CCV centrum voor criminaliteitspreventie en veiligheid

Mkb weerbaar maken tegen cyberbedreigingen

Projectrapport

Utrecht, juli 2023
Eva Whyte, Mirjam Prinsen

Aanleiding

Ransomware en andere vormen van cybercriminaliteit zijn inmiddels zo'n groot probleem geworden dat de nationale veiligheid in gevaar is, waarschuwt de NCTV[1]. Belangrijke onderdelen van de infrastructuur zouden kunnen uitvallen, als ze door ransomwareaanvallers worden gekraakt. Maar niet alleen grote (overheids)organisaties worden slachtoffer van dit soort aanvallen, ook (kleinere) bedrijven en gemeenten worden getroffen door ransomware. Harde cijfers voor het mkb zijn er helaas niet, mede vanwege lage aangiftebereidheid[2], aldus Matthijs Jaspers van de Ransomware Taskforce – Politie Oost Brabant. Uit een vooronderzoek van het Centre of Expertise Cyber Security van De Haagse Hogeschool bleek wel dat een op de vijf mkb-ondernemers die deelnamen aan het onderzoek slachtoffer zijn geworden van een cyberaanval[3]. Ransomware behoort volgens de NCTV (2021[4]) dan ook tot een van de belangrijkste manieren waarop cybercriminelen bedrijven en organisaties proberen te raken.

Cybercriminelen richten zich niet alleen op grote bedrijven, maar 'schieten met hagel' tot ze een doel treffen en leggen daarmee gemakkelijk hele bedrijfsprocessen plat, ook van kleine ondernemers. NCTV noemt dit opportunistische aanvallen[5], niet gericht op een specifieke persoon of organisatie, maar op schaalvoordeel als verdienmodel; hoe hoger het aantal getroffen bedrijven, personen en individuen hoe beter. In het geval van ransomware wordt veelal een lager losgeldbedrag gevraagd, omdat ze met een grote hoeveelheid kleinere bedragen ook winst weten te maken.

Cyberaanvallen leiden enerzijds tot de onbeschikbaarheid van systemen, maar anderzijds ook tot het potentieel lekken van vertrouwelijke (persoons)gegevens. Concreet betekent het dat je systeem gegijzeld wordt, je niet meer bij je eigen bestanden kunt en criminelen toegang hebben tot gevoelige (persoons)informatie die men kan misbruiken om fraude mee te plegen of verspreiden. Met alle ontwrichtende gevolgen van dien voor de organisatie, de onderneming, de (bedrijfs-)keten en/of de maatschappij.

Ondanks de waarschuwingen en adviezen van de overheid, banken en brancheorganisaties, treffen mkb'ers nog te weinig maatregelen om zichzelf goed te beschermen tegen ransomware en andere vormen van cybercriminaliteit.[6] In opdracht van het ministerie van Justitie en Veiligheid heeft het CCV in 2022 onderzoek verricht naar de motivaties en gedrag van mkb'ers ten aanzien van ransom- en cyberweerbaarheid.

[1] https://nos.nl/artikel/2387046-nctv-ransomware-is-bedreiging-voor-nationale-veiligheid

2 https://www.rtlnieuws.nl/tech/artikel/5250115/ransomware-mkb-nederland-ondernemers-cybercrime

3 ttps://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkbmkbmkb/infographic-nulmeting-cybersecurity-mkb.pdf

4 https://www.digitaltrustcenter.nl/nieuws/publicatie-csbn-2021-voor-ondernemers

5 https://www.digitaltrustcenter.nl/informatie-advies/ransomware

6 https://www.deondernemer.nl/innovatie/cybersecurity/nederlandse-bedrijven-laks-cybersecurity-vodafone~4280438?referrer=https%3A%2F%2Fwww.google.com%2F; https://www.abnamro.nl/nl/media/rapport-mkbmkbmkb-isoleert-zich-door-beperkt-bewustzijn-cyberdreiging-mei-2023_tcm16-195076.pdf; https://www.rijksoverheid.nl/actueel/nieuws/2022/10/05/nederland-digitaal-bewuster-maar-deel-kleiner-mkbmkbmkb-onderneemt-nog-geen-actie

Inhoud

1 Vooronderzoek en vervolg

Het initiële onderzoek naar het weerbaar maken van het mkb tegen ransomware had onderstaande doelen:

1. Inzicht en overzicht in mogelijke weerstanden bij het mkb om zich te wapenen tegen ransomware (verkenning);
2. De aard van deze weerstanden (onderzoek); en
3. Op welke wijze deze weggenomen kunnen worden en hoe zelfbeschermende initiatieven gestimuleerd kunnen worden (interventie).

1.1 Resultaten vooronderzoek

Op basis van ons vooronderzoek (eind 2022) concludeerden we dat er al veel onderzoek is gedaan naar de motivatie en het gedrag van mkb'ers als het gaat om het wel of niet treffen van maatregelen om ransomware tegen te gaan. Ook de aannames die wij op basis van deskresearch hadden gevorm,d werden herkend door de gesproken experts:

- De basisprincipes van cybersecurity[7] worden voor een deel opgevolgd[8], het (1) draaien van updates en (2) gebruik van antivirussoftware wordt door het merendeel van het mkb (ongeacht de grootte) in principe al gedaan. Echter zien we dat een aantal activiteiten die voortvloeien uit de andere drie basismaatregelen nog achterblijven. Dit zijn onderstaande basisprincipes:
  - Kwetsbaarheden inventariseren
  - Beperken toegang
  - Veilige instellingen

  Deze basisprincipes zijn complexer, niet geautomatiseerd, maken geen onderdeel van het primair proces uit en/of er is specifieke kennis of expertise voor nodig. Updates daarentegen kunnen vaak geautomatiseerd worden en antivirussoftware zit vaak al geïntegreerd in nieuwe technologie/systemen en vraagt geen (frequente) extra handeling.
- Grootte van het mkb is gekoppeld aan het percentage getroffen maatregelen: er is waarschijnlijk een relatie tussen de grootte van het mkb en het treffen van de nodige maatregelen[9]. Hoe groter de onderneming (50 – 250), hoe hoger het percentage getroffen maatregelen (ongeacht om welk basisprincipe het ging). Met name de mkb's met fte grootte 2 – 10 en 10 – 50 lopen nog achter bij het treffen van maatregelen.
- Motivatie van de mkb'er om maatregelen te treffen is laag: men ziet deze niet als noodzakelijk, omdat ze inschatten dat zij niet geraakt zullen worden; maatregelen verstoren de dagelijkse werkprocessen of zijn geen onderdeel van hun core business; de waan van de dag is belangrijker (inflatie, personeelstekort en dergelijke); onbekendheid met goede leveranciers van IT-diensten en/of betrouwbare branchespecifieke maatregelen/applicaties; onbekendheid met mogelijke gevolgen; niet de expertise in huis; schuiven verantwoordelijkheid af ("daar heb ik een ICT'er voor").

1.2 Vervolg onderzoek

De meerwaarde van dit project lag na het vooronderzoek niet zozeer in het verder onderzoeken van motivaties en effecten van mogelijke interventies, maar in het toewerken naar een integrale aanpak van het probleem. Integrale aanpak, samen met verschillende partijen (overheid, mkb-brancheorganisaties, verzekeraars, producenten en dergelijk).

