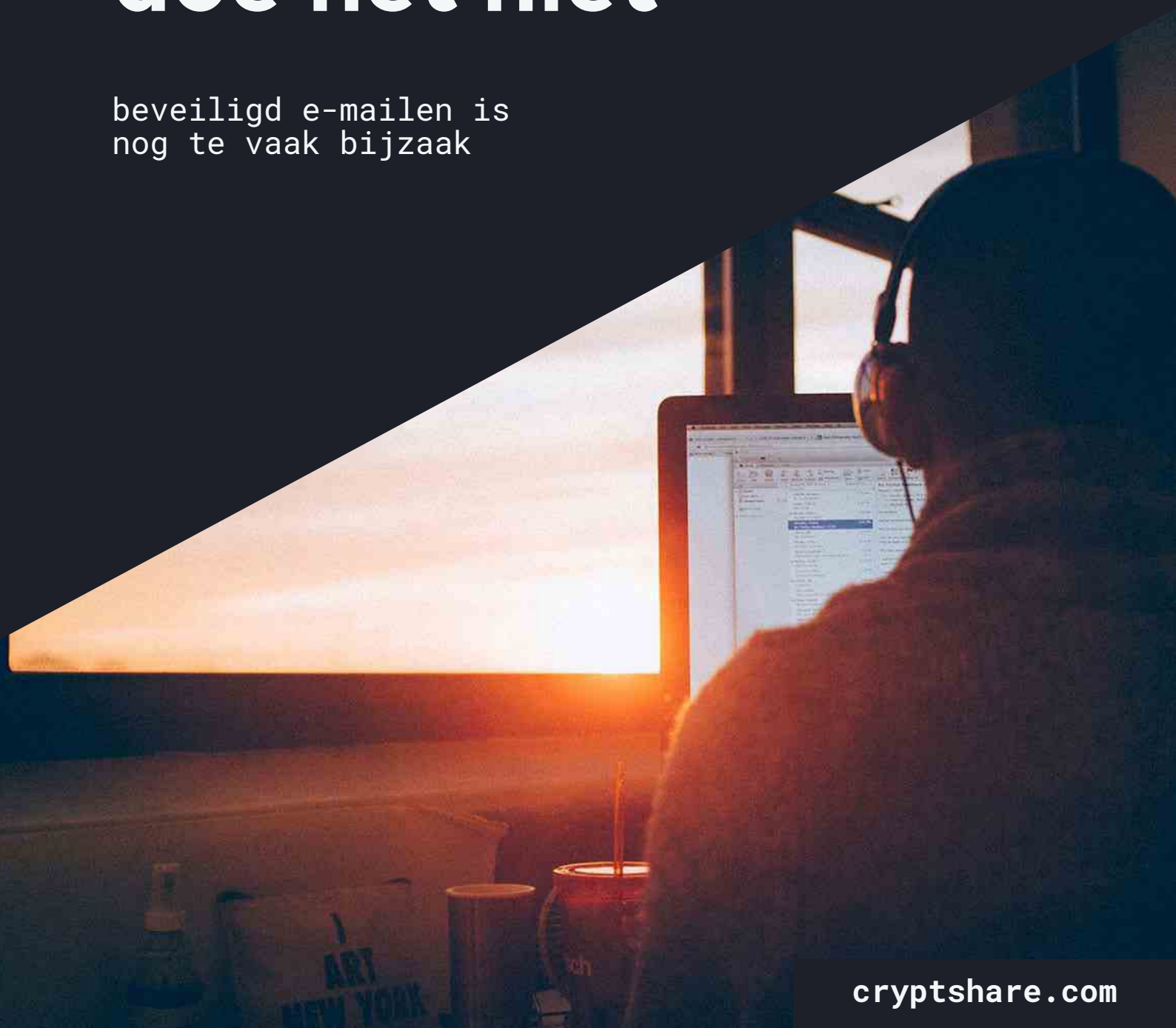
POINTSHARP

Doe het veilig of doe het niet

beveiligd e-mailen is
nog te vaak bijzaak



cryptshare.com

Regelmatig is het in het nieuws

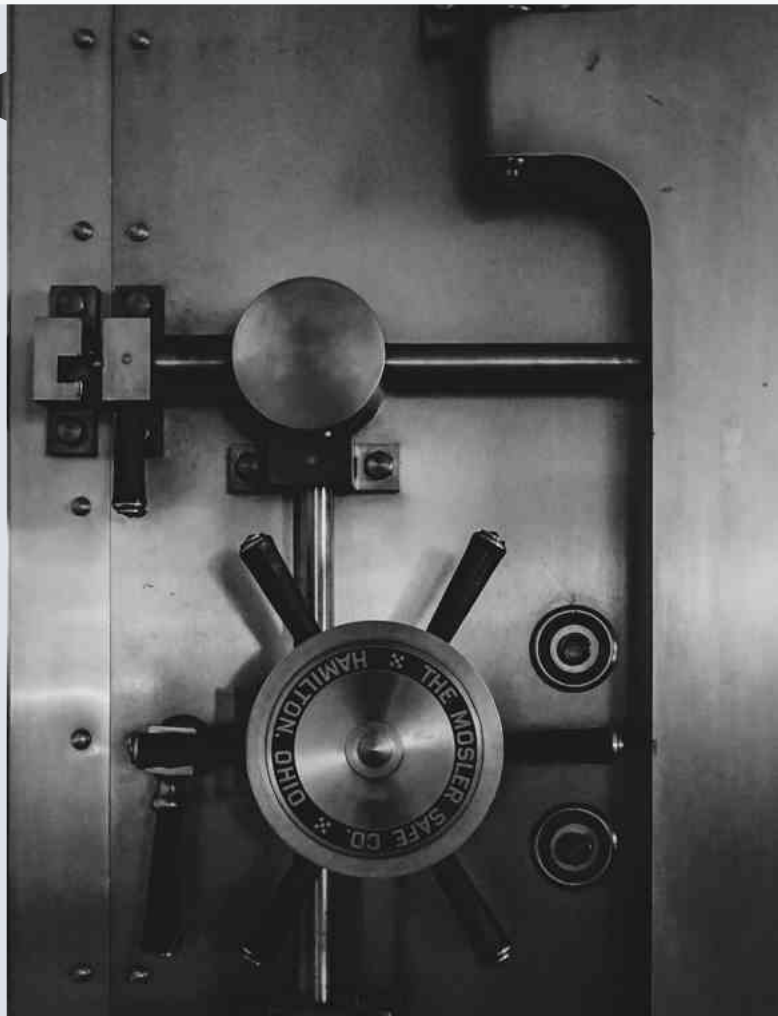
Een datalek bij een bedrijf waardoor duizenden persoonsgegevens op straat liggen. Gemeentes, tandartsen of autofabrikanten; er is geen sector die niet ooit eens te maken krijgt met cybercriminelen. Cybersecurity staat bij veel organisaties dan ook hoog in het vaandel en ze investeren veel tijd en geld om criminelen buiten de deur te houden. Want digitale veiligheid raakt iedereen. Maar niet elke organisatie heeft dit op orde. En dat kan grote gevolgen hebben: hackers die systemen platleggen en diefstal van gevoelige data, zoals financiële gegevens of e-mail- en internetfraude.

Bedrijven implementeren allerlei systeembeveiligingen om een datalek of hack te voorkomen. Maar er wordt niet altijd stilgestaan bij het feit dat een simpele e-mail ook voor problemen kan zorgen. Een phisingsmail zie je immers zo over het hoofd en medewerkers klikken zo op een link die niet helemaal zuiver blijkt te zijn. Niet zo gek, want de tijd dat phisingsmails bestonden uit slecht geformuleerde e-mails met taalfouten en random waarschuwingen is voorbij. Informatie beveiligd verzenden binnen een organisatie is dus des te belangrijker. Ook bestaat er de mogelijkheid dat een ander het mailverkeer onderschept.

