BETTER FOOD SAFE THAN SORRY

NIS2 en cybersecurity in de foodsector

Gast: Bartel Debbaut (Kleemans) · Host: Alexander Platteeuw (A+ Quality) · Transcript

Introductie

Alexander Platteeuw, A+ Quality:

Stel, het is een doodgewone dinsdagochtend. De lijn draait, de machine staat op temperatuur, de orders lopen binnen. En dan plots: niets meer.

Geen recepturen, geen etikettendruk, geen traceerbaarheid. De productie ligt stil, niet omdat de machine kapot is, maar omdat iemand aan de andere kant van de wereld jouw systeem heeft gegijzeld. Dat is nochtans geen sciencefiction.

Het is wat een grote Amerikaanse vleesverwerker in 2021 dagenlang platlegde en 11 miljoen dollar kostte. En het is precies daar waar de Europese wetgever met NIS2 een streep onder trekt. Hier komt de oncomfortabele vraag.

Jij hebt je HACCP-plan, je hebt je allergenenbeheer, je hebt je food defense op punt, maar wie bewaakt de software die eigenlijk gans je fabriek aanstuurt? Vandaag zit iemand tegenover mij die in twee werelden tegelijk leeft, voedselveiligheid en cybersecurity. En hij zegt: de foodsector slaapt nog.

Welkom bij Better Food Safe Than Sorry. Ik ben Alexander Platteeuw van A+ Quality. Het profiel van mijn gast vandaag is behoorlijk atypisch.

Enerzijds kwaliteit, anderzijds informatiebeveiliging. Denk aan ISO 27001, security awareness, NIS2-compliance. Na 10 jaar als paramedicus in de geriatrie en een managementopleiding in de social profit bekleedde hij een directiefunctie met verantwoordelijkheid over strategie, HR en facilitair management.

Bij Kleemans België bouwde hij zich vervolgens om tot brede certificeringsadviseur over verschillende sectoren. Een man met een brede kijk dus. En dus zeer goed geplaatst om de wondere wereld van cybersecurity te komen toelichten in deze podcast.

Welkom Bartel Debbaut.

Bartel Debbaut, Kleemans:

Dankuwel, dank u. Dank dat ik hier mag zijn en mijn verhaal mag doen over NIS2.

Twee werelden die samenkomen

Alexander Platteeuw, A+ Quality:

Ja, goed. Let's go. Bartel, jij werkt zowel met voedselveiligheidsstandaarden, de BRC's en de IFS'en van deze wereld, als met informatiebeveiliging.

Nu, voor de meeste mensen in onze sector, kwaliteitsmanagers dan voornamelijk, zijn dat twee aparte werelden. Waarom zijn ze dat volgens jou niet? En wanneer ben je dat zelf gaan beseffen?

Bartel Debbaut, Kleemans:

Wel, eigenlijk vrij snel al, zonder dat ik het besefte. Als je het goed bekijkt, zitten we altijd met scopes en focusgebieden. We zitten met voedselveiligheid, we zitten met informatiebeveiliging, wat inderdaad twee werelden lijken die ver uit elkaar liggen.

Maar in alle eerlijkheid, als je het bekijkt op strategisch niveau, is het eigenlijk hetzelfde. Want bij voedselveiligheid gaat het over de beschikbaarheid en de integriteit van de voeding. En bij informatiebeveiliging gaat het over de beschikbaarheid en de integriteit van de informatie.

Dus eigenlijk is dat krek hetzelfde. En als je er verder over nadenkt, zit je met een bepaald model waar we tegenwoordig heel vaak naar verwijzen, het GRC-model. Dat is governance: we vertrekken vanuit een beleid, vanuit een beleidsverklaring, vanuit een doelstelling.

Wat doen we daarna? We gaan een risicoanalyse uitvoeren en tot slot gaan we beheersmaatregelen opstellen. Bij voedselveiligheid doen we dat eigenlijk ook.

We hebben een basisvoorwaardenprogramma, we hebben een HACCP-analyse en we vertrekken vanuit dat principe. We zien natuurlijk wel dat BRCGS en IFS heel specifiek en heel standaardgericht zijn, of heel erg productgericht. Maar als je bijvoorbeeld kijkt naar ISO 22000, of daarvan afgeleid naar FSSC 22000, en voor ons ligt dat gelijk, feed en food, dan zien we dat die high-level structuur ook dezelfde is. Dat is allemaal de structuur van ISO 9001 en ISO 27001. Dus zo verschillend zijn die nu ook weer niet.

Wat is NIS2?

Alexander Platteeuw, A+ Quality:

Zelfde principe dus. Nu, concreter: NIS2, ik haalde het daarnet al even aan. Even in mensentaal uitleggen, wat is dat juist?

En waarom net nu, voor de mensen die er nog nooit van gehoord hebben?

Bartel Debbaut, Kleemans:

Ja, NIS2 is opgesteld vanuit Europees standpunt om de cyberweerbaarheid, de cyber resilience zoals ze dat noemen, te gaan verhogen. Wat wil dat nu eigenlijk zeggen? NIS2 is een richtlijn, zoals het er staat.

Daar komen we straks nog op terug, maar dat is geen wetgeving. Dat wordt later vertaald en bekrachtigd in nationale wetgeving. Wat er staat, is dat bepaalde organisaties met een bepaalde criticiteit of belangrijkheid aan bepaalde voorwaarden moeten voldoen op het gebied van cybersecurity en IT.

Denk daarbij bijvoorbeeld aan energie, transport en zorg, maar eigenlijk ook food. Voedingsbedrijven, zeker in de toelevering, zijn wel een belangrijke. Nu, een heel belangrijk feit hierbij is dat de aansprakelijkheid ten hoofde van de directie hier ook aanwezig is.

