

'IT-incident' AH past in trend groeiende kwetsbaarheid bedrijven

Albert Heijn en zijn (internationale) zusterketens zijn het slachtoffer van een nog onbekend IT-incident. Wat er ook exact aan de hand is, het past in een inmiddels lange geschiedenis van verstoringen van processen in de supermarktsector door externe partijen. Het lijkt erop dat door de toegenomen digitalisering ook de risico's op dit soort incidenten steeds groter worden.

‘De foodbranche heeft tot nu toe ook altijd een goed antwoord gehad op cybercriminelen. Probeer bijvoorbeeld maar eens een groot bestand te mailen naar een supermarktketen. Gaat je niet lukken. Supermarkten halen pas iets binnen als alles compleet gecheckt en gescreend is. Het is bij de hoofdkantoren hyperafgezegeld.’ Een citaat uit een interview met Jules van Well uit 2022, toen hij nog binnen het Centraal Bureau Levensmiddelenhandel verantwoordelijk was voor het thema veiligheid.

Het klinkt bijna vier jaar later als een citaat uit het stenen tijdperk. Cybercriminelen hebben de afgelopen jaren in toenemende mate hun slag geslagen in de foodbranche. Supermarktketens zijn daarbij zeker niet buiten beeld gebleven. Het is zonder twijfel een gevolg van de toenemende mate van digitalisering binnen de sector. Formules willen steeds meer weten van hun klanten, leggen steeds meer informatie vast en gebruiken al die big data om de operatie en winstgevendheid te verbeteren.

Ook voor het digitale tijdperk was data waardevol

Het willen stelen van data is overigens niet iets nieuws. Zelfs toen archieven nog waren opgeslagen in papieren dossiers of op ponskaarten was de informatie interessant. Het verzet had het in de Tweede Wereldoorlog niet voor niets gemunt op de burgeradministratie. Door het vernietigen of stelen daarvan werd het werk van de bezetter aanzienlijk bemoeilijkt. Maar nu de meeste systemen van op (virtuele)servers zijn opgeslagen, aan elkaar zijn gekoppeld en op afstand benaderd kunnen worden, is het allemaal een stuk eenvoudiger geworden. Van overal op de wereld kunnen onverlaten gebruikmaken van gaten in de beveiliging en binnendringen in de systemen van bedrijven.

Zelfs dat was jaren voorbehouden aan intelligente ict'ers die wisten wat ze deden. Met de snelle opmars van kunstmatige intelligentie en zogenoemde ai-agenten die eindeloos kunnen zoeken naar gaten in de beveiliging is het voor een veel grotere groep mogelijk om data te stelen of systemen te ontregelen. De gegevens kunnen vervolgens worden verkocht of worden gebruikt voor het afpersen van bedrijven. Het is een bedrijftak waarin vele miljoenen omgaan.

Albert Heijn waarschuwde al in 2009 klanten voor hack

Al in 2009 moest Albert Heijn een brief sturen aan 500 klanten in Breukelen die gebruikmaakten van het toen omstreden betaalsysteem Tip2Pay. Een biometrie-expert liet bij RTL Nieuws zien hoe hij met behulp van gestolen vingerafdrukken klanten geld afhandig kon maken. Datzelfde jaar kwam naar buiten dat de onlinesupermarkt van Albert Heijn het slechtst beveiligd was van twintig onderzochte webshops. Een door AD ingeschakelde hacker kon ingevulde persoonsgegevens buitmaken.

Het zijn twee vroege voorbeelden van kwetsbare technologie bij de marktleider. Albert Heijn was echter natuurlijk niet de enige partij die hier last van heeft. Zo lekten in 2012 tienduizenden e-mailadressen van klanten van Dirk. Oorzaak was het gebruik van een verouderde module. "Het was ontwikkeld met een minimaal budget en minimale controle. Daar hebben we nu last van. De module die is gehackt was een haastklus", zo klonk het toen. Ook foodfabrikanten hadden hier

last van, zo kwamen in 2015 de gegevens van honderdduizenden consumenten die mee hadden gedaan aan acties van Bavaria op straat te liggen.

