Rapport DEN Cyber Security Scan

23 mei 2023

DEN

Rode draden uit de resultaten

DEN

Respondenten

De respondenten vertegenwoordigen grote en kleine organisaties van alle typen, waarbij met name museum en erfgoedorganisaties, podiumkunsten en poppodia goed zijn vertegenwoordigd.

Respondenten zijn met name directeuren en bestuurders van organisaties, of medewerkers die betrokken zijn bij de ICT van organisaties: hun antwoorden kunnen anders zijn dan die van medewerkers in andere rollen.

De vragenlijst is door 120 respondenten geheel of gedeeltelijk ingevuld. De resultaten zijn daarmee niet representatief, maar zeker **indicatief**.

Incidenten

Bij bijna **3 op elke 10 organisaties** heeft de afgelopen 3 jaar een **digitaal veiligheidsincident** plaatsgevonden waarbij IT-systemen bewust zijn ontregeld en/of waarbij gegevens zijn ontvreemd. **Bij 1 op elke 20 organisaties zelfs méér dan eens.**

Inzicht

Er zijn verhoudingsgewijs **geen verschillen tussen grote en kleine organisaties** waar het aantallen incidenten betreft.

Regelmatig wordt aandacht besteed aan een **sterk wachtwoord** dat regelmatig wordt gewijzigd, **uitsluitend toegang** verlenen tot systemen en gegevens die nodig zijn voor het takenpakket, een **apart gasten(wifi-)netwerk** voor bezoekers, **up-to-date antivirus software**. Aan het herkennen van **phishing e-mails en onbetrouwbare links** en aan het **downloaden en installeren van software op systemen** van de organisatie wordt vaker af en toe dan regelmatig aandacht besteed.

De meeste respondenten geven aan dat het voor hen **duidelijk is welke gegevens en systemen interessant zijn voor cybercriminelen**, grote organisaties meer dan kleine. Ook geeft bijna driekwart van de respondenten aan zich zeker **wel bewust** te zijn van digitale veiligheid en daarom zorgvuldig te handelen met systemen, apparaten, applicaties en (persoons-)gegevens, maar de grote organisaties zijn zich hier meer bewust van dan de kleine.

Beleid en schade

De meeste organisaties hebben **geen overkoepelend beleid** voor digitale veiligheid, **delen geen kennis** met de medewerkers over beveiligingsincidenten en datalekken en hebben **geen handleidingen** voor medewerkers beschikbaar over hoe met welke gegevens en informatie moet worden omgegaan. 65% van de organisaties heeft **geen budget** specifiek voor cybersecurity-maatregelen gereserveerd.

Voor **DEN** wordt een mogelijke rol gezien bij ondersteuning door **kennis** delen en **voorlichting** geven, het faciliteren van een **community** en ook door verzorgen van **educatie**, **tooling** en centraal georganiseerde producten en diensten (**shared services**), zoals een collectieve verzekering, informatie over minimale eisen aan de beveiliging en ondersteuning bij het in kaart brengen van risico's en het treffen van adequate maatregelen.

Er is **ruime behoefte aan (extra) ondersteuning** op het gebied van digitale veiligheid/cyber security.

De helft van de respondenten geeft aan dat de organisatie **zeker geen verzekering** tegen cybercriminaliteit heeft, nog eens een derde weet het niet.

Behoeften en rol van DEN

De schade van een incident waarbij digitale systemen niet meer werken is **voor 44% van de organisaties zeer hinderlijk tot zeer ingrijpend**, met beperkte tot aanzienlijke (financiële) schade tot gevolg.

Uitkomsten van de vragenlijst

Inzicht
Respondenten, met name directeuren en bestuurders van organisaties, of medewerkers die betrokken zijn bij de ICT van organisaties, hebben een goed beeld van welke gegevens en systemen interessant zijn voor cybercriminelen. Ook zijn de meeste respondenten zich zeker bewust van digitale veiligheid en handelen daarom zorgvuldig met systemen, apparaten, applicaties en (persoons)gegevens. Geldt wel: grote organisaties hebben een beter beeld en zijn zich meer bewust dan kleinere organisaties.

Digitale veiligheid & beleid
Het onderwerp digitale veiligheid krijgt aandacht bij culturele organisaties. Regelmatig wordt aandacht besteed aan sterke wachtwoorden autorisatie tot systemen en gegevens, een apart gasten(wifi-)netwerk voor bezoekers, up-to-date antivirus software een – in mindere mate - aan phishing emails, onbetrouwbare links en het downloaden en installeren van onbekende software.

Tegelijk hebben de meeste organisaties geen overkoepelend beleid voor digitale veiligheid, delen ze geen kennis met de medewerkers over beveiligingsincidenten en datalekken en/of hebben ze geen handleidingen voor medewerkers beschikbaar over hoe met welke gegevens en informatie moet worden omgegaan. 65% van de organisaties heeft bovendien geen budget specifiek voor cybersecurity-maatregelen gereserveerd, de overgrote meerderheid heeft zeker geen verzekering tegen cybercriminaliteit of weet het niet.

Incidenten
En dat terwijl digitale veiligheidsincidenten bij culturele organisaties wel vaker voorkomen: 3 op de 10 organisaties, naar verhouding evenveel kleine als grote, werden in de afgelopen 3 jaar IT-systemen bewust ontregeld en/of werden gegevens van ontvreemd. De schade van een incident waarbij digitale systemen niet meer werken is voor de bijna de helft van de organisaties zeer hinderlijk tot zeer ingrijpend, met beperkte tot aanzienlijke (financiële) schade tot gevolg.

Respondenten
De vragenlijst is door 120 respondenten geheel of gedeeltelijk ingevuld. De resultaten zijn daarmee niet representatief, maar zeker indicatief. De respondenten vertegenwoordigen grote en kleine organisaties van alle typen, waarbij met name museum en erfgoedorganisaties, podiumkunsten en poppodia goed zijn vertegenwoordigd.

Vervolgstappen DEN

Behoefte aan ondersteuning
Er is onder de respondenten ruime behoefte aan (extra) ondersteuning op het gebied van digitale veiligheid/cyber security. Belangrijke factoren bij ondersteuning op het gebied van digitale veiligheid zijn voor respondenten deskundigheid, meedenken over privacy en ethiek, onpartijdigheid en ook bekend zijn met de culturele sector en kunnen helpen met andere ICT- en digitaliseringsvraagstukken.

Voor DEN wordt zeker een mogelijke rol gezien bij ondersteuning door kennis delen en voorlichting geven, het faciliteren van een community en ook door verzorgen van educatie, tooling en centraal georganiseerde producten en diensten (shared services), zoals een collectieve verzekering, informatie over minimale eisen aan de beveiliging en ondersteuning bij het in kaart brengen van risico's en het treffen van adequate maatregelen.

