Lime Networks
Verfrissend in IT!

Whitepaper Security

Werk veilig met data en applicaties in 'Coronatijd'

Veilig thuiswerken is topsport

Introductie

Toen COVID19 begon, speelde IT een belangrijke rol in de continuïteit van werk. En nu nog steeds. Wij merkten dit bij onze klanten en zagen hoe lastig het kon zijn om veilig thuis te werken. Daarom wilden wij de situatie in kaart brengen en heldere antwoorden krijgen over hoe jij altijd en overal veilig kunt werken – dus ook thuis!

Door COVID19 is er extra druk komen te staan op data en de beveiliging van bedrijven. Is jouw bedrijf hierop voorbereid? Ben je op de hoogte van de risico's die je momenteel loopt? Weet je welke maatregelen er zijn getroffen en welke je nog kunt (of moet) treffen? Veilig thuiswerken is topsport en geen gemakkelijke zaak. Zo is het aantal hackpogingen op particulieren, bedrijven en overheden na de uitbraak van COVID19 toegenomen, volgens de Verenigde Naties en de Nederlandse Nationaal Coördinator Terrorismebestrijding en Veiligheid (RTL Nieuws).

Wij wilden dit graag beter in kaart brengen. Hoeveel mensen zijn er eigenlijk thuis gaan werken en hoe veilig werken die? Welke maatregelen hebben zij wel en niet getroffen? Deze Whitepaper is gebaseerd op een onderzoek dat wij hebben uitgevoerd. Wij willen iedereen die hieraan heeft meegewerkt bedanken voor de deelname en de enthousiaste reacties!

Er zijn zorgen om techniek en de vaart van techniek.
Hoe blijf je bij en welke leverancier kun je vertrouwen?

Over Lime Networks – het meest verfrissende IT-bedrijf van Nederland

IT moet gewoon werken, vinden wij. Jij wilt overal veilig kunnen werken. Met IT wil je compleet verzorgd worden door gepassioneerde mensen die hier helder over communiceren. Wij bieden deze verfrissende IT-oplossingen voor het MKB met een goed geschoold team en maken het simpel voor jou.

Wat ons verfrissend maakt? No-nonsense experts in IT die op jou zijn gericht en jou totaal verzorgen. 'Secure-by-design' is onze focus. Wij laten jou voorop lopen met techniek en communiceren hier helder over, zodat jij een stap voor bent op je concurrent in de digitale transformatie.

Meer weten over security?

- ✓ 10 manieren om je beveiliging eenvoudig te versterken
- ✓ IT kan beter, ook als de mens de zwakste schakel is
- ✓ Zes tips om je netwerk te beveiligen
- ✓ Spam of phishing mail herkennen, voorkomen en oplossen
- ✓ Thuiswerken in verband met corona? Zo kun je dat veilig doen!

Security risico's

De wereldwijde informatiebeveiligingsmarkt zal in 2022

€143,7 MILJARD

waard zijn, volgens voorspellingen (Gartner)

Als cybercrime een land zou zijn, zou het de derde wereldeconomie zijn (na de US en China). Het kost ons jaarlijks wereldwijd

€5 BILJOEN

($6.000.000.000.000,-) aan schade (Cybersecurity Ventures)

68%

van de bedrijfsleiders heeft het gevoel dat hun cyberbeveiligingsrisico's toenemen (Accenture)

Van alle cyberinbreuken in 2020 had

86%

een financieel doeleinde en ging het bij

10%

om spionage (Verizon)

De risico's van thuiswerken

17%

van alle bestanden met gevoelige informatie zijn beschikbaar voor alle medewerkers (Varonis)

Het aantal open servers is met meer dan

60%

gestegen tussen 2018 en 2021 (Networking4All)

Het aantal gevallen van cybercrime is flink toegenomen sinds COVID19 is begonnen. Dat is slecht nieuws, als wij die naast de bovenstaande cijfers leggen. Medewerkers hebben – vaak onbedoeld en onbewust – toegang tot ontzettend veel bestanden. Dat is op zich niet zo'n probleem, behalve als de beveiliging van de bedrijven niet op orde is. Dat is waar de risico's voor cybercrime ontstaan. (Networking4All)

Maar er zijn nog veel meer risico's van thuiswerken buiten datatoegang. Slecht bijgehouden servers of ouderwetse IT-structuren vormen gaten in de online beveiliging waar hackers maar al te graag gebruik van maken.