En lekt, onbedoeld, je data. Organisaties kunnen bijvoorbeeld werken met voorschriften hoe medewerkers informatie moeten delen. En afhankelijk van de inhoud zijn er vaak verschillende voorschriften van toepassing voor het uitwisselen van gegevens en informatie. Organisatie kunnen regels voorschrijven, maar deze worden niet altijd trouw nageleefd door werknemers.

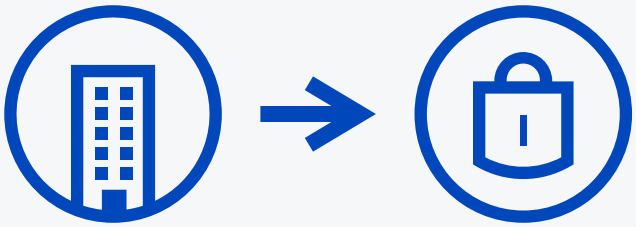
Want hoe gaat dit in de praktijk?

In dit e-book zijn de resultaten gebundeld van het onderzoek dat wij hebben uitgevoerd onder ruim **1.000** Nederlandse kantoormedewerkers naar de stand van zaken omtrent veilig e-mailen op de Nederlandse kantoren. Houden werkenden zich bezig met het beveiligd versturen van informatie? En wat doen organisaties hier aan? Doen ze het veilig? Of doen ze het niet?



Hoofdstuk 1: Organisaties en cybersecurity

Organisaties in Nederland zijn zich bewust van de noodzaak van cybersecurity. Om als organisatie goed bestand te zijn tegen het toenemend aantal hackaanvallen is het cruciaal dat cybersecurity onderdeel is van de bedrijfsvoering. Bij drie op de vijf **(63%)** organisaties heeft cybersecurity dan ook een hoge prioriteit. En 73 procent van de organisaties is momenteel al bewust bezig met het voorkomen van datalekken. Bovendien geeft de helft **(52%)** van de organisaties aan dat zij de deuren stevig gesloten houden voor cybercriminelen. Maar doen ze dit ook daadwerkelijk of zitten er wat kieren in hun communicatiemiddelen?



Voorkeur voor e-mailen

Binnen organisaties worden verschillende communicatiemiddelen gebruikt voor het intern uitwisselen van informatie en gegevens. Het overgrote deel **(82%)** gebruikt hiervoor e-mailen, gevolgd door Teams **(49%)** en Whatsapp **(26%)**. Slechts vijftien procent maakt gebruik van beveiligd e-mailen. Voor het extern uitwisselen van informatie en gegevens gebruikt ook het grootste percentage **(77%)** e-mailen en Teams **(26%)**. Opvallend is dat er bij externe communicatie vaker wordt teruggevallen op de post **(24% tegenover 7%)**. Ook wordt voor het extern delen van informatie vaker beveiligd e-mailen ingezet **(20%)**.

Beveiligd e-mailen

E-mail is dus het populairste communicatiemiddel voor zowel intern als extern gebruik. Maar beveiligd e-mailen wordt nog niet veel ingezet. Bij één op de vijf **(20%)** organisaties is er dan ook nog nooit gesproken over beveiligd e-mailen. En maar bij twintig procent worden standaard beveiligde e-mails verstuurd. Bij dertig procent van de organisaties gebeurt dit af en toe.

Daarbij weet één op de vijf **(19%)** werkenden niet of de organisatie bezig is met beveiligd e-mailen. Of ze zij niet voldoende op de hoogte van hoe dit onderwerp in zijn organisatie behandeld wordt. Dit is allemaal opmerkelijk, omdat het overgrote deel **(71%)** van de werkenden wel vindt dat beveiligd e-mailen de standaard zou moeten zijn binnen zakelijke communicatie. Werkend Nederland lijkt het nut van beveiligd e-mailen dus wel in te zien, maar hier nog niet naar te handelen. De deuren zijn dus momenteel toch wat minder stevig gesloten dan gedacht wordt. Want het wordt lang niet altijd veilig gedaan, dat e-mailen.