Je kunt dus als bestuurder van de zaak persoonlijk aansprakelijk gesteld worden voor bepaalde zaken. Dat heeft wel impact, want vroeger zei je: het is het bedrijf of de entiteit die opdraait, maar nu zijn het persoonlijke dingen. Er wordt dus een bepaalde betrokkenheid en een bepaald engagement verlangd van de directie, maar ook van iedereen die er werkt en dus bepaalde maatregelen moet volgen.

Wat wordt daar eigenlijk gezegd? Er zijn een zestal thema's waarop gekeken wordt. Ten eerste de risico's.

Ken je je risico's? Weet je waar je risico's zitten? Weet je waar je kroonjuwelen zitten?

En neem daarbij de passende maatregelen. Heel erg belangrijk voor NIS2 is het melden van incidenten. Daar zijn ze nogal streng op.

Als dat systeem niet in orde is, dan gaat men daarover vallen, net zoals over de betrokkenheid van de directie.

Alexander Platteeuw, A+ Quality:

Om even terug te komen op dat melden van incidenten. Daarmee bedoel je: we zijn gehackt geweest, we moeten dat aan onze klanten en aan onze stakeholders melden. Is dat wat je daaronder verstaat?

Bartel Debbaut, Kleemans:

Sowieso denk ik dat je dat in een business continuity planning of in een disaster recovery planning intern moet gebruiken. Dus: wat ga je doen als er een ramp gebeurt en hoe houden we onze continuïteit aan? Maar het is niet alleen dat je bij wijze van spreken je kot afbrandt. Wat ga je doen als je kot afgebrand is?

Je moet heropstarten, daar komt het op neer. Wat ga je doen? Dan zijn er natuurlijk ook zaken, en dat staat heel specifiek in de wetgeving, dat je incidenten of bijna-incidenten moet melden.

Ook aan het Centre for Cybersecurity Belgium, het CCB. Dat valt misschien een beetje buiten de scope van deze podcast, maar we hebben ook nog de AVG-wetgeving, de privacywetgeving. Dat is eigenlijk hetzelfde verhaal.

Er zijn spelregels en wetgeving om dergelijke incidenten te melden en tijdig op te volgen. Dat is ook wel belangrijk. Als je ziet dat bepaalde bedrijven en organisaties hardleers zijn, dan treedt de overheid daar nogal hardhandig tegen op.

Alexander Platteeuw, A+ Quality:

Oké. En als je aantoont dat je goed bezig bent, zijn ze dan meegaander tegenover datzelfde bedrijf?

Bartel Debbaut, Kleemans:

Ja. Het is natuurlijk ook een bepaalde situatie: het is meestal niet bedoeld, het is iets wat gebeurt waar je niet aan kunt doen. Maar als je dan ziet dat je de juiste, directe maatregelen hebt genomen en preventief aan het werken bent, dan zijn ze wel meegaander. En als het al een tweede of een derde keer is, we hebben al inspecties gedaan en het is nog altijd niet opgelost, dan volgt er toch wel een zware boete.

Alexander Platteeuw, A+ Quality:

Ja, ja. En de boetes zijn ook vastgelegd in NIS2?

Bartel Debbaut, Kleemans:

De boetes zijn inderdaad vastgelegd voor beide, voor de AVG zowel als voor NIS2. Ik ken ze nu niet van buiten, het is een beetje afhankelijk van de grootte, maar het gaat toch over een serieus bedrag.

Voor de AVG is het, geloof ik, 4% van je wereldwijde jaaromzet of 20 miljoen euro. En voor NIS2 dacht ik 10 miljoen euro.

Maar sla me niet dood op die cijfers, dat moeten we even gaan bekijken. Ze zijn toch niet mals ten opzichte van de investering die je in principe moet doen om in compliance te zijn.

Is NIS2 ook voor de foodsector?

Alexander Platteeuw, A+ Quality:

Ja. Ik kom alle dagen in voedingsbedrijven en ik hoor wel eens: ah ja, maar NIS2, dat is voor de grote jongens, dat is voor de banken, de verzekeraars, de Nestlé's van deze wereld, dat is niet voor ons.

Ik hoorde je daarnet al zeggen: de food en de kritieke sectoren. Verklaar dat eens nader.

Bartel Debbaut, Kleemans:

Ja, wel, in feite denken zoveel mensen: is het op mij van toepassing of niet? Er zijn een aantal factoren die bepalen of je NIS2-plichtig bent. En daar komen we straks ook op terug.

Maar die NIS2-plichtigheid hangt af van de sector waarin je zit, de essentiële of de belangrijke sector. En bij voeding zou je kunnen zeggen: ja, er zijn hier tien bedrijven in de straat die hetzelfde doen, ik ben niet zo bepalend.

Vergeet niet dat wij ook toeleveren aan retail. Die grote retailer kan wel NIS2-plichtig zijn en legt in zijn lastenboek lasten op aan ons, waardoor wij ook NIS2-plichtig worden. Dus in feite is de klassieke denkfout hierbij, Alexander, dat iedereen denkt dat het niet voor hem is, terwijl in principe iedereen onder NIS2 valt.

Alexander Platteeuw, A+ Quality:

Ja, dat probeer ik inderdaad ook aan mijn klanten duidelijk te maken. En zie je dat concreet al opduiken in de contracten van de retailers, dat ze die NIS2-plicht aan hun leveranciers opleggen?