Maar is het echt zo erg...? Ja!

Maart 2021: Microsoft Exchange Server gehackt

In maart dit jaar werd de Microsoft Exchange gehackt door de aanvalsmethode 'Microsoft Hafnium', waarbij kwetsbaarheden werden ingezet om binnen te dringen op de Exchange server. Zo werd niet alleen toegang verkregen tot de server maar waren de aanvallers ook in staat om een eigen stuk code te draaien en schrijfrechten te verkrijgen in elke map op de server. Met een zogenaamde 'web shell' konden de hackers de aangetaste server op afstand besturen en zo gegevens stelen.

Hoewel veel bedrijven zijn overgestapt naar een cloudalternatief zoals Microsoft 365, gebruiken nog steeds bedrijven Exchange Server. Honderdduizenden bedrijven maken namelijk wereldwijd gebruik van Exchange voor hun mail en kalender. Binnen een week was de web shell al geïnstalleerd op meer dan 5.000 mailservers in meer dan 115 landen.

Op 2 maart bracht Microsoft een patch uit, die de kwetsbaarheden zouden dichten. Getroffen bedrijven konden deze patch installeren en zich zo beschermen tegen de hackers. Helaas deed niet elk bedrijf dat. Daar maakten de hackers gretig gebruik van door ransomware te installeren. Hierdoor waren de hackers in staat om losgeld te vragen voor het ontsleutelen van bestanden. Deden de bedrijven dit niet, dan waren de bestanden niet meer toegankelijk. Bedrijven zonder goede back-ups kwamen daardoor in de problemen.

Gebruikers van de Exchange Server hadden weinig kunnen doen om de aanval te voorkomen, maar ze konden wél van alles doen om de impact te minimaliseren. Denk aan het installeren van updates, het maken van goede back-ups, een slimme indeling van het bedrijfsnetwerk en het controleren of de server al geïnfecteerd is geraakt. (Microsoft)

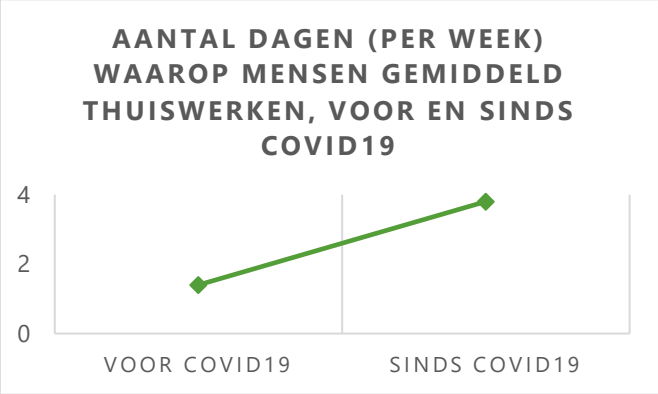
Juli 2020: hack Apollo Vredestein door verouderde software

'Hoe kan een bedrijf nou apparatuur gebruiken die al 10 jaar niet meer is bijgewerkt?!' vraag je je misschien af. Toch is verouderde digitale beveiliging volgens IT-kenners en cyberexperts exemplarisch voor Nederlandse bedrijven. En dat is zorgwekkend. Dat het grote gevolgen kon hebben, ondervond bandenfabriek Apollo Vredestein in 2020 toen zij gehackt werden.

