Transcipt De SeniorWeb Podcast

Zegert van der Linde in gesprek met Elmer Lastdrager

00:00:00

Zegert van der Linde: Welkom bij de SeniorWeb Podcast, mijn naam is Zegert van der Linde, fijn dat u luistert.

00:00:07

Zegert van der Linde: De maand maart staat bij SeniorWeb in het teken van online veiligheid en privacy. In deze vier podcast afleveringen praat ik met verschillende gasten over dit thema. U krijgt achtergronden, verdieping, en praktische tips om veilig online te gaan.

00:00:20

Zegert van der Linde: Digitale assistenten als Siri of Google Home zijn onderdeel van the internet of things, of in het Nederlands: het internet der dingen. Een nog relatief nieuw onderdeel van het internet dat in korte tijd onze huiskamers heeft veroverd. Maar waar moet je nu op letten als je gebruik maakt van the internet of things? Dat bespreek ik vandaag op afstand met Elmer Lastdrager Lastdrager, hij werkt bij het SIDN, waar hij zich bezighoudt met de thema's veiligheid en privacy rondom the internet of things. Welkom, Elmer Lastdrager.

00:00:54

Elmer Lastdrager: Dank je wel.

00:00:56

Zegert van der Linde: Ik noemde net al even Siri, Google home, dat zijn van die digitale assistenten. Wat kunnen die?

00:01:03

Elmer Lastdrager: Wat ze in feite doen is zogezegd spraak naar tekst, dus ze verstaan wat je zegt, en vervolgens zetten ze dat om naar tekst. Daar kan de achterliggende organisatie, dus Google of Apple bijvoorbeeld, die kunnen dat daar dan interpreteren en jou helpen. Dus daarmee kun je bijvoorbeeld vragen: "Wat is het weer in Amsterdam?" En dan kunnen ze dat aan de andere kant begrijpen, en dan kunnen ze daar het weer van Amsterdam laten zien.

00:01:35

Zegert van der Linde: Dan hebben we het dus bijvoorbeeld over Siri, dat gewoon op je iPhone zit. Je hebt tegenwoordig ook van die praatpalen, Amazon heeft ze, Google heeft ze, die werken ook een beetje op die manier.

00:01:48

Elmer Lastdrager: Ja, dat is eigenlijk dezelfde technologie. Het enige verschil is dat, bijvoorbeeld Siri draait op je telefoon, op je iPhone, en zo een ander apparaat, bijvoorbeeld die van Amazon, dat is echt een fysiek apparaat wat je in de woonkamer neerzet of waar dan ook. Die heeft dezelfde functionaliteit, maar dan als fysiek apparaat.

00:02:07

Zegert van der Linde: Dan heb je dus een soort apparaat in je kamer staan, en dat luistert dan mee. Dat klinkt een klein beetje gek, kun je dat uitzetten op de één of andere manier?

00:02:17

Elmer Lastdrager: Dat is vrij lastig, want de hele functionaliteit van zo'n apparaat gaat er natuurlijk om dat die meeluistert. Mocht jij tegen dat apparaat willen praten, dan moet het wel luisteren. Als die dat niet doet, als je daar naartoe moet lopen en op een knop moet drukken, dan is de hele functionaliteit een beetje weg, dus ze gaan er wel vanuit dat het apparaat altijd aanstaat, en altijd meeluistert.

00:02:37

Zegert van der Linde: Zo'n digitale assistant. Jij zei net: "Wat is het weer?" Maar mensen gebruiken het ook bijvoorbeeld al om de lichten aan te doen en zo?

00:02:45

Elmer Lastdrager: Ja, ook heel populair. Een stuk gemakkelijker als je vanaf de bank kunt zeggen: "Hé, Siri!" – of welke assistent je dan ook gebruikt – "Doe de verlichting aan of uit." Dat is natuurlijk gemakkelijker voor veel mensen dan

om even naar de schakelaar te lopen. Het klinkt een beetje als een luxeprobleem natuurlijk, als ik het zo zeg, maar het heeft voordelen die je op die manier kunt gebruiken.

00:03:09

Zegert van der Linde: Dan die slimme speakers, die kennen we nu een beetje, maar wat maakt er nu nog meer onderdeel uit van the internet of things?

