



HackAtlas

LEARNING REPORT

CASE · 2026

Ahold Delhaize

Cyberincident legt websites, bezorging en distributiecentra van Albert Heijn stil (oktober 2026)

WANNEER

11 oktober 2026

LAND

Nederland (ook Delhaize in België en Amerikaanse merken geraakt)

SOORT AANVAL

Overig

AANVALSPAD BEKEND

onbekend

OPGESTELD DOOR

HackAtlas.nl

VERSIE 1

12 oktober 2026



Gegenereerd met behulp van AI (Claude, Anthropic). Controleer belangrijke feiten aan de hand van de bronnen in de bijlage.

Ahold Delhaize: cyberincident legt websites, bezorging en distributiecentra van Albert Heijn stil (oktober 2026)

In het kort. Sinds zondagmiddag 11 oktober 2026 heeft Ahold Delhaize, het moederbedrijf van Albert Heijn, Etos en Gall & Gall, een cybersecurity-incident en zijn er systemen uit voorzorg uitgezet.^{1,2} Hoe het begon, wie erachter zit en of er gegevens zijn gestolen, is niet bekend: het bedrijf noemt geen oorzaak en geen dader.^{3,4} De websites, apps en klantenservice liggen eruit en in meerdere distributiecentra ligt het werk stil, waardoor lege schappen dreigen, maar de winkels blijven open.^{1,3}

Aanvalspad onbekend:  2 bevestigd ·  1 gemeld ·  1 afgeleid ·  5 onbekend

Stand: maandagavond 12 oktober 2026, op basis van bronnen tot ongeveer 18.20 uur. Het incident loopt nog. Wat hier "niet bekend" heet, kan later wel bekend worden.

1. In één oogopslag

Organisatie	Ahold Delhaize, een grote Nederlandse supermarktgroep (detailhandel) met meer dan 9.400 winkels in Europa, de Verenigde Staten en Indonesië. Albert Heijn, Etos en Gall & Gall horen erbij. ⁵
Wanneer	Het begin van de aanval is niet bekend. Albert Heijn zegt dat het incident begon op zondagmiddag 11 oktober 2026. Een woordvoerder van het bedrijf zegt dat het die dag is vastgesteld. ^{1,4} Het bedrijf maakte het maandag 12 oktober bekend: Albert Heijn vanaf 7.30 uur, Ahold Delhaize om 8.29 uur. ^{1,2}
Dader	Onbekend. In de gelezen bronnen heeft geen groep zich gemeld en heeft geen overheid een dader genoemd. ⁶
Soort aanval	Nog niet vastgesteld. Het bedrijf spreekt van een cybersecurity-incident en van een beveiligingsprobleem in het netwerk. ^{1,2} Een woordvoerder sprak tegenover RTL van een cybersecurityaanval. De topvrouw van Albert Heijn kon tegenover de NOS niet zeggen of kwaadwillenden zijn binnengedrongen. ^{4,3} Of er ransomware of datadiefstal speelt, is niet bevestigd. ^{7,8}
Eerste toegang	Niet bekend. Ahold Delhaize heeft niet gezegd hoe of wanneer iemand binnenkwam. ^{2,4}
Gevolgen	Websites, apps en klantenservice van Albert Heijn, Etos en Gall & Gall liggen eruit. Online bestellingen worden niet bezorgd en al geplaatste bestellingen zijn geannuleerd. ¹ Persoonlijke kortingen en spaarsystemen (zoals Koopzegels en Air Miles) werken niet, en de schapkaartjes tonen de acties van vorige week. ¹ In meerdere distributiecentra ligt het werk stil. Daardoor dreigen lege schappen, vooral bij verse producten. ^{3,1} De winkels en de kassa's werken wel. ¹ Het aandeel Ahold Delhaize stond op een gegeven moment ruim 2 procent lager. ⁴ Ook in België en de Verenigde Staten zijn merken geraakt. ^{9,10} Of er gegevens zijn gestolen, is niet bekend. Over losgeld, kosten of boetes is niets gemeld. ⁴

2. Wat er gebeurde

Het bedrijf. Ahold Delhaize is een van de grootste supermarktgroepen ter wereld, met bijna 400.000 medewerkers.⁵ Albert Heijn, Etos en Gall & Gall zijn Nederlandse merken. Delhaize zit in België. In de Verenigde Staten hoort onder meer Food Lion en Stop & Shop erbij.⁵

Zondag 11 oktober 2026. Albert Heijn zegt dat het sinds zondagmiddag te maken heeft met een cybersecurity-incident. Het nam direct maatregelen om de eigen IT te beschermen. Daarbij zette het een aantal systemen tijdelijk uit, uit voorzorg.¹ Een woordvoerder van Ahold Delhaize zei later tegenover RTL dat het bedrijf die dag een cybersecurityaanval had vastgesteld en de systemen had uitgezet zodat niemand binnen kon komen.⁴ Zondagavond lagen de websites en apps eruit.⁷ Een bezorger van online boodschappen vertelde de NOS dat alle bezorgers tegelijk uit hun app werden gezet en daarna niet meer konden inloggen.³