Moederbedrijf Apollo Tyres viel ten prooi aan cybercriminelen en daarmee werden de fabrieken wereldwijd getroffen. Zo bleek dat de servers veel bekende kwetsbaarheden bevatten en dat er gebruik werd gemaakt van verouderde software, welke makkelijk te ontregelen was. De gevolgen? De mailsystemen waren niet meer te gebruiken, waardoor bestellingen niet op tijd afgerond konden worden. Een logistieke ramp voor een grote multinational. (AD)

Uitkomsten van ons onderzoek

Aantal thuiswerkers

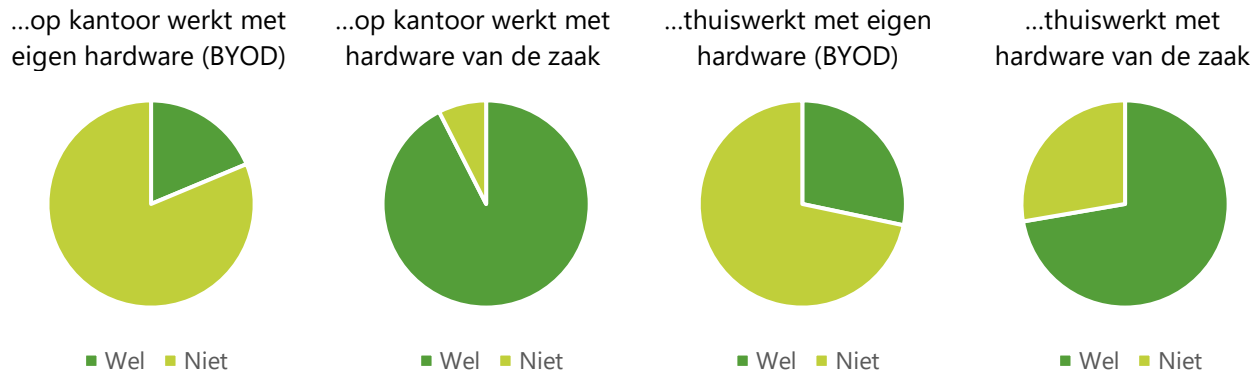


Uit het onderzoek blijkt dat het aantal thuiswerkers hard is gestegen sinds COVID19 is begonnen. Waar vóór de pandemie ongeveer een-derde (34%) van de medewerkers (regelmatig) thuiswerkten, is dit sinds COVID19 gestegen naar 84%. Dit is bijna 2,5 keer zo veel. Ter illustratie, in een bedrijf van 20 werknemers zou het aantal thuiswerkers dus van 6 of 7 (voor COVID19) naar 16 of 17 (sinds COVID19) zijn gegaan.

Het aantal dagen steeg nog harder. Medewerkers werkten gemiddeld 29% van de week thuis voor COVID19 begon. Uit ons onderzoek bleek dat dit inmiddels 76% is. Dat is meer dan 2,5 keer zo veel, 1 tot 2 dagen (1,4) naar bijna 4 dagen per week (3,8).

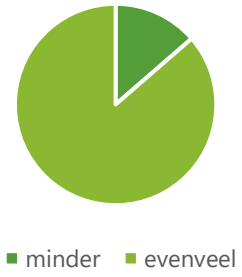
Hardware en data

Percentage van de werknemers dat...

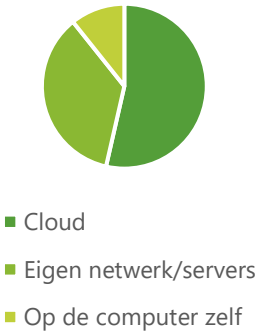


Ongeveer een-vijfde (19%) van de medewerkers werkt op de zaak met eigen hardware. Thuis is dit getal hoger, namelijk meer dan een kwart (28%). In deze cijfers zit nog iets verborgen: vaak gebruiken werknemers hun eigen telefoon en tablets voor zakelijke doeleinden. Daarmee kan bijvoorbeeld worden gemaild, maar soms kan er ook data mee bekeken en bewerkt worden. Uit het onderzoek blijkt dat er hoofdzakelijk op hardware van de baas wordt gewerkt, zowel thuis als op kantoor.