Bartel Debbaut, Kleemans:

Ik heb dat toch al gezien bij bepaalde klanten, en ik spreek nu voornamelijk over de logistieke dienstverleners in de food. In mijn klantenportefeuille heb ik al gezien dat er vanuit de voeding en vanuit de logistieke sector gevraagd wordt om voor NIS2 in orde te komen. We zetten dan meestal in op een ISO 27001, omdat er al een bestaande ISO 22000 of FSSC 22000 aanwezig is, om daarmee compliant te zijn.

Maar we zien inderdaad ook in de lastenboeken van grotere organisaties, grote retailers, dat er toch eisen gesteld worden over toegangsrechten en paswoordgebruik. Misschien zonder de term NIS2 zelf te gebruiken, maar inhoudelijk komt het daarop neer.

Er zijn natuurlijk heel wat initiatieven die daarbij ontstaan. Als je een gewone Google-search doet, vind je een matrix NIS2 versus de norm die jij hanteert. Die vind je makkelijk, dat is geen rocket science, en met AI kun je die ook opstellen, en dan is die toch zeker voor 85% juist.

Maar ja, ik merk het toch wel. En deels ook omdat een stuk daarvan al voortkomt uit de verplichtingen die er al zijn in de BRCGS: food defense, food fraud, food safety.

En als je dan ziet dat de cijfers zeggen dat ongeveer 80% te wijten is aan het bewustzijn van mensen, dan komen we natuurlijk in een moeilijke situatie terecht.

Alexander Platteeuw, A+ Quality:

Ik hoorde onlangs een podcast over het internetverkeer, dat we nu in een situatie zitten waarin er meer bots dan mensen op het internet zitten. 57% van het internetverkeer wordt gegenereerd door bots.

Dus als daar wat bots met verkeerde bedoelingen tussen zitten, amai.

Bartel Debbaut, Kleemans:

En zeker en vast ook met de opkomst van de artificiële intelligentie. Ja, dat is gevaarlijk. Als we nu beginnen met agents, en die agents beginnen op te zetten, die dragen zelfstandig operaties mee.

Een paar maanden geleden was daar een sprekende situatie van.

Alexander Platteeuw, A+ Quality:

Ja.

Bartel Debbaut, Kleemans:

Er was een soort sociaal netwerk opgericht, als grap, waarin gewoon agents tegen agents zaten te praten. En dan kom je inderdaad wel tot bepaalde dystopische, futuristische ideeën.

Alexander Platteeuw, A+ Quality:

Ja, maar het is wel de realiteit.

Bartel Debbaut, Kleemans:

Er zitten grote bewegingen in de digitalisering. En inderdaad, de gevolgen voor de voedingsindustrie zijn dan ook niet min, als je bedrijf op de een of andere manier door een hack wordt platgelegd.

Een cyberaanval als voedselveiligheidsprobleem

Alexander Platteeuw, A+ Quality:

Ja, maak dat eens concreet. Een voedingsbedrijf wordt platgelegd. Niemand kan nog aan zijn computer.

Een IT-probleem, uiteraard. En waarom is dat ook een voedselveiligheidsprobleem?

Bartel Debbaut, Kleemans:

Ik denk, Alexander, dat er natuurlijk meerdere zaken zijn. We denken nog altijd in termen van de computer van de directeur die daar staat. Maar als je goed kijkt, zit je in een voedingsbedrijf niet alleen met computers en hardware.

Je zit daar ook met OT, operational technology. Dat is ook zo'n term. Dus je hebt naast de information technology ook operational technology.

Ik denk aan transportbanden die op zichzelf draaien. Ik denk aan optische sorteerders. Ik denk aan PLC-sturingen, etikettenprinters, ERP-systemen, temperatuurcontroles.

En zo kunnen we nog een half uur doorgaan. Er zijn dus heel wat zaken die daaraan hangen. Stel dat dat op een bepaald moment gehackt wordt, op de een of andere manier.

Stel dat iemand je PLC-sturing omkeert. In plaats van input is er alleen nog output. Dus alles wat er normaal uit moet komen, draait terug.

Ik heb onlangs ook een andere podcast gehoord. Vanuit mijn interesse volg ik natuurlijk ook IT-podcasts. En daar ging het over een kartonnagebedrijf.

Die maken kartonnen dozen. Je zou denken dat karton weinig om het lijf heeft. Maar alles wat vandaag digitaal gekocht wordt in online shopping, zit in een doosje.

En die waren ook platgelegd door een hack. Nooit ransomware betaald. En die verloren, niet verschieten Alexander, 1 miljoen euro per uur.

Zolang ze niet konden draaien. Ze hebben 6 uur stilgelegen. Dat betekent 6 miljoen euro verlies op simpele kartonnen dozen.

Dus met andere woorden, er zijn toch wel een aantal zaken. Zoals gezegd, voedselveiligheid: we zijn niet alleen afhankelijk van onze computer die zegt dat we gaan opstarten en waaruit we een registratieformulier afdrukken.

Wat is onze werkorder van vandaag, of wat moet de ingangscontrole doen? Al die systemen hangen natuurlijk aan elkaar. En als die systemen met elkaar verweven zijn en vastzitten, dan zit je met het feit dat als dat platvalt, heel je bedrijf stilvalt.

Dan kun je nog zeggen: ja, we zitten even met een tijdelijke stilstand in het bedrijf. Maar wat met klantschade, met imago? Het is nu eenmaal gebeurd, je moet het melden.

Je zal er misschien ook mee in het nieuws komen. Dat zal zeker niet de voorkeur zijn, denk ik. Ik heb dat ooit eens meegemaakt, lang geleden, toen ik bij een groot logistiek bedrijf zat dat de logistieke dienstverlening deed.

Dus eigenlijk de opslag en het transport voor elektronica. En op dat moment was het Black Friday en het systeem was gehackt. Dat was best interessant.