---

[7] https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

[8] Cybersecurity monitor 2021, CBS

[9] Cybersecurity monitor 2021, CBS

Wij differentieerden daarin vier thema's:

- Bewustwording:
    - Basale informatie: hou het simpel (de techniek/taal is voor velen te ingewikkeld), hou het praktisch en branchespecifiek.
    - Stop met generieke verhalen. Blijf niet zenden met algemene kennis.
    - Differentieer in communicatie: maak het sector/grootte mkb specifiek. Maak samen met brancheverenigingen risicoprofielen en ga op basis daarvan interventies ontwikkelen en campagnes uitrollen.
- Makkelijk maken
    - Gebruik de basisscan van het Digital Trust Center als startprincipe, deze wordt goed gewaardeerd door het mkb.
    - Maak cyberveiligheid onderdeel van de primaire processen. Bijvoorbeeld securitymaatregelen inbouwen in hardware en software en producenten en leveranciers ook verplichten dit aan te bieden, niet als keuze, maar als standaard. Dus met grote leveranciers om tafel en mogelijkheden bespreken.
    - Geef gerichte structurele subsidies.
    - Werk samen met verschillende partijen die een hands-on aanpak hebben ontwikkeld voor het mkb waarin er opvolging gegeven wordt aan bewustwording door concreet handelingsperspectief en actie. Zoals bijvoorbeeld projecten van het CCV, Platvorm Veilig Ondernemen (PVO) en het project RAAK.
- Wettelijke ondersteuning
    - Introduceer een meldplicht bij incident/beveiligingsregels voor digitale producten en diensten die binnen de EU op de markt komen (Cyber Resilience Act).
    - Ontwikkel certificering mkb voor op orde hebben cyberveiligheid. Koppel het wel aan een financiële prikkel (bijvoorbeeld dat je zonder certificering geen toegang krijgt tot de markt of iets dergelijks).
    - Verplicht software/hardware of ICT-leveranciers tot maatregelen.
    - Meer regulering. Cybersecurity moet onderdeel zijn van veilige bedrijfsvoering.
- Onderhoud
    - Verricht periodiek onderhoud. Cybercrime blijft zich ontwikkelen dus je moet mee blijven gaan in deze ontwikkelingen en jezelf als mkb goed blijven beschermen. Werk hierin samen met diverse partijen (zoals overheid, mkb brancheorganisaties, verzekeraars en producenten).

Na gesprekken tussen het CCV en het ministerie van Justitie en Veiligheid is ervoor gekozen om als eerste stap verder te onderzoeken wat er nodig is om de bewustwording bij het mkb te vergroten. Het vervolg van dit onderzoekstraject moest aanknopingspunten bieden om een gerichte campagne te ontwikkelen op het gebied van ransomware (en cyberdreigingen in z'n algemeenheid). Ons advies daarbij was om niet alleen te focussen op bewustwording, maar er ook een duidelijk handelingsperspectief aan te koppelen en dit zoveel mogelijk te laten aansluiten bij de werkprocessen van de specifieke mkb'er.

2 Segmentatie van branches

Om een campagne (of interventie) zo effectief mogelijk te laten verlopen is segmentatie binnen de doelgroep nodig. Het mkb is geen homogene groep. Het is een diverse groep ondernemers, die om diverse benaderingen vraagt. Uit het vooronderzoek bleek dat de mate van gerichtheid op een specifieke branche een belangrijke factor is bij het doen slagen van interventies. Helemaal als er in de aanpak een concreet handelingsperspectief wordt gegeven en niet alleen algemene informatie wordt gedeeld. De grootste kans van slagen heb je als je dicht bij de belevingswereld van de ondernemer kunt komen.

Dat betekent:

- Specifieke informatie die aansluit bij het werkproces van de sector/branche.
    - Concreet en simpel handelingsperspectief dat haalbaar is, ongeacht het (technische) kennisniveau.
    - Het ministerie van Justitie en Veiligheid kiest in dit verband voor het doen van de basisscan van het Digital Trust Center als handelingsperspectief.
- Bewustwording op sector/brancheniveau over de specifieke gevolgen van een ransomwareaanval op hun bedrijf (weerleggen van de optimism bias, het kan namelijk iedereen raken).

Het mkb segmenteren kan op verschillende manieren:

- Grootte bedrijf (kleine bedrijven treffen minder maatregelen dan grote bedrijven);
- Risico gestuurd (welke sectoren worden vaker slachtoffer of lijden de grootste schade);
- Bereikbaarheid van de doelgroep (hoe makkelijk kunnen we de doelgroep benaderen);
- Laaghangend fruit (van welke doelgroep is al veel bekend over schade en slachtofferschap en is goed te benaderen).

2.1 Ad 1 Grootte bedrijf

Uit het vooronderzoek (CBS Cybersecuritymonitor) blijkt dat met name mkb-bedrijven met minder dan 50 medewerkers slecht maatregelen treffen. Segmentatie op basis van grootte van het bedrijf levert echter op zichzelf niet echt een werkbare segmentatie op, omdat de groep dan nog steeds te groot en te divers is om te benaderen in een pilot. Wel zien we mogelijkheden in een segmentatie op grootte van het bedrijf op het moment dat er voor een bepaalde branche is gekozen. Dit kunnen we echter achteraf bepalen als we meer inzicht in de branches hebben.

2.2 Ad 2 Risicogestuurd

Segmentatie of basis van schade en frequentie van ransomware-aanvallen is een waardevolle segmentatie. Echter, hier ontbreekt goede informatie om te kunnen segmenteren. We hebben geen gegevens over in welke sectoren/branches de meeste slachtoffers vallen en welke schade dat tot gevolg heeft. Ook het bepalen van de ernst van de schade en deze wegen/waarderen is een onderzoek op zich. Er zijn namelijk verschillende vormen van schade, denk aan aantasting van:

- Kwaliteit van psycho-sociaalmaatschappelijk leven
- Economie/financieel
- Milieu/natuur
- Arbo/veiligheid/stress
- Fysieke veiligheid
- Imago

Wat weegt het zwaarst? Dat is lastig te bepalen. Als men de schade bijvoorbeeld uitdrukt in concrete bedragen, dan kan €10.000 voor een eenmanszaak grotere gevolgen hebben dan voor een groot bedrijf.

2.3 Ad 3 en 4 Bereikbaarheid van de doelgroep en laaghangend fruit

Sectoren/branches die goed georganiseerd zijn, een representatieve brancheorganisatie hebben en een duidelijke mediaconsumptie hebben, zijn makkelijker te bereiken door middel van een campagne. Het ministerie van Justitie en Veiligheid kan via betrouwbare kanalen op het juiste moment aansluiten bij de doelgroep. Dat betekent ook kiezen voor het laaghangend fruit: een

branche waar we veel over weten en waar we de aanpak in de vorm van een pilot kunnen uittesten (om de gekozen aanpak in de toekomst te verbeteren en verder uit te rollen naar andere sectoren/branches). De SBI-codes van het CBS kunnen we gebruiken voor de afbakening van de sector/branche.

2.4 Keuze segmentatie

In overleg met Michiel Hillenaar (JenV) en Jacco van der Kolk (DTZ- EZK) is gekozen voor een segmentatie op basis van deels 1 (verdere segmentatie op basis van grootte binnen de branche, voor zover de data dat mogelijk maakt), 3 en/of 4.

2.5 Drie branches: restaurants (horeca), makelaars en kinderopvang

Op basis van de segmentatiekeuze is in eerste instantie gekozen voor restaurants (horeca), goederenvervoer over land (transportbranche) en bakkers (detailhandel). Echter, toen we de brancheorganisaties benaderden, bleek dat Transport en Logistiek Nederland zelf al bezig was met een traject op het gebied van cyberveiligheid, Samen Digitaal Veilig[10]. We wilden niet twee overlappende trajecten tegelijk laten lopen, daarom werd besloten om een vervangende branche te kiezen. Dit werden de makelaars. Met de bakkersbranche kregen we geen contact, niet via de officiële kanalen van de brancheorganisaties, en ook niet via persoonlijke contacten. Mede omdat bakkers in deze periode hard getroffen werden door een gascrisis die waarschijnlijk al hun aandacht vroeg, werd besloten om deze branche te vervangen voor de kinderopvang.