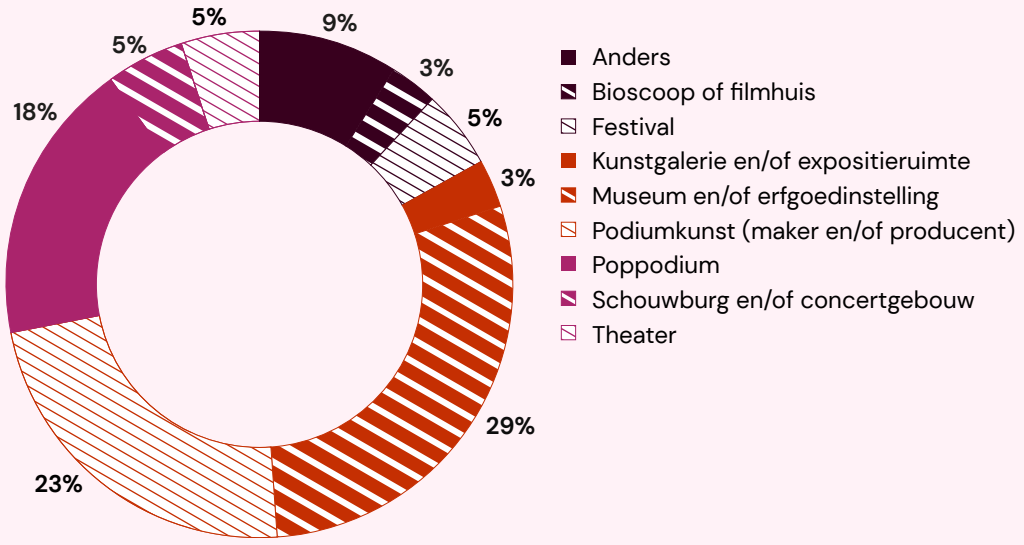
Voornemens vanuit DEN
Op basis van deze uitkomsten wil DEN het volgende gaan aanbieden:

- **Aandacht voor het onderwerp in alle uitingen** – digitale veiligheid is een integraal en onlosmakelijk onderdeel van digitale transformatie. Inclusief bewustwordingscampagne. DEN publiceert hierover op den.nl en via LinkedIn.
- I**nformatie en doorverwijzingen voor organisaties bieden:** handige tools (zoals van het Digital Trust Center van het ministerie van EZK) om de eigen cyberveiligheid te testen en tips voor verbetering
- **Ontwikkelen van een stappenplan** specifiek voor de cultuursector
- **Opzetten van een community** van professionals en geïnteresseerden in de cultuursector rondom het thema digitale veiligheid
- **Onderzoek naar collectieve producten en diensten**, zowel preventief als reactief: aansluiten op een security operations center, collectieve verzekeringen, collectieve diensten voor hulp/herstel bij een incident, etc.

Mooi indicatief beeld van de brede culturele sector

153 respondenten hebben de vragenlijst geopend, 120 van hen hebben de vragenlijst deels of volledig ingevuld. In deze presentatie zijn de antwoorden per vraag weergegeven in percentage van het aantal respondenten dat de vraag heeft beantwoord (n=...), waarbij sommige vragen door aanzienlijk meer respondenten zijn beantwoord dan andere. Op basis van de aantallen kan niet gesproken worden van (statistisch) representatieve uitkomsten, wel van een mooi indicatief beeld.

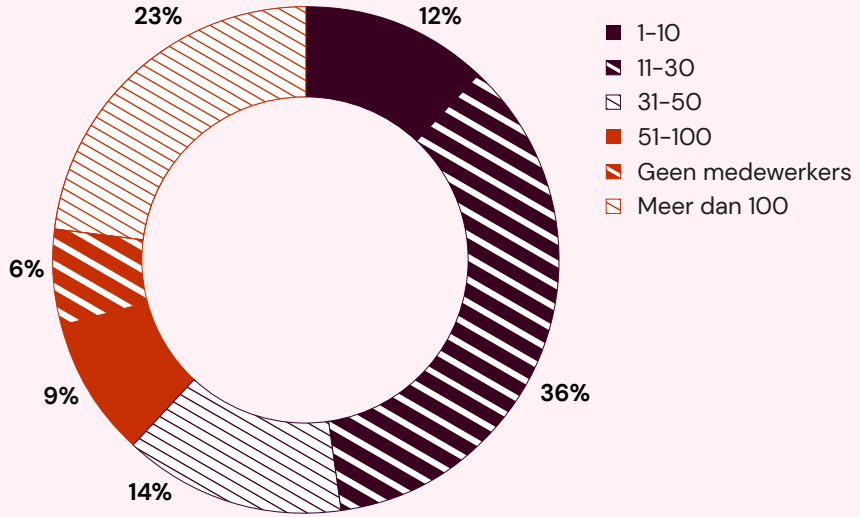
Er is een aardige spreiding over verschillende typen organisaties, waarbij met name museum en erfgoedorganisaties, podiumkunsten en poppodia goed zijn vertegenwoordigd.



Hoeveel werknemers (vast én zzp) werken in je organisatie? (n=77)

Mooi indicatief beeld van de brede culturele sector

Het betreft organisaties van diverse grootte: van grote met meer dan 100 medewerkers tot organisaties zonder medewerkers. Respondenten waren het vaakst werkzaam in organisaties met 11 tot 30 medewerkers of in organisaties met meer dan 100 medewerkers.



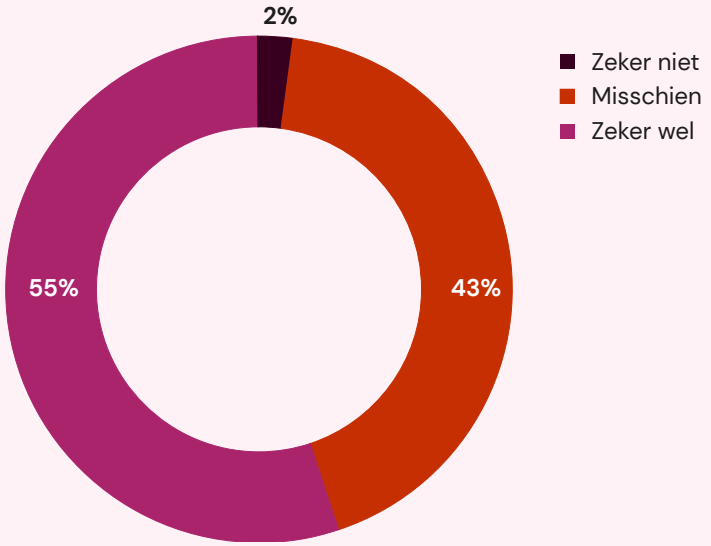
Hoeveel werknemers (vast én zzp) werken in je organisatie? (n=66)