Maandag 12 oktober, ochtend. Om 7.30 uur meldde Albert Heijn dat websites, apps en klantenservice niet beschikbaar waren. Ook de logistieke systemen waren uit, dus er werd niets bezorgd.¹ In de eerste versie sprak het bedrijf van een IT-incident. Later op maandag werd dat "cybersecurity incident".^{11,12} Moederbedrijf Ahold Delhaize sprak om 8.29 uur van een beveiligingsprobleem in het eigen netwerk. Teams beoordeelden het probleem en haalden systemen offline. De winkels bleven open. Het bedrijf zegt in dat bericht dat het voorkennis bevat. Dat is informatie die de koers van het aandeel kan raken.² Wie op maandagavond ah.nl opent, krijgt een melding dat de website niet werkt.¹³

In de winkels. De kassa's werken. De landelijke Bonusaanbiedingen van deze week gelden. Maar de persoonlijke kortingen en spaarprogramma's werken niet, en op de elektronische schapkaartjes staan nog de acties van vorige week. Klanten die kortingen mislopen, krijgen later een compensatie als ze hun kassabon bewaren.^{1,9}

Maandagmiddag en -avond. De topvrouw van Albert Heijn zei tegen de NOS dat het werk in sommige distributiecentra volledig stilligt, omdat de systemen preventief zijn uitgezet. Albert Heijn heeft er zes in Nederland. Ze wilde niet zeggen hoeveel er stilliggen of welke nog werken.³ Op de vraag of kwaadwillenden zijn binnengedrongen, zei ze dat het onderzoek loopt en dat ze daar nu niets over kan zeggen.³ RTL Z schrijft, op basis van een mail van Albert Heijn aan leveranciers, dat de meeste eigen distributiecentra stilliggen. De kop van het artikel zegt zelfs "vrijwel alle". Alleen het centrum in Zaandam zou nog werken. Leveranciers moeten daar leveren op een vast tijdstip. Albert Heijn wilde daar tegenover RTL niet op ingaan.⁴ Albert Heijn verwacht dat vooral groente en fruit schaars worden. Diepvries, brood en houdbare producten blijven naar verwachting beter beschikbaar.¹ Rond 17.20 uur meldde Albert Heijn dat alle online bestellingen zijn geannuleerd. Klanten die al hadden betaald, wil het bedrijf compenseren zodra de systemen weer werken.¹

Medewerkers en partners. Volgens een bron van RTL Z worden medewerkers van winkels en distributiecentra afgebeld. Dat gaat niet vanzelf, omdat ook hun gegevens in het afgesloten systeem staan.⁴ Een lokale nieuwssite meldt dat medewerkers zijn gewaarschuwd: het hoofdkantoor of een andere partij belt hen niet om informatie of codes te vragen.¹⁴

Andere landen en merken. In België kunnen klanten van Delhaize deze week geen nieuwe bestellingen doen, en de klantenservice is niet bereikbaar. De app en de website werken daar wel.⁹ In de Verenigde Staten lagen de websites van Food Lion, The Giant Company, Giant Food, Hannaford en Stop & Shop eruit. Ahold Delhaize USA gaf geen tijdstip voor herstel.¹⁰ Volgens BleepingComputer, dat zich baseert op berichten van medewerkers, hadden medewerkers van Stop & Shop moeite om hun rooster en loonstrook te zien.⁵ Webwinkel bol had volgens een woordvoerder geen aanwijzing dat het erbij betrokken was.¹⁵

Reacties. De staatssecretaris van Landbouw zegt dat het incident laat zien hoe belangrijk het is dat de hele voedselketen weerbaarder wordt.⁴ De Autoriteit Persoonsgegevens zegt dat een bedrijf een datalek binnen 72 uur moet melden en dat het aan bedrijven zelf is om dat openbaar te maken. Ahold Delhaize kon nog niets zeggen over een mogelijk datalek.^{4,16}

