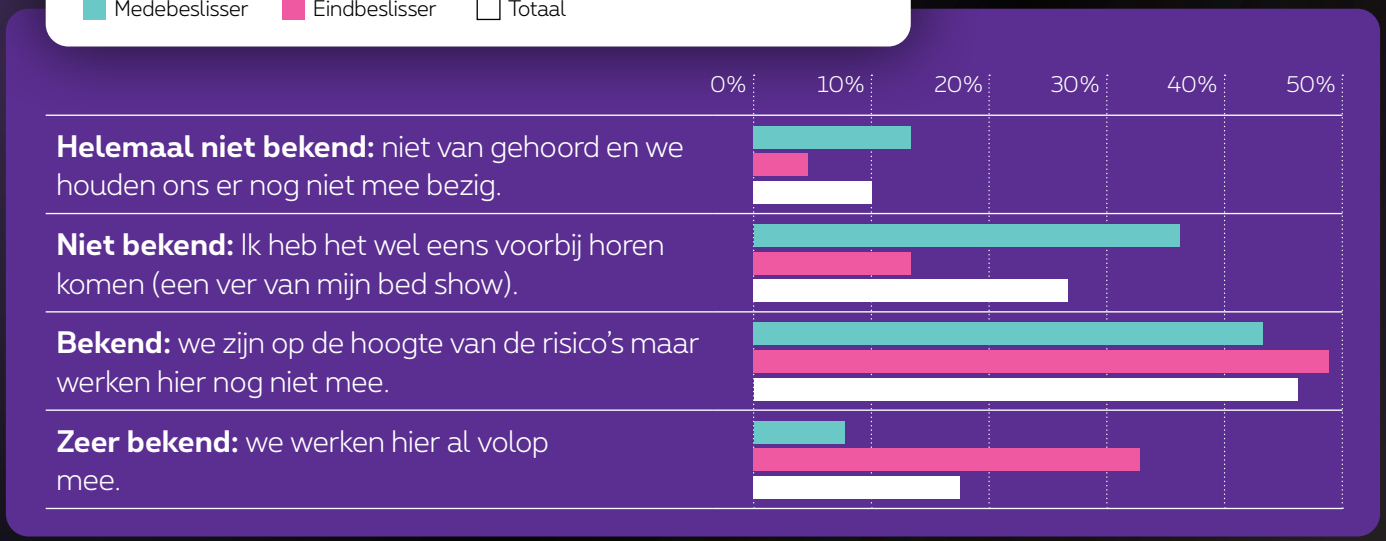
Een post-quantumveilige toekomst begint vandaag

Quantumcomputers staan op het punt om de technologische wereld drastisch te veranderen. Hun ongekende rekenkracht biedt enorme mogelijkheden voor innovatie, maar brengt ook risico's met zich mee. Deze nieuwe generatie computers kan bestaande encryptie breken, waardoor data die vandaag veilig lijkt, morgen kwetsbaar kan zijn.

Bedreigingen voor versleutelde data

Wat is nu precies de bedreiging? In de kern komt het erop neer dat quantumcomputers gebruikt kunnen worden om bestaande beveiligingsstandaarden, zoals RSA-encryptie, te doorbreken. Data die nu versleuteld wordt, kan met het 'store now, decrypt later'-principe later ontcijferd worden wanneer quantumcomputers voldoende krachtig zijn. Hackers stelen nu al geheime informatie om deze te ontcijferen zodra voldoende krachtige quantumcomputers beschikbaar komen. Of dat in 2030, 2035 of 2040 is, weten we niet. Daarover zijn de meningen verdeeld. Het advies van de AIVD is om gepaste maatregelen te nemen voor de data die na 2030 nog veilig moet zijn. Deze data noemen we langlevende data.

In hoeverre is quantum safe security bekend binnen jouw organisatie?



Onderzoek onder 382 IT-beslissers, Proximus NXT Nederland, 2024

proximus NXT
Nederland

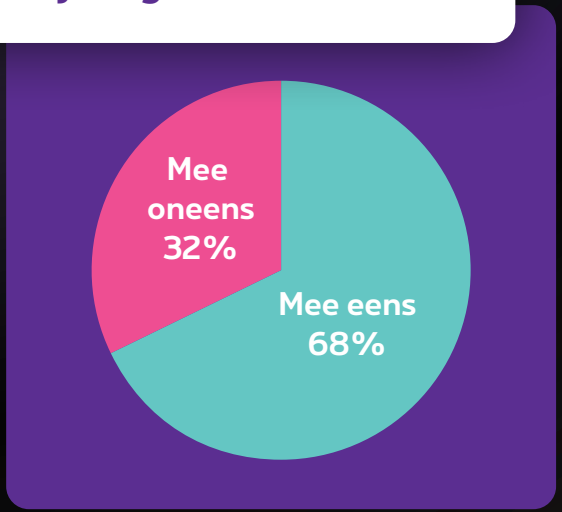
Toekomstbestendige beveiliging

Organisaties met gevoelige en langlevende data, zoals persoonsgegevens of intellectueel eigendom, moeten nu stappen ondernemen om toekomstige beveiliging te waarborgen. Binnen de zorg en andere sectoren is het essentieel om, ook in het kader van NIS2, de risico's van quantumcomputing in kaart te brengen. Zorg dat je voorbereid bent op nieuwe dreigingen en betrek dit bij de initiatieven om NIS2-compliant te zijn en blijven.

Nu beginnen met toekomstbestendige security

Het moge duidelijk zijn: uit bovenstaand onderzoek blijkt dat je als organisatie met gevoelige bedrijfsdata niet kunt afwachten en achteroverleunen. Vanuit het principe 'store now, decrypt later' is het dus slim om nu al te beginnen met de ontwikkeling van je quantum-safe roadmap. Het begint bij inzicht in je IT-infrastructuur. Hoe ziet het cryptografisch landschap eruit? Hoe zien de roadmaps van je leveranciers eruit met betrekking tot quantumbeveiliging? Breng risico's in kaart en prioriteer waar je als eerste maatregelen moet nemen. Welke langlevende data moet als eerste beveiligd worden?

Ik zie post-quantum decryptie niet als een reële dreiging voor mijn organisatie



Onderzoek onder 382 IT-beslissers, Proximus NXT Nederland, 2024

Dan is de vraag welke technologieën er nu al beschikbaar zijn om je te wapenen voor het post-quantum tijdperk. Er zijn drie oplossingen in de markt beschikbaar:

1. **Symmetrische encryptie**
2. **Quantum key distribution (QKD)**
3. **Post-quantum cryptografie**

Symmetrische encryptie wordt als quantumveilig beschouwd omdat de quantumcomputer in de toekomst, als hij voldoende krachtig is, de tijd om de beveiligingssleutel te kraken maximaal kan halveren. Dat komt neer op duizenden, zo niet miljoenen jaren. Als dit onvoldoende is, is het advies om te migreren naar de nu beschikbare post-quantum cryptografiestandaarden. Het is ook mogelijk om gebruik te maken van quantum key distribution. Dit is quantumveilig, maar erg kostbaar en nog niet stabiel over lange afstanden.

Beschermd en beschikbaar

Proximus NXT zorgt voor een sterke beveiliging door symmetrische en asymmetrische encryptie samen te gebruiken. Organisaties kunnen hiermee nu direct hun data goed beschermen én zich voorbereiden op de toekomst met post-quantumtechnologie. Onze aanpak zorgt ervoor dat gevoelige informatie veilig blijft, zelfs als quantumcomputers krachtiger worden. En dat worden ze. De vraag is alleen hoe snel. Gaat jouw organisatie de race aan om dataveiligheid?