De rollen van de respondenten zijn wellicht minder representatief

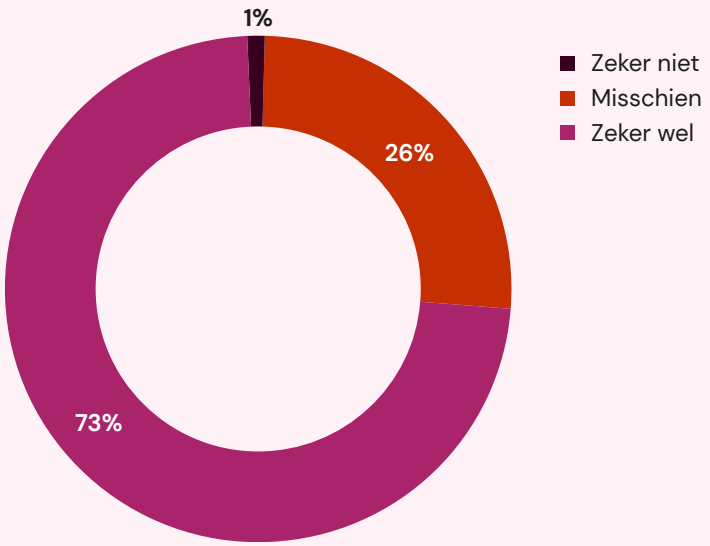
De vragenlijst is grotendeels ingevuld door directeuren en bestuurders van organisaties of door medewerkers die betrokken zijn bij de ICT van ogani-saties. Door de complexiteit van de vragen is deze doelgroep opgeroepen de vragenlijst in te vullen. Deze groep heeft namelijk waarschijnlijk het beste zicht op wat er binnen de organisatie geregeld is en gebeurt op het gebied van gegevensbeveiliging. Deze groep zal zich ook goed bewust zijn van de waarde van systemen, apparaten, applicaties en (persoons)gegevens voor de bedrijfsvoering, alsmede van de risico's van cybercrime. Het is wel denkbaar dat medewerkers in andere rollen binnen de culturele organisaties een ander kennisniveau hebben en zich minder bewust zijn van risico's van cybercrime.

Een goed bewustzijn van waarde van systemen en gegevens en van risico's

De meeste respondenten geven aan dat het voor hen duidelijk is welke gegevens en systemen interessant zijn voor cybercriminelen. Ook geeft bijna driekwart van de respondenten aan zich zeker wel bewust te zijn van digitale veiligheid en daarom zorgvuldig te handelen met systemen, apparaten, applicaties en (persoons)gegevens.



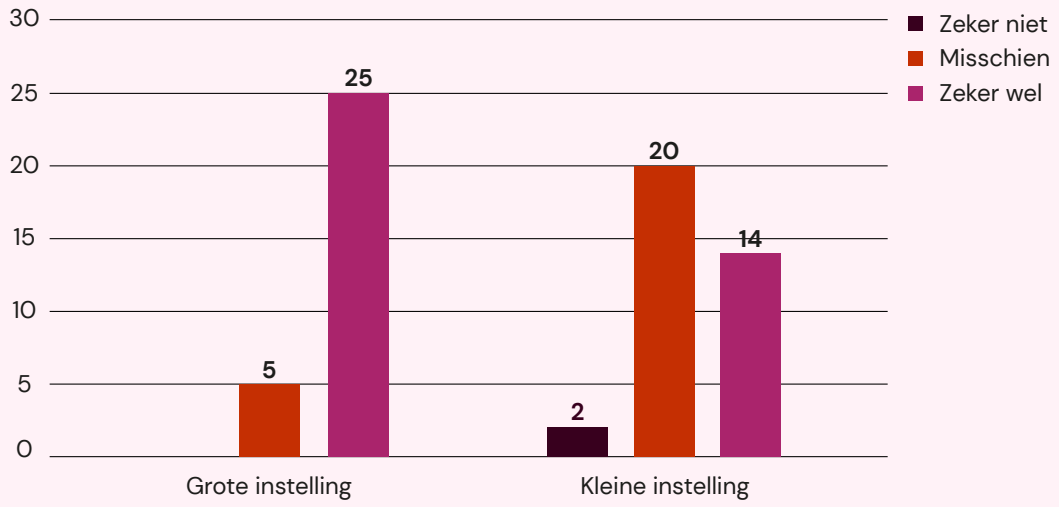
Het is voor mij duidelijk welke systemen en gegevens interessant zijn voor cybercriminelen (n=120)



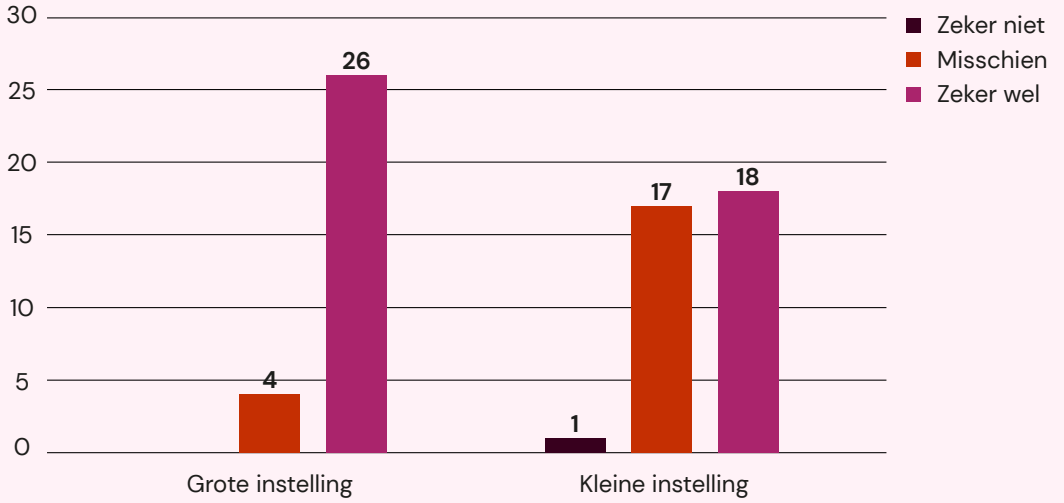
Ik ben mij bewust van digitale veiligheid en handel zorgvuldig met systemen, apparaten, applicaties en (persoons)gegevens. (n=117)

Een goed bewustzijn van waarde van systemen en gegevens en van risico's

Uitgesplitst naar kleine (tot en met 30 medewerkers) en grote organisaties (meer dan 30 medewerkers) blijken (respondenten van) kleine organisaties minder zeker te weten welke gegevens en systemen interessant zijn voor cybercriminelen en minder bewust van digitale veiligheid en zorgvuldig omgaan met systemen, apparaten, applicaties en (persoons)gegevens.