Hoofdstuk 2: Beveiligd e-mailen nog geen prioriteit voor werkenden

Het moge duidelijk zijn dat werkend Nederland massaal kiest voor e-mail om te communiceren, met zowel collega's als externen. Volgens drie op de vijf **(62%)** werkenden is e-mailen dan ook de veiligste manier om zakelijk te communiceren. Dit wordt gevolgd door aangetekende post **(44%)** en Teams **(40%)**. Het hoge percentage dat kiest voor e-mail is wellicht te wijden aan het feit dat meer dan de helft **(56%)** denkt dat een e-mail versturen veiliger is dan een ansichtkaart. Opvallend, want als je deze niet veilig verstuurd dan zijn ze voor hackers net zo makkelijk te lezen als de ansichtkaart voor de postbode. En hoewel **44 procent** van de werkenden aangetekende post als een van de veiligste manieren van zakelijk contact, wordt dit merkwaardig weinig gebruikt. Intern komt dit in vijf procent van de gevallen voor, extern is dit wel iets meer met vijftien procent.

Grote bestanden versturen

Maar waar kiest de werkende Nederlander dan voor als het gaat om het verzenden van bestanden binnen en buiten de organisatie? Opvallend is dat meer dan de helft **(52%)** bijna altijd WeTransfer gebruikt als zij grote bestanden moeten mailen, terwijl maar achttien procent dit ziet als het veiligst voor zakelijk contact. Het groot aantal werkenden dat dergelijke openbare online diensten, zoals WeTransfer, Google Drive of Dropbox, gebruikt is zorgelijk, want zij kunnen een datalek creëren.

Niet relevant

Het lijkt erop dat werkenden wel het nut inzien van beveiligd e-mailen, maar dat zij dit niet per se nodig vinden bij henzelf. De meerderheid **(57%)** vindt dan ook dat beveiligd e-mailen alleen relevant is voor branches die omgaan met gevoelige informatie. Het besef dat alle informatie gevoelig kan zijn, moet duidelijk nog indalen. Bovendien willen mensen liever geen complexe stappen volgen om veilig informatie te versturen. Twee op de vijf **(37%)** vindt beveiligd e-mailen dan ook erg omslachtig. Daarbij kiest veertig procent meestal voor gebruiksgemak als zij in zijn werk moet kiezen tussen veiligheid en gebruiksgemak, waardoor hackers vrij spel krijgen.

Gebruikersgemak

Binnen een groot deel van de organisatie wordt wel eens gesproken over het beveiligd e-mailen van gegevens. We zien dus dat het onderwerp van gesprek is, maar bij de uitvoering zijn nog de nodige stappen te zetten. Zo past nog één op de vijf werkenden weleens andere middelen toe om informatie te beveiligen, dan dat de organisatie heeft voorgeschreven. Daarbij zoekt 26 procent een manier om veiligheidsmaatregelen te omzeilen in plaats van zich erin te verdiepen. Dit doen zij als zij niet snappen hoe de veiligheidsmaatregelen werken of als ze vinden dat het te veel tijd kost. Een duidelijke illustratie van hoe werknemers gemak boven veiligheid verkiezen. Maar liefst zestien procent omzeilt zeker eens per maand de veiligheidsmaatregelen vanuit zijn organisatie om zijn werk zo efficiënter te kunnen uitvoeren.