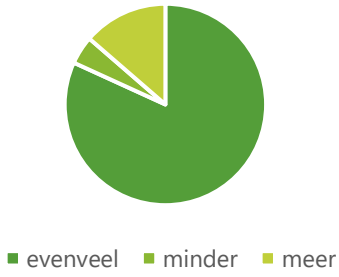
Hoeveel toegang hebben medewerkers thuis tot bedrijfsdata en -diensten (versus op kantoor)?



Waar staan bedrijfsdata en -diensten (applicaties)?



Hoeveel beveiligingsmaatregelen trof je voor thuiswerkers? (versus op kantoor)



Er is niet veel verschil in de toegang tot bedrijfsdata en -diensten. Gemiddeld hebben medewerkers thuis even veel toegang tot de data en diensten van het bedrijf waar ze werken. 86% gaf dit aan en 14% gaf aan minder toegang te hebben.

Als wij kijken naar waar de applicaties staan, valt op dat het grootste gedeelte (68%) van de bedrijven aangeeft al met data en/of applicaties in de cloud te werken. Bijna de helft (45%) van de bedrijven gaf aan nog met data en diensten op het eigen netwerk te werken. In 14% van de gevallen staan de applicaties op de computer zelf.

Het aantal beveiligingsmaatregelen is in de meeste gevallen gelijk gebleven en in een aantal gevallen toegenomen. In aanzienlijke mindere mate is aangegeven minder te doen aan beveiliging voor thuiswerkers. Afnemende maatregelen, dat horen wij natuurlijk niet graag. Want hoe weet jij wie er op je netwerk zit? Hoe goed is je netwerk beveiligd? Heeft je oppas je Wi-Fi wachtwoord ook nog? Welke slimme apparaten heb je allemaal op je netwerk? Hoe staat je firewall of router ingesteld en wie controleert dit? Werk je met een VPN? Het is belangrijk om over deze zaken na te denken, want op een onveilig netwerk ben je per definitie niet veilig.

Zorgen

Waar maak je je zorgen om?

Contact met werknemers of collega's werd vaak genoemd. In het 'nieuwe normaal' zien wij dat persoonlijk contact lastig is, maar wel hoog op de sociale eisenlijst staat. Een gevolg hiervan is weinig sociale controle, wat scherp werd opgemerkt door een respondent. Een terechte zorg die wij ook zien! Ben je zonder contact met die ene slimme college wel opgewassen tegen phishing?

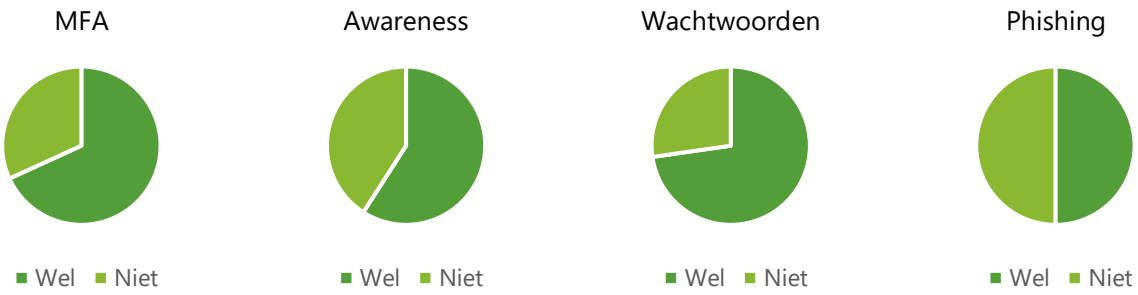
Ook kwam 'techniek' vaak voor. Denk aan updates die niet op orde zijn en slecht geregelde privacy op eigen apparaten (BYOD). Maar ook doen sommige metingen of tools het niet meer goed doordat medewerkers van IP-adres wisselen of andere hardware/netwerken gebruiken.

