Experts over digitale veiligheid en weerbaarheid:

‘Bespaar niet op preventie, werk aan bewustwording’

De coronacrisis heeft onze manier van werken ingrijpend veranderd; onder andere internetfraude ligt op de loer nu veel ondernemers en werknemers intensief digitaal (thuis)werken. Hoe veilig zijn we online? Hoe maken we onszelf weerbaarder tegen dit soort aanvallen? En hoe kunnen ondernemers en bedrijven zichzelf beschermen tegen criminaliteit online? Wij vroegen het vier Friese ondernemers met verstand van zaken.

Wordt in jouw eigen onderneming digitaal veilig gewerkt?

Jacco Kuiper, directeur Kuiper Verzekeringen: Binnen onze organisatie werken we digitaal veilig. Dit is voor alle organisaties van essentieel belang, want we zijn afhankelijk geworden van systemen en data en hierdoor zijn we kwetsbaar. Van jongs af aan ben ik geïnteresseerd in IT, digitale infrastructuur en data. De IT-afdeling en onze IT-partners werken intensief samen en zijn continu op zoek naar de beste oplossingen. Wij gaan mee met de ontwikkelingen en laten onze digitale veiligheid structureel controleren.

Ronald Zijlstra, oprichter/eigenaar Oké-PC IT: Omdat wij ICT-diensten en -beheer verzorgen voor bedrijven en scholen, is onze interne beveiliging net zo belangrijk als die van onze klanten. Het is van groot belang dat gegevens optimaal worden beveiligd om ongeautoriseerde toegang te voorkomen. De perfecte beveiliging bestaat niet. Al onze werkzaamheden zijn erop gericht om de kans op storingen, dataverlies en gegevenslekken zoveel mogelijk te voorkomen. Naast technische beveiliging van systemen (dichten van lekken en preventief onderhoud) is het van belang deze regelmatig te testen, en een plan klaar te hebben over hoe te handelen in geval van een incident. Bedrijven zijn hiertoe verplicht in het kader van de AVG.

Van der Schaaf: ‘Eén van de grootste gevaren is de mens: bewustzijn van de gevaren is van wezenlijk belang’

Gerben van der Schaaf, eigenaar Faber Telecom & Data.

Kuiper: 'Als een organisatie doelwit is van internetcriminelen heeft dit enorme gevolgen. Het voorkomen hiervan ligt in handen van ondernemers'

Jacco Kuiper, directeur Kuiper Verzekeringen.

Gerben van der Schaaf, eigenaar Faber Telecom & Data: Uiteraard zijn wij ons van de digitale bedreigingen bewust en proberen we deze maximaal te beperken door het gebruik van de technische oplossingen die beschikbaar zijn. Maar één van de grootste gevaren is de mens: een goed bewustzijn van de aanwezige gevaren onder de medewerkers is van wezenlijk belang. Een zelf-georganiseerde 'phishing aanval' draagt hier enorm aan bij: het zet mensen aan het denken. Door bewustwording te creëren krijg je ook draagvlak voor technische beveiligingsoplossingen, die soms als vervelend en onhandig worden gezien.
Eduard Vrieling, directeur Accent Automatisering: Ja, er wordt bij ons veilig digitaal gewerkt. We hebben diverse certificeringen: ISO27001, NEN7510 en ISAE 3402, die dit aantonen en waarvoor wij jaarlijks grondig worden gecontroleerd. Simpel gezegd houdt dit in dat wij aan zeer hoge eisen voldoen op het gebied van informatiebeveiliging.

Speelt digitale veiligheid en weerbaarheid een grote rol in jullie dagelijkse bedrijfsprocessen?

Zijlstra (Oké-PC IT): Absoluut, in alle aspecten van ons werk wordt hier rekening mee gehouden. Onze klanten vertrouwen ons hun digitale gegevens toe en verwachten dat we hier verstandig mee omgaan. We adviseren onze klanten hoe ze een goede balans kunnen vinden tussen beveiliging en gebruiksgemak. We werken hierin intensief samen met ESET, de toonaangevende leverancier van oplossingen voor beveiliging, versleuteling en toegangscontrole. Ook verzorgen we trainingen voor bedrijven, onder andere om medewerkers phishing-pogingen beter te leren herkennen.