Kennis en kunde

Dat beveiligd e-mailen nog niet zo is ingeburgerd als zou moeten, ligt over het algemeen niet aan een gebrek aan kennis. Driekwart van de werkende Nederlanders **(76%)** geeft namelijk aan dat zij weten wat beveiligd/versleuteld e-mailen inhoudt en 55 procent heeft weleens een beveiligde e-mail verstuurd. Maar het vertrouwen voor veilig e-mailen wordt vaak gelegd in de standaard e-mailproviders. Zo vertrouwt **78** procent op de beveiliging van het e-mailprogramma dat zij gebruiken . De overgrote meerderheid **(81%)** geeft dan ook aan voldoende middelen te hebben om de informatie die bij zijn werk hoort, te beveiligen.

Risico's/angst of een gebrek daaraan

Twee op de vijf **(38%)** staan eigenlijk nooit stil bij de risico's die horen bij het versturen van e-mails. **44 procent** denkt er dan ook nooit over na of zij een e-mail misschien beveiligd moeten versturen. Hier is dus nog een duidelijke taak voor de werkgevers weggelegd om werknemers te onderwijzen en te laten inzien dat ook via de mail data gelekt kan worden. Want daar zijn veel werknemers nog niet bang voor: veertig procent heeft geen angst voor een datalek in zijn organisatie. Wat wel opvalt is dat maar een op de vijf **(17%)** denkt dat er geen risico's zijn bij het versturen van e-mails via bijvoorbeeld Outlook of Gmail, terwijl we ieder zagen dat er wel vertrouwen wordt op de beveiliging van deze programma's. Van de werkenden die geen angst hebben voor een datalek in hun organisatie zegt **44 procent** dat zij er ook nooit over nadenken om e-mail beveiligd te versturen.