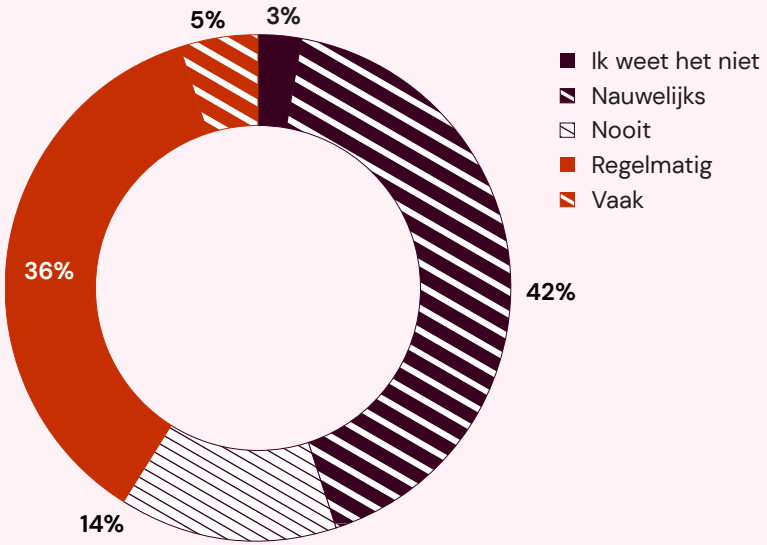
Het is voor mij duidelijk welke systemen en gegevens interessant zijn voor cybercriminelen (n=120)



Ik ben mij bewust van digitale veiligheid en handel zorgvuldig met systemen, apparaten, applicaties en (persoons)gegevens. (n=117)

Beleid voor digitale veiligheid, kennisdeling en handleidingen

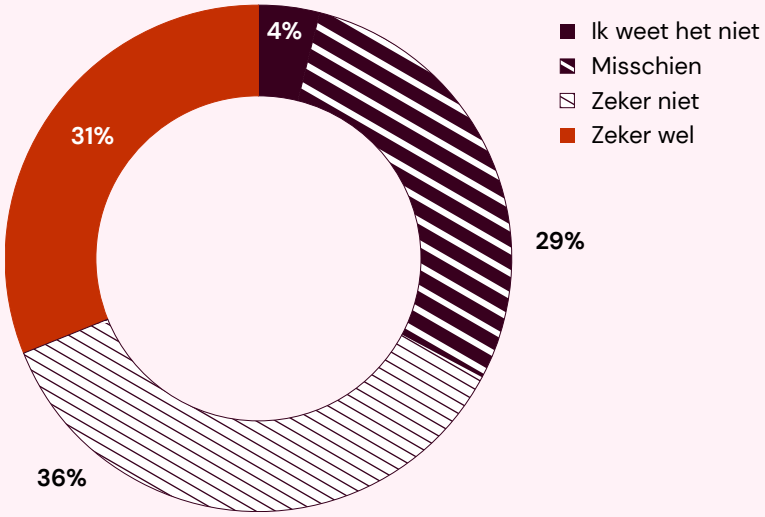
Veruit de meeste respondenten geven aan dat hun organisatie zeker geen (42%) of misschien (35%) een overkoepelend beleid heeft voor digitale veiligheid, zodat alle medewerkers een actueel beeld hebben wat er op dat gebied te doen is. Ook wordt in ruim de helft van de gevallen geen (14%) of nauwelijks (42%) kennis gedeeld met de medewerkers over wat beveiligingsincidenten en datalekken zijn en hoe men deze kan voorkomen.



De organisatie waar ik voor werk deelt kennis met de medewerkers over wat beveiligingsincidenten en datalekken zijn en hoe men deze kan voorkomen (n=110)

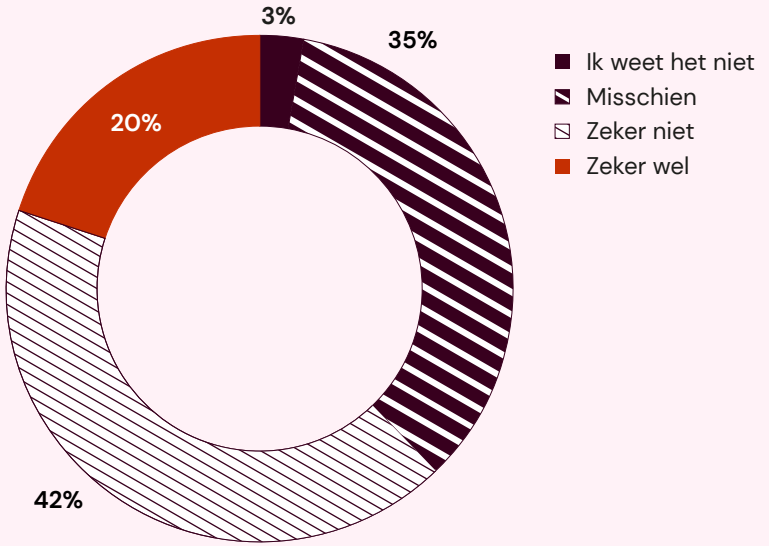
Beleid voor digitale veiligheid, kennisdeling en handleidingen

De meeste organisaties hebben zeker geen (36%) of hooguit misschien (29%) handleidingen voor medewerkers beschikbaar over hoe met welke gegevens en informatie moet worden omgegaan.



De organisatie waar ik werk heeft handleidingen voor medewerkers beschikbaar over hoe met welke gegevens en informatie moet worden omgegaan (n=113)

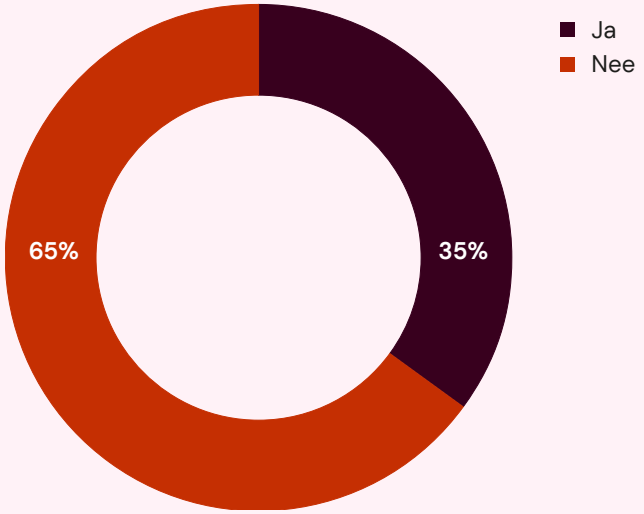
65% van de respondenten geeft aan dat hun organisatie geen budget specifiek voor cybersecurity-maatregelen heeft gereserveerd.



