Deloitte.

AUDIT VLAANDEREN

Cyber hygiëne en veiligheid voor lokale besturen

14 September 2022

Introductie

Hoe kijkt uw organisatie naar cyber security?

Aanpak ICT-veiligheidsaudit

Cyberveiligheid vereist een holistische aanpak

Governance IT-beveiliging			
Strategie en operationeel model	Richtlijnen, standaarden en architectuur	Cultuur en gedrag	Risicobeheer, metrieken en rapportering
Beveiliging		**Waakzaamheid**	**Veerkracht**
Cloud & Beheer derde partijen	Opzet en beheer infrastructuur	Identificatie en beheer van kwetsbaarheden	Beheer van IT-beveiligingsincidenten
Identiteits- en toegangsbeheer	Informatiebescherming	Dreigingsbeheer	IT-beveiliging in bedrijfscontinuïteit en herstel
Applicatie ontwikkeling en beheer	Personeel en gebouwen	Monitoring events IT-beveiliging	

Aanpak ICT-veiligheidsaudit

Externe Infrastructuur Securitytest

Interne Infrastructuur Securitytest

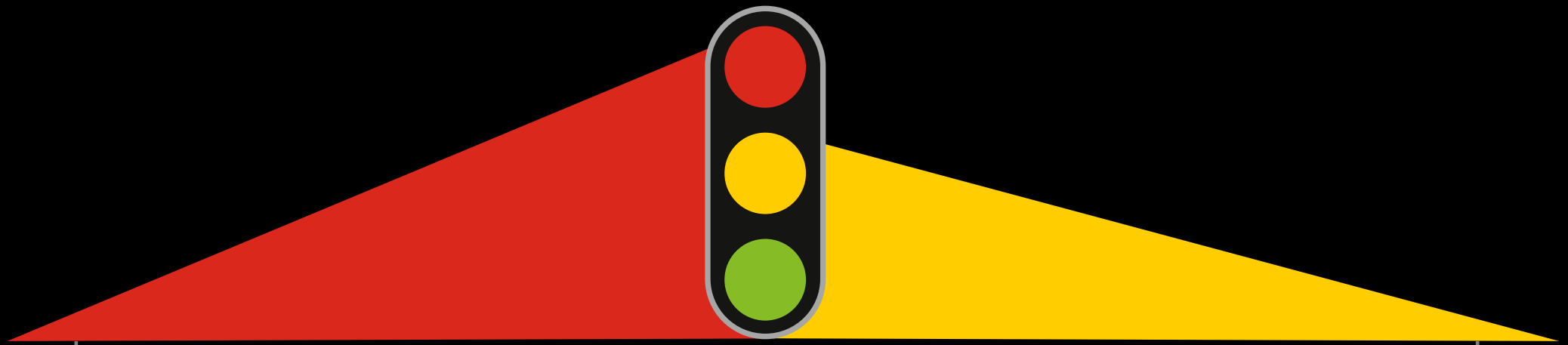
Toegangscontrole Securitytest

Analyse kader en rapportering Organisatie-beheersing & aanpak ICT-risico's

Analyse Bedrijfscontinuïteit

Testen zoals cyber-aanvallers denken & werken

Belangrijkste kwetsbaarheden



- **Interne Infrastructuur Securitytest**
- **Toegangscontrole Securitytest**
- **Analyse Bedrijfscontinuïteit**
- **Externe Infrastructuur Securitytest**
- **Analyse kader en rapportering organisatiebeheersing & aanpak ICT-risico's**