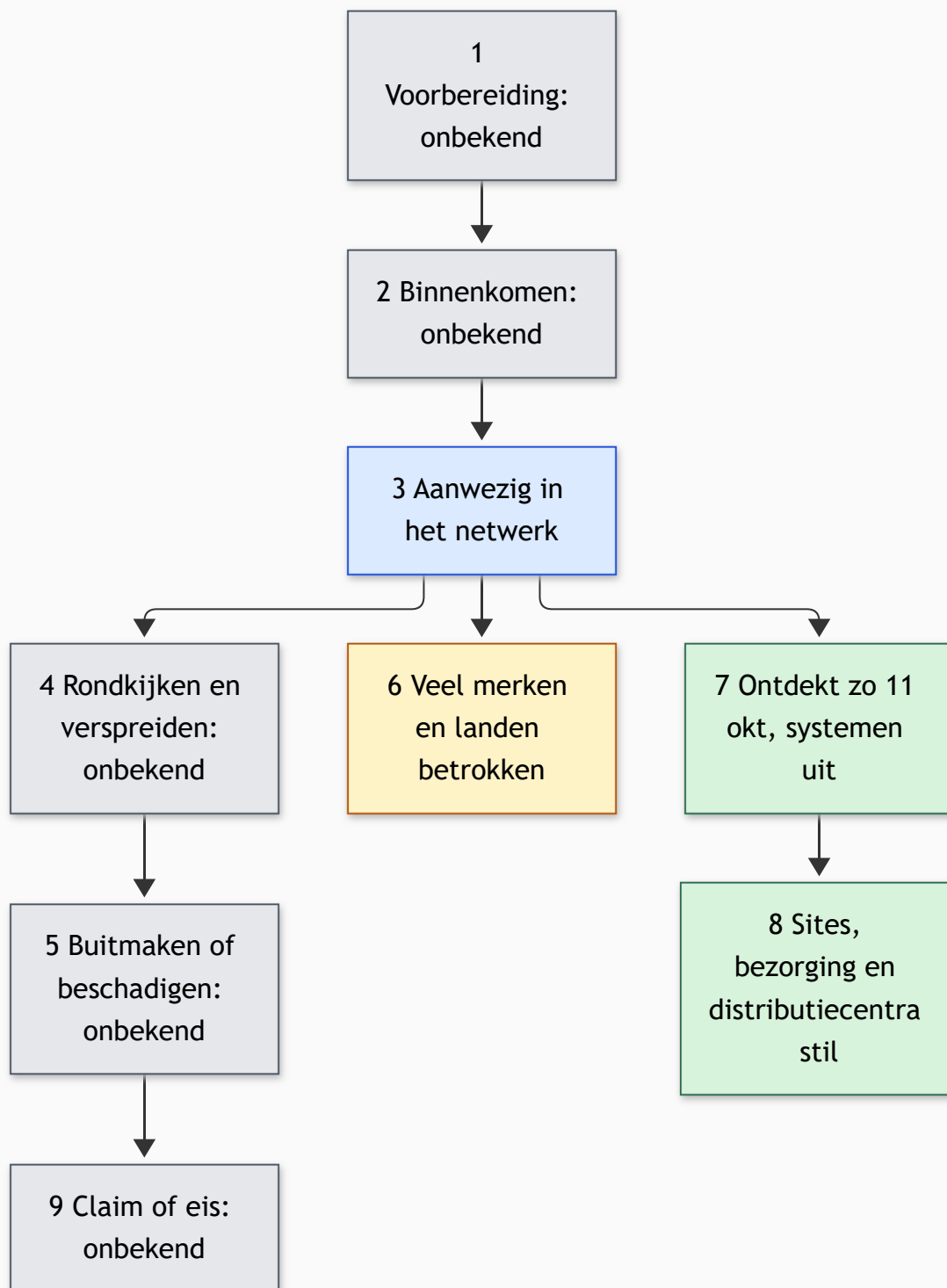
Op dezelfde dag, in Frankrijk. In de nacht naar maandag 12 oktober werden ook honderden Franse supermarkten getroffen door een aanval op koelsystemen. De temperatuur in koelcellen liep op tot 50 graden. Volgens de NOS kwamen de aanvallers binnen via verouderde software van een Deense fabrikant van koelapparatuur.¹⁷ BleepingComputer schrijft dat er nog geen bewijs is dat de twee incidenten verband houden.¹⁸ Een deskundige zei tegen het AD dat er geen aanwijzingen zijn voor dezelfde dader. Ahold Delhaize kon ook niet bevestigen dat er een verband is.¹⁹

Eerdere incidenten. In november 2024 kreeg Ahold Delhaize USA te maken met een cyberaanval. De aanvallers kwamen op 6 november 2024 binnen. De groep INC Ransom claimde de aanval in april 2025. Het bedrijf bevestigde toen dat er bestanden zijn gestolen, maar zei niet of er ransomware was gebruikt. In juni 2025 meldde het bedrijf dat het om gegevens van 2.242.521 mensen ging.^{20,21} In oktober 2025 werd Bun, de grootste franchisenemer van Albert Heijn, gehackt. Daarbij zijn onder meer paspoorten en personeelsdossiers gestolen.²² In de gelezen bronnen staat geen bewijs dat het huidige incident daarmee te maken heeft.^{6,5}

Stand per maandagavond. Er is geen oorzaak, geen dader en geen claim bekend. Er is ook geen tijdstip voor herstel.^{1,6}

3. Het aanvalspad

De bronnen noemen geen enkele aanvalstechniek. Deze keten laat daarom vooral zien wat we nog niet weten. Wat zeker is, zijn de ontdekking en de gevolgen. Bij elke stap staat hoe zeker we zijn. Waar de techniek niet bekend is, staat "Techniek onbekend".



#	Fase (ATT&CK-tactiek)	Wat de aanvallers deden	Techniek	Zekerheid
1	Voorbereiding (Reconnaissance en Resource Development)	Hoe lang de aanvallers zich voorbereidden en hoe ze Ahold Delhaize kozen, is niet gemeld. ^{2,4}	Techniek onbekend	?
2	Initial Access (binnenkomen)	Hoe, wanneer en via welk systeem iemand binnenkwam, is niet gemeld. Ahold Delhaize noemt geen manier van binnenkomen. ^{2,4,3}	Techniek onbekend	?