De organisatie waar ik werk heeft een overkoepelend beleid voor digitale veiligheid (cyber security) en deelt dit intern zodat de medewerkers een compleet en actueel beeld hebben van wat er op dat gebied is ingericht (n=107)

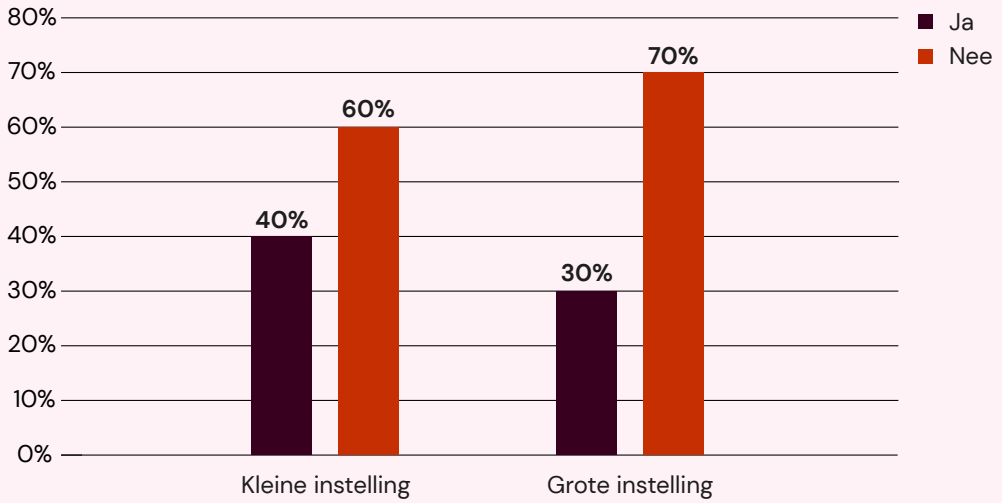
Budget voor digitale veiligheid

Ruim tweederde van de organisaties hebben geen budget gereserveerd specifiek voor cybersecuritymaatregelen.



De organisatie waar ik werk heeft budget gereserveerd specifiek voor Cyber Security maatregelen (n=98)

Wanneer we deze cijfers uitsplitsen naar kleine (tot en met 30 medewerkers) en grote organisaties (meer dan 30 medewerkers) dan blijken de percentages elkaar niet veel te ontlopen: het is verhoudingsgewijs niet zo dat grote organisaties veel vaker een budget reserveren voor cybersecurity dan kleine organisaties.

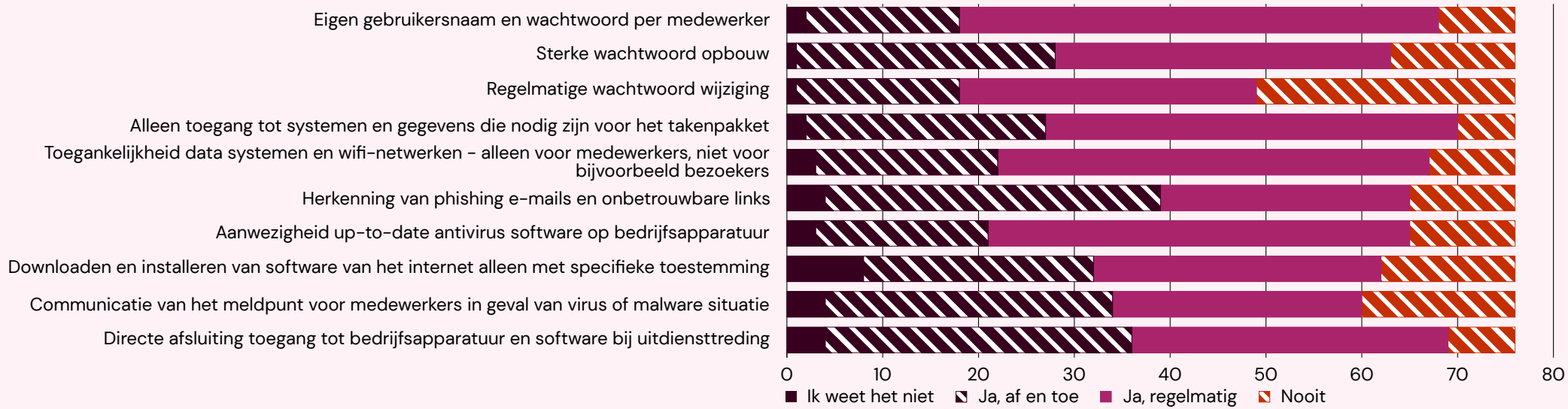


De organisatie waar ik werk heeft budget gereserveerd specifiek voor Cyber Security maatregelen (n=98, verdeeld naar grote en kleine organisaties)

Aandacht voor onderwerpen rondom digitale veiligheid

Instelllingen besteden regelmatig aandacht aan een sterk wachtwoord dat regelmatig moet worden gewijzigd, uitsluitend toegang verlenen tot systemen en gegevens die nodig zijn voor het takenpakket, een apart gasten (wifi-) netwerk voor bezoekers, up-to-date antivirus software.

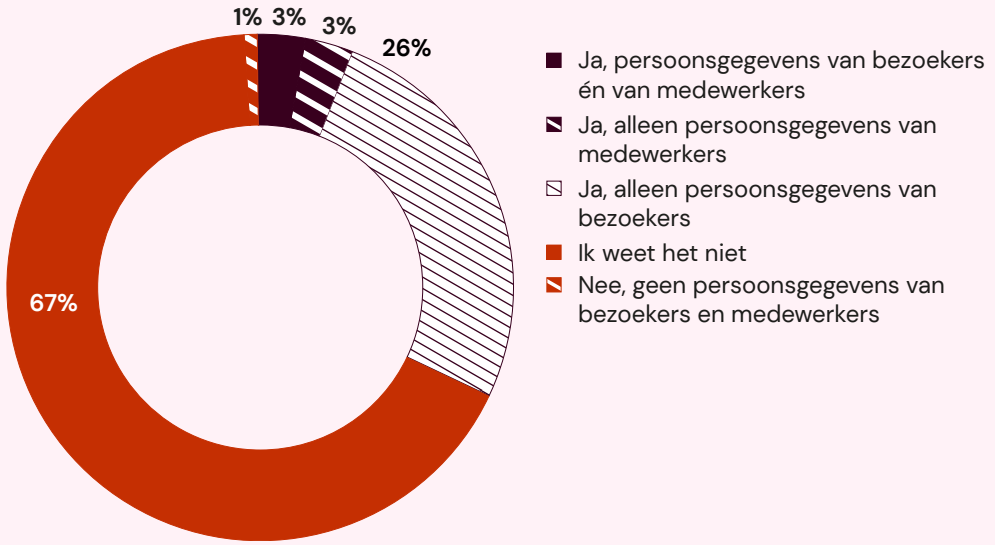
Aan het herkennen van phishing emails en onbetrouwbare links en aan het downloaden en installeren van software op systemen van de organisatie wordt vaker af en toe dan regelmatig aandacht besteed.



Aan welke van de volgende onderwerpen rondom digitale veiligheid en cyber security besteedt de organisatie waar jij werkt (regelmatig) aandacht?

Persoonsgegevens en andere digitale gegevens met waarde

Nagenoeg alle respondenten geven aan persoonsgegevens te verwerken binnen hun organisatie: twee derde van medewerkers én bezoekers, een kwart alleen persoonsgegevens van medewerkers.