Van der Schaaf (Faber Telecom & Data): Als ICT-leverancier zijn we niet alleen verantwoordelijk voor onze eigen veiligheid, maar hebben we ook een verantwoordelijkheid richting onze klanten. Diensten en apparatuur veilig houden is daardoor dagelijkse kost. Veel klanten hebben bijvoorbeeld geen weet van beveiligingszaken met betrekking tot hun telefonie-omgeving. Dat kun je ze niet kwalijk nemen: het is hun dagelijkse materie niet, daar ligt ónze expertise.

Kuiper (Kuiper Verzekeringen): Absoluut! De regels rondom veiligheid en privacy worden steeds aangescherpt. Wij hebben het onderwerp cyberveiligheid en weerbaarheid altijd op de agenda staan. We investeren continu in digitale oplossingen om de beveiliging van de 'online infrastructuur' te verhogen. Een kleine 'breuk' kan een enorme impact hebben op onze reputatie en betrouwbaarheid. Wij kijken naar de hele keten van partners, leveranciers, zzp-ers en andere partijen. Daarbij moeten wij het goede voorbeeld geven. Wij adviseren onze klanten om de online risico's te beschermen en een cyber- en datariskverzekering af te sluiten. Dan moeten wij onze zaken zeker op orde hebben.

Vrieling (Accent Automatisering): Jazeker. Als IT-organisatie spelen wij een grote rol in de informatiebeveiliging van onze klanten. Het is aan ons om ervoor te zorgen dat organisaties niet alleen efficiënt, maar vooral ook veilig kunnen werken. Wij zijn daarom constant bezig met de inzet van kwalitatief hoogwaardige producten en diensten, het implementeren van slimme security-oplossingen, de training en bewustwording van gebruikers en het monitoren en beschermen van systemen.

Ben je goed op de hoogte van de laatste ontwikkelingen op het gebied van internetcriminaliteit?

Van der Schaaf (Faber Telecom & Data): We volgen ontwikkelingen uiteraard op de voet. Veel informatie krijgen we via onze leveranciers, ICT-partners en nieuwsberichten. Daarnaast hebben we ook een netwerk van branchegenoten waarmee we regelmatig kunnen sparren.

Zijlstra: 'Geef gebruikers alleen toegang tot systemen en informatie die ze écht nodig hebben'

Vrieling (Accent Automatisering): Security is een groot onderdeel van ons vak en daarom zijn we constant bezig met ontwikkelingen op dit gebied. We zijn actief op fora rondom dit onderwerp, maar krijgen ook vanuit het Nationaal Cyber Security Centrum meldingen als er online dreigingen zijn ontstaan. Wij scannen verder al onze systemen automatisch op de mogelijke installatie van 'patches' voor beveiligingslekken. Zo blijven we constant op de hoogte en kunnen we indien nodig direct schakelen.

Kuiper (Kuiper Verzekeringen): Wij zijn goed op de hoogte van de ontwikkelingen en de nieuwste oplossingen. Wekelijks zitten wij met onze leveranciers om tafel om optimalisaties door te voeren in de systeemveiligheid. Daarnaast worden wij van tijd tot tijd getraind door onze IT-partners en de grote verzekeraars om kennis en ervaring uit te wisselen.

Zijlstra (Oké-PC IT): Van jongs af aan ben ik al geïnteresseerd in computertechniek en digitale processen.: ik heb van mijn hobby mijn werk kunnen maken. Het aantal veiligheidslekken in apparatuur en software die in omloop is, is immens groot en er komen dagelijks nieuwe kwetsbaarheden aan het licht. Het vergt veel om hier overzicht in te houden. Tegenwoordig geef ik ook lezingen over Cyber Security voor onder meer ondernemersclubs. Hierin schets ik de risico's en werkwijze van cybercriminelen. Het is opvallend dat maar weinigen het onderwerp erg serieus nemen, terwijl elke ondernemer wel toegeeft volledig afhankelijk te zijn van digitale gegevens en processen.