#	Fase (ATT&CK-tactiek)	Wat de aanvallers deden	Techniek	Zekerheid
3	Onbekend (onbevoegde toegang tot het netwerk)	Ahold Delhaize spreekt van een beveiligingsprobleem in het netwerk. Een woordvoerder sprak tegenover RTL van een cybersecurityaanval. De topvrouw van Albert Heijn kon tegenover de NOS niet zeggen of kwaadwillenden binnen zijn gekomen. Deskundigen vermoeden een hack. ^{2,4,3,19}	Techniek onbekend	
4	Discovery en Lateral Movement (onbekend)	Wat de aanvallers in het netwerk zagen en deden, en hoe ver ze kwamen, is niet gemeld. ⁴	Techniek onbekend	?
5	Collection, Exfiltration of Impact (onbekend)	Of er gegevens zijn gekopieerd of bestanden zijn versleuteld, is niet bekend. Ahold Delhaize kon over een mogelijk datalek nog niets zeggen. ^{4,3,8}	Techniek onbekend	?
6	Onbekend (gedeelde of centrale systemen)	Merken in Nederland, België en de Verenigde Staten hebben tegelijk last, en dat gaat over veel verschillende onderdelen. Dat wijst op gedeelde of centrale systemen die zijn betrokken of uit voorzorg zijn losgekoppeld. ²³	Techniek onbekend	
7	Geen aanvalstechniek: ontdekking en reactie	Albert Heijn en Ahold Delhaize stelden het incident op zondagmiddag 11 oktober vast, namen maatregelen en zetten systemen preventief uit. ^{1,4}	Geen techniek (reactie van het bedrijf)	
8	Impact	Websites, apps, klantenservice en logistieke systemen liggen eruit. Online bestellingen zijn geannuleerd. Spaar- en persoonlijke kortingen werken niet. In meerdere distributiecentra ligt het werk stil. ^{1,3}	Geen techniek toegekend ²⁴	
9	Impact (afpersing, onbekend)	Er is geen claim van een dadergroep, geen losgeldeis en geen lekkage gemeld in de gelezen bronnen. ^{6,4}	Techniek onbekend	?

Zekerheid:  bevestigd door de organisatie, een overheid, de rechter of een onafhankelijk onderzoek ·  gemeld door betrouwbare media of onderzoekers ·  afgeleid, met de redenering in de noot · ? onbekend

4. Waarom het lukte

De oorzaak van de inbraak is niet bekend. Dit hoofdstuk legt daarom vooral uit waarom één incident zoveel gevolgen had. Waar we de oorzaak niet kennen, staat dat erbij.

- Hoe het begon is niet bekend (?).** Bij ransomware en datadiefstal komen aanvallers meestal binnen via phishing, via niet bijgewerkte software, via gestolen inloggegevens of door in te breken in het netwerk.²⁵ In 2025 schreef het Britse NCSC over aanvallen op winkels dat de pers speculeerde over misleiding van de helpdesk, om wachtwoorden en tweede inlogstappen te laten resetten.²⁶ Dit zijn algemene voorbeelden. Geen bron zegt dat ze hier speelden. Een deskundige zegt dat aanvallers vaak in het weekend toeslaan, omdat er dan minder mensen zijn die meteen kunnen ingrijpen.⁴ Of dat hier zo was, is niet bekend.

2. **Veel systemen hangen aan elkaar (🔴 afgeleid).** De storing raakt websites, apps, klantenservice, logistiek, schapkaartjes en distributiecentra, bij meerdere merken en landen tegelijk. Dat past bij systemen of verbindingen die door veel onderdelen worden gedeeld.²³ Eén incident kan dan veel stilleggen.
3. **Uit voorzorg uitzetten stopt ook je eigen werk.** Albert Heijn zette systemen preventief uit. Daardoor ligt het werk in meerdere distributiecentra stil.³ De kassa's werken nog wel, maar het bestellen, plannen en afbellen van medewerkers gaat niet vanzelf.^{1,4} Zo'n besluit is begrijpelijk, maar het maakt de gevolgen groot.
4. **Supermarkten hebben weinig voorraad.** Winkels worden twee tot drie keer per dag beleverd. Verse producten zijn gemiddeld ongeveer drie dagen op voorraad, houdbare producten ongeveer een week, zegt de branchevereniging CBL.²⁷ Een onderzoeker van Clingendael zei in augustus dat dit systeem "extreem efficiënt" is, maar bij een crisis snel in de problemen komt.²⁷ Daarom dreigen er snel lege schappen.³
5. **Eerdere incidenten en een aantrekkelijk doelwit.** Ahold Delhaize USA kreeg in 2024 te maken met een cyberaanval waarbij bestanden werden gestolen, en de grootste franchisenemer van Albert Heijn werd in 2025 gehackt.^{21,22} Deskundigen noemen Albert Heijn een goed doelwit vanwege de hoge omzet en de vele klantgegevens.⁴ Of de eerdere incidenten iets met dit incident te maken hebben, is niet bekend.