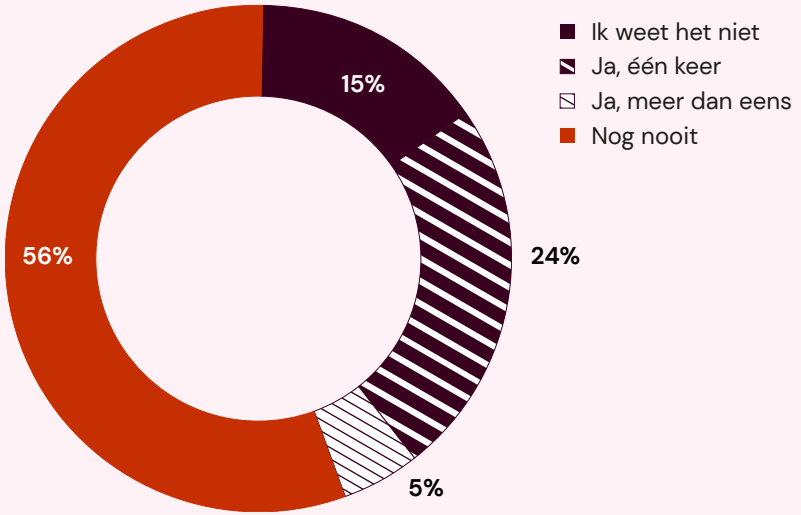
Verwerkt de organisatie waar je werkt persoonsgegevens van bezoekers en/of medewerkers? (n=103)

De helft van de organisaties beheert zelf digitale gegevens, documenten en/of media (foto's, films, gedigitaliseerde objecten, etc) waarvan diefstal, het blokkeren van toegang en/of beschadiging of vernietiging tot schade zal leiden.

Is er in de organisatie waar jij werkt sprake van digitale gegevens, documenten en/of media (foto's, films, gedigitaliseerde objecten, etc) waarvan diefstal, het blokkeren van toegang en/of beschadiging of vernietiging tot schade zal leiden? (n=89)

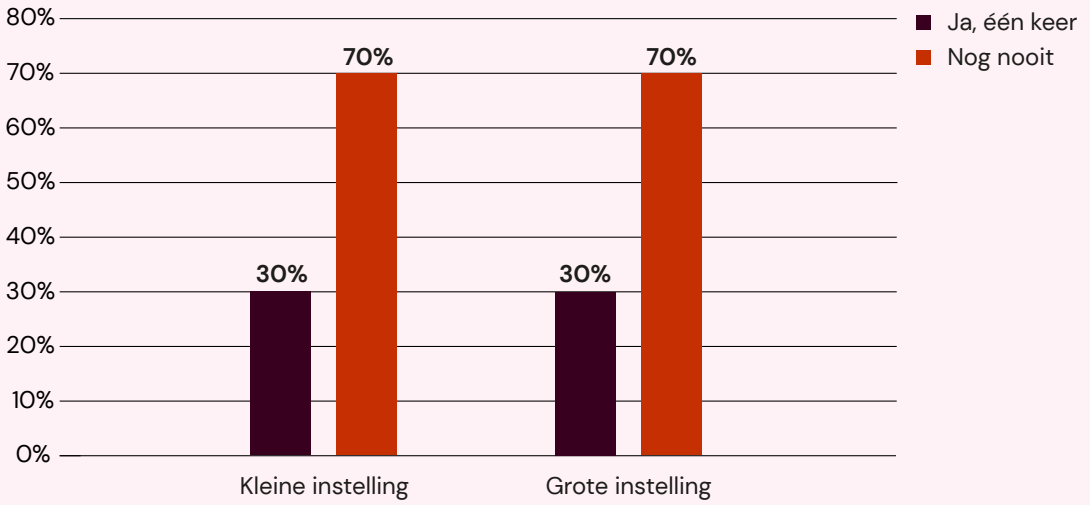
Komen cyberincidenten ook daadwerkelijk voor?

Bij bijna 3 op elke 10 organisaties waar de respondenten werkzaam zijn heeft de afgelopen 3 jaar een digitaal veiligheidsincident plaatsgevonden waarbij IT-systemen bewust zijn ontregeld en/of waarbij gegevens zijn ontvreemd. Bij 1 op elke 20 organisaties zelfs méér dan eens.



Heeft bij de organisatie waar jij werkt de afgelopen 3 jaar een digitaal veiligheidsincident plaatsgevonden waarbij IT-systemen bewust zijn ontregeld en/of waarbij gegevens zijn ontvreemd? (n=85)

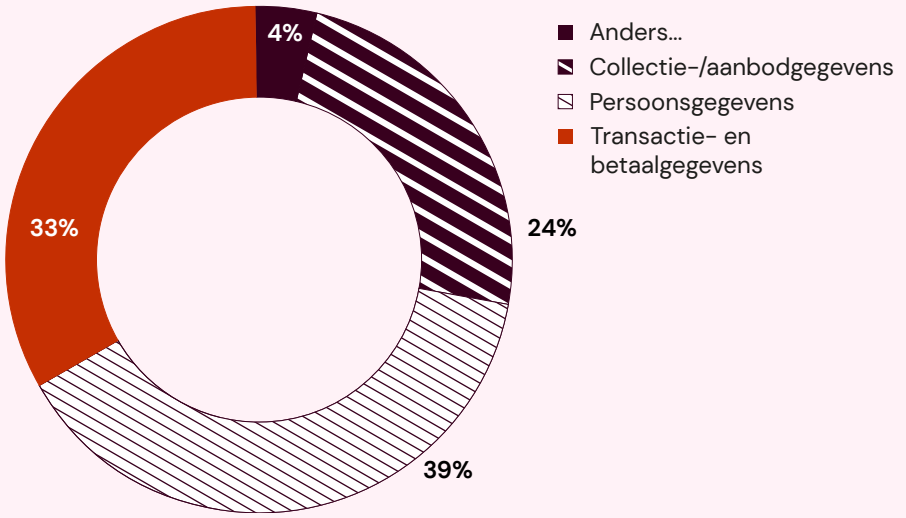
Wanneer we deze cijfers uitsplitsen naar kleine (tot en met 30 medewerkers) en grote organisaties (meer dan 30 medewerkers) dan blijken de percentages gelijk: verhoudingsgewijs komen incidenten even vaak voor bij kleine als bij grote organisaties.



Heeft bij de organisatie waar jij werkt de afgelopen 3 jaar een digitaal veiligheidsincident plaatsgevonden waarbij IT-systemen bewust zijn ontregeld en/of waarbij gegevens zijn ontvreemd? (percentages van de organisaties die hebben aangegeven hoeveel medewerkers ze in dienst hebben – geen van de organisaties die 'ja, meer dan eens' heeft ingevuld heeft aangegeven hoeveel medewerkers ze in dienst hebben)

Welke gegevens leiden tot schade? En hoe erg is een incident?