Paniek in de tent. Maar het was natuurlijk wel best interessant. Op dat moment liep ik daar rond voor een interne audit en ik dacht: hoe robuust zijn jullie systemen?

Laat het mij nu eens zien. Maar het was toch alle hens aan dek, want het kwam erop neer dat men fysiek de kabel doorsneed tussen de systemen van de retailer en de systemen van de logistieke dienstverlener. Om te kunnen zeggen: we moeten zien dat onze systemen niet geïmpacteerd raken.

Alexander Platteeuw, A+ Quality:

En ik moet je niet zeggen: Black Friday, dat zijn de drukste weken voor die grote spelers, de topdag van het jaar.

Bartel Debbaut, Kleemans:

Ja, en in voorbereiding ook, want alles moet er natuurlijk binnenstaan in die bedrijven. Dat bedrijf stond vol, en er kon niets naar buiten omdat de systemen gehackt waren.

Ik heb nooit geweten of er effectief betaald is of niet.

Alexander Platteeuw, A+ Quality:

Dat raakt meestal ook niet naar buiten.

Bartel Debbaut, Kleemans:

Maar als we dan even terugkeren naar de vraag "maak het eens tastbaar, waar kunnen we dan op werken?": ik denk in de eerste plaats aan toegangsbeheer. En we denken dan altijd: wie heeft de code om in het bedrijf binnen te komen?

Heel typisch voor de BRCGS-audit: als je rond het bedrijf gaat, zijn alle deurtjes al op slot gedaan. Maar toegangsbeheer kan natuurlijk ook via logins. En wat ik heel vaak zie in voedingsbedrijven, is dat alles met camera's bewaakt wordt.

Dus in feite, als je toegang hebt tot een digitaal systeem en ook tot de camera's, heb je volledig zicht en controle over de productie. Ik denk bijvoorbeeld ook aan back-ups, in het kader van onze traceerbaarheid en onze traceerbaarheidsoefening, en dat is fundamenteel in veel normen.

Als we geen back-up meer hebben, kun je opeens je traceeroefening niet meer doen. Of toch niet met zekerheid. Ik ga niet zeggen dat het op het moment dat je aan het produceren was niet voldoende veilig was, maar je kunt het niet meer aantonen.

Etikettering is ook nog zo'n mooi voorbeeld. Dat zit tegenwoordig ook allemaal op IoT, zodat je dat vanuit het kantoortje kunt aansturen. Maar dan is er geen controle meer over wat erop staat.

Het recepturenbeheer is ook zo'n geestige. Vroeger zat dat bij wijze van spreken allemaal in een kast achter slot en grendel, want dat was de schatkist van het bedrijf.

Maar nu zit dat in digitale kluizen. Dus stel dat iemand daar toegang toe heeft: je bent je unieke receptuur kwijt. Je kunt het niet meer maken.

De voorbeelden zijn legio, maar het ligt allemaal dichterbij dan je denkt. Ik denk dat we cybersecurity niet los kunnen zien van voedselveiligheid, maar dat we het moeten zien als een integraal onderdeel daarvan.

Cyber als nieuwe food-defense-vector

Alexander Platteeuw, A+ Quality:

Ja, je hebt de term food defense al aangehaald. Alle GFSI-standaarden hebben food defense uiteraard in hun standaard opgenomen. Is een cyberaanval niet gewoon een nieuwe vector in het food defense verhaal?

Bartel Debbaut, Kleemans:

Ja, absoluut. Dat is een nieuw onderdeel daarvan. Ik denk dat we dat niet kunnen onderscheiden.

Ik merk nog heel vaak op dat je in de food defense en de food fraud risicoanalyse wel de menselijke factor meeneemt, maar dan nog heel vaak in de zin van: er komt iemand vreemd binnen. Eerlijk gezegd zijn er maar weinig bedrijven waar ik als vreemde zomaar zou binnenraken.

Als ik bij wijze van spreken binnenloop en ze kennen mij daar niet, dan komt er toch wel rap iemand naar mij toe: wie ben jij, wat kom je hier doen? Of dat overal zo is, durf ik in deze podcast niet te

zeggen. Maar terug naar het verhaal: het is niet alleen fysieke toegang. Het is een account dat gehackt wordt, waar je niets van weet, en dan heeft die persoon toegang tot heel het systeem. Ik zei het al: een besmette laptop, of leveranciers die op onze systemen werken, of leveranciers in wiens systemen wij kunnen kijken en fouten maken. Denk ook aan servers die nog lokaal staan, ergens in een hoekje van een productieruimte, waar je makkelijk poorten kunt gaan switchen.

Dus ja, ik denk: als je effectief slechte bedoelingen hebt en je wilt bewust schade toebrengen, dan is het makkelijker om dat digitaal te doen dan fysiek. Het is meer onzichtbaar. Ja, daar zit het hem in.

En natuurlijk: wat gebeurt er allemaal? Je ziet het ook niet. Naast de onzichtbaarheid van het feit dat het geen persoon is, weet je ook niet goed wat er gebeurt. De cijfers tonen dat aan. In de wetgeving wordt gevraagd om binnen X tijd te melden, en voor NIS2 is dat binnen de eerste 24 uur na vaststelling, en dan heel specifiek: na vaststelling.

Alexander Platteeuw, A+ Quality:

Oké.

Bartel Debbaut, Kleemans:

Want als dat bij wijze van spreken op een vrijdagavond gebeurt en je stelt het pas maandagochtend vast, dan heb je vanaf maandagochtend nog 24 uur. Maar in alle eerlijkheid, daar is onderzoek naar gedaan, en het komt er gewoon op neer, Alexander, dat er tussen de eerste keer dat er iemand ongewenst binnenkomt en het effectief uitvoeren van de daad, het plaatsen van de malware of welke schade dan ook, heel vaak al een half jaar zit.