Bij het 'thuisnetwerk' kan je er het beste van uit gaan dat het gewoonweg niet veilig is. Onbeheerde (vaak matige) apparatuur, geen inzicht in wie er allemaal op je netwerk zit (de buren, de oppas, vage vrienden, de slimme thermostaat… bescherm jouw werknemers en de endpoints tegen alle voor de hand liggende gevaren. Zie het als een soort thuisversie van een internetcafé en vertrouw niemand.

Buiten de security, is 'efficiënt werken' ook belangrijk. Stel je een bedrijf van 100 man voor, die 50% van de tijd thuiswerken maar dan slechts 80% efficiënt zijn (door verschillende problemen). Dat levert elke maand een kostenpost op van 10 volledige werknemers die je als het ware 'mist'. Als een gemiddeld salaris dan €35.000,- per jaar is, spreken wij over bijna €30.000,- aan kosten. Bizar! Het is even een voorbeeldje, maar wat als je echt naar de mensen gaat kijken?

Maatregelen

Op welke onderwerpen nam je al concrete maatregelen ter beveiliging?



Misschien wel het meest schokkende van het onderzoek: basismaatregelen voor beveiliging worden door gemiddeld 30 tot 50% van de ondervraagde bedrijven niet toegepast. Denk aan MFA instellen, awareness training, wachtwoordenbeleid en phishingbeleid. Deze maatregelen zijn minimaal nodig om (zowel thuis als op kantoor) veilig te kunnen werken, maar liggen veelal niet in het zicht van de respondenten. Gelukkig vind je op de volgende pagina's tips over hoe jij dit wél kunt doen – vandaag nog.

Als tipje van de sluier: met alleen een inlognaam en wachtwoord ben je niet veilig. Het is tegenwoordig zo goed als noodzakelijk om MFA (Multi Factor Authenticator) in te stellen. Dit geldt voor accounts met toegang tot gevoelige informatie maar eigenlijk voor al je accounts, zakelijk of privé. En die oude accounts die je nooit meer gebruikt? Gewoon even je account opzeggen, dan heb je weer een zorg minder.

Vragen over veilig thuiswerken

Wat is de kern van veilig werken met bedrijfsdata en -applicaties?
Kijk verder dan alleen de toegang, het diefstal of het misbruik. Denk ook aan het up-to-date zijn van informatie en de relevantie, actualiteit en correctheid van data.

Hoe moet ik dat dan zien? Als een proces?
Veilig werken is geen probleem, oplossing, dienst of product. Je kunt het niet leveren of er blind op varen. Het is een continu proces met uitdagingen. Hierover in gesprek blijven is belangrijk om inzicht te krijgen in de huidige situatie en actie te kunnen ondernemen waar nodig.

Deze vragen geven toch geen 100% accuraat beeld? Deze informatie kan toch niet toegepast worden op alle bedrijven?
Wij snappen deze gedachten. Daarom willen wij graag benadrukken dat het in dit onderzoek draait om het zien van de trends en de percentages niet te zien als exacte wetenschap. Het gaat vooral om de context van het onderzoek en het inzicht die het kan verschaffen in de complexiteit van veilig werken, bij zowel bedrijven als werknemers. Thuiswerken is een essentieel onderdeel geworden van de nieuwe manier van werken, aangewakkerd door COVID19. Focus daarom op de 'learnings' die je uit dit onderzoek kunt halen. Wij hebben dan ook allerlei tips en tricks verzameld om dit onderzoek te concluderen.

Ons advies

Wij hebben natuurlijk tussendoor al een aantal tips gegeven en geven je hierna 10 concrete tips om je beveiliging te verbeteren. Toch willen wij graag nog even uitzoomen en kijken wat wij precies kunnen leren van dit onderzoek. Wat is ons advies aan bedrijven? In het kort: security is topsport. Iets uitgebreider willen wij je 3 dingen meegeven.