We hebben uiteindelijk gekozen voor drie branches die verschillende kenmerken in hun digitale werkprocessen hebben:

- Digitale uitwisseling van informatie hoort niet bij het primaire proces maar de branche wordt digitaler (restaurants).
- Onderdeel van een informatieketen en dus (relatief) veel digitale uitwisseling van gegevens (makelaars).
- Branche is goed georganiseerd, bereikbaar, wisselt veel persoonsgegevens uit, maar dit is ondersteunend aan het primaire proces (kinderopvang).

[10] https://www.tln.nl/samen-digitaal-veilig/

3 Resultaten Onderzoek

In dit hoofdstuk koppelen we de resultaten van ons onderzoek terug. Dit op basis van:

- Deskresearch
- Gesprekken met brancheorganisaties
- Online vragenlijst aan mkb'ers uit de branche

Een kanttekening bij de resultaten van de online vragenlijst: hoewel de branche-organisaties aangeven dat ze het een erg belangrijk thema vinden en er ook graag zelf aandacht aan besteden, zie je een lage betrokkenheid bij de ondernemers als het gaat om het invullen van de vragenlijsten. Bij de makelaars hadden we een respons van 14, bij de horeca 16, waarvan de meerderheid een café heeft en slechts twee een restaurant. Bij de kinderopvang hebben we gebruikgemaakt van twee vragenlijsten: één voor gastouders en één voor de overige kinderdagopvang. Deze twee vormen van opvang verschillen namelijk wezenlijk van elkaar. Gastouders zijn vooral zzp'ers die per dag maximaal zes kinderen opvangen. Bij de kinderdagopvang wordt vaak met meer personeel gewerkt en worden er meer kinderen opvangen. De respons op de vragenlijsten was ook in deze branche niet heel hoog: 14 reacties van de gastouders en 40 reacties bij de kinderdagopvang.

Aanvankelijk was onze insteek om de gesprekken met de brancheorganisaties te gebruiken als input voor de online vragenlijsten. Vanwege de geringe respons is het onderzoek meer kwalitatief van aard geworden. De antwoorden op de online vragenlijsten zien we vooral als ondersteuning van het verhaal dat de brancheorganisaties vertelden.

We hebben geen onderzoek gedaan naar mogelijke verklaringen voor de lage respons. De gesprekken met de brancheorganisaties geven echter wel aanknopingspunten voor verklaringen:

  - Cybersecurity behoort niet tot het primaire proces.
  - Een van de brancheorganisaties gaf vooraf aan dat de respons op vragenlijsten over het algemeen laag is, zeker als het niet om zaken in het primaire proces gaat.
- Ondernemers hebben andere (actuele) zorgen:
  - Hoge energiekosten en inflatie (restaurants, deels ook kinderopvang)
  - Druk op de huizenmarkt (makelaars)
  - Komende stelselwijzigingen (kinderopvang)
  - Personeelstekort (restaurants, kinderopvang)

3.1 Restaurants[11]

Naast deskresearch hebben we gesproken met de Koninklijke Horeca Nederland (KHN) om een beeld te krijgen van de branche. KHN heeft ongeveer 18.000 leden, dat is ongeveer 30% van alle horecaondernemingen in Nederland (1e kwartaal 2021)[12]. Zij zijn de grootste beroepsvereniging op het gebied van de Horeca in Nederland. 80% van de leden van KHN is mkb'er.

3.1.1 Algemeen beeld

Een restauranthouder "dopt zijn eigen boontjes". Hij richt een zaak op uit passie voor het vak, aldus de KHN. Centraal voor hem staat de klant een fijne ervaring bieden. De kwaliteit van het eten en drinken, de service en hospitality zijn daarin het belangrijkst. Restaurantondernemers kijken veel naar hun "concullega's", ze zijn erg op elkaar gericht, maar houden hun kaarten voor de borst als het gaat om samen dingen te bespreken/oppakken.

[11] Ondernemers met eetcafés vallen ook onder deze doelgroep.

[12] https://trendrapport.s-bb.nl/vgg/economische-ontwikkelingen/gastvrijheid/#:~:text=In%20de%20horeca%20waren%20in,bedrijven%20in%20die%20periode%20toe.

Digitale veiligheid zien ze niet als onderdeel van hun professie. Toch is het restaurantwerk de laatste jaren steeds digitaler geworden. Niet alleen door digitale hulpmiddelen bij het werk (zoals handhelds voor bestellingen bijvoorbeeld), maar ook door het toegenomen gebruik van bezorgdiensten, online reserveringen en het aanbieden van wifi aan klanten. KHN ziet dat door allerlei "randzaken" die de ondernemers erbij krijgen, ondernemers steeds verder verwijderd raken van de passie waarmee ze hun zaak zijn begonnen.

Het thema veiligheid zien ze als een van de randzaken en niet als onderdeel van het primaire proces. Het staat erg laag op de agenda van ondernemers. Als restauranthouders al bezig zijn met het thema, dan is het met name de fysieke veiligheid. Maar pas als men ermee geconfronteerd wordt (zelf of indirect door verhalen van andere horecaondernemers) dan wil men daar wel wat mee doen. Dat geldt waarschijnlijk ook voor het thema digitale veiligheid.

3.1.2 Digitaal werken en cybersecurity

De restaurantwereld is digitaler geworden, niet alleen door online reserveringssystemen, afhaal- en thuisbezorgdiensten, maar ook de bedrijfsprocessen zelf. Denk hierbij aan: HR-systemen, roostersystemen, payroll, uitbetalingen, loonadministratie (die wordt ook vaak wel uitbesteed aan externe partijen), bestellingen opnemen (via handheld of mobiel), kassasysteem, gebruik van QR-codes of apps om bestellingen te plaatsen.

Met name kleinere mkb'ers gebruiken vaak hun mobiel als belangrijkste digitale device en niet zozeer een computer of laptop. Het is makkelijk en ze kunnen snel schakelen. Ondernemers met wat meer personeel hebben wellicht een centrale laptop of computer die ze gebruiken waar meerdere mensen toegang toe hebben. "Grote kans dat het lijstje met de wachtwoorden ernaast ligt".

Een enkeling, de wat groteren hebben misschien een bureau ingehuurd of een ICT'er die voor hen het een en ander regelt. Met daarbij de gedachte "ik heb het geregeld, dus klaar". Of men er dan nog naar omkijkt is de vraag.

3.1.3 Communicatie en informatievergaring

Horecaondernemers willen snel relevante informatie hebben. Omdat horecaondernemers veel naar elkaar kijken wordt informatie die andere horecaondernemers delen ook vaak als relevant gezien. Dit kan via social media, whatsappgroepen (van horecapleinen bijvoorbeeld) maar ook via vakbladen en KHN-media (website, nieuwsbrief).

Het doen van de basisscan van DTC zou wel een goed begin kunnen zijn volgens de KHN. De brancheorganisatie heeft hier ook wel eens eerder aandacht aan besteed en stimuleert het doen van de scan ook; op hun eigen site staat ook een link naar de scan. Nadeel is dat de scan niet erg bekend is bij de ondernemers.

3.1.4 Welke boodschap zou aansluiten?

Het thema digitale veiligheid leeft niet bij de doelgroep. Ze zijn niet met het onderwerp bezig omdat het te ver van het primaire proces af ligt. Belangrijk is daarom het volgende:

- Sluit in de boodschap richting restaurantondernemers aan bij de bron van hun passie, de onderneming zelf. Je onderneming bescherm je ook door digitaal de zaken op orde te hebben. Laat de klantbeleving niet eindigen in een ransomware drama. Maak inzichtelijk hoe de gevolgen van cybercriminaliteit de onderneming raken. Hoe raakt het daar waar ze hun passie, tijd, energie en geld insteken.
- Restauranthouders zijn erg bezig met elkaar. Het inzetten van een "slachtofferverhaal" kan helpen om de boodschap over te brengen. Als een ervaringsdeskundige het verhaal vertelt, kan dat indruk maken. Daarbij moet afschrikken niet het hoogste doel zijn, maar met name hoe de getroffene de nodige maatregelen heeft doorgevoerd die passen bij het bedrijfsproces en daarmee in de toekomst veilig werkt.