00:03:18

Elmer Lastdrager: Het internet of things, of in het Nederlands: het internet der dingen, gaat eigenlijk over apparaten die op het internet aangesloten worden, en dat zijn dan apparaten die niet dat eerst niet waren. Dus je kunt daarbij denken aan – traditioneel zijn dat lampen, koelkasten misschien. Ik heb zelfs al een wasmachine gezien die je op het internet kunt aansluiten, en dat kan superhandig zijn, want als de wasmachine klaar is met de was, dan krijg je een signaaltje op je telefoon dat het tijd is om er naartoe te gaan. Dat is wat ik als voordeel zie, want ik vergeet het nog wel eens. Dus in die zin kan het veel voordelen bieden. Maar er zijn ook andere apparaten, robot stofzuigers om iets te noemen, zonnepanelen voor heel veel mensen. Mensen hebben zonnepanelen op het dak, daar zit dan een internetverbinding bij, en dan kun je op je telefoon bekijken hoe veel energie ze opgewekt hebben. Er zijn vrij veel apparaten die je op het internet aan kunt sluiten, los van de standaard apparaten, zoals telefoons, laptops…

00:04:21

Zegert van der Linde: Die kennen we allemaal natuurlijk. Auto's zijn ook vaak al online, nieuwe auto's dan, nieuwe modellen. Waarom is dat?

00:04:28

Elmer Lastdrager: Daar zitten voordelen aan, ze kunnen extra functionaliteit bieden, denk aan het automatisch updaten van de kaarten in de auto, voor de navigatie. Maar ook bijvoorbeeld het merk Tesla, die doet ook automatisch updates 's nachts, van de auto. Dan wordt de software van de auto automatisch van een update voorzien. Die kan functionaliteit bieden of problemen oplossen. En juist door dat 's nachts te doen, en geautomatiseerd, zijn er veel meer updates voor die auto's die uitgerold worden, vergeleken met auto's die naar de garage terug moeten om zo een update te krijgen. Het biedt hen gewoon voordelen.

00:05:06

Zegert van der Linde: Klinkt eigenlijk ook ergens wel gek, dat je auto geüpdatet moet worden.

00:05:11

Elmer Lastdrager: Of als je weg wil rijden, en de auto zegt: "Nee, dat kan nog niet, want ik moet even updaten." Dat voelt een beetje vreemd, maar dat is de nieuwe wereld.

00:05:19

Zegert van der Linde: Dan hebben we het nu best wel over thuisgebruik inderdaad, je noemt de koelkast, de wasmachine, de slimme speaker, de auto, maar zijn er ook andere plekken buitenshuis?

00:05:29

Elmer Lastdrager: Absoluut, en daarmee moet je bijvoorbeeld denken aan verkeerslichten, of verlichting, straatverlichting, die kun je ook op het internet aansluiten, of op een eigen netwerk, en daarmee op afstand beheren. Bijvoorbeeld op zijn zacht te zetten 's nachts, midden in de nacht zijn er misschien wat minder mensen op straat, dus dan wil je ze op halve kracht zetten. Maar ook andere scenario's, denk aan waterinstallaties, waterleidingen of pompen, misschien Rijkswaterstaat die bezig is met de verschillende sluizen bijvoorbeeld, die wil je vanop afstand kunnen besturen. Dus die zou je dan – het is veiliger om dat op een eigen netwerk te doen – maar je zou ze in feite ook op het internet kunnen aansluiten.

00:06:13

Zegert van der Linde: Nog niet zolang geleden was er een storing bij Google. Toen lagen er allerlei servers van Google op dat moment plat, en later las ik daarover een tweet van iemand die schreef dat hij twee uur in een donker huis had gezeten, want hij kon zijn verlichting alleen bedienen met zijn Google Home. Er waren online wel een beetje twijfels over hoe echt de tweet was, het verhaal, maar ik vroeg me af: "Hoe realistisch is zo'n scenario?"