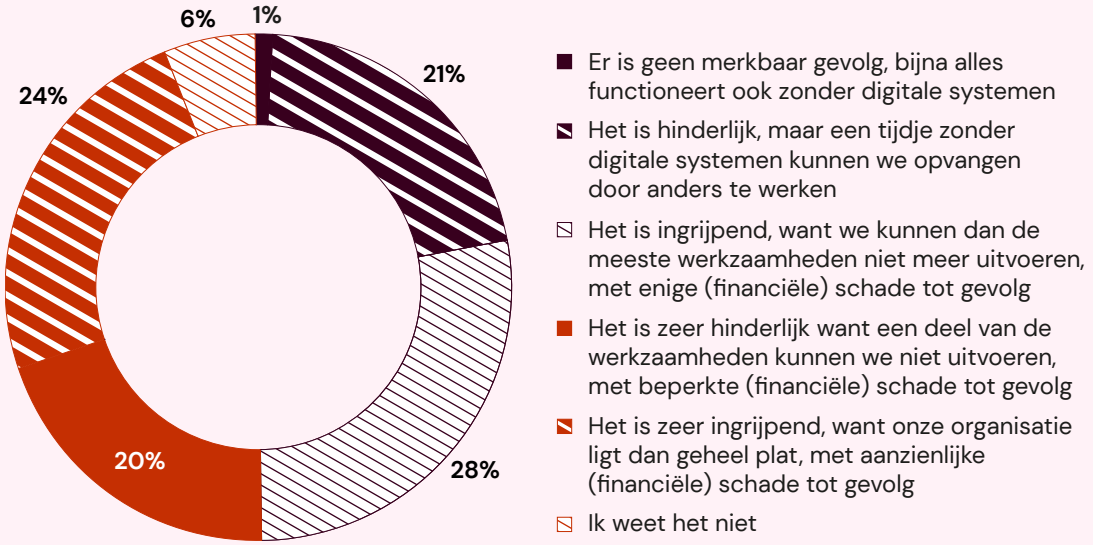
Respondenten gaven aan dat bij diefstal, het blokkeren van toegang en/of beschadiging of vernietiging naast collectie-/aanbodgegevens en persoonsgegevens (van medewerkers en bezoekers) ook transactie- en betaalgegevens tot schade zullen leiden. Bij 'anders …' werden bovendien nog subsidieaanvragen en gegevens over bruiklenen, transporten etc. genoemd. Ook werd genoemd dat elke diefstal van gegevens leidt tot schade: al zou niets (van waarde) worden ontvreemd dan zou het alleen al reputatieschade tot gevolg hebben.



Weet je het type gegevens waarvan diefstal, het blokkeren van toegang en/of beschadiging of vernietiging tot schade zal leiden? (meer dan 1 antwoord mogelijk, n=171)

Welke gegevens leiden tot schade? En hoe erg is een incident?

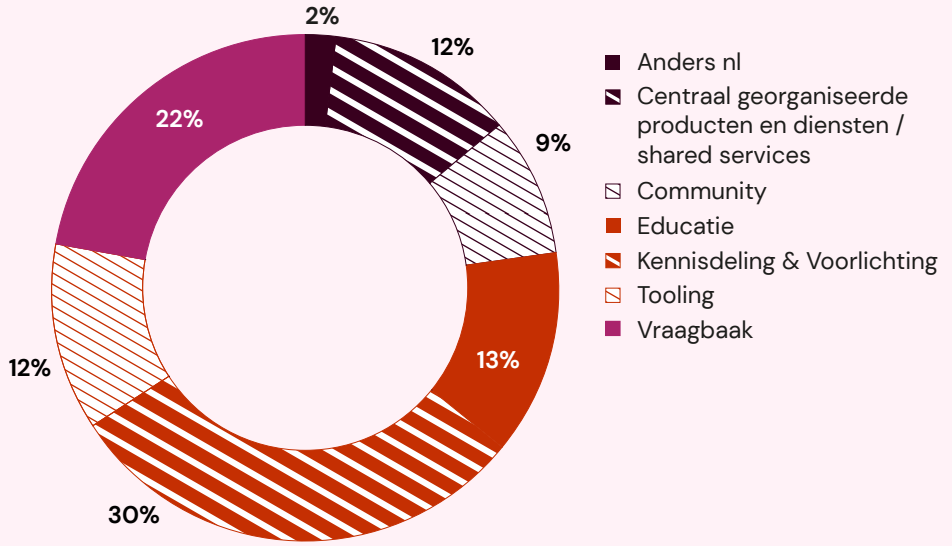
De schade van een incident waarbij digitale systemen niet meer werken zullen voor de 44% van de organisaties zeer hinderlijk tot zeer ingrijpend zijn, met beperkte tot aanzienlijke (financiële) schade tot gevolg. 21% van de respondenten geeft aan dat het hooguit hinderlijk is, 1% dat er zelfs geen merkbaar gevolg is.



Ken je de (mogelijke) gevolgen van een incident waarbij digitale systemen in jouw organisatie niet meer werken? (n=86)

Er is behoefte aan ondersteuning op het gebied van cybersecurity

44% van alle respondenten geeft aan dat de organisatie waar ze werken (extra) ondersteuning op het gebied van digitale veiligheid/cyber security zou willen. Een partij die deze ondersteuning biedt moet noodzakelijkerwijs deskundig zijn, maar factoren die ook als belangrijk tot zeer belangrijk worden gevonden zijn onpartijdigheid, bekend zijn met de cultuursector, helpen met andere ICT- en digitaliseringsvraagstukken, 24/7 beschikbaarheid, geringe kosten, maatwerk, ontzorgen en meedenken over privacy en ethiek. Respondenten zien ten aanzien van digitale veiligheid/ cyber security zeker een mogelijke rol voor DEN bij het ondersteunen van de organisatie waar ze werken, op verschillende gebieden. Kennis delen en voorlichting geven en het faciliteren van een community werd het vaakst genoemd. Ook voor educatie, tooling en centraal georganiseerde producten en diensten (shared services) is belangstelling. Als concrete voorbeelden van mogelijke ondersteuning werden genoemd: Collectieve, sectorale verzekering; informatie over minimale eisen aan de beveiliging; benchmarking met voorlopers (in de eigen en eventueel andere sectoren) en ondersteuning bij het in kaart brengen van risico's en het treffen van adequate maatregelen.