5. Wat het had kunnen stoppen

Dit zijn voorstellen op basis van algemene richtlijnen. Ze zijn niet getest bij Ahold Delhaize. Het is niet bekend welke maatregelen het bedrijf al had, en ook niet welke stap hier de zwakke plek was.²⁸

Stap	Maatregel	Moeite	Effect
2	Maak binnenkomen moeilijker. Gebruik phishing-bestendig inloggen (passkeys of beveiligingssleutels) voor medewerkers en leveranciers. Werk software bij die vanaf internet bereikbaar is. Maak vaste regels voor de helpdesk bij het resetten van wachtwoorden en inlogmiddelen. ^{29,26,30}	middel	Sluit de deuren die het vaakst worden gebruikt. Of dat hier de deur was, is niet bekend.
3 en 4	Verdeel het netwerk in aparte stukken (segmentatie) en geef accounts zo min mogelijk rechten. Let op ongewone activiteit bij accounts met veel rechten. ^{30,26}	hoog	Een inbraak blijft kleiner en er hoeven minder systemen uit.
5	Bewaar back-ups offline, houd ze gescheiden van het gewone netwerk en test of terugzetten lukt. ^{30,31}	middel	Zijn bestanden versleuteld, dan kom je sneller terug.
6	Houd webwinkel, winkelsystemen, logistiek en distributiecentra zoveel mogelijk los van elkaar. Bepaal vooraf wat er mag blijven draaien als één onderdeel uit moet.	hoog	De kassa's bleven werken. ¹ Met meer scheiding hadden misschien ook de distributiecentra kunnen doorwerken.
7	Oefen een draaiboek voor "systemen preventief uitzetten": wie beslist, wat blijft aan, hoe werken magazijnen en winkels in een noodstand door, en hoe bereik je medewerkers zonder het systeem. ^{30,4}	middel	Het uitzetten kost minder tijd en schade.

Stap	Maatregel	Moeite	Effect
7 en 8	Maak een lijst van de meest kritieke systemen, zoals bevoorrading, en leg vast in welke volgorde je ze herstelt. ³⁰	middel	Herstel begint bij wat de winkels nodig hebben.
8	Spreid de risico's in de keten. Maak afspraken met leveranciers over leveren in een noodstand, bepaal minimale voorraden voor verse producten en zoek alternatieve routes. Overheid en branche werken aan een crisisplan voor voedselzekerheid. ^{27,4}	hoog	Lege schappen komen later en zijn minder groot.
7 en 9	Bereid de communicatie voor: één duidelijke naam voor het incident, een kanaal voor klanten als de klantenservice uitvalt, en een waarschuwing voor nepberichten. ^{1,32}	laag	Minder verwarring, en criminelen krijgen minder ruimte om het gat te vullen.
5 en 9	Weet vooraf wie binnen 72 uur een datalek meldt bij de Autoriteit Persoonsgegevens en wie klanten informeert. ^{16,25}	laag	Sneller en juist melden.

6. Lessen

Voor bestuur en management - ☐ Welke onderdelen van onze bedrijfsvoering stoppen als we onze IT uit voorzorg moeten uitzetten, en hoe lang kunnen we dan nog leveren?^{3,4} - ☐ Hebben we een draaiboek voor preventief uitzetten, en oefenen we dat? Wie mag dat besluit nemen?³⁰ - ☐ Hoeveel voorraad hebben we, en welke alternatieve routes zijn er als een distributiecentrum uitvalt?²⁷ - ☐ Wie meldt een datalek binnen 72 uur, en wie praat met pers, klanten, leveranciers en franchisenemers?¹⁶ - ☐ Hoe communiceren we als we nog niets weten? Albert Heijn sprak 's ochtends van een IT-incident en later van een cybersecurity-incident.^{11,12}

Voor IT en security - ☐ Gebruik phishing-bestendig inloggen (passkeys) voor medewerkers, beheerders en leveranciers.^{29,30} - ☐ Verdeel het netwerk: webwinkel, kantoor-IT, logistiek en winkelsystemen horen niet op één plat netwerk.³⁰ - ☐ Houd offline back-ups en test of de logistieke systemen echt terug te zetten zijn.^{30,31} - ☐ Controleer hoe de helpdesk wachtwoorden en tweede inlogstappen reset.²⁶ - ☐ Maak een alarm voor ongewone activiteit bij accounts met veel rechten.²⁶ - ☐ Bewaar logboeken op een aparte logserver, zodat ze niet worden gewist.²⁵ - ☐ Zorg dat u uw eigen mensen kunt bereiken als het systeem uit is, bijvoorbeeld met een lijst op papier of een ander kanaal.⁴

Voor iedere medewerker - ☐ Belt iemand die zich voordoeft als het hoofdkantoor of een andere partij en vraagt om informatie of een code? Geef niets door, hang op en bel terug op een nummer dat u kent.^{14,26} - ☐ Twijfelt u? Meld het meteen. Snelheid telt meer dan schaamte.²⁸ - ☐ Bent u klant of leverancier? Wees alert op berichten die het incident noemen en om geld, inloggegevens of een nieuw rekeningnummer vragen. Controleer ze via een nummer dat u kent.³²

7. Voor securityprofessionals

Technieken (MITRE ATT&CK)

Gebruikte versie: ATT&CK Enterprise v19.2 (augustus 2026). In v19 is Defense Evasion opgesplitst in Stealth (TA0005) en Defense Impairment (TA0112). [T1562](#) is vervangen door [T1685](#). Alle hieronder genoemde ID's staan in dat gegevensbestand en zijn niet ingetrokken.³³

Er is op maandagavond 12 oktober geen openbaar technisch rapport. Geen enkele gelezen bron noemt een aanvalstechniek, malware of kwetsbaarheid. Daarom is aan dit incident geen techniek toegekend en staat het veld `attck` leeg.