00:06:38
Elmer Lastdrager: Behoorlijk realistisch. Dit exacte scenario ken ik niet, maar er zijn genoeg andere problemen ontstaan wanneer het internet uitvalt. Het mooie is, in Nederland hebben wij heel stabiel internet, het werkt eigenlijk bijna altijd. Dus als het niet werkt, dan is het de uitzondering. Als je bijvoorbeeld die verlichting thuis aan en uit zet via het internet, bijvoorbeeld via zo een spraak-assistent, of misschien een slim deurslot dat het internet nodig heeft. Dat werkt altijd, tot het moment dat het internet een keer uitvalt, of zelfs de stroom uitvalt. Dan merk je dat je toch tegen behoorlijke problemen aanloopt. Zo zijn er wel meer voorbeelden, dus de verlichting bijvoorbeeld, maar ik heb ook voorbeelden gelezen van mensen die een slimme thermostaat hebben. Als dan het internet uitvalt, zaten zij ook in de kou, ze konden het niet meer aanpassen.
00:07:34
Zegert van der Linde: Een paar uurtjes in de kou zitten is vervelend, maar overleven we waarschijnlijk. Zeker hier in Nederland kunnen we dat hebben over het algemeen. Maar je noemt ook slimme sloten, dat lijkt me ergens wel gevaarlijk als je huis ineens niet meer op slot kan bijvoorbeeld. Zijn apparaten daar op de één of andere manier voor beveiligd?
00:07:55
Elmer Lastdrager: Je ziet dat veel fabrikanten er nog mee bezig zijn, dus die hebben er wel over nagedacht. Vooral bij slimme sloten, zo een slot moet eigenlijk altijd blijven werken, dus vaak zitten daar batterijen in, en dan werkt het bijvoorbeeld via bluetooth, of dat je alsnog een sleutel erin kan stoppen. Dus er zijn wel manieren waarop het werkt, maar ik zou zeggen als consument moet je daar ook zelf even over nadenken. Dus probeer het bijvoorbeeld eens, trek de stekker van het internet er eens uit en kijk wat er gebeurt in het huis. Dat kan eigenlijk geen kwaad, om dat even te bekijken, terwijl je comfortabel op een zondagmiddag bijvoorbeeld, even daarnaar wil kijken. Wat gebeurt er dan? Als het een keer echt misgaat, dat je dan in ieder geval weet waar je afhankelijkheden liggen.
00:08:40
Zegert van der Linde: Privacy is natuurlijk ook altijd een thema als het hierover gaat. Bijvoorbeeld we noemden net al die slimme speakers, die eigenlijk altijd aanstaan, wie luistert er daar dan mee?
00:08:51
Elmer Lastdrager: Ja, wie luistert mee? Dat is een moeilijke vraag. Technisch gezien luisteren er best wel veel mee, bijvoorbeeld de fabrikant zou kunnen meeluisteren. Het is altijd de vraag: doen ze het ook, en wat is het nut er bijvoorbeeld van? Maar om een voorbeeld van slimme deurbellen te geven, je hebt zo een deurbel en daar zit een camera in, en daar zit ook een app bij en dergelijke. Die slaat ook beelden op in een cloudservice, een cloud-dienstverlening, dus dan wordt het op het internet opgeslagen, en dan zie je bijvoorbeeld in de Verenigde Staten dat daar de politie ook heel geïnteresseerd in is. Dus die willen heel graag van alle slimme deurbellen in de wijk de camerabeelden hebben, om te zien als er iets is gebeurd in de buurt. Dan kun je zeggen dat het voordelen heeft. Aan de andere kant heeft dat ook potentieel nadelen, want wat gebeurt er met al die beelden? De fabrikant heeft misschien toegang tot alle beelden, en dan zouden er heel veel mensen zeggen: "Ja, de politie mag van mij ook wel toegang hebben." Maar wat als hier ook bijvoorbeeld een privé beveiligingsbedrijf toegang heeft tot die beelden, of misschien heel iemand anders, of het kan best zijn dat er een hacker is die zegt: "Ik wil dat ook wel even zien." Dus die verschaft dan toegang tot zo een systeem, en heeft hij vervolgens ook toegang tot de beelden. Als je hoort dat de fabrikant en de politie toegang hebben, dan denk je: "Oké, veel mensen vinden dat dan wel prima." Maar het kan natuurlijk ook zijn dat de bad guys – om het zo maar even te zeggen – dat die ook toegang verschaffen.
00:10:22
Zegert van der Linde: Hoe meer mensen er eigenlijk toegang hebben tot dat systeem, hoe groter de kans is dat er iemand meekijkt waarvan je eigenlijk niet wil dat die meekijkt.
00:10:30
Elmer Lastdrager: Ja, dat is precies het geval. Als die data er niet is, dus als je geen slimme deurbel hebt, dan is er ook

geen risico. En als je die slimme deurbel wel hebt, dan kan er dus wat misgaan. Dan moet je voor jezelf nadenken: "Is dat iets wat ik prima vind als dat gebeurt?"