- Geef concrete adviezen, kleine, korte informatie. Bij veel horecaondernemers is het hollen of stilstaan. In deze dynamiek moet informatie makkelijk “te verteren” zijn. En maatregelen makkelijk toe te passen zijn.

3.2 Makelaars

Om een beeld te krijgen van de makelaarsbranche hebben we gesproken met:

- Nederlandse Coöperatieve Vereniging van Makelaars en Taxateurs in onroerende goederen (NVM): grootste ledenorganisatie van Nederland (4400) van makelaars, taxateurs en vastgoeddeskundigen.
- VastgoedPro: beroepsvereniging voor makelaars, taxateurs en bouwkundig keurders (700 leden).
- VBO: Vereniging voor makelaars, taxateurs en huurbemiddelaars (1400 leden).

3.2.1 Algemeen beeld

Er zijn ongeveer 11.000 makelaars in Nederland, waarvan 69% zelfstandig is[13]. Ongeveer 60% is lid van bovenstaande branchevereniging.

Tijdens een van de gesprekken met de brancheorganisaties werden makelaars beschreven als “vrije jongens en meiden”. Ze zijn van oudsher veel op pad, daar ligt hun passie en dat is waar ze hun geld mee verdienen. De client is belangrijk. Makelaarswerk is regionaal werk: ze verkopen doorgaans daar waar ze zelf ook wonen. Vaak zijn ze afhankelijk van mond-tot-mondreclame. Betrouwbaarheid is een belangrijk onderdeel van hun werk.

De administratieve werkzaamheden als gevolg van bezichtigingen, taxaties e.d. (het primaire proces) zijn werkzaamheden die ze het liefst uitbesteden. Hoewel deze ook belangrijk zijn in het primaire proces, zijn dit de werkzaamheden die vaak energie en tijd kosten die ze liever aan de contacten met klanten besteden. Daarom willen ze in de administratieve bijzaken graag ontzorgd worden. De wat grotere makelaardijen hebben administratief personeel dat deze zaken voor hen afhandelt, maar veel zelfstandige makelaars zijn hier zelf verantwoordelijk voor en maken daarom graag gebruik van diverse CRM-systemen en ondersteunende applicaties. NVM-leden maken bijvoorbeeld gebruik van het CRM-systeem van de NVM.

Makelaars die kiezen voor een lidmaatschap van een brancheorganisaties doen dat vanwege een aantal redenen:

- Het laat zien dat je een professional bent. Het is als het ware een keurmerk, dat je geen “cowboy” bent, je bent onderdeel van een betrouwbaar merk.
- Je hebt toegang tot databases met historische en actuele informatie over de woningmarkt.
- Je wordt ondersteund bij je bedrijfsvoering.
- Je houdt je kennis op peil (dit is ook een verplichting om lid te zijn).
- Je krijgt inkoopvoordeel en korting op producten en diensten.
- Je krijgt gratis juridisch advies.
- De brancheorganisatie behartigt je belangen.

3.2.2 Digitaal werken en cybersecurity

Makelaars zijn veel op pad en werken naast een laptop/pc ook veel met mobiele devices. Voornamelijk hun mobiel, blijkt uit de enquête. Bijvoorbeeld om foto’s te maken van informatie van/voor klanten. Andere werkzaamheden die vooral digitaal van aard zijn, zijn afspraken inplannen, biedingen bijhouden, documentuitwisseling met kopers/verkopers, taxateurs, notarissen en andere makelaars. Hiervoor worden vaak digitale systemen gebruikt, zoals een CRM (verplicht bij de NVM),

[13] https://www.rodi.nl/dijkenwaard/280992/recordaantal-nieuwe-makelaars-in-2021#:~:text=Met%20een%20stijging%20van%206,van%20deze%20makelaars%20is%20zelfstandig.

maar ook digitale bidlogbooks, waardebepalingsapplicatie, een CMA-applicatie (Customer Market Analysis) en soms loonadministratieprogramma's (bij kantoren met meerdere werknemers).

Cybersecurity heeft niet direct prioriteit zeggen de brancheorganisaties. Makelaars vinden het wel belangrijk, maar "alles wat niet core business is, wat er niet mee te maken heeft is afleiding, gedoe". Ze vinden het pas urgent als het hun geld, reputatie of vertrouwen van de klant kost. Dat zie je ook in de resultaten van de digitale vragenlijst. De meerderheid neemt maatregelen om zich te beschermen tegen cybercriminaliteit omwille van hun klanten. De meerderheid vindt het daarom ook belangrijk om informatie van klanten in een beveiligde omgeving te plaatsen. De belangrijkste reden om maatregen te treffen tegen cybercriminaliteit: beschermen van hun eigen onderneming.

Over het algemeen schatten makelaars in dat ze redelijk tot gemiddeld beschermd zijn tegen cybercriminaliteit. Een kleine meerderheid van de makelaars die de vragenlijst hadden ingevuld huurde een ICT-specialist in. Degenen die dat niet deden troffen zelf de volgende maatregelen:

- Gebruik van een sterk en uniek wachtwoord
- Multi-factorauthenticatie
- Regelmatige update van hun systemen
- Antivirusprogramma

Een goede basis, toch zien we ook dat als een makelaar meerdere collega's heeft, deze ook toegang hebben tot dezelfde ICT-apparatuur, waarbij in de helft van de gevallen men elkaars wachtwoord ook weet.

3.2.3 Communicatie en informatievergaring

De brancheorganisatie is voor de makelaars die de vragenlijst hebben ingevuld een belangrijke informatiebron. 78% van de makelaars die de vragenlijst heeft ingevuld geeft aan dat ze ook door de brancheorganisatie geïnformeerd zouden willen worden als het gaat om het thema cybercriminaliteit. Daarna volgt het ministerie van Justitie en Veiligheid (44%), de Kamer van Koophandel (22%) en de PVO's (11%).

Brancheorganisaties zelf merken ook dat hun leden goed gebruikmaken van de communicatie- en informatiemiddelen die zij aanbieden. Met name de digitale kanalen: nieuwsbrieven, webinars, e-learningmodules en de eigen ledenportalen. Fysieke bijeenkomsten worden over het algemeen minder goed benut als informatiebron. Relevante vakbladen en andere media: Vastgoedjournaal, BusinessNL en social media (Facebook, LinkedIn, Instagram).

3.2.4 Welke boodschap zou aansluiten?

We hebben in de interviews gevraagd wat in de boodschap richting makelaars zou moeten zitten om hen te overtuigen van het belang van cybersecurity en het daadwerkelijk ook treffen van maatregelen. De brancheorganisaties waren het erover eens dat een "slachtofferverhaal" makelaars zou kunnen overhalen om maatregelen te treffen. De argumenten hiervoor zijn:

- Zo kunnen makelaars zich beter voorstellen dat ze ook zelf geraakt kunnen worden (over het algemeen schat men die kans vrij laag in). De gevolgen worden direct zichtbaar, ze kunnen zich beter verplaatsen in wat ze zouden verliezen.
- Verhalen van andere makelaars worden goed gelezen in de branchemedia.
- Een ervaringsdeskundige kan als geen ander de gevolgen koppelen aan het primaire proces. Dat maakt de boodschap geloofwaardiger. Gegevens die op straat liggen bijvoorbeeld zijn erg, maar dat je er niet meer bij kunt of dat je je klanten moet vertellen dat je niet weet wat er met hun gegevens is gebeurd, dat is misschien nog wel het ergste. Dit werd bevestigd door een makelaar die (anoniem) bereid was om zijn ervaring te delen over een ransomware aanval. Hoewel het 10 jaar geleden is gebeurd, heeft het op hem een blijvende impact gehad en heeft hij zijn gedrag aangepast. Zie bijlage 1.