Tactiek	Techniek	Zekerheid	Toelichting
Reconnaissance (TA0043) en Resource Development (TA0042)	Techniek onbekend	?	Niets gemeld over voorbereiding of infrastructuur van de aanvallers. ²
Initial Access (TA0001)	Techniek onbekend	?	Ahold Delhaize noemt geen manier van binnenkomen. ^{2,4}
Onbekend	Techniek onbekend		Beveiligingsprobleem in het netwerk; woordvoerder spreekt van een cybersecurityaanval, de topvrouw kan niet bevestigen dat iemand binnen is gekomen. ^{2,4,3}
Discovery (TA0007) en Lateral Movement (TA0008)	Techniek onbekend	?	Niets gemeld. ⁴
Collection (TA0009) en Exfiltration (TA0010)	Techniek onbekend	?	Niet bekend of gegevens zijn gekopieerd. ^{4,8}
Impact (TA0040)	Geen techniek toegekend	 (gevolg)	Uitval door preventief uitzetten van systemen. ^{1,24}
Impact (TA0040)	Techniek onbekend	?	Geen losgeldeis of claim gemeld; niet bekend of iets is versleuteld. ^{6,4}

Technieken om als eerste te onderzoeken (hypothesen, geen bevindingen). Deze lijst is een hulpmiddel voor onderzoekers. Er is geen bron die zegt dat een van deze technieken hier is gebruikt, dus ze zijn niet toegekend.³⁴

Waar	Techniek	Waarom onderzoeken
Initial Access	T1078 Valid Accounts	Het Britse NCSC adviseerde na aanvallen op winkels in 2025 om misbruik van legitieme toegang te bewaken. CISA noemt gestolen inloggegevens als veelgebruikte ingang. ^{26,30}
Initial Access en Stealth	T1566 Phishing en T1684.001 Social Engineering: Impersonation	Misleiding van helpdesk of medewerkers. Medewerkers kregen een waarschuwing voor telefoontjes die om codes vragen, maar dat kan ook een voorzorg zijn. ^{26,14}
Initial Access	T1190 Exploit Public-Facing Application en T1133 External Remote Services	Niet bijgewerkte software en externe toegang (VPN, RDP) als bekende ingangen. ^{25,30}
Initial Access	T1199 Trusted Relationship	Derden en beheerders als ingang; veel partners in de keten. ³⁰

Waar	Techniek	Waarom onderzoeken
Lateral Movement	T1021 Remote Services	Zijwaartse beweging, waartegen segmentatie helpt. ³⁰
Impact	T1486 Data Encrypted for Impact en T1490 Inhibit System Recovery	Deskundigen vinden ransomware niet onwaarschijnlijk. Niet bevestigd. ^{19,4}
Impact	T1657 Financial Theft	Afpersing met losgeld of lekdreiging is volgens deskundigen mogelijk. Niet bevestigd. ⁴
Exfiltration	T1567 Exfiltration Over Web Service	Datadiefstal is niet uitgesloten; Albert Heijn zet de bescherming van gegevens voorop. ^{8,1}

Software en malware. In de gelezen bronnen staat geen malware, ransomware of hulpprogramma. Ook is geen ransomwaregroep genoemd.^{6,5}

Kwetsbaarheden

Geen CVE bekend. Geen bron noemt een kwetsbaarheid bij Ahold Delhaize.^{6,5} Voor het aparte Franse incident met koelsystemen noemt BleepingComputer een eerdere waarschuwing van CISA over [CVE-2025-41450](#) in Danfoss-apparatuur. Er is geen bewijs dat dit iets met Ahold Delhaize te maken heeft.¹⁸

Sporen van de aanvallers

Er zijn geen IP-adressen, domeinen, bestandshashes of vermeldingen op een leksite openbaar gedeeld in de gelezen bronnen.^{6,5} Wat wel openbaar is, is niet technisch. Medewerkers kregen de waarschuwing dat het hoofdkantoor of een andere partij hen niet belt om informatie of codes te vragen.¹⁴

Detectie en respons

Wat Ahold Delhaize en Albert Heijn zelf deden. Het incident werd op zondagmiddag 11 oktober vastgesteld. Het bedrijf nam direct maatregelen en zette systemen preventief uit, waaronder logistieke systemen en klantsystemen.^{1,4} Het onderzoek loopt.¹ In de gelezen bronnen staat niet of externe experts, de politie of het NCSC zijn ingeschakeld. Bij het incident in 2024 zei het bedrijf dat wel te hebben gedaan.³⁵