Ik heb ooit eens een audit informatiebeveiliging gedaan in een oncologisch ziekenhuis. Ze hadden een hack gehad en ze zeiden: ja, maar dat valt nog mee, we hebben onze back-ups. En die hackers zeiden gewoon: we zijn al in februari geïnfiltreerd, dus uw data is op dit moment al 8 maanden corrupt. Dat betekent dat er gedurende die 8 maanden, en het gaat dan over oncologie, foto's genomen zijn van tumoren waarop bestraling berekend wordt. Die berekeningen klopten dus niet meer, en daar wordt met heel drastische behandelingen gewerkt. Doordat het onzichtbaar is, is de ethiek heel vaak ver te zoeken, en dat maakt ons juist zo kwetsbaar. Dus ik zeg het: ik zou dat niet als een apart deel naast iets anders zetten, maar zoveel mogelijk proberen te integreren in de managementsystemen die er al zijn.

Alexander Platteeuw, A+ Quality:

Dus die IT-manager nog eens bij de kraag vatten als het over food defense gaat?

Bartel Debbaut, Kleemans:

Ja, wel, zeker in het kader van de aansprakelijkheid, want uiteindelijk draag je die zelf als ondernemer of als zaakvoerder. En daar zit ook weer een risico: veel voedingsbedrijven zijn afhankelijk van IT-leveranciers. Het zijn niet allemaal grote bedrijven met een aparte ICT-dienst. Heel vaak gaat het om kleinere bedrijven met 10 mensen, waar een aantal laptops staan en waar IT volledig afhankelijk is van een externe partij. Dus met andere woorden: kijk toch even wat daar gebeurt. Niet dat die externe een slechte partij is, maar wel dat het goed geregeld moet zijn.

Registreren en controle in België

Alexander Platteeuw, A+ Quality:

Ja, dat hij zichzelf ook goed beschermt, ja. Even praktisch voor onze Belgische luisteraars: moet je je als bedrijf ergens registreren, en wat zijn de gevolgen als je dat niet doet? En ja, natuurlijk, wetgeving is maar zo streng als diegene die komt controleren.

Wie komt dat überhaupt controleren in België? We beginnen met België.

Bartel Debbaut, Kleemans:

Wel, in België is het zo, ik zei het al, het Centre for Cybersecurity Belgium, het CCB, is verantwoordelijk voor NIS2. Er is een website, Safeonweb@work, en daar moet je je registreren. Het eerste en het belangrijkste wat je moet doen: wacht niet tot je een brief met een uitnodiging krijgt, want we lopen eigenlijk al achter op de feiten, Alexander. Die wetgeving is al enige tijd van kracht in België.

Ik spreek er inderdaad al over sinds 2025, toen dat begonnen is. Normaal moest alles geregeld zijn tegen 1 april 2026, maar veel bedrijven schoten een week voor de deadline in een kramp en belden mij: moeten we dat nog gaan regelen? Wat moeten we doen op een week tijd?

Dus het eerste wat je kunt doen, is blijven zitten en zeggen: we wachten op een brief over NIS2 en we zien wel wat er komt. Dat is precies wat je niet moet doen. Wat je wel moet doen, is je registreren.

Uiteindelijk moet ik eerlijk zeggen dat dat heel goed geregeld is vanuit de overheid. Er is een Excel-file waarmee je kunt nagaan of je effectief onder NIS2 valt, en onder welke sector: belangrijk, essentieel of geen van beide.

En als je erbij zit, dan moet je effectief ook bepaalde zaken gaan opstellen. Ik vertelde het net al: vergeet niet dat er boetes zijn als het er nog niet is, omdat de wetgeving al meer dan een jaar van kracht is. Er moeten dus al heel wat zaken geregeld zijn. Dus nogmaals: wacht niet op een brief.

Maar je moet er natuurlijk ook niet in een kramp van schieten alsof alles tegelijk moet gebeuren. De boetes zijn alleen niet mals. Wat kun je doen? Naast het feit dat er bij het CCB bepaalde tools staan om dat te beheersen, kun je al bepaalde zaken doen om daarmee in orde te zijn.

Een van de meest voor de hand liggende, en dan spreken we meteen over de meest drastische oplossing, is je laten certificeren voor ISO 27001. Ook daar zijn er een aantal zaken rond de full scope, maar daar komen we straks op terug, dat is misschien een beetje high level. Maar het Centre for Cybersecurity Belgium heeft ook een framework ontwikkeld, het Cyber Fundamentals Framework.

En op basis van de sector waarin je zit, essentieel, belangrijk of gewoon, worden er een aantal niveaus bepaald die je zou moeten halen en die passen bij het niveau van de sector waarin je zit.

Alexander Platteeuw, A+ Quality:

En eenmaal je je registreert bij de overheid, dan krijg je dat te zien?

Bartel Debbaut, Kleemans:

Je ziet dat nu ook al: als je naar de website van Safeonweb gaat en naar de website van het Centre for Cybersecurity Belgium, dan vind je die Cyber Fundamentals. Dat is de vertaling die België in de wetgeving gemaakt heeft. De richtlijn, ik zei het net al, is een Europese richtlijn. Die Europese richtlijn moet vertaald worden in nationale wetgeving.

België heeft dat op die manier vertaald. Als we dan naar Nederland kijken, dan zitten die een stukje achter, want België wil op dat punt heel vaak ook best of class zijn.

Ze zijn daar in alle eerlijkheid ook wel in geslaagd. Er komen nog initiatieven aan, omdat ze op dat punt bij de beste van Europa willen zijn. Waarom?