Neem security serieus en maak er een proces van in je bedrijf

Veel klanten maken zich zorgen om thuiswerken. Terecht, wat ons betreft, want security is topsport en dat onderschatten kan je duur komen te staan. Neem de veiligheid van jouw IT en je medewerkers serieus, want de cijfers in de introductie en de uitkomsten van dit onderzoek liegen er niet om. Zorg dat jouw IT en security goed in kaart zijn gebracht. Ga dus in gesprek met je leveranciers over security en blijf dit doen.

Zorg voor training en begeleiding van personeel

Training van personeel is nog een onderbelicht onderwerp voor bedrijven. Security draait om kennis en ervaring. Het draait om nieuwe onderwerpen én om technische zaken die vaak onbekend zijn voor werknemers. Een training is hierdoor een efficiënt middel om snel orde op zaken te stellen.

Breng risico's, maatregelen en continuïteit in beeld

Als je niet weet waar je tekort schiet op het gebied van veiligheid, kan je het niet verbeteren. Neem de uitkomsten van deze Whitepaper als uitgangspunt en kijk waar jij nog werk aan de winkel hebt. Neem echt de tijd voor deze analyse en breng alle risico's en maatregelen in kaart. Dat is nu even wat werk maar je zal jezelf dankbaar zijn.

Tips: 10 tips om geen laaghangend fruit te zijn

Beveiliging en IT gaan hand in hand. Een veilige online omgeving is essentieel voor de veiligheid van je bedrijf. Misschien doe je al veel om jezelf online te beschermen, maar wij geven hier 10 tips om je beveiliging samen naar topniveau te tillen. Zo voorkom je dat je tot de 95% van de bedrijven hoort die laaghangend fruit zijn voor hackers…

#1: Zorg dat je up-to-date bent

Door altijd de laatste updates te installeren voorkom je veel problemen. Bekende beveiligingsproblemen (en dat zijn er heel veel) hebben zo geen impact op jouw apparaten of software. Update je besturingssysteem op je computer of laptop, je smartphone en je tablet. Update stuurprogramma's, firmware, software/programma's en gebruik de nieuwste versie. Doe dit altijd! Updaten is de beste beveiliging.

#2: Gebruik encryptie

Klinkt heel eng, maar encryptie betekent eigenlijk gewoon dat je bestanden versleuteld zijn. Stel BitLocker in op je Windows machine, FileVault op je Apple Mac of de interne functies van je telefoon. Informeer welke mogelijkheden je hebt om dat eenvoudig te doen.

#3: Beheer mobiele devices in je bedrijf met MDM

MDM (Mobile Device Management) heeft ermee te maken dat jouw smartphone binnen een organisatie wordt beheerd en dat de toegang tot bedrijfsgegevens of applicaties wordt ingetrokken of de data eraf wordt gehaald bij diefstal. MDM kan nog veel, maar het is wel zo prettig om te weten dat je toch nog iets kunt doen om je gegevens te beschermen, ook als het mis gaat.

Hoe voorkom je dat je tot de 95% van de bedrijven hoort die laaghangend fruit zijn voor hackers?

#4: Gebruik antivirus en antimalware

Antivirus en antimalware zijn verschillende technieken om gevaar tegen te gaan. Antivirus werkt tegen ouderwetse type virussen en antimalware tegen de nieuwste types. Gebruik een goed antivirusproduct en monitor het. Check bijvoorbeeld of het wel aan staat en goed werkt. Zorg ervoor dat je een melding krijgt als je een virus hebt en laat iemand dit proactief oppakken.