Belangrijkste kwetsbaarheden

Externe Infrastructuur Securitytest

Geen Multi-Factor Authenticatie

78%

Beheersinterfaces beschikbaar over het Internet

31%

Verouderde en kwetsbare software

30%

Mogelijkheid om e-mails te versturen in naam van anderen

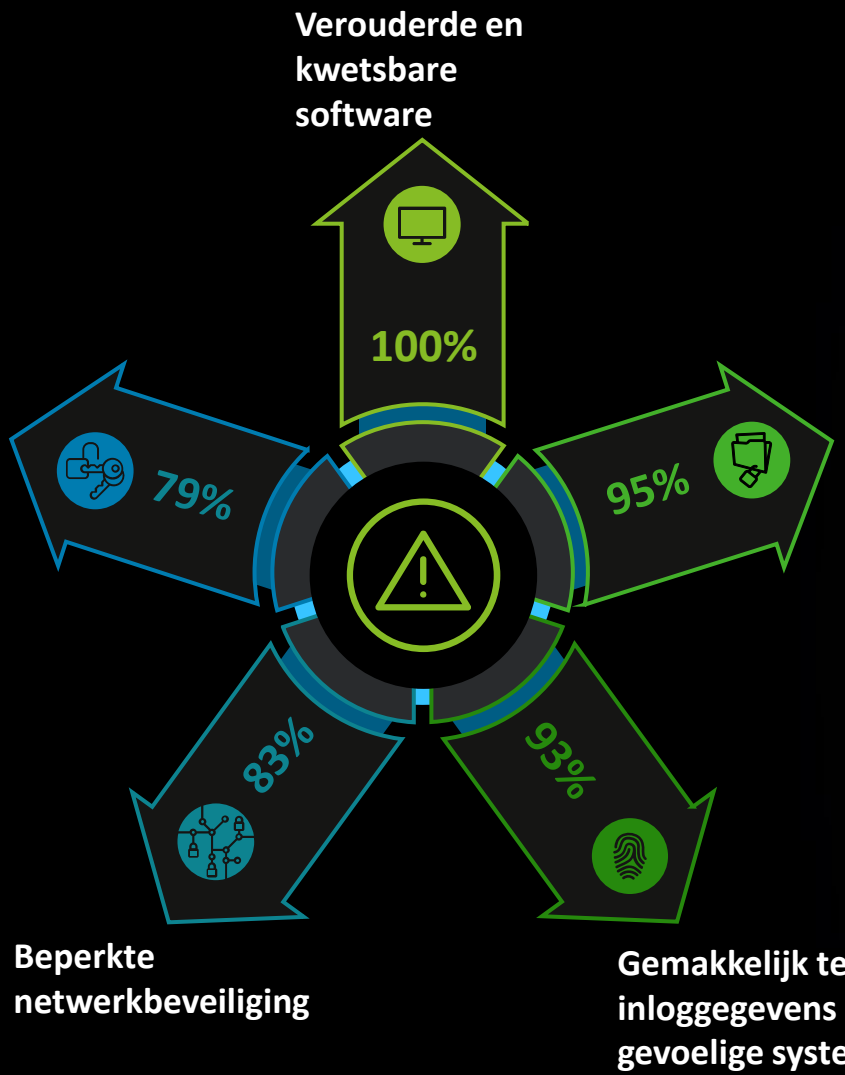
20%

Externe systemen

Percentage van de geteste lokale besturen waar deze kwetsbaarheden gevonden zijn