Omdat de voorganger van NIS2, NIS1, ons het slechtste kindje van de klas maakte. Daar waren we toch wel laat mee.

Dus uiteindelijk loopt België daar een stukje voor en loopt Nederland een stukje achter. Nu, primeur voor deze podcast: op 6 en 7 juli is de NIS2-wetgeving ook in Nederland bekrachtigd in de Tweede Kamer.

En die wordt van kracht vanaf medio augustus dit jaar. Wat we daarom natuurlijk niet meteen gaan zeggen, is dat Nederland achterloopt op België.

Want waar komt het op neer? In de beheersing van het systeem dat we opzetten, zit een bepaalde maturiteit. En daar zien we toch wel dat Nederland vaker voorloopt op het vlak van maturiteit.

Waarom? Omdat ze toch meer gewend zijn aan certificering. Ik werk zowel in Nederland als in België.

En ik merk dat in België een certificering vaak volgt vanuit een klantvraag of vanuit een verplichting in de wetgeving. In Nederland wordt er vaker gestart met certificering omdat het toegevoegde waarde kan brengen.

Vier stappen voor kmo's

Alexander Platteeuw, A+ Quality:

Veel van mijn luisteraars zijn kmo's met een beperkt of, zoals je daarnet zelf zei, uitbesteed IT-team. Wat zijn drie of vier dingen met de grootste impact die ze eigenlijk volgende week al kunnen doen, zonder een fortuin uit te geven?

Bartel Debbaut, Kleemans:

Je zei het al daarnet: we gaan niet in een kramp schieten. Dat moeten we zeker en vast niet doen. Maar als je heel praktische zaken wilt bekijken, dan zijn er er wel een aantal.

Ik denk dat een back-up heel belangrijk is. Maar niet gewoon een dode back-up waarvan je zegt: we hebben er ooit een genomen en we kunnen 14 dagen terug. Wel effectief met een bepaald beheer en een systeem waarvan je zegt: een back-up die zeker offline staat en die niet rechtstreeks overschrijfbaar is.

Er zijn daar ook bepaalde regels voor, de 3-2-1-regel: het aantal back-ups, het aantal dragers en het aantal locaties waarop je bewaart. Dus met andere woorden: niet alleen dat je ze hebt, maar test ook eens de integriteit. Heel belangrijk.

Alexander Platteeuw, A+ Quality:

We gaan ervan uit dat de back-up er is als we hem nodig hebben, dat we eraan kunnen, en dan komt het moment dat hij er niet is of dat hij niet integer is.

Bartel Debbaut, Kleemans:

Dat is heel erg belangrijk. Een tweede tip die ik wil meegeven bij die back-ups: stel dat je in een ransomware-aanval of in een hack terechtkomt. Mensen zeggen dan: ik heb een back-up, en ze gaan die direct terugzetten.

Dat is een van de grootste kapitale fouten die je kunt maken, want je systeem is op dat moment, zoals ze dat in ICT-termen noemen, nog niet contained. Het is nog niet ingedamd.

Alexander Platteeuw, A+ Quality:

Dus de back-up wordt dan eigenlijk mee gehackt.

Bartel Debbaut, Kleemans:

Gecorrumpeerd, ja. Maar een back-up is wel heel belangrijk.

Een volgende, heel erg belangrijke, is multifactorauthenticatie. Ik weet dat het soms storend is dat je telkens als je je e-mail opent bij wijze van spreken je telefoon moet nemen en een cijfercode moet ingeven. Maar het wordt vandaag makkelijker en makkelijker om paswoorden te kraken, zelfs met veertien karakters en meer.

Ik was naar een opleiding geweest die ging over de inzet van quantum computing. In 2030 wordt dat verwacht, en dan worden de meest complexe wachtwoorden in no time gekraakt. Waardeloos, hè.

Dus met andere woorden: met multifactorauthenticatie moet je een code ingeven op een gekend toestel. Het weet wie je bent via Face ID, via je gezichtsherkenning.

Je telefoon weet dat jij het bent, het is een gekend toestel waarop je aanmeldt, het is een bepaalde code, het is een gekend IP-adres. Dat is toch wel een extra veiligheidsbarrière. Dan is er ook nog een heel belangrijke: patching en updates.

Dat vind ik ook superbelangrijk. Waarom? Het is niet altijd even evident, er zit ook een kanttekening bij.

Normaal gezien heb ik de gewoonte om op mijn laptop meteen te installeren zodra er een patch of update is. Want heel vaak vertrekt men van wat ze een zeroday-exploit noemen. Dat wil zeggen dat hackers, mensen die aanvallen om de kwetsbaarheid in software bloot te leggen, vaststellen dat er op een bepaald moment een kwetsbaarheid in die toepassing zit die nog niet gekend is. Dat is de reden waarom je heel veel updates krijgt op je Windows, of waarom patching en updates nodig zijn.

Nu is er daar ook wel een kanttekening bij. Heel vaak draaien je systemen daarop, een OT-systeem. Ik heb ook klanten, zoals een drukkerij, die zeggen: wij wachten minimaal 14 dagen, want het zou niet kunnen dat heel het ERP-systeem en de CRM niet meer draaien door een update en dat het systeem plat ligt. Dus met andere woorden, dat is wel een belangrijke. Derde punt, Alexander: train je mensen, op welke manier dan ook.