Voorstellen (geen bevindingen). - Isoleer getroffen systemen. Zijn meerdere netwerkdelen getroffen, dan kun je het netwerk op switchniveau offline halen. Prioriteer daarbij de kritieke systemen.³⁰ - Ga uit van het slechtste scenario voor gegevens. Bij ransomware kun je er niet van uitgaan dat de inbreuk beperkt is tot de zichtbaar versleutelde bestanden. Geen bewijs van kopiëren is niet hetzelfde als bewijs van niet kopiëren.²⁵ - Bewaar logboeken apart. Ransomware kan logs wissen.²⁵ - Controleer de logboeken van de identiteitsdienst op risicovolle logins, nieuwe inlogmiddelen en ongewone herstelacties van de helpdesk.²⁶ - Herstel in een vaste volgorde, op basis van een lijst van kritieke systemen, op een schone omgeving.³⁰ - Beoordeel direct de meldplicht van 72 uur bij de Autoriteit Persoonsgegevens en de informatieplicht naar betrokkenen.¹⁶ - Houd leveranciers, medewerkers en klanten op de hoogte, en waarschuw voor misbruik van het incident.^{32,14}

8. Wat we niet weten

- **Hoe kwamen de aanvallers binnen, en sinds wanneer?** Ahold Delhaize noemt het niet.^{2,4} Een evaluatie van het bedrijf of een uitspraak van een toezichthouder zou dit kunnen oplossen.
- **Is het een aanval, en wat voor een?** Een woordvoerder sprak tegenover RTL van een cybersecurityaanval. De topvrouw van Albert Heijn kon tegenover de NOS niet zeggen of kwaadwillenden zijn binnengedrongen. NU.nl schreef dat Ahold Delhaize en Albert Heijn het nog niet hebben bevestigd. Het AD meldt dat een woordvoerder het niet wilde bevestigen.^{4,3,7,19} Een latere verklaring van het bedrijf kan dit beslissen.
- **Zijn gegevens gestolen of bestanden versleuteld?** Ahold Delhaize kon over een datalek nog niets zeggen.⁴ Het AD wijst erop dat het bedrijf in zijn verklaring meteen over de bescherming van gegevens spreekt.⁸ Er is geen losgeldeis of lekdreiging gemeld.⁶ Een melding bij de Autoriteit Persoonsgegevens of een bericht aan betrokkenen zou het aantonen.¹⁶
- **Wie zit erachter?** Er is geen claim en geen toeschrijving in de gelezen bronnen.⁶ Een leksite van een dadergroep zou een claim kunnen tonen. Die is hier niet bekeken.
- **Welke systemen zijn uit, en waarom raakt dit meerdere landen?** Het bedrijf noemt de systemen niet.² De bronnen verschillen: RTL schrijft dat het systeem in België en bij alle Amerikaanse ketens uit ligt, terwijl de NOS meldt dat in België app en website werken en alleen bestellen en klantenservice uit zijn.^{4,9} Ahold Delhaize USA had geen verdere verklaring.¹⁰
- **Hoeveel distributiecentra liggen stil?** De topvrouw noemt geen aantal.³ RTL Z schrijft op basis van een mail aan leveranciers dat de meeste eigen centra stilliggen, behalve Zaandam. Die mail hebben wij niet gezien.⁴
- **Hoe lang duurt het herstel, en wat kost het?** Geen tijdstip bekend. Over kosten, boetes of verzekering is niets gemeld.^{1,4}
- **Is er een verband met de aanval op Franse koelsystemen van dezelfde dag?** Er is geen bewijs voor.^{18,19} Ahold Delhaize kon het niet uitsluiten of bevestigen.³ BNR schrijft dat het erop lijkt dat er een groter cyberincident speelt.³⁶ Dat is een inschatting, geen vaststelling.
- **Is er een verband met eerdere incidenten, zoals de aanval op Ahold Delhaize USA in 2024 (geclaimd door INC Ransom) of de hack bij een franchisenemer in 2025?** In de gelezen bronnen staat geen bewijs.^{6,5}
- **Wat betekent de waarschuwing aan medewerkers?** Het kan een voorzorg zijn tegen oplichters die het incident misbruiken, of een aanwijzing voor de aanvalsmethode. Die bron is een lokale nieuwssite, en de waarschuwing zelf is niet gelezen.¹⁴
- **Wie is ingelicht, en onder welke regels?** In de gelezen bronnen staat niet of het NCSC, de politie of de Autoriteit Persoonsgegevens zijn ingelicht. De Autoriteit Persoonsgegevens zegt wel dat een datalek binnen 72 uur moet worden gemeld.^{4,16}

9. Begrippen

Aanvalspad: de stappen die aanvallers zetten, van binnenkomen tot de schade.

Back-up: een kopie van gegevens, voor als het origineel kwijt of kapot is. Een offline back-up staat los van het netwerk en kan niet worden versleuteld door een aanval.

Cybersecurity-incident: een gebeurtenis waarbij de digitale beveiliging van een organisatie in gevaar is. Het kan een aanval zijn, maar de naam zegt dat niet.

Datalek: gegevens komen bij mensen die ze niet mogen hebben.

Distributiecentrum: een groot magazijn waar producten binnenkomen en naar de winkels gaan.

Franchisenemer: een ondernemer die onder de naam van een groot merk winkels runt, zoals sommige Albert Heijn-filialen.

Helpdesk: de afdeling waar medewerkers hulp krijgen, bijvoorbeeld als ze hun wachtwoord kwijt zijn. Oplichters proberen soms de helpdesk te misleiden.

Just-in-time: bevoorraden met weinig voorraad. Producten komen vlak voor ze nodig zijn bij de winkel.

MITRE ATT&CK: een overzicht van technieken die aanvallers gebruiken. Het helpt om aanvallen op dezelfde manier te beschrijven.