Niet altijd noodzakelijk

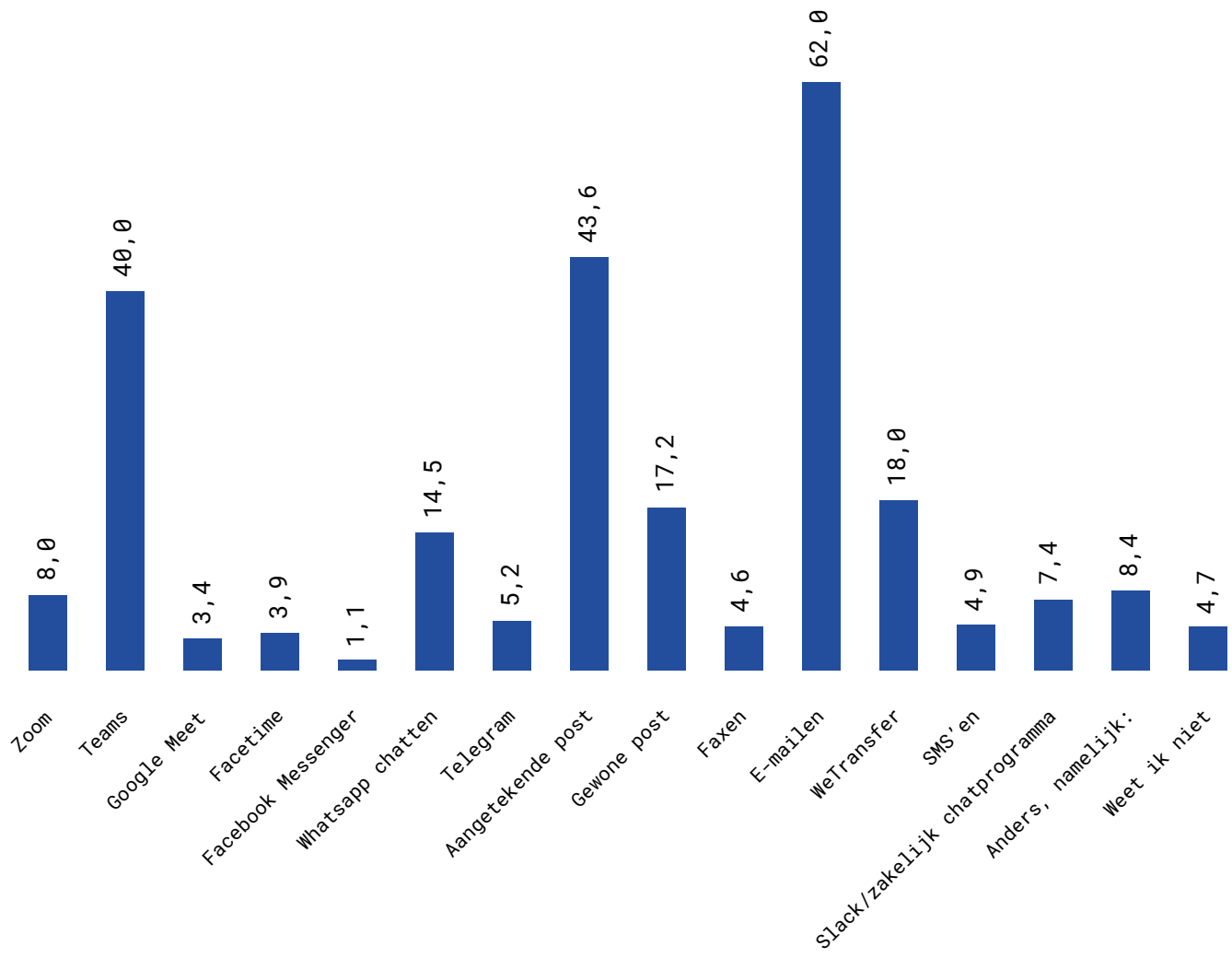
Het versleuteld versturen van berichten is enorm belangrijk voor de veiligheid. Want op deze manier weet men zeker dat alleen de verzender en de ontvanger toegang hebben tot het bericht. Berichten kunnen niet meer doorgestuurd worden en derden hebben geen toegang tot de informatie. Maar wanneer denkt werkend Nederland dat het nodig is om gegevens versleuteld te versturen? Maar zestien procent denkt dat beveiligd e-mailen nodig is bij iedere mail die zij versturen. Dit aantal groeit naar **36 procent** als het gaat om zakelijk e-mailverkeer. Iets meer dan de helft **(54%)** denkt dat beveiligd e-mailen nodig is als zij documenten versturen. Het overgrote deel **(82%)** denkt dat beveiligd e-mailen nodig is als zij gevoelige informatie versturen in de mailtekst zelf. Tot slot denkt **84 procent** dat beveiligd e-mailen nodig is als zij gevoelige informatie versturen als documenten in de bijlage. Het wordt dus lang niet altijd veilig gedaan.

Conclusie

Cybersecurity staat bij menig bedrijf hoog in het vaandel. Sommige organisaties stellen zelfs een speciale CICO aan om een veilige online omgeving te handhaven. En daarbij verdient goede e-mailbeveiliging wel wat meer aandacht. Toch wordt er onder werkenden soms nog te licht gedacht over het e-mailen van informatie en gegevens en het gebrek aan veiligheid hierbij. Met grote gevolgen: de organisatie is kwetsbaar voor datalekken. Werkenden erkennen dat het in sommige gevallen erg nuttig kan zijn, maar om hier vervolgens ook naar te handelen lijkt soms een stap te ver. Organisaties hebben soms een beleid hoe werknemers informatie moeten delen, maar in de praktijk blijkt dat werknemers hier niet naar luisteren. En in sommige gevallen de regels zelfs actief omzeilen. Hier is voor organisaties dus nog winst te behalen om hun bedrijf te beschermen tegen cyberaanvallen.