Aandachtspunten hierbij zijn:

- Een slachtofferverhaal maakt wel bang, maar een slachtoffer kan ook meteen aangeven wat je niet moet doen, of juist wel. Dat handelingsperspectief bieden gerelateerd aan de dagelijkse werkzaamheden van de makelaar is essentieel.
- Omdat de meerderheid van de makelaars éénpitters zijn, of een klein kantoor hebben, is het belangrijk om een verhaal te vertellen van iemand in een vergelijkbare situatie. Niet een voorbeeld van een groot kantoor dat gehackt werd bijvoorbeeld. Dat staat te ver van hen af.

3.2.5 Andere haakjes

Naast informatievoorziening en het bieden van een handelingsperspectief via een campagne, zien wij nog enkele haakjes die ook benut zouden kunnen worden om makelaars op het gebied van cybersecurity te bewegen:

- Punten via brancheorganisaties:
  Makelaars die lid zijn van een brancheorganisatie moeten punten behalen om lid te mogen blijven. Denk hierbij aan punten die men behaalt door trainingen of opleidingen te volgen. Door dit puntensysteem garandeert de brancheorganisatie de kwaliteit van aangesloten leden. Met de brancheorganisatie zou verkend kunnen worden of leden ook punten kunnen verdienen als ze bepaalde maatregelen treffen op het gebied van digitale veiligheid.
- Klanten inzetten:
  Informeer klanten dat ze nagaan of een makelaar een systeem gebruikt voor de opslag van persoonsgegevens. Die systemen zijn vaak het beste beveiligd. Motto zou kunnen zijn: Stuur alleen kopieën van persoonlijke documentatie via beveiligde portals naar de makelaar.

3.3 Kinderopvang

Om een beeld te krijgen van de kinderopvangbranche hebben we gesproken met:

- KennisNetwerk gastouderopvang (KNGO); 2000 leden (inclusief 360 van de in totaal 500 gastouderbureaus), met name middelgrote en individuele leden (niet onderdeel van een keten).
- Brancheorganisatie Kinderopvang (BK); grootste van Nederland met ongeveer 1055 leden (met leden die locaties hebben voor 50 gezinnen tot ongeveer 450.000 gezinnen).

Er zijn meer brancheorganisaties actief in deze branche, helaas kregen we geen contact met andere partijen. Op basis van de informatie die we van de twee gesproken organisaties ontvingen, verwachten we echter wel een representatief beeld van de branche te hebben gekregen en hebben we ook diverse aanknopingspunten kunnen vinden.

Wat betreft de online vragenlijst was de respons laag. Ook hier speelt de actualiteit een rol, er staan veel veranderingen te wachten bij de kinderopvang en er is ook een personeelstekort.

3.3.1 Algemeen beeld

De kinderopvangbranche is een sterk gereguleerde branche. Jaarlijks worden kinderopvanglocaties, zowel gastouders, als gastouderbureaus en kinderdagopvanglocaties (inclusief BSO) geïnspecteerd door de GGD. Veiligheid van het kind, ontwikkeling, een veilige omgeving en geschoold personeel zijn tijdens deze inspecties belangrijke thema's.[14] Op dit moment bevindt de branche zich in een stelselwijzigingstraject. Het kabinet wil gratis opvang, hoewel dit voorlopig is uitgesteld[15] zijn er toch wel belangrijke ontwikkelingen in de branche[16]. Zoals bijvoorbeeld het loslaten van de koppeling tussen gewerkte uren en kinderopvangtoeslag[17]. Daarnaast kampt deze branche, net als vele andere branches met een personeelstekort. Wachttijden lopen op, groepen zijn drukker, roosters krijgt men niet rond, onervaren personeel staat op de groep en personeel krijgt het steeds drukker. Door de oplopende wachttijden ontstaat ook een sneeuwbaleffect naar andere branches; ouders blijven

[14] https://www.rijksoverheid.nl/onderwerpen/kinderopvang/kwaliteitseisen-kinderopvang-en-peuterspeelzalen

[15] https://nos.nl/artikel/2472949-frustratie-maar-ook-opluchting-vanwege-uitstel-gratis-kinderopvang

[16] https://nos.nl/artikel/2475257-kritiek-uit-kamer-over-schrappen-voordeel-voor-ouders-terwijl-opvang-niet-gratis-wordt

[17] https://www.rijksoverheid.nl/actueel/nieuws/2022/02/23/kinderopvangtoeslag-niet-meer-afhankelijk-van-gewerkte-uren

noodgedwongen thuis of werken minder uren waardoor in andere branches ook een personeelstekort ontstaat[18].

Er zijn verschillende soorten kinderopvang:

- Gastouders/gastouderbureaus
    - Gastouders zijn zzp'ers. Een gastouderbureau koppelt vaak gastouders en ouders/kinderen.
    - Gastouders willen vooral met de kinderen bezig zijn, dat is hun prioriteit. Alles wat daarvan afleidt zien ze als randzaken.
    - Gastouders hebben gemiddeld tussen de 5 en 20 gezinnen (max 6 kinderen per dag).
    - Het opleidingsniveau van de gastouders kan heel erg verschillen, van mbo-niveau 1 en 2 tot universitair geschoold.
    - Registratie bij gastouderbureau is verplicht. Gastouders kunnen wel wisselen van gastouderbureau als ze het bureau te veeleisend vinden. Sommigen kiezen wel bewust voor bepaalde gastouderbureaus omdat die voor kwaliteit staan. Er zijn geen eenduidige kwaliteitseisen voor deze bureaus.
    - Gastouders zijn gevoelig voor datgene wat ouders belangrijk vinden. Er is veel interactie tussen ouders en gastouders. Ouders hebben vaak maar weinig contact met het gastouderbureau, alleen bij de registratie, plaatsing en als er wellicht iets niet goed gaat.
- Kinderdagverblijf
    - Bij de kinderdagverblijven zie je grote ketens, maar ook kleinere spelers met slechts één locatie en alles er tussen in.
    - Kinderdagopvangorganisaties die lid worden van een brancheorganisatie doen dat vooral om gebruik te maken van opleidingsmogelijkheden, informatievoorziening, Cao-onderhandelingen, schakel tussen kinderopvang en ministerie.
- BSO
    - Buitenschoolse opvang (BSO) is opvang voor kinderen tussen de vier en de dertien jaar. De BSO vindt plaats voor, na schooltijd en tijdens vakanties. Ook in de vakanties en op studiedagen biedt de BSO opvang aan kinderen. Sinds 2007 zijn scholen verplicht om BSO aan te bieden, dit gaat vaak via de kinderdagopvangorganisaties.

Het thema cybersecurity speelt nagenoeg geen rol. De brancheorganisaties kennen ook geen voorbeelden van organisaties waar het ooit is misgegaan. In de online vragenlijst geven echter 5 van de 40 kinderdagopvangondernemers aan dat zij wel eens slachtoffer zijn geworden van cybercriminaliteit. En dat kan goed misgaan. Een voorbeeld uit 2020, toen er een cyberaanval plaatsvond in Antwerpen, werd ook de stedelijke kinderopvang geraakt. Medewerkers konden niet meer bij medische gegevens van kinderen (medicijngebruik, allergieën, dieetverplichtingen e.d.), locaties waren niet bereikbaar, crisisberichten konden niet meer verzonden worden en de app met alle gegevens van ouders en kinderen werkte niet meer[19]. In dit geval zie je dat digitale veiligheid ook van invloed is op de fysieke veiligheid van kinderen. Dat laatste vindt de branche wel erg belangrijk (en daarop houden de ondernemers en GGD goed toezicht).