00:10:47

Zegert van der Linde: Toch was er twee jaar geleden een schandaal rondom Google, medewerkers zouden kunnen meeluisteren via de Google Home, ook op het moment dat ik niet tegen het apparaat praat. Hoe is het daar nu mee? Weet jij dat?

00:11:01

Elmer Lastdrager: Daar zijn ze wel redelijk mee bezig geweest, en ook Apple om een voorbeeld geven, daar gebeurde dat ook. Bij meerdere leveranciers leidde dat echt wel tot ophef, en dat was op zich wel te begrijpen dat ze meeluisteren. Om een voorbeeld te geven, bij heel veel van die apparaten roep je bijvoorbeeld: "Hé, Google!" om dat te activeren, en het kan best zijn dat op bepaalde momenten dat apparaat denkt: "Ben ik nu geroepen of niet?" Die weet het niet helemaal zeker, dus dan kan het handig zijn om die audio te laten beluisteren door medewerkers, om te bepalen of het apparaat hier een goede keuze heeft gemaakt door te luisteren, of niet? Dat is om het product te verbeteren, in die zin. Maar daardoor moeten ze dus wel meeluisteren met wat er gebeurt in huis, en dat vonden heel veel mensen geen prettig idee, waarschijnlijk terecht. Dus wat je ziet is dat dit soort bedrijven dat heel vaak via het zogenaamde opt-in zijn gaan doen, dus dat je expliciet toestemming moet geven, of het op zijn minst kunt uitschakelen dat je meedoet bij dit soort productverbetering. Dus als je het dan geen leuk idee vindt dat iemand mee kan luisteren, dan kun je dat gewoon uitzetten.

00:12:12

Zegert van der Linde: En dan luisteren ze ook echt niet meer mee? Dan doet alleen Google Home – dat apparaat – wat met jouw commando's?

00:12:20

Elmer Lastdrager: Dat is wat er gezegd wordt. Dat is natuurlijk wat lastig om helemaal te checken, als consument zijnde. Je weet niet wat er gebeurt, maar ze beloven dat ze niet meeluisteren, en dan moet je ze geloven daarop, of niet.

00:12:34

Zegert van der Linde: Je hoort toch best wel vaak van die verhalen van mensen die ergens over praten, iets heel specifieks, en dan zonder dat ze dat ooit opgezocht hebben, toch ineens advertenties daarvoor voorgeschoteld krijgen op internet. Zou dat ook door die apparaten kunnen komen?

00:12:50

Elmer Lastdrager: Ik ga het niet uitsluiten, maar ik durf dat niet te zeggen. Ik heb er nog geen bewijs voor gezien.

00:12:56

Zegert van der Linde: De fabrikanten zeggen: "Dat zijn wij niet in ieder geval."

00:12:59

Elmer Lastdrager: Ja, dat zullen ze zeggen.

00:13:01

Zegert van der Linde: Als ik nu zo een handig – want het is ook gewoon een handig apparaat, we hebben zelf ook zo een klein Google apparaatje in de woonkamer staan, en het is supergemakkelijk om even vanaf de keuken te roepen: "Hé, Google, speel de SeniorWeb Podcast af!" en dan gaat hij lekker de podcast afspelen bijvoorbeeld. Maar wat is voor jou een tip om deze apparaten goed en veilig te kunnen gebruiken?

00:13:30

Elmer Lastdrager: Lees je goed in, veel apparaten hebben ook een mogelijkheid om een wachtwoord in te stellen, doe dat ook. Dus zelfs als er al een standaard wachtwoord ingesteld staat, verander dat naar een eigen gekozen goed wachtwoord. Zorg dat de standaarddingen die je thuis moet doen, zorg dat je wifi netwerk goed beveiligd is. Een aantal van dat soort stappen kun je doen. Lees je goed in, kijk op het internet naar reviews, naar productbeoordelingen over die producten, en kijk wat andere mensen er over schrijven, en of daar ook iets over

privacy genoemd is. Voor heel veel apparaten kun je best logisch nadenken van wat er gebeurt. Zo een Google Home-apparaat stuurt de audio, dus alles wat het hoort, naar Google in dit geval. Maar voor sommige mensen die zeggen: "Dat maakt me helemaal niks uit." Andere mensen die zeggen: "Dat wil ik liever niet." Daar moet je dus even goed over nadenken wat je daarin prettig vindt.