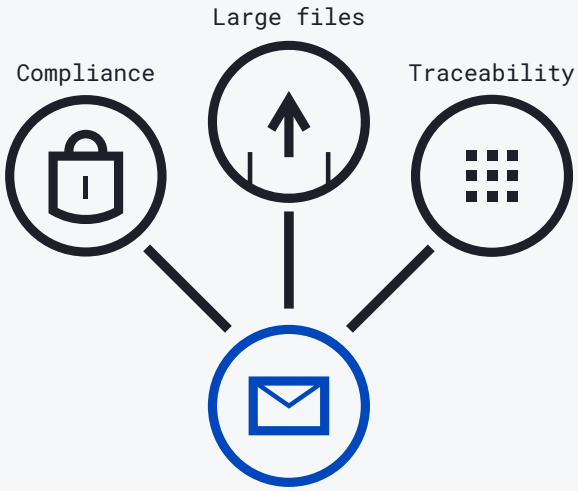
Over het onderzoek

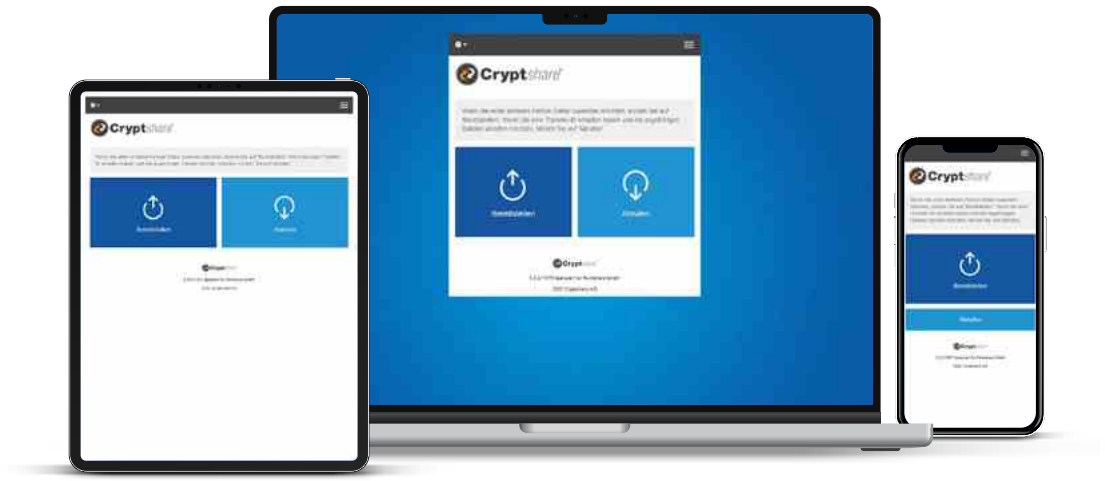
In **oktober 2022** nam het onderzoeksbureau Panelwizard op verzoek van Cryptshare een online enquête af onder werkenden met een kantoorbaan. Aan het onderzoek deden **1070** werkenden Nederlanders van **18** jaar en ouder mee. Deze zijn evenredig verspreid over geslacht, opleidingsniveau en leeftijd. Dit maakt het onderzoek representatief voor alle werkenden met een kantoorbaan in Nederland.



Over Cryptshare

Pointsharp is onder andere de leverancier van het product Cryptshare, de e-mailencryptiesoftware: een digitale communicatieoplossing voor het veilig uitwisselen van informatie. E-mails en bestanden van elke grootte kunnen gemakkelijk en veilig worden uitgewisseld. Met meer dan 3 miljoen tevreden gebruikers wereldwijd in meer dan 30 landen zijn zij een gerenommeerd bedrijf in deze sector. Ze zijn ervan overtuigd dat digitale communicatie enorm waardevol is voor ondernemingen. Met hun veilige dienst voor digitale overdracht stellen zij mensen in staat om samen te werken aan projecten en ontvouwt de ware waarde van data, waardoor iedereen in de onderneming met elkaar in contact komt. Cryptshare zorgt ervoor dat gegevens worden beschermd op alle risicopunten op de reis van afzender naar ontvanger, dat wil zeggen vanaf het moment dat het de relatieve veiligheid van de firewall verlaat totdat het de beoogde bestemming bereikt.





Pointsharp – Security made easy

Bezoek onze website voor meer informatie of een demo

www.cryptshare.com

POINTSHARP