Heeft de coronacrisis - en intensiever thuiswerken - geleid tot stappen op het gebied van veilig digitaal werken?

Vrieling (Accent Automatisering): Locatieonafhankelijk werken is voor ons niet nieuw en hiervoor maakten we uiteraard gebruik van onze eigen security-oplossingen. Wel hebben we een extra check gedaan onder medewerkers of de laptop of PC thuis ook door gezinsleden werd gebruikt. Was dit het geval, dan realiseerden we een extra werkplek om de toegang tot onze systemen extra te beveiligen. Verder hebben we natuurlijk veel klanten ondersteund bij de noodzakelijke stappen op het gebied van veilig thuiswerken.
Kuiper (Kuiper Verzekeringen): Onze organisatie is aan het begin van de coronacrisis heel soepel van een kantooorganisatie overgegaan naar een thuiswerkorganisatie. Natuurlijk hebben wij kritisch onderzocht of de informatieveiligheid door het thuiswerken niet in het geding kwam, maar hier was geen sprake van.

Zijlstra (Oké-PC IT): We hebben begin dit jaar in korte tijd veel organisaties geholpen (massaal) thuiswerken mogelijk te maken. Erg belangrijk is dat er tweestapsverificatie wordt toegepast om toegang te krijgen tot systemen. Een wachtwoord alleen is niet meer voldoende, omdat dit kan worden onderschept, afgekeken of gebruteforced (geraden) . Om toegang te krijgen met tweestapsverificatie is niet alleen iets nodig wat je weet (een wachtwoord), maar ook iets wat je bezit (een smartphone). Dit maakt het voor kwaadwillenden vele malen lastiger om binnen te komen.

Van der Schaaf (Faber Telecom & Data): Vooral aan het begin van de coronacrisis zagen we dat veel mensen thuis gingen werken: er vond bijna een explosie plaats van internetverkeer en mobiel datagebruik, zowel bij onszelf als bij onze klanten. Doordat de meeste systemen al voorbereid zijn op plaatsonafhankelijk werken konden we snel schakelen, waarbij veiligheid eigenlijk niet eens een issue was. Veiligheid is in de basis altijd onderdeel van het plan.

Hoe kunnen ondernemers zichzelf beschermen tegen criminaliteit online?

Zijlstra (Oké-PC IT): Er zijn een aantal zaken die hierin belangrijk zijn. Digitale systemen hebben de neiging om te groeien, c.q. steeds complexer te worden. Dit maakt het lastiger om vlot goede beveiligingsmaatregelen toe te passen. Het is verstandig om zaken zo eenvoudig mogelijk in te richten en goed te documenteren. Geef gebruikers alleen toegang tot systemen en informatie die ze écht nodig hebben. Ondernemers doen er goed aan regelmatig in gesprek te blijven met hun ICT-partner. Die weet waar de nieuwste dreigingen en ontwikkelingen liggen. Bespaar niet op preventief onderhoud en zorg dat alle beveiligingsupdates voor software en apparatuur snel worden toegepast.

Van der Schaaf (Faber Telecom & Data): Voor de technische kant heb je als bedrijf een ICT-partner. Zelf kun je werken aan bewustwording en gedragsregels afspreken. Bijvoorbeeld: als een medewerker een e-mail ontvangt met ogenschijnlijk een factuur, deze niet zomaar wordt doorgestuurd naar de financiële afdeling, maar er eerst wordt geïnformeerd of er van deze instantie een factuur verwacht wordt. Er zijn legio praktijkvoorbeelden waarbij een corrupte e-mail eerst vier of vijf keer intern doorgestuurd werd voor de bijlage werd geopend, met alle gevolgen van dien. Het boerenverstand gebruiken en het onderbuikgevoel niet negeren zijn de sleutel tot het vergroten van de veiligheid.