00:14:30

Zegert van der Linde: Moet ik mijn modem of router ook nog speciaal instellen om dit soort apparaten goed te kunnen beveiligen?

00:14:36

Elmer Lastdrager: Veel modems en routers worden door de provider geleverd, die zijn vaak standaard goed beveiligd. Je zou nog een aantal dingen kunnen instellen, bijvoorbeeld de zogenaamde UPnP, dat zorgt ervoor dat apparaten binnen je netwerk automatisch hun poorten kunnen openzetten naar het internet, om daarmee dus binnenkomend verkeer mogelijk te maken. Dat zou je nog uit kunnen zetten als extra maatregel.

00:15:06

Zegert van der Linde: UPnP uitzetten is wel hogere internet-kunde, dus mocht u dat overwegen, kijk dan even in de tekst die bij deze aflevering staat. Daar staat een link naar een artikel waarin uitgelegd wordt hoe dit werkt. Elmer Lastdrager terug naar jou, nog andere tips voor de router?

00:15:22

Elmer Lastdrager: Verder is het een apparaat wat je aan het internet hangt, dus je bent wel een beetje afhankelijk van wat voor software er op dat apparaat staat, en wat die doet, dat is niet zo goed te zien. In dat geval moet je een goede fabrikant selecteren.

00:15:37

Zegert van der Linde: Moet je die software bijvoorbeeld dan ook nog updaten af en toe?

00:15:41

Elmer Lastdrager: Als er updates beschikbaar zijn, absoluut. Net als op de telefoon, net als op de computer, als er een update beschikbaar is, zorg altijd dat je die installeert, want er worden heel vaak beveiligingslekken mee gedicht. Dat geldt voor de internet of things apparaten natuurlijk helemaal. Niet voor alle apparaten is er een update beschikbaar, en sommige apparaten krijgen nooit updates. Dat is vooral voor de mensen die het zelf uit China importeren, van wat onbekendere merken. Die krijgen geen update, dus als daar een keer een beveiligingslek in gevonden wordt, dan valt dat nooit meer opgelost. Dat is ook wel het grote probleem, en daar is niet echt een oplossing voor, behalve apparaten kopen die wel geüpdatet kunnen worden. Dat kun je ook prima als een vraag stellen voordat je iets koopt. Stel de vragen aan de leverancier, of de winkel waar je het wil kopen: "Krijgt dit apparaat updates of niet?" Zolang er wel updates zijn, kunnen ze in ieder geval de boel beter beveiligen.

00:16:43

Zegert van der Linde: Dit klinkt allemaal best wel een beetje futuristisch, je koelkast die op het internet aangesloten is en dergelijke, maar ik heb ook ergens het gevoel dat we nog heel erg aan het begin staan hiervan. Wat denk jij? Hoe gaat dit zich ontwikkelen?

00:17:00

Elmer Lastdrager: Ik denk dat het echt nog in de kinderschoenen staat. In die zin is het eigenlijk een soort nieuwe industrie, dus het is een nieuwe groep producten. Ook al bestonden de producten misschien al, door ze met het internet te verbinden is er toch wat nieuws aangemaakt. Je ziet dat bij heel veel bedrijven hun businessmodel. Waar verdienen dat soort bedrijven hun geld mee? Met het verkopen van apparaten, en niet met het zorgen voor veilige apparaten. Dat verkoopt niet echt goed. Het is een heel veilig zonnepaneel omdat die goeie software-updates krijgt en dergelijke. Er zijn niet veel mensen die daar interesse in hebben. Bij een zonnepaneel denken mensen eerder: "Het moet zoveel mogelijk energie opleveren, en er moet een lage prijs zijn, en de installatie moet makkelijk zijn." Dus de veiligheid is in die zin niet echt een verkoopsargument voor de leverancier, en daar zie je dus ook dat het echt in de kinderschoenen staat, er zijn weinig regels. Die komen er overigens wel, het internet der dingen is niet heel nieuw,