#5: Gebruik een automatische update tool

Gebruik tools (of software) die jouw beveiliging automatisch up-to-date houdt zodat je hier geen omkijken meer naar hebt. Moderne varianten kunnen zelfs een online aanval stoppen die nog niet bekend is en door Artificial Intelligence (AI) leren om hier beter in te worden. Zo krijg je overzicht op updates met je OS, Software pakketten, drivers en beveiligings-updates. Zorg er hier wederom voor dat je het monitort, dus dat je weet als er iets niet werkt en ook wat er niet werkt en hoe je dat oplost.

#6: Stel MFA in

Zoals wij in de blog over spam en phishing aankaartten is het van groot belang om een MultiFactor Authenticatie (MFA / 2FA) te hebben. Hierbij wordt er een berichtje gestuurd naar je telefoon of je e-mail wanneer er iemand vanaf een nieuw device probeert in te loggen. Alleen een gebruikersnaam en een wachtwoord is dan dus niet meer genoeg voor een inbreker, waardoor je je beveiliging echt een boost geeft. De meeste bedrijven geven je de mogelijkheid om dit online in te stellen. Zo niet, vraag dan of ze dit willen doen. Als dit niet mogelijk is, stap dan over naar de concurrent. Zo belangrijk is het echt!

#7: Train je personeel

Voorkomen is beter dan genezen. Veel issues op het gebied van veiligheid in de IT kunnen voorkomen worden. Zorg dat je personeel op de hoogte is van basis security regels. Het trainen van nieuw personeel en periodiek bijspijkeren van al het personeel is essentieel om veilig te werken.

#8: Stel een wachtwoordenkluis in

Met LastPass creëer je een soort wachtwoordenkluis, waar je alleen in komt met een master password. Zo kun je gecompliceerde wachtwoorden als 1y2@q0DXd$!vu%Do instellen, wat mensen veel minder snel raden dan Scheldestraat@18 (je adres, een geboortedatum of iets anders wat je makkelijk onthoudt). Je hoeft dus alleen het master wachtwoord te onthouden. Extra handig: LastPass heeft een app voor je smartphone waardoor je ook op andere computers of gewoon je smartphone in kunt loggen wanneer je je telefoon bij je hebt.