3.3.2 Digitaal werken en cybersecurity

De ondernemers zijn volgens de enquêteresultaten gemiddeld tot redelijk goed beschermd tegen cybercriminaliteit. Over de koepelorganisaties of de gastouderbureaus is men positiever, daarvan schatten ze in dat die beter beschermd zijn dan andere ondernemers in de branche. Ondernemers gaan ervan uit dat deze partijen de cybersecurity[20] op orde hebben. Cybersecurity wordt bij de grotere opvangorganisaties geregeld via het hoofdkantoor, die hebben daar technische ondersteuning voor. Maar de meerderheid van de kinderopvangondernemers heeft dat niet. Wel zie je dat veel

[18] https://www.nhnieuws.nl/nieuws/313671/druk-op-personeel-kinderopvang-brengt-steeds-meer-risicos-wachten-tot-het-echt-misgaat

[19] https://www.antwerpen.be/info/6391e243ce24eff5c505c9db/cyberaanval-stad-antwerpen-impact-op-stedelijke-kinderopvang

[20] https://www.computest.nl/nl/over-computest/klanten-en-partners/computest-zorgt-voor-structurele-security-ondersteuning-kidskonnect-platform/

ondernemers gebruik maken van software voor kinderdagopvang waarin alle belangrijke informatie voor medewerkers en ouders staat over het kind. Een grote speler in het aanbod van dit soort software is KidsKonnect, 65% van de kinderdagverblijven maakt gebruik van hun diensten.

De meeste medewerkers in deze branche hebben een aantal basisvaardigheden als het gaat om digitaal werken, maar dat is puur in relatie tot de dagelijkse werkzaamheden gericht op de kinderen. Bij de kinderdagopvang hebben met name de eigenaren/directeuren de online vragenlijst ingevuld. Die staan niet altijd op de groep en hebben wellicht meer kennis van digitale processen, omdat zij daar dagelijks ook mee bezig zijn. Gastouders zijn over het algemeen vooral met de kinderen bezig en minder met administratieve/digitale werkzaamheden.

Bij gastouders ziet men wel dat hoe hoger ze zijn opgeleid, hoe digitaal vaardiger. In de enquêteresultaten zie je terugkomen dat kinderdagopvang over het algemeen best goed op de hoogte is van de verschillende vormen van cybercriminaliteit (ondernemers achten de kans echter klein dat men slachtoffer wordt). Ook vindt de meerderheid dat cybersecurity bij hun werk hoort en dat ze daarom zoveel mogelijk maatregelen treffen ten behoeve van de veiligheid van kinderen, ouders en hun eigen onderneming. Maar eigenlijk weten kinderopvangondernemers niet zo goed wat de gevolgen zouden kunnen zijn voor hun specifieke situatie.

De branche werkt behoorlijk digitaal, er worden verschillende apparaten maar ook kanalen gebruikt, met verschillende doeleinden:

<u>Gastouders</u>

- Documenteren van evaluatiegesprekken
    - Vaak op een tablet of laptop in het huis van de gastouder waarop wellicht meerdere huisgenoten van de gastouder toegang hebben.
- Social media
    - Facebook, ook in openbare Facebook-groepen waar ook informatie gedeeld wordt.
- WhatsApp als communicatiemiddel met ouders
- Mobiel gebruik
- Tablets en computers voor spelletjes, educatie en games
- Ouders helpen met toeslagen
    - Er zijn gevallen bekend waarin de gastouders de DigiD van ouders kregen.
- Oudercommunicatie apps
- Risico-inventarisatie app
    - Risico-inventarisatie van de werkplek van de gastouder, wordt door de gastouderbureaus gebruikt, gaat met name om fysieke veiligheid.
- Administratie
    - Veel informatie-uitwisseling via de mail, GGD-gegevens, financiële gegevens en andere belangrijke informaties van ouders en kinderen.

<u>Kinderdagverblijf</u>

- Software voor opvangplanning (kindplanning), facturatie en communicatie
    - Zoals eerder genoemd KidsKonnect. De financiële administratie van de opvanglocatie is daaraan gekoppeld.
    - Via deze apps wordt ook daginformatie van de kinderen gedeeld met de ouders, inclusief foto's.
    - Hiervoor worden ook iPads of mobiele telefoons gebruikt op de groep.
- Administratie
    - Roosterplanning, uitbetaling aan medewerkers, innen van gelden van ouders.
    - Personenregister Kinderopvang (PKR), waar de VOG's gekoppeld worden aan de locatie. Voor continue screening.
    - LRK: Landelijk Register Kinderopvang, waar je op nummer en naam kunt kijken naar het GGD-verslag van de opvanglocatie.
- Camerasystemen
    - Vanwege personeelstekort wordt nog wel eens gewerkt met camera's (ouderraden moeten dit wel goedkeuren).

<u>BSO's</u>

- Software voor kindplanning en delen van informatie over de kinderen aan de ouders (zie ook kinderdagverblijf).
- Computers en/of tablets voor het gebruik door kinderen (spelletjes, educatie, games)

Hoewel de respons op de vragenlijst klein is, zie je wel een interessant verschil tussen het belang hechten aan cybersecurity (houding) en de daadwerkelijke maatregelen treffen (gedrag). Cybersecurity vindt men belangrijk, maar:

- Laptops, tablets e.d. worden door meerdere mensen gebruikt en meerdere mensen hebben hier de wachtwoorden ook van. Met name bij de kinderdagopvang is dat het geval. Bij gastouders zie je wel dat het vaak alleen de gastouder is die toegang heeft tot de apparaten. Maar bij beide groepen wijst men de andere gebruikers van de apparaten weinig op de risico's van verdachte linkjes.
- Multifactorauthenticifactie of het gebruik van vingerafdruk en/of gezichtsherkenning wordt nog niet veel gebruikt. Met name op mobiele devices (mobiele telefoons, tablets) zijn dit goede maatregelen. Deze worden veel gebruikt in de communicatie met ouders en het delen en maken van beeldmateriaal. De vraag is of deze goed beschermd zijn. Ook zijn wachtwoorden niet altijd uniek voor de verschillende apparaten en systemen. Antivirusprogramma's, automatische updates en unieke wachtwoorden worden wel gebruikt.

3.3.3 Communicatie en informatievergaring

Belangrijke informatiebronnen voor de kinderopvang zijn:

- Platform KinderopvangTotaal, Kinderopvang management vakblad (voor de hele branche een belangrijke bron van informatie).
- StaPP magazine, kennisbank, website, social media en nieuwsbrief van de KNGO (gastouders).
- Social media, met name Facebook (gastouders) en LinkedIn (kinderdagopvang)
- Magazine Kiddo.
- Brancheorganisatie voor Kinderopvang (BK) website, nieuwsbrief, social media, podcast.

Als het gaat om specifieke informatie ontvangen over cyberveiligheid dan geven kinderdagopvang aan dat ze deze informatie graag ontvangen van/via de brancheorganisaties, het Ministerie van Justitie en Veiligheid en vakbladen. Gastouders zien deze drie partijen ook als belangrijke informatieverstrekkers, maar voegen daar de GGD aan toe (op de derde plek na de brancheorganisatie en JenV) en de gemeente.

3.3.4 Welke boodschap zou aansluiten?

In deze behoorlijk gereguleerde branche is men soms wel een beetje klaar met de "bemoeienis" van de overheid. Belangrijk is daarom dat de boodschap zich vooral richt op het helpen van de branche om dit thema op te pakken. En niet om de administratieve last te verzwaren.

Het inspelen op de intrinsieke motivatie van de ondernemers is belangrijk. Passie en professionaliteit van de medewerkers: die willen niets liever dan dat kinderen veilig bij hen zijn, dát is hun core business. Incidenten met kindermisbruik hebben dat aspect van veiligheid wel door laten dringen. Cybersecurity vindt men wel belangrijk, maar men ziet nog niet heel goed wat de gevolgen kunnen zijn voor hun situatie. De vertaalslag van bewustwording (houding) naar het juiste en meest effectieve gedrag wordt nog niet gemaakt. Men heeft behoefte aan een concreet handelingsperspectief. Hierin is het belangrijk om te laten zien wat de positieve, dan wel negatieve, effecten zijn op de veiligheid van kinderen als dit wel of niet wordt opgevolgd. Daarbij kan een slachtofferverhaal helpen om de aandacht te trekken.