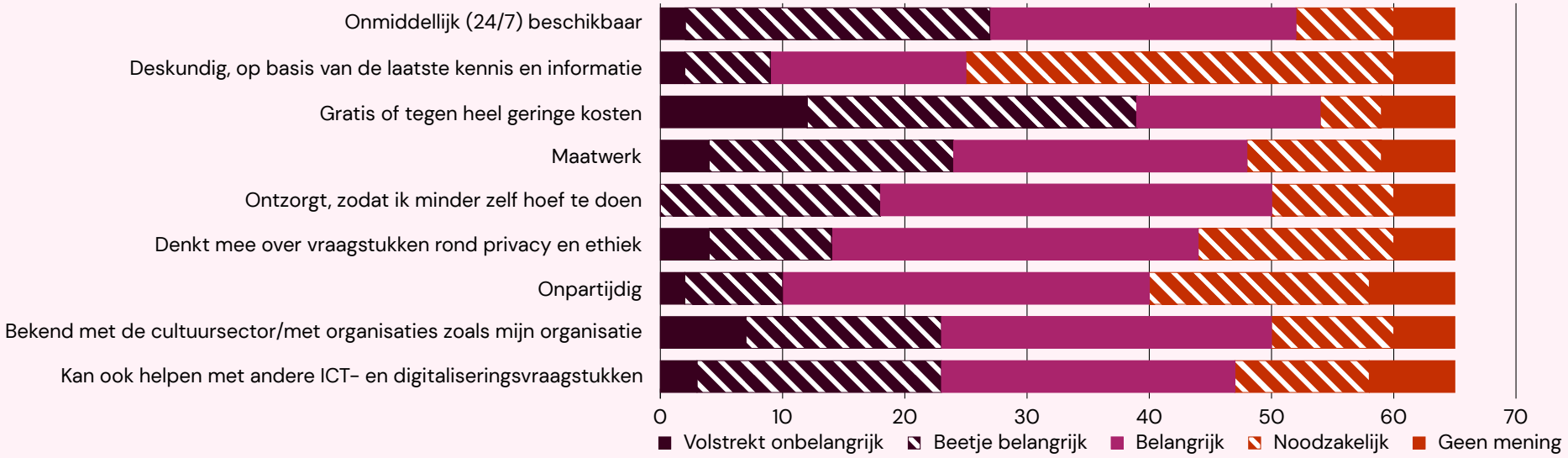


Wat verwacht jij van DEN bij het ondersteunen van de organisatie waar jij werkt in digitale veiligheid/ cyber security? (meerdere antwoorden mogelijk, n=191)

Factoren belangrijk voor ondersteuning

Belangrijke factoren bij ondersteuning op het gebied van digitale veiligheid zijn voor respondenten deskundigheid, meedenken over privacy en ethiek, onpartijdigheid en ook bekend zijn met de sector en kunnen helpen met andere ICT- en digitaliseringsvraagstukken.

Andere aspecten die als waardevol worden genoemd zijn kennis delen en voorlichting geven, het faciliteren van een community en ook door verzorgen van educatie, tooling en centraal georganiseerde producten en diensten (shared services), zoals een collectieve verzekering, informatie over minimale eisen aan de beveiliging en ondersteuning bij het in kaart brengen van risico's en het treffen van adequate maatregelen.



Welke factoren zijn voor de organisatie waar jij werkt belangrijk voor ondersteuning?

Volgende stappen

Op basis van deze uitkomsten zet DEN in op:
- Aandacht voor het onderwerp in alle uitingen
- Het bieden van informatie en doorverwijzingen voor organisaties
- Het ontwikkelen van een stappenplan specifiek voor de cultuursector
- Het opzetten van een community rondom dit thema
- Onderzoek naar collectieve producten en diensten

Wat kun je als organisatie nu al doen?
Wil je in jouw organisatie nu al aan de slag met digitale veiligheid? Kijk dan eens op digitaltrustcenter.nl van het Ministerie van EZK. Hier kun je de Cyberveilig Check doen. Deze check geeft snel een eerste inzicht in hoe jij ervoor staat en welke stappen je kunt zetten.

CyberVeilig Check - Eerste set vragen en antwoorden

- Draait er **antivirussoftware** op alle apparaten waar dat mogelijk is?
- Weten jij en je collega's meestal **phishing** te herkennen?
- Wordt er geregeld een **back-up** gemaakt van jouw belangrijkste bedrijfsgegevens?
- Heb je een (geprinte) **lijst met belangrijke contactgegevens** als je te maken krijgt met een cyberaanval?
- **Log je in 2 stappen** in bij belangrijke bedrijfsapplicaties zoals e-mail, administratie of bedrijfsnetwerk? Met bijvoorbeeld eerst een wachtwoord en daarna een sms-code of vingerafdruk?
- Weet je zeker dat jouw **e-mail beveiliging** op orde is?
- Staat **automatisch updaten** aan op alle met internet verbonden apparaten?

Rapport CyberVeilig Check

Bedrijfsprofiel

Werkzame personen	20 - 49 personen
Sector	cultuur en recreatie

Antivirus

Draait er antivirussoftware op alle apparaten waar dat mogelijk is?	Nee

Phishing

Weten jij en je collega's meestal phishing te herkennen?	Weet ik niet

Back-up

Wordt er regelmatig een back-up gemaakt van de belangrijkste bedrijfsgegevens?	Ja

Paraatheid

Heb je een (geprinte) lijst met belangrijke contactgegevens als je te maken krijgt met een cyberaanval?	Nee

Inloggen in 2 stappen

Log je in 2 stappen in bij belangrijke bedrijfsapplicaties zoals e-mail, administratie of bedrijfsnetwerk? Met bijvoorbeeld eerst een wachtwoord en daarna een sms-code of vingerafdruk?	Nee

Is je e-mailverkeer veilig?

☐ **Antivirus**

Actie: Activeer op alle apparaten waar dat mogelijk is een antivirusprogramma of laat dit doen door je IT-dienstverlener.

Hoe: Vraag je IT-dienstverlener om een overzicht van alle computers en servers en de aanwezigheid van een up-to-date antivirusprogramma. Maak daarnaast afspraken over wie wat doet als er een virusmelding is. Vergeet ook niet je antivirusprogramma's periodiek te (laten)controleren op de aanwezigheid van de nieuwste softwareversie.

Waarom: Het is belangrijk dat alle computers en servers binnen je bedrijf voorzien zijn van een up-to-date antivirusprogramma. Een goede virusscanner wordt door de leverancier regelmatig bijgewerkt zodat het je IT-systemen beschermt. Ook tegen de meest recente virussen.

☐ **Phishing**

Actie: Test de kennis over phishing bij je collega's en maak iedereen bewust van de gevaren van klikken op verdachte links.

Hoe: Doe vandaag de Phishing Quiz en laat je collega's deze kennistest ook doen. Vergelijk de uitkomsten en probeer zoveel mogelijk van elkaar te leren. Bespreek indien nodig met je IT-dienstverlener of je een Phishingtest kunt inkopen.

☑ **Back-up**

Actie: Maak vandaag een back-up van je belangrijkste bedrijfsgegevens.

Hoe: Vraag aan je IT-dienstverlener welke afspraken er over het maken van back-ups gemaakt zijn. Zijn er geen afspraken? Maak deze dan alsnog zo snel mogelijk. Vergeet niet om vast te leggen hoe back-ups worden getest en laat de uitkomsten inzichtelijk maken.

Waarom: 1 op de 4 mkb-bedrijven wordt slachtoffer van een cyberaanval. Een kwalitatief goede back-up beperkt de impact van zo'n aanval. En het zorgt ervoor dat je sneller weer operationeel bent, ook bij 'ongelukjes' zoals een menselijke fout.

Colofon

Dit onderzoek is in opdracht van DEN uitgevoerd door TwynstraGudde