dat bestaat al een aantal jaren, dus daar wordt echt wel aan gewerkt. Bijvoorbeeld door het agentschap Telecom in Nederland. Er komen wel regels aan, ook in Europees verband, met bijvoorbeeld minimum beveiligings-eisen, of een eis aan een fabrikant om tenminste een aantal jaar software-updates terug te leveren. Dus er wordt daar wel wat aan gedaan, maar het staat nog wel in de kinderschoenen, want er zijn heel veel apparaten beschikbaar die slecht beveiligd zijn. Die kunnen dan bijvoorbeeld gehackt worden, denk aan baby-camera's waarbij onbekende mensen kunnen meekijken, dat is altijd al een sprekend voorbeeld voor veel mensen. Maar ook verlichting die gehackt kan worden. En dan denken heel veel mensen: "Wat gebeurt er als mijn lamp gehackt wordt? Wat is dat? Dan kunnen ze de lamp aan of uit doen." Dat is natuurlijk één ding, maar ze kunnen je lamp ook gebruiken om een aanval op het internet uit te voeren, bijvoorbeeld om een banksite plat te leggen met een zogenaamde DDoS-aanval.

00:19:11

Zegert van der Linde: Elmer Lastdrager heeft mij later nog even precies uitgelegd hoe dat werkt, zo een gehackte lamp. Als een hacker toegang kan krijgen tot het systeem dat uw lampen bestuurt, kan die hacker daar een virus opzetten, dat kan hij doen bij onze lamp, maar natuurlijk ook bij alle andere slimme lampen in de buurt. Dat virus neemt dan de controle over de lamp over. Daar merken wij niks van, maar dat virus legt ook contact met de maker van dat virus, en die maker kan dan aan al die lampen die hij onder controle heeft tegelijkertijd een opdracht geven, bijvoorbeeld een DDoS-aanval. Al die lampen bezoeken tergelijkertijd dezelfde website, de servers van de site die op de achtergrond de website in de lucht houden kunnen al dat verkeer niet aan, en de site wordt platgelegd. Die is dan niet meer te gebruiken, en dat allemaal met zo een lamp.

00:19:58

Elmer Lastdrager: Allemaal via je lamp, dus dan draag je eigenlijk bij aan het platleggen van een bedrijf, en het uitvoeren van een internet-aanval, puur via de lamp. Dat is minder prettig, ook al ben je dan zelf niet echt slachtoffer, iemand anders is dat wel.

00:20:13

Zegert van der Linde: Even concluderend, wat zou jij zeggen: dit soort apparaten wel gebruiken, niet gebruiken of gewoon goed opletten?

00:20:23

Elmer Lastdrager: Ik zou het absoluut gebruiken, ik doe het zelf ook, maar kijk even goed wat je koopt, dus probeer het niet zelf te importeren uit China met onbekende merken, maar kijk goed dat het een betrouwbaar bedrijf is, een merk dat al bestaat. Denk aan Google Home bijvoorbeeld, je kunt er heel veel gevoelens hebben over de privacy, maar er zit wel een heel groot bedrijf achter dat niet het risico kan lopen dat er echt iets heel erg fout gaat. Dan krijg je enorme rechtszaken en dergelijke. Dus het feit dat er een enorm bedrijf achter zit, is aan de ene kant misschien een beetje eng, want data verzamelen is wat ze doen, aan de andere kant kan het ook geruststellend zijn dat er dus wel heel veel geld beschikbaar is om een goed product leveren. Dus denk er vooral goed over na, en als je toevallig een mooie wasmachine ziet met een wifi-verbinding, doe het vooral als je denkt dat het nuttig is.

00:21:20

Zegert van der Linde: Elmer Lastdrager Lastdrager, dank je wel. Dit was de vierde aflevering van de SeniorWeb Podcast. U luisterde naar een gesprek met Elmer Lastdrager Lastdrager van het SIDN, over the internet of things. Wilt u meer tips en informatie over online veiligheid en privacy? Kijk dan op www.seniorweb.nl en klik op online veiligheid en privacy. Wilt u de SeniorWeb Podcast volgen, dan kan dat het gemakkelijkste via een podcast-app op uw telefoon. Kijk voor een uitleg op seniorweb.nl/podcast. Dit was de laatste aflevering van deze serie van de SeniorWeb Podcast. Bedankt voor het luisteren.