3.3.5 Andere haakjes

- Richt je niet alleen op de kinderopvang ondernemers, maar met name ook op de ouders. Zij kunnen ook invloed uitoefenen op de ondernemers in de branche. Informeer ouders waarop ze moeten letten als het gaat om cyberveiligheid bij de keuze voor gastouders of kinderdagopvang.

- Richt je ook op andere partijen die hier van invloed in kunnen zijn, denk aan gastouderbureaus en scholen (met name bij BSO's).
- Werk samen met de GGD. De GGD houdt toezicht op onder andere de veiligheid van kinderen op de opvanglocaties. Nu fysieke criminaliteit steeds meer verschuift naar gedigitaliseerde criminaliteit, zou veiligheid van kinderen bij de GGD ook meer moeten behelzen dan de fysieke veiligheid waar nu met name op gecontroleerd wordt. Digitale onveiligheid van beelden en/of informatie van kinderen heeft immers ook grote gevolgen voor zowel kinderen als ouders en de opvanglocaties zelf. Je zou kunnen verlangen dat een kinderopvanglocatie ook een veilige digitale omgeving moet bieden.
- De branche werkt met een Risicomonitor[21] voor inventarisatie van Arbo, gezondheid en veiligheid. We hebben nagevraagd het bij de Risicomonitor, maar cybersecurity en de digitale veiligheid van kinderen is (nog) geen onderdeel van de monitor. De Risicomonitor stimuleert ondernemers het gesprek aan te gaan met personeel over hoe het huidige beleid in de praktijk wordt toegepast. Bij uitstek zou het een goed middel kunnen zijn om cybersecurity als onderwerp in mee te nemen.

[21] https://www.risico-monitor.nl/veiligheid/rm/rmclient.nsf/index.html#/over-de-risicomonitor

4 Samenvatting aanbevelingen

In dit rapport worden per branche verschillende aanbevelingen gedaan. Samengevat zijn dat:

4.1 Algemeen

- Zet slachtofferverhalen in. Een slachtoffer dat vertelt wat hem/haar is overkomen, wat de specifieke gevolgen waren van cybercriminaliteit: het maakt de boodschap geloofwaardiger. Omdat het direct gekoppeld wordt aan de eigen herkenbare situatie. Niet alleen omdat iemand het vanuit de eigen ervaring vertelt in plaats van een overheid die er over vertelt. Het is ook iemand waarmee de ondernemer zich kan identificeren. Dus het slachtoffer moet ook een vergelijkbare onderneming hebben. Belangrijk is om niet alleen het verhaal te gebruiken om bang te maken, of bewustwording te creëren, maar met name om te laten zien welke maatregelen er daarna werden getroffen (handelingsperspectief).
- Verhalend communiceren. Maak het persoonlijk, wat verlies je, wat zijn de gevolgen voor anderen (klanten, collega's, ketenpartners)? En voor jezelf.
- Sluit aan bij de core business van de branche. Laat zien hoe cybercriminaliteit het primaire proces in gevaar brengt en hoe haalbaar het is om maatregelen daartegen in te passen bij de dagelijkse werkprocessen? Maak ook gebruik van de passie, intrinsieke motivatie en de belangrijke waarden die de ondernemers in de branche hebben, sluit aan bij wat men belangrijk vindt. En laat zien hoe die belangen en waarden beschermd kunnen worden (of verloren kunnen gaan).
- Werk samen met overheidsinstanties die bijvoorbeeld toezicht houden op primaire processen e.d. Dat kan per branche verschillen. Onderzoek waar er haakjes zijn om samen te werken vanuit het primaire proces (zie bijvoorbeeld de GGD bij kinderopvang).
- Werk samen met partijen die pakketten/applicaties aanbieden voor de branches. Zorgen dat zij ook voor bewustwording gerelateerde informatie toesturen en handelingsperspectief aanbieden.
- In alle branches wordt veel gewerkt met mobiele devices. Ook belangrijk om de branches te informeren over welke maatregelen hiervoor getroffen kunnen worden.

4.2 Restaurants

- Restauranthouders zijn erg bezig met elkaar. Inzetten op sociale bewijskracht bij deze doelgroep kan helpen bij het doorvoeren van cyberweerbaarheidmaatregelen.
- Geef concrete adviezen: kleine, korte informatie. Bij veel horecaondernemers is het hollen of stilstaan. In deze dynamiek moet informatie makkelijk "te verteren" zijn. En maatregelen makkelijk toe te passen zijn. Begin daarbij met 1 stap, niet alles tegelijk.

4.3 Makelaars

- Punten via brancheorganisaties:
  Makelaars die lid zijn van een brancheorganisatie moeten punten behalen om lid te mogen blijven. Denk hierbij aan punten die men behaalt door trainingen of opleidingen te volgen. Door dit puntensysteem garandeert de brancheorganisatie een bepaalde kwaliteit van aangesloten leden. Met de brancheorganisatie zou verkend kunnen worden of leden ook punten kunnen verdienen als ze bepaalde maatregelen treffen op het gebied van digitale veiligheid.
- Klanten inzetten:
  Informeer klanten dat ze nagaan of een makelaar een systeem gebruikt voor de opslag

van persoonsgegevens. Die systemen zijn vaak het beste beveiligd. Stuur niet zomaar kopieën van persoonlijke documentatie via de mail naar de makelaar.

4.4 Kinderopvang

- Werk samen met de GGD. De GGD houdt toezicht op onder andere de veiligheid van kinderen op de opvanglocaties. Veiligheid van kinderen zou verder kunnen gaan dan de fysieke veiligheid waar nu met name op gecontroleerd wordt. Fysieke onveiligheid op opvanglocaties heeft gevolgen, maar digitale onveiligheid van beelden en/of informatie van kinderen heeft ook grote gevolgen voor zowel kinderen als ouders en de opvanglocaties zelf. Er valt veel voor te zeggen om te verlangen dat een kinderopvanglocatie ook een veilige digitale omgeving moet kunnen bieden.
- Richt je op de ouders als belangrijke partij bij het creëren van bewustwording. Informeer ouders waarop ze moeten letten als het gaat om cyberveiligheid bij de keuze voor gastouders en kinderdagopvang.
- Scholen en gastouderbureaus kunnen ook belangrijke partijen zijn als het gaat om het stimuleren van cyberveiligheid. Scholen zijn verplicht op BSO aan te bieden en werken daarbij vaak samen kinderopvangorganisaties. Informeer hen daarom ook waar ze op moeten letten als het gaat om cyberveiligheid bij de keuze voor een samenwerkingspartner.
- De branche werkt met een Risicomonitor[22] voor inventarisatie van Arbo, gezondheid en veiligheid. We hebben nagevraagd bij de Risicomonitor, maar cybersecurity en de digitale veiligheid van kinderen is nog geen onderdeel van de monitor. De Risicomonitor stimuleert de ondernemer om het gesprek aan te gaan met het personeel over hoe het huidige beleid in de praktijk wordt toegepast. Bij uitstek zou het een goed middel kunnen zijn om cybersecurity als onderwerp in op te nemen.