Belangrijkste kwetsbaarheden

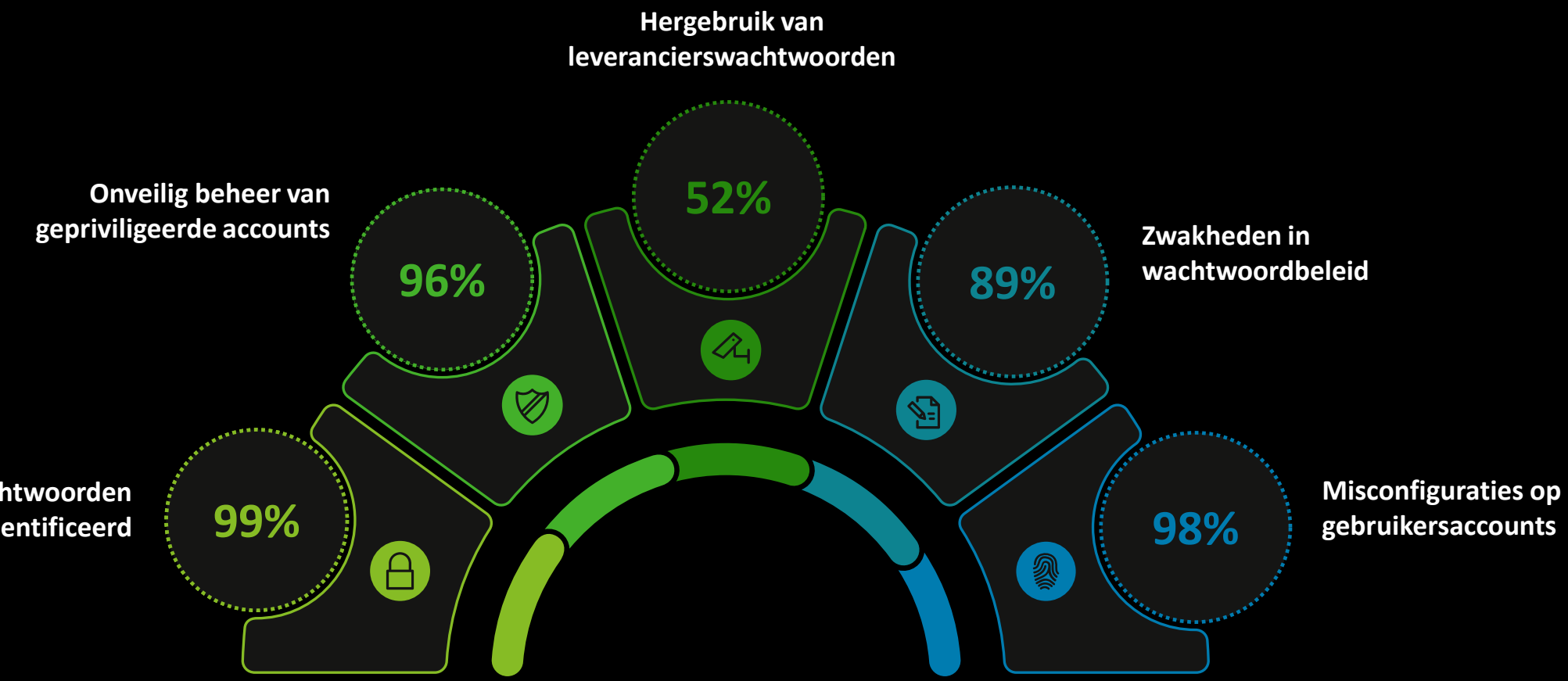
Interne Infrastructuur Securitytest



Percentage van de geteste lokale besturen waar deze kwetsbaarheden gevonden zijn

Belangrijkste kwetsbaarheden

Toegangscontrole Securitytest



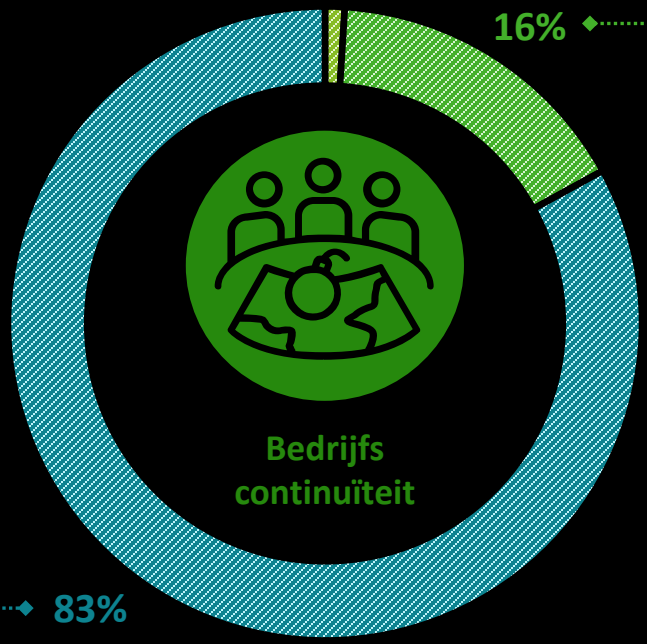
Percentage van de geteste lokale besturen waar deze kwetsbaarheden gevonden zijn