#9: Maak een beleid voor je beveiliging

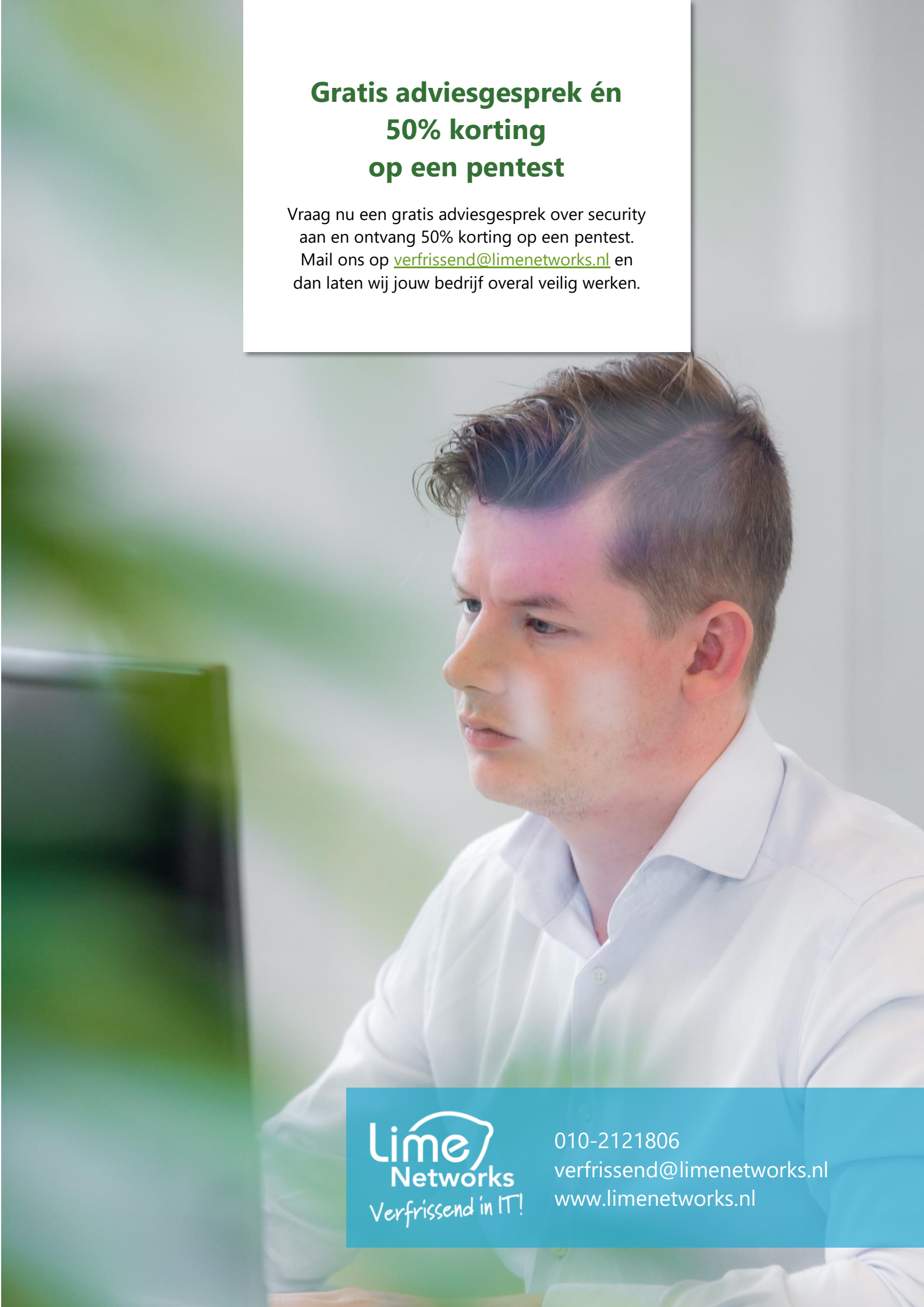
Stel een beleid op voor IT-beveiliging en schrijf hier procedures op. Bijvoorbeeld: wat doen we als het mis gaat? Welke producten moeten er gebruikt worden? Wie is er verantwoordelijk? Wij snappen dat dit even wat werk is, maar het is essentieel. Heb je hier advies of hulp bij nodig? Wij helpen je graag!

#10: Laat pentesten uitvoeren

Last but not least: laat tests uitvoeren om je beveiliging te checken. Met pentesten kun je je gehele IT-netwerk controleren. Een ingehuurde hacker gaat dan kijken op welke manieren hij of zij in je netwerk kan komen. Door deze gaten in je beveiliging te identificeren, kun je ze fixen en je beveiliging versterken. Voer deze tests twee keer per jaar zelf uit en laat het één keer door een externe partij controleren. Let op: laat ze echt uitvoeren en ga niet zelf aan de slag. Voor het uitvoeren heb je namelijk jarenlange ervaring nodig!

Maar dit vind ik helemaal niet zo eenvoudig…

Ons doel is om IT simpel te maken. Daarom hebben wij geprobeerd om algemene en simpele tips te geven om je beveiliging te versterken. Maar soms ligt het binnen jouw bedrijf net wat gecompliceerder of kom je er niet helemaal uit. Geen probleem, daar zijn wij voor. Heb je een IT-probleem of een vraag op het gebied van beveiliging? Onze helpdesk staat altijd voor je klaar, neem gerust even contact met ons op via 010-2121806.



Gratis adviesgesprek én 50% korting op een pentest

Vraag nu een gratis adviesgesprek over security aan en ontvang 50% korting op een pentest. Mail ons op verfrissend@limenetworks.nl en dan laten wij jouw bedrijf overal veilig werken.

Lime Networks
Verfrissend in IT!

010-2121806
verfrissend@limenetworks.nl
www.limenetworks.nl