Het lijkt ook best lang geduurd te hebben voordat dit soort bedreigingen serieus werden genomen. In 2020 onderzocht het bureau SecuriGuide de onlinebeveiliging van 67 webwinkels. Websites voor het bestellen van boodschappen kwamen hier het slechtst uit. Twee jaar later was het Makro dat het slachtoffer werd van een cyberaanval, iets wat het gevolg was van een hack bij moederbedrijf Metro enkele maanden eerder. In 2023 was het de beurt aan een toeleverancier van de supermarkten. Tomra ontkoppelde zijn statiegeldautomaten uit voorzorg na een cyberaanval.

‘Veilig houden levensmiddelenbranche grootste uitdaging’

Het was in 2024 in Distrifood dat cyberexpert Dave Maasland waarschuwde dat supermarkten hun digitale veiligheid onvoldoende op orde hebben. Hij noemde het veilig houden van de levensmiddelenbranche en de vele toeleveranciers ‘een van de grootste uitdagingen van deze tijd’. ‘Het uitvallen van een leverancier in een supermarkt heeft meteen fysieke impact. Kijk maar naar de hack bij Bakker Logistiek in 2021: er was direct geen kaas meer in de winkels’, zei hij in het interview.

Maasland verwijst daarmee naar een van de meest beruchte zaken tot nu toe in de foodbranche. Bakker Logistiek werd in 2021 het slachtoffer van een aanval met gijzelsoftware. Dat zorgde voor lege schappen bij de marktleider in voorverpakte kaas. Ook concurrent Plus werd hierdoor getroffen. Het duurde lang voordat alle zaken weer op orde waren en de schappen gevuld waren.

Personeelsgegevens buit bij datahack Ahold Delhaize

Vorig jaar waren er verschillende incidenten. De wereldwijde datahack bij Ahold Delhaize trok daarbij extra de aandacht. Gegevens van veel Nederlandse medewerkers zijn daarbij buitgemaakt. Het zou gaan om namen, bankrekeningnummers en het bedrag van de salarisbetaling van begin april 2021. Hackers zouden voor zes terabyte aan data van Ahold Delhaize in handen hebben gehad. Als dader werd de ransomwaregroep INC Ransom genoemd, die wordt verdacht van banden met Rusland.

Dit gebeurde een jaar nadat Boni slachtoffer werd van een bende internationale hackers. Hackmanac, een partij gespecialiseerd in cybersecurity, maakte melding van een hack bij de supermarktketen. Er zou volgens dit bedrijf 16 GB aan data van Boni zijn gestolen. Het zou gaan om financiële gegevens, persoonlijke gegevens en interne bedrijfsbestanden. De zogenoemde Akira ransomware group claimt Boni te hebben beroofd van data.

Cyberincidenten bij AH-multifranchiser en Flink

De aanvallen blijven niet beperkt tot hoofdkantoren. Zo sloegen cybercriminelen in oktober 2025 hun slag bij AH-multifranchiser Jan Bun. Hackers zouden daarbij paspoorten en personeelsdossiers met informatie over salaris, ziekteverzuim en beoordelingen hebben buitgemaakt. Een deel daarvan is op het zogenoemde dark web gepubliceerd. Vorige maand stelde een hackerscollectief te hebben ingebroken bij flitsbezorger Flink. Klanten en medewerkers van Flink moesten geld overmaken via crypto om hun gegevens veilig te houden. Als de boodschappendienst zelf in totaal 100 ether zou overmaken, een cryptovaluta, zouden de gegevens verwijderd. 100 ether is ongeveer €238.000 waard.

Het is maar een beknopt overzicht van incidenten rond data en systemen bij bedrijven uit de supermarktsector en hun toeleveranciers. Bij Albert Heijn lijkt het inmiddels het gevolg te zijn van wat de onderneming omschrijft als een IT-incident op het niveau van moederbedrijf Ahold Delhaize. Nadere gegevens over wat er precies gebeurd is, ontbreken op dit moment nog. Maar het incident maakt weer duidelijk hoe kwetsbaar bedrijven zijn en mogelijk hoe kwetsbaar consumenten zijn die hun data aan bedrijven overhandigen.

Bron: [distrifood.nl](https://www.distrifood.nl)