Belangrijkste kwetsbaarheden

Analyse Bedrijfscontinuïteit

Volledig uitgewerkt bedrijfscontinuïteitsplan — 1%

Geen volwaardig bedrijfscontinuïteitsplan — 16%

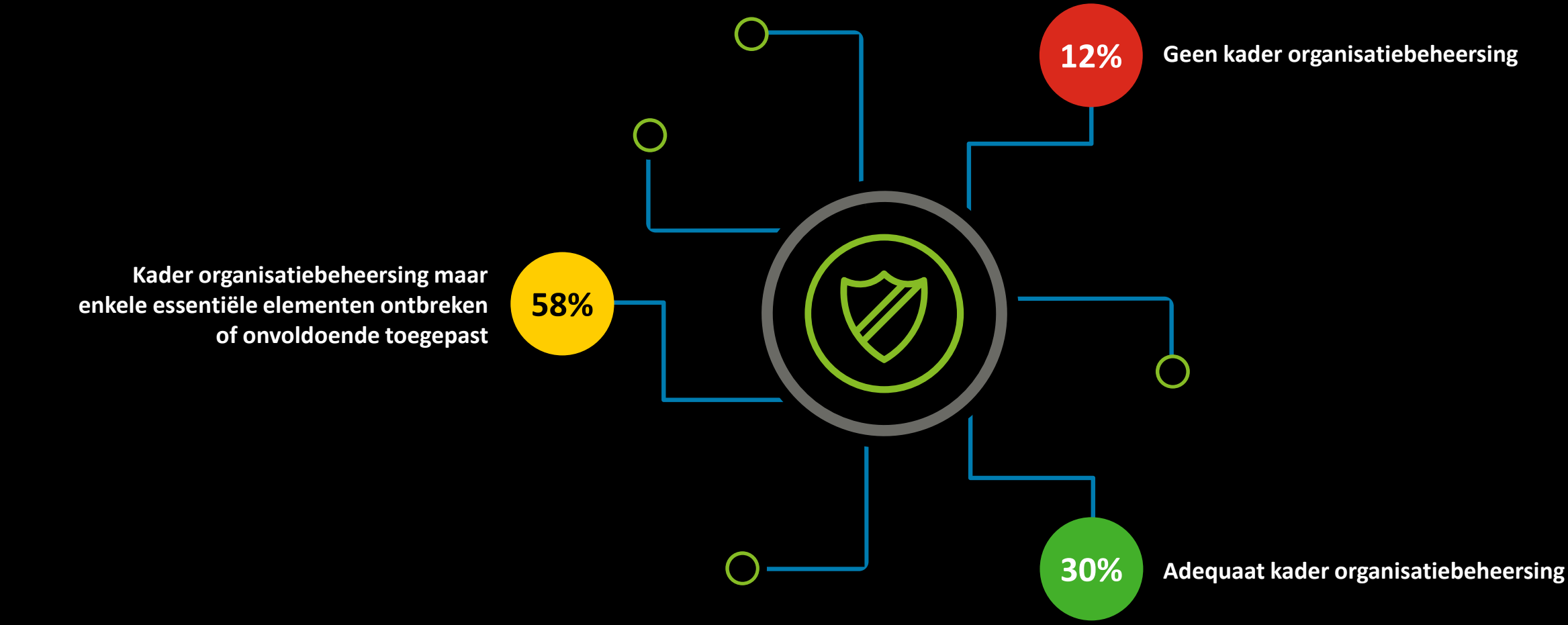


Geen bedrijfscontinuïteitsplan beschikbaar — 83%

Percentage van de geteste lokale besturen waar deze kwetsbaarheden gevonden zijn

Belangrijkste kwetsbaarheden

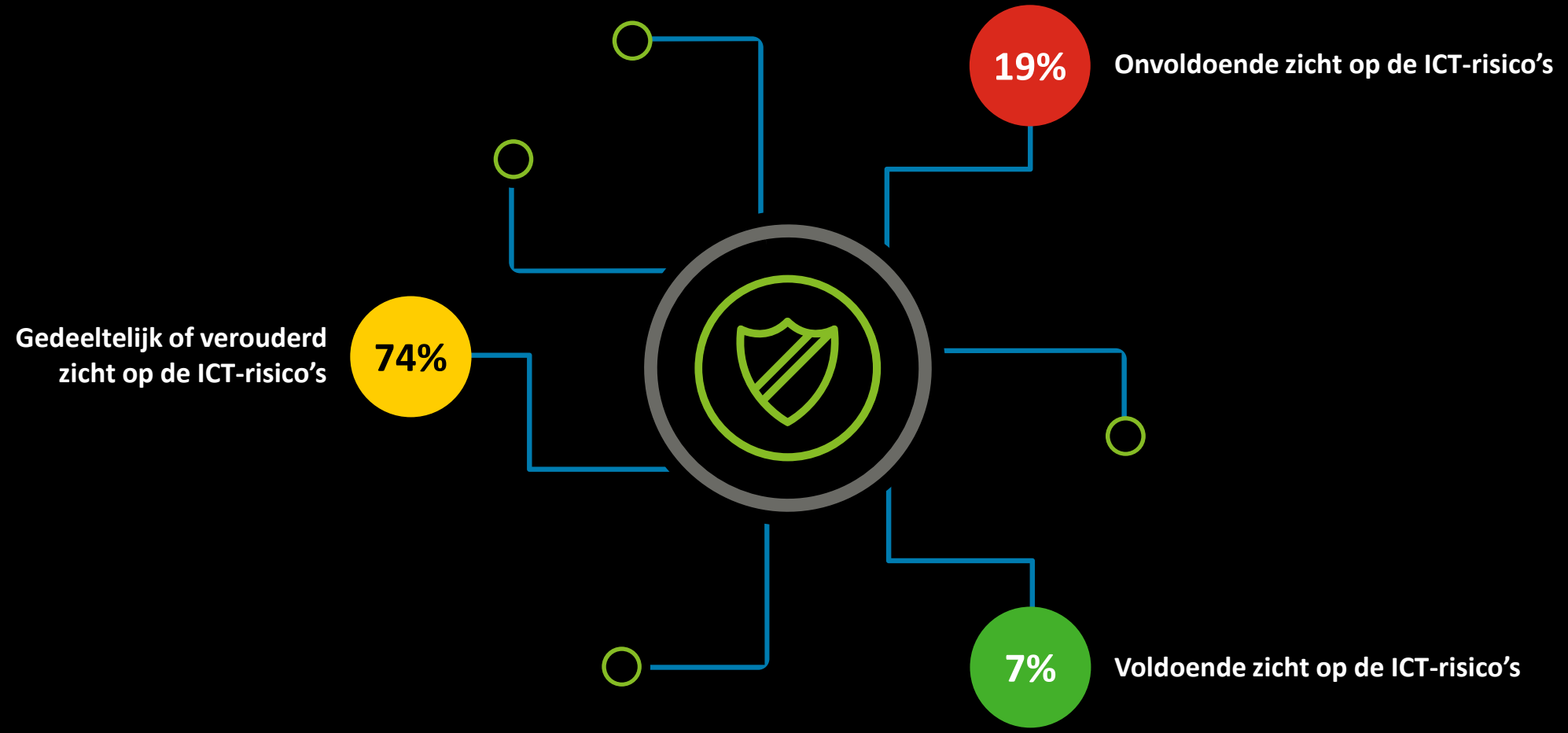
Analyse kader en rapportering organisatiebeheersing & aanpak ICT-risico's



Percentage van de geteste lokale besturen waar deze kwetsbaarheden gevonden zijn

Belangrijkste kwetsbaarheden

Analyse kader en rapportering organisatiebeheersing & aanpak ICT-risico's



Percentage van de geteste lokale besturen waar deze kwetsbaarheden gevonden zijn

Aanbevelingen

- Security Bewustzijn
- Multi-Factor Authenticatie
- Cyber risico beheer & regelmatig testen
- Bedrijfscontinuïteit
- ICT-veiligheidsaudit

Resultaten na de ICT-veiligheidsaudits

“De audit leverde ons interessante info aan waarmee onze ICT-dienst verdere stappen kan zetten.”

“We zijn tevreden over de samenwerking en zijn onmiddellijk aan de slag gegaan om de ICT-veiligheid van onze gemeente te verbeteren. Samen met onze IT-partner hebben we een actieplan opgesteld, waarvan de eerste acties werden uitgevoerd.”