Dat hoeft niet het meest academische te zijn. Je hoeft je mensen niet naar de universiteit te sturen om informatieveiligheid te gaan studeren, maar er bestaan ook heel makkelijke tools: phishing, awareness, online webinars. Dat is toch wel belangrijk, want ik zei het ook al: ongeveer 80% van de hacks die gebeuren, vertrekt vanuit de kwetsbaarheden van mensen. Ik ken situaties waarbij ik naast een test zat bij een groot bedrijf met 7.500 mensen, waarbij op het moment van de test de boodschap naar de laptops van de mensen gestuurd werd: "je systeem is gehackt".

Er zijn dan mensen die gewoon in de lach schieten en voortwerken. Dat gebeurt. Dus awareness vind ik dan heel erg belangrijk.

Als ik iets vaststel dat niet normaal is, dan ga ik een extra vraag stellen. Soms leidt dat tot wat ongenoegen bij collega's, die dan zeggen: waarom stuur je dat nu, Bartel?

Maar toch, je kunt maar beter zeker zijn. En denk ook niet dat je, omdat je klein bent of maar een kmo, niet interessant bent. Het is juist omdat je die hoge beveiligingsstandaarden niet hebt, dat je makkelijker te hacken bent.

Het is niet de kwestie van "Word ik gehackt?", maar de kwestie is eerder "Wanneer word ik gehackt?".

Klassieke fouten

Alexander Platteeuw, A+ Quality:

Wat zijn de klassieke fouten die je bedrijven ziet maken? Want bedrijven zijn er wel al mee bezig. Bedrijven denken: ah ja, we zijn in orde, we hebben het er al even over gehad, de back-up, we denken dat onze back-up ons wel zal redden.

Zijn er nog van die klassieke fouten die je ziet?

Bartel Debbaut, Kleemans:

Het eerste heb ik eigenlijk al verteld: denken dat je niet interessant genoeg bent om te hacken. Ik denk dat ieder bedrijf op zich interessant is. Ik vergeleek dat vroeger altijd met de maffiafilms, de Godfather of de Sopranos-reeks.

De Sopranos, ja. Dat waren zware mannen. Die kwam je liever niet tegen, want als je die tegenkwam, wist je: dit gaat pijn doen.

Vandaag is dat bij wijze van spreken een jong gastje van 17 jaar dat op zijn zolderkamer zit te hacken in opdracht van iemand. Dus vergeet niet: je kent je tegenstander niet meer. Je bent sowieso interessant, bij elke mogelijkheid die ze kunnen pakken, bij elke poging die ze doen om toch maar te slagen.

Het gaat er niet over dat het voedingsbedrijf X of Y is. Het gaat erover dat ze iemand gehackt hebben, en dat is een businessmodel.

Dus denk niet dat jij degene bent voor wie dat niet interessant is. Het tweede punt dat ik zou kunnen aanhalen, is hardware kopen. Ik heb bedrijven waar mensen zeggen: ik ga toch even naar de grote elektronicaretailer, want daar zijn de laptops toch wel een stuk goedkoper dan wanneer ik ze koop bij mijn IT-leverancier.

Er is een reden waarom ze duurder zijn bij je IT-leverancier: omdat ze in het domein zitten, beveiligd zijn en gemonitord worden. De systemen bij de retailers zijn heel vaak modellen die op zich goed zijn, maar al verouderd, en waarvan je de updates niet doet. Dus met andere woorden, als dat uitvalt, zit je daar natuurlijk ook wat makkelijker binnen.

En dan is het derde het niet scheiden van netwerken. Wat bedoel ik daarmee? Ik kom heel vaak bij bedrijven en vraag: mag ik de wificode hebben? En dan krijg ik de wificode van het algemene netwerk.

En dan kom ik blijkbaar ook op de printers, en dan heb ik ook camerabewaking, en dan kom ik op bepaalde momenten ook op de netwerkschijven terecht, waar je dan ook privéfoto's van de zaakvoerder vindt. Niet gezegd dat dat allemaal zo erg is, maar vergeet natuurlijk niet: ik zit dan binnen op het kantoor bij mijn klant, maar het wifisignaal gaat door de muur, en als je aan de voordeur staat, kun je dat wifisignaal ook gaan kraken.

En als je dan alles op je netwerk hebt hangen, ook je OT, dus ook je PLC-sturing, je optische sorteerder, je ERP-systeem, je mailserver, je traceerbaarheidssysteem, je etikettenprinters, dan zit dat daar natuurlijk allemaal op. Ze moeten dan alleen nog maar binnen geraken.

Alexander Platteeuw, A+ Quality:

Dus jij pleit voor een duidelijke scheiding?

Bartel Debbaut, Kleemans:

Ja, en dat is makkelijker te doen dan je denkt. Je kunt beginnen met bij wijze van spreken een gastennetwerk in te richten. Dat zie ik heel vaak, dat mensen met een gastennetwerk werken. Dat staat dan open, en eigenlijk scheiden we dat van het bedrijfsnetwerk.

En dan zie je ook wel dat er voor de OT nog een apart deel voorzien wordt. En brand new, wat we deze week te weten zijn gekomen: er bestaat ook een systeem om je oplossingen in de cloud te segmenteren. Wat is de cloud?

De cloud is eigenlijk iets dat weggeschreven wordt naar een externe server of een externe opslagplaats. Ook daar kun je die verschillende operaties al scheiden. Dus dat is ook wel een belangrijke.

Certificeren voor NIS2

Alexander Platteeuw, A+ Quality:

Ja, juist. Nu, je hebt al even gesproken over ISO 27001. Kun je je eigenlijk laten certificeren voor NIS2? Concreet, kun je in België naar de buitenwereld zeggen: ik ben NIS2-compliant?

Bartel Debbaut, Kleemans:

Inderdaad, met ISO 27001 kun je dat doen. Natuurlijk gaat ISO 27001 heel specifiek over informatiebeveiliging en informatiedragende systemen, en NIS2 gaat over cyber resilience. Dus in principe verschilt het doel wel een stuk van de norm.