Passkey: een inlogmiddel zonder wachtwoord dat aan je eigen apparaat is gekoppeld. Het is lastig te misleiden. Het Nederlandse NCSC raadt het aan.²⁹

Phishing: nepberichten om gegevens of geld los te krijgen.

Preventief uitzetten: systemen uit voorzorg uitschakelen om verdere schade te voorkomen.

Ransomware: schadelijke software die bestanden versleutelt. Daarna eisen de aanvallers geld om ze weer vrij te geven. Soms dreigen ze ook de gestolen gegevens te publiceren.³⁷

Segmentatie: het netwerk in aparte delen verdelen, zodat een inbraak niet overal komt.

Toezichthouder: een overheidsdienst die let op de regels voor persoonsgegevens. In Nederland is dat de Autoriteit Persoonsgegevens.¹⁶

Versies

- v1 (2026-10-12): eerste versie, op basis van bronnen tot maandagavond 12 oktober 2026.

Bijlage: bronnen en noten

1. Albert Heijn. (2026, 12 oktober). *Mediastatement inzake cybersecurity incident* [Persbericht]. Nieuwsroom Albert Heijn. <https://nieuws.ah.nl/mediastatement-inzake-it-incident/> (Gelezen met de update van 17.20 uur; de eerdere versie van 7.30 uur staat onderaan dezelfde pagina. De titel noemt het een cybersecurity incident; het webadres bevat nog "it-incident".)
2. Ahold Delhaize. (2026, 12 oktober). *Ahold Delhaize takes precautionary measures following cybersecurity incident* [Persbericht]. Ahold Delhaize Newsroom. <https://newsroom.aholddelhaize.com/ahold-delhaize-takes-precautionary-measures-following-cybersecurity-incident/> (Geplaatst om 08.29 uur Nederlandse tijd. Het bericht zegt zelf voorkennis te bevatten in de zin van artikel 7, lid 1, van de Europese verordening marktmisbruik.)

3. NOS. (2026, 12 oktober). Meerdere distributiecentra Albert Heijn liggen stil door digitaal veiligheidsincident, kans op lege schappen. *NOS Nieuws*. <https://nos.nl/artikel/2634698-meerdere-distributiecentra-albert-heijn-liggen-stil-door-digitaal-veiligheidsincident-kans-op-lege-schappen> (Gepubliceerd 16.24 uur, aangepast 17.54 uur. Bevat de uitspraken van de topvrouw van Albert Heijn en van een bezorger.)
4. RTL Z. (2026, 12 oktober). Chaos bij Albert Heijn: vrijwel alle distributiecentra liggen plat, lege schappen dreigen. *RTL Nieuws*. <https://www.rtl.nl/nieuws/economie/artikel/5658604/chaos-albert-heijn-bevoorrading-distributiecentra-plat> (Gelezen na 18.20 uur; het artikel is na de eerste publicatie aangepast. De kop op de voorpagina sprak van "meeste" distributiecentra, de kop van het artikel van "vrijwel alle". De mail aan leveranciers heeft RTL Z naar eigen zeggen in handen; wij hebben die mail niet gezien.)
5. Gatlan, S. (2026, 12 oktober). Retail giant Ahold Delhaize takes systems offline after cyberattack. *BleepingComputer*. <https://www.bleepingcomputer.com/news/security/retail-giant-ahold-delhaize-takes-systems-offline-after-cyberattack/> (Voor de Amerikaanse kant baseert het bericht zich op berichten van medewerkers op Reddit en op een intern bericht dat een medewerker deelde. Die berichten zijn niet geopend.)
6. Kavichselvan. (2026, 12 oktober). Ahold Delhaize network security incident triggers precautionary system shutdowns. *Cyber Press*. <https://cyberpress.org/ahold-delhaize-security-incident/> (Secundaire bron. Meldt dat geen ransomwaregroep de aanval heeft opgeëist en dat geen indicatoren van compromittering zijn gepubliceerd. De eigen analyse van het bericht is niet als feit overgenomen. In de andere gelezen bronnen staat ook geen claim.)
7. NU.nl. (2026, 12 oktober). Distributiecentra Albert Heijn plat door cybersecurityincident, lege schappen dreigen. *NU.nl*. <https://www.nu.nl/economie/6412904/distributiecentra-albert-heijn-plat-door-cybersecurityincident-lege-schappen-dreigen.html> (Gepubliceerd 16.45 uur door de economieredactie. Gelezen via de doorverwijzing van Google Nieuws.)
8. Louws, B., & Luimstra, J. (2026, 12 oktober). Techredacteur Jelmer Luimstra over cyberincident Ahold: 'Saillant dat ze het meteen over klantgegevens hebben'. *AD*. <https://www.ad.nl/binnenland/techredacteur-jelmer-luimstra-over-cyberincident-ahold-saillant-dat-ze-het-meteen-over-klantgegevens-hebben~a6d1fb8b/> (Gepubliceerd 13.10 uur, laatste update 18.20 uur. Gelezen via Google Nieuws.)
9. NOS. (2026, 12 oktober). Geen bezorging en verkeerde winkelprijzen na 'cyberveiligheidsincident