“Dit resulteerde in een degelijk rapport met aanbevelingen en te ondernemen acties om alles IT-veiliger te maken zowel voor de interne als de externe gebruikers van ons IT-platform”

“We hebben al wel wat audits gehad, maar nog geen in zo’n duidelijke en klare taal (lees niet in het ‘ICT-nees’ voor de niet IT profielen) en acties waarmee we dadelijk aan de slag konden gaan”

“Bedankt voor jullie bijdrage aan de verbetering van onze IT Infrastructuur”

Resultaten na de ICT-veiligheidsaudits

Alle lokale besturen zijn aan de slag gegaan om de vastgestelde kwetsbaarheden weg te werken

De impact van een cyberaanval en de gevolgen op de werking zijn duidelijker voor de leidinggevenden

Min. 15 lokale besturen zijn met behulp van de auditfirma gestart met de opmaak van een BCP

Bij 8 lokale besturen werd door de auditfirma nadien een hertest uitgevoerd met aanzienlijk verbeterde resultaten (minder kwetsbaarheden vastgesteld)

Tussentijdse resultaten, aantallen kunnen ondertussen hoger liggen

Vragen?

AUDIT VLAANDEREN

ICT-veiligheidsaudits@vlaanderen.be

Deloitte.

beauditvlcyber@deloitte.com