Maar het is wel zo dat als je de beheersmaatregelen uit ISO 27001 voorschrijft en opvolgt, je eigenlijk wel NIS2-compliant bent. Het Centre for Cybersecurity Belgium heeft ook een standaardframework voorgeschreven, het Cyber Fundamentals Framework, kortweg CyFun. Het hangt van de klasse en de categorie waarin je valt af hoe je bepaalde beheersmaatregelen gaat inrichten.

En dan kun je zeggen: ik laat een assessment doen, en dan kun je aantonen dat je NIS2-compliant bent volgens CyFun, op dat type en dat niveau.

Alexander Platteeuw, A+ Quality:

En dat assessment, kun je dat laten doen door de overheid?

Bartel Debbaut, Kleemans:

Nee, dat is niet de overheid, dat gaat ook via de certification bodies.

Er zijn er heel wat gekend voor ISO 27001. En voor CyFun zijn er 2 of 3 in België. Je hebt er kleinere, maar er zitten er ook wel grotere bij.

En dus met andere woorden, een beetje afhankelijk van wat je doet, en dat is misschien nog een belangrijk detail: als je in de essentiële sector valt, dan moet je je ook laten certificeren binnen X tijd. En dan heb je inderdaad de keuze om een ISO 27001 te doen of die CyFun.

Alexander Platteeuw, A+ Quality:

Dat zijn dan dus de Engie's van deze wereld?

Bartel Debbaut, Kleemans:

Ja, de grotere bedrijven. Ja, en die vallen dan eigenlijk ook onder andere wetgeving, Digital Operational Resilience.

Dus zeker als je essentieel bent, is het eigenlijk ook wel een bepaalde verplichting. Terwijl als je belangrijk bent of kleiner bent, dan is het eigenlijk een vrijwillige keuze om dat assessment te laten doen.

Alexander Platteeuw, A+ Quality:

En denk je dat dat zal evolueren naar verplichte certificering voor de niet-essentiële entiteiten?

Bartel Debbaut, Kleemans:

Goh, dat weet ik niet. Dat durf ik niet te zeggen. Want uiteindelijk gaan we daar ook weer een stuk wetswijziging voor moeten doen.

Ze vertrekken vanuit een NIS2-richtlijn die vertaald wordt in Belgische wetgeving. Dan zou er een amendement moeten komen op die Belgische wetgeving dat zegt: vanaf nu moet je je laten certificeren. Het kan natuurlijk wel zijn dat men op basis van een boeteclausule zegt: je hebt dit hier verschillende keren gedaan.

Dan gaan we ons ermee moeien. Dan moet je je wel laten certificeren. Maar dat er een harde richtlijn in zit, dat wil ik niet zeggen.

Eén boodschap

Alexander Platteeuw, A+ Quality:

Zeer interessant, maar wel een beetje freaky allemaal. Geen positieve boodschap die je hier kon brengen. Ik voel dat je er nog uren over kunt doorgaan.

Maar als je één boodschap zou mogen meegeven aan elke kwaliteitsmanager of bedrijfsleider in de food die nu aan het luisteren is: wat moeten ze morgenochtend doen?

Bartel Debbaut, Kleemans:

Morgenochtend is het zaterdag, Alexander, want we nemen dit op een vrijdag op.

Maar als ze maandag binnenkomen, is het gewoon even de vraag stellen wat onze kroonjuwelen zijn.

Alexander Platteeuw, A+ Quality:

Wat bedoel je met de kroonjuwelen?

Bartel Debbaut, Kleemans:

Hoe kwetsbaar zijn wij en hoe vatbaar zijn wij voor aanvallen op bepaalde systemen? Ik heb bijvoorbeeld een klant waar de optische sorteerder tegelijk ook de calibrator is, met andere woorden de grootte van de producten die gesorteerd worden.

Dat is een zeer duur toestel. Als dat bij wijze van spreken gehackt wordt, dan kan heel die lijn niet gebruikt worden. Dan moet je het manueel doen, maar dat duurt al snel 10 keer zo lang.

Dus met andere woorden: als we dat weten, neem het dan mee in de food fraud risicoanalyse en vraag je af: wat gaan we nu doen? Wat is de impact? Wat is de kans dat het gebeurt?

Wat is precies de vulnerability? Welke zaken kunnen onze voedselveiligheid, onze traceerbaarheid en onze etikettering effectief gaan schaden? En wat gaan we daaraan doen?

Ik zei het al, Alexander: schiet niet in een kramp. Begin niet met maandagmorgen dure consultants uit te nodigen, of eender wie op te bellen en de duurste oplossing te kiezen, want het zou kunnen zijn dat het helemaal goed geregeld is en dat je verkeerde investeringen doet. Maar denk er eerst even rustig over na: waar moeten we hier aan beginnen?

Wat zijn mijn kroonjuwelen? En hoe kan ik die het best beschermen? Ik denk dat dat een belangrijk vertrekpunt is.

Alexander Platteeuw, A+ Quality:

Zeer wijze woorden om hiermee af te sluiten. Hartelijk dank, Bartel. Prachtig.

Ik hoop dat onze luisteraar niet te veel de schrik van zijn of haar leven heeft opgelopen. Maar eens te meer: een verwittigd voedingsbedrijf is er twee waard. Weer eens duidelijk.

Hartelijk dank voor je inzichten. Dit was Better Food Safe Than Sorry. Ik ben Alexander Platteeuw van A+ Quality.

Vergeet niet te abonneren en deze aflevering te liken. Luister je via Spotify, geef dan sterren. Tot de volgende keer.