4.5 Tot slot: de basisscan

Bij de voorbereiding van dit onderzoek was het doen van de basisscan van het Digital Trust Center de stap op weg naar een cyberweerbaar mkb. In de gesprekken die we gevoerd hebben, viel op dat alle brancheorganisaties de basisscan kenden en vaak ook hiernaar verwezen op hun websites en nieuwsbrieven. Onder de respondenten bleek echter slechts een enkeling de basisscan te kennen. Zelden werd deze gebruikt.
Dit bevestigd wat naar voren kwam in de gesprekken met de brancheorganisaties: ondernemers vinden cyberweerbaarheid wel belangrijk, maar zetten geen stappen om maatregelen te treffen tegen cybercriminaliteit. Gedragspsychologen noemen dit ook wel inertia: men vindt iets wel belangrijk maar blijft passief, omdat andere dingen belangrijker zijn, meer aandacht of energie vragen, omdat men moe is, er tegenop ziet of denkt dat men de situatie toch niet kan veranderen.

De 5 stappen in de basisscan, ook al kost de scan de ondernemer 10 minuten, zijn er behoorlijk veel, zeker als de uitslag (steeds) is: je hebt de basis niet op orde. En dan moet een ondernemer nog in actie komen om de echte aanbevelingen uit de scan ter harte te nemen. Dat kan ontmoedigen, een reden zijn om af te haken, of er niet eens aan te beginnen. Dit is het depletie-effect: de wilskrachtspier is uitgeput, mensen zien er tegenop, hebben er geen vertrouwen dat ze in staat zijn om alle stappen te zetten.
Belangrijk voor de stimuleringsstrategie is dan om aan te haken bij motieven waar de ondernemers gevoelig voor zijn (de klantbeleving, de betrouwbare naam, de kinderveiligheid), om zelfvertrouwen van de ondernemer te stimuleren (dat hij in staat is om de verandering in gang te zetten) en om kleine stappen te laten zetten.

[22] https://www.risico-monitor.nl/veiligheid/rm/rmclient.nsf/index.html#/over-de-risicomonitor

Hierbij is cruciaal dat je de ondernemer niet overvraagt. Forceer daarom niet in één keer alle benodigde stappen, maar laat hem de eerste stap zetten. En beloon hem daarvoor, niet materieel, maar in complimenten, aanmoediging, e.d. Geef het gevoel dat hij zijn onderneming op weg heeft gebracht naar een cyberveilige werkomgeving.

Benadruk bij de eerste stappen vooral wat de ondernemer al bereikt heeft (terugkijkend). Naarmate ze dichter bij de eindstreep zijn kun je benadrukken dat ze er bijna zijn en op alle aspecten goed scoren (vooruitkijkend). Bij loyalty programma's van bedrijven zie je daar slimme voorbeelden van met spaarpuntenprogramma's en stempelkaarten. In het begin ligt de nadruk op: "wat goed, je bent begonnen, je hebt al zoveel punten gespaard". Op het eind hoor je: "je stempelkaart is bijna vol voor een gratis kopje koffie". Vaak worden er zelfs al stempels voorbedrukt, om het gevoel te geven van "je bent goed bezig, je bent echt al op weg".

Een alternatieve invulling kan zijn: zorg dat de eerste stappen makkelijk gezet kunnen worden, dan hebben ondernemers daar al de voldoening van. Deze beïnvloedingstactiek is gebaseerd op het goal gradient-effect: naarmate we dichter bij de eindstreep zijn, zijn we meer betrokken en gaan we harder lopen.

Ook uit de gamingindustrie kunnen we ideeën halen, zeker op de website van de basisscan zelf. Denk dan bijvoorbeeld aan het gebruik van spelelementen:

- Punten - vooruitgang
- Levels – badges/trofeeën
- Opdrachten – uitdagingen
- Avatars – leaderboards (benchmark)

De BestDriver-app is een voorbeeld hiervan. Deze wordt ingezet om bestuurders zuiniger te laten rijden en maakt gebruik van punten, ranking e.d..[23]

Vanzelfsprekend vragen deze adviezen om nadere uitwerking. Ons advies is om daar met specialisten verder naar te kijken.

[23] https://www.cgi.com/nl/nl/nieuws/cgi-lanceert-bestdriver-app-voor-chauffeurs

5 Bijlage 1: Verhaal van een makelaar

29 maart 2023

Zo'n tien jaar geleden gebeurde het.
Ik had een zakelijke computer die ook door anderen werd gebruikt. Het was een mailtje over een verkeersboete. Vanuit de gedachte "he, niet weer" klikte iemand die ook toegang had tot mijn werkcomputer op de link en meteen werden alle bestanden versleuteld (encrypted). We konden bij geen enkel bestand meer. Nu draaiden we wel een back-up, maar de foto's die we als bedrijf gebruikten (o.a. foto's van identiteitsbewijzen) draaiden niet mee met de back-up omdat deze bestanden toen nog te zwaar waren.

We hebben een week lang met behulp van een ICT-bedrijf geprobeerd om de encryptie te kraken, maar dat is niet gelukt. Het kostte ons zeker €1500,- zonder resultaat. Uiteindelijk hebben we het gevraagde losgeld aan de cybercrimineel betaald om zo onze bestanden terug te krijgen. Ik heb serieus getwijfeld of het losgeld wel zou bijdragen aan een oplossing. Zou de crimineel dan niet nog meer extra vragen? Maar uiteindelijk heb ik het wel gedaan. Het vermoeden was dat als de als crimineel niet de bestanden terug zou geven hij ook zijn verdienmodel zou ondermijnen; als bekend wordt dat je na het betalen van losgeld niks krijgt, zou immers niemand meer betalen. We hebben dus betaald. Achteraf was het misschien niet veel. Drie bitcoins ter waarde van ongeveer 750 euro. Maar dat was tien jaar geleden. Nu zou je het veelvoudige moeten betalen. Bij het overmaken van het geld kregen we trouwens wel meteen een seintje van de bank, dat dit wel een verdachte transactie was. Dat wisten we natuurlijk, maar ik wilde die bestanden terug. Het ergste wat ik namelijk kon bedenken, was dat ik mijn klanten zou moeten vertellen dat ik hun gegevens kwijt was en dat ik niet wist wat ermee zou gebeuren. Dat was misschien nog wel erger dan die paar duizend euro die ik kwijt was. Ook al had ik €5.000,- moeten betalen, of meer, dan nog had ik het gedaan.

Na de betaling kregen we de bestanden meteen terug. Alles was onbeschadigd, met uitzondering van de twee bestanden waar we met het ICT-bedrijf aan hadden zitten sleutelen.

Ik heb veel van het voorval geleerd (en dat zijn meteen ook de tips die ik zou meegeven):
Draai altijd back-ups!
Zorg dat de back-ups niet in een cloud, zoals OneDrive of Google Drive, worden opgeslagen, maar op een externe locatie. Ook die clouds raken versleuteld als ze gekoppeld zijn aan je systeem.
Zorg dat je werkcomputer of laptop alleen door jou gebruikt wordt, niet door collega's of het thuisfront.
Kijk altijd goed naar de afzender van een e-mailbericht. Twijfel je? Niet op klikken en verwijderen. Is het toch een legitieme mail, dan nemen ze nog wel een keer contact met je op.
Betaal in plaats van zelf sleutelen. Voorkomen is beter dan genezen, maar je kunt beter betalen dan sleutelen en documenten beschadigen of het risico lopen dat gegevens op straat belanden.

Belangrijkste vooral... denk niet dat het jou niet overkomt. Het kan echt iedereen overkomen. Niemand is onfeilbaar, criminelen zijn slim genoeg om te weten wat werkt.
Het was wel een andere tijd qua gegevensuitwisseling en wetgeving op AVG toen het me overkwam. Maar het is iets wat nu nog steeds kan gebeuren.

CCV centrum voor criminaliteitspreventie en veiligheid

Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is een onafhankelijke stichting die partijen en veiligheidsprofessionals helpt om Nederland veiliger en leefbaarder te maken.

Centrum voor Criminaliteitspreventie en Veiligheid
Churchilllaan 11, 3527 GV Utrecht
Postbus 14069, 3508 SC Utrecht

T (030) 751 6700
E info@hetccv.nl
I www.hetccv.nl