Vrieling (Accent Automatisering): Er zijn talloze technische oplossingen, maar die hebben geen zin als medewerkers zich niet bewust zijn van de online risico's. Je kunt alles proberen dicht te timmeren, maar als een collega op een verkeerde link klikt gaat het toch mis. Dat zie je ook in de praktijk. Of het nu gaat om de bakker op de hoek of een grote organisatie: beveiligingslekken ontstaan voornamelijk doordat een medewerker in een phishing-mail is getrapt. Om je als organisatie écht te beschermen is het noodzakelijk om middels trainingen bewustzijn te creëren onder medewerkers.

Kuiper (Kuiper Verzekeringen): Wanneer het over bescherming gaat van de digitale infrastructuur komt onze expertise om de hoek kijken. Wanneer een organisatie doelwit is van internetcriminelen kan dit enorme gevolgen hebben voor de omzet, klanten en bedrijfskansen. Het voorkomen hiervan ligt in eigen handen van ondernemers. De risico's en gevolgen zijn te verkleinen met een combinatie van best practices, een responsplan en een goede cyber- en datariskverzekering. Deze dekt de aansprakelijkheid met betrekking tot bijvoorbeeld diefstal van privacygevoelige gegevens, het digitaal onbedoeld schenden van auteursrecht en het verspreiden van laster en virussen.

Speelt digitalisering en online veiligheid een rol in de ontwikkeling van jouw bedrijf?

Kuiper (Kuiper Verzekeringen): Onze organisatie groeit en dat geldt zeker voor de komende jaren. Begin volgend jaar verwachten wij onze klanten een digitale omgeving aan te kunnen bieden. Dit zorgt ervoor dat wij hier ook kritisch naar de digitale veiligheid moeten kijken. Daarbij gaan de ontwikkelingen op het gebied van online veiligheid erg snel en zullen wij daar zeker in meegaan.

Vrieling (Accent Automatisering): Absoluut, dat is als IT-bedrijf een gegeven. Sterker nog: door de razendsnelle digitale ontwikkelingen gaat dit alleen nog maar belangrijker worden. Online werken wordt verder geïntensiveerd, organisaties worden hiervan steeds meer afhankelijk en tegelijkertijd wordt de werkwijze van cybercriminelen alsmaar geavanceerder. Dat zet online veiligheid de komende jaren permanent hoog op de agenda bij ons.

Van der Schaaf (Faber Telecom & Data): In de basis houdt ons bedrijf zich over vijf jaar nog ongeveer met dezelfde activiteiten bezig. Onze klanten blijven ondanks het flexibel werken bedrijfspanden houden. Hierdoor blijft de vraag naar een betrouwbaar datanetwerk, camerabeveiliging, veilige wifi en telefonische bereikbaarheid bestaan. We zien wat telecom betreft een grotere verschuiving naar onze (private-) cloud-oplossingen. Ook bij ons werken collega's vaker vanuit huis. Doordat we onze systemen online voor hen toegankelijk maken, vraagt dat automatisch om een kritische blik op de beveiliging. We hebben veel kennis en ervaring op vlak, waardoor we dit voor onszelf en onze klanten goed geregeld hebben.

Zijlstra (Oké-PC IT): Over vijf jaar zal online veiligheid verreweg het belangrijkste deel van onze werkzaamheden vormen. Al langere tijd worden bedrijven gericht aangevallen en afgeperst zodra systemen en digitale gegevens zijn gegijzeld (ransomware). De nieuwste trends zijn dat ook de back-ups worden versleuteld, zodat slachtoffers vrijwel geen andere optie hebben dan te betalen. Slachtoffers worden onder druk gezet door het losgeld steeds te verhogen en er wordt gedreigd met het lekken van de gestolen bedrijfsgegevens. Medewerkers krijgen geld aangeboden van criminelen om mee te werken aan het verlenen van toegang tot interne systemen. Onlangs wist bij Tesla een medewerker een aanbod van één miljoen dollar gelukkig te weerstaan…

Vrieling: 'Je kunt alles dichttimmeren, maar als een collega op een verkeerde link klikt gaat het toch mis'

Eduard Vrieling, directeur Accent Automatisering.