op de tien respondenten zeggen elektronisch te communiceren met hun patiënten. De helft van de Nederlandstaligen doet dit via een beveiligd zorgberichtensysteem, tegenover slechts een vijfde van de Franstaligen.

MS152278N

Wachtwoorden, back-up en dubbele authenticatie

Veranderen professionals in de gezondheidszorg regelmatig de wachtwoorden van hun professionele IT-apparaten (computers, applicaties of websites)? Uit onze enquête blijkt dat 61% van de respondenten dat niet systematisch doet.

Als ze het doen, is dat (in dalende volgorde) omdat ze een beveiligingswaarschuwing krijgen (23%) of omdat de IT-manager van de instelling hen dat vraagt (20%).

Een derde (28%) verandert zijn wachtwoord nooit. Huisartsen lijken minder voorzichtig te zijn dan specialisten en apothekers, aangezien 44% van hen hun wachtwoord nooit wijzigt in vergelijking met 28% van de specialisten en apothekers. Dat is niet verwonderlijk, aangezien een derde van de ziekenhuisapothekers en specialisten zegt dat ze dit doen op verzoek van de IT-manager van hun instelling.

Hoe zit het met het updaten van de programma's die ze gebruiken in hun professionele activiteit? De meerderheid (72%) vertrouwt erop dat hun apparatuur automatisch wordt bijgewerkt. Waarschuwingen zetten 22% van de respondenten ertoe aan om hun programma's bij te werken. 5% doet het als ze eraan denken en 1% doet het nooit.

De meerderheid (63%) van de gegevensback-ups wordt automatisch uitgevoerd. Nederlandstaligen verkiezen automatische back-ups boven Franstaligen (69% vs. 57%). Een vijfde van de respondenten maakt nog regelmatig manuele back-ups.

Huisartsen verkiezen de *cloud* boven beveiligde lokale schijven voor de opslag van hun medische gegevens (68% vs. 19%). Dit in tegenstelling tot specialisten, die de voorkeur geven aan beveiligde lokale servers (43%) boven de ***cloud*** (19%).

Verrassend genoeg weet een vijfde van de respondenten niet waar hun gegevens zijn opgeslagen.

Een manier om elektronische apparaten te beveiligen is het gebruik van dubbele authenticatie. 52% van de Nederlandstalige respondenten heeft deze praktijk al toegepast, tegenover slechts 38% van de Franstaligen. Degenen die dubbele authenticatie gebruiken doen dit (in dalende volgorde) via een specifieke applicatie, door een code te gebruiken die per sms wordt verstuurd en door een notificatie te ontvangen.

Hoe vaak veranderen artsen en apothekers de wachtwoorden van hun professionele IT-apparatuur ?

MEER INFORMATIE OVER MEDISCHE HULPMIDDELEN

Hackers krijgen soms toegang tot IT-systemen via medische apparatuur. Acht van de tien respondenten op onze enquête vinden dat producenten van *connected* medische apparaten beter moeten communiceren over de mogelijke kwetsbaarheden van hun producten en specifieke training over de cyberveiligheid van hun medische apparaten moeten aanbieden op het verkooppunt. Artsen zijn meer geïnteresseerd in deze transparantie en ondersteuning dan apothekers.

NIS2: EEN WEINIG BEKENDE RICHTLIJN

De meerderheid van de respondenten (92%) op onze enquête had nog nooit gehoord van de Europese normen die verbonden zijn aan de NIS2-richtlijn (informatiebeveiliging), die in oktober 2024 van kracht wordt en van invloed zal zijn op bedrijven met meer dan 50 werknemers of een jaaromzet van meer dan €10 miljoen. Slechts 6 van de 903 respondenten waren betrokken bij werkvergaderingen om deze normen in hun instelling te implementeren. Het is daarom de hoogste tijd voor zorgorganisaties om artsen bewust te maken van de implicaties van de overstap naar NIS2.

METHODOLOGIE

- Online enquête uitgevoerd via de media *De Specialist*, *Medi-Sfeer* en *Farma-Sfeer*.
- Enquêteperiode: januari-april 2024
- Aantal respondenten: 903 (59% mannen/41% vrouwen)
  - Huisartsen: 38%
  - Specialisten in ziekenhuizen: 34%
  - Specialisten buiten ziekenhuizen: 19%
  - Apothekers: 9%.
- Geografische spreiding van de praktijkplaats (praktijk of apotheek): Vlaanderen (40%), Brussel (11%) en Wallonië (49%).

REACTIES OP ONZE WEBSITE www.despecialist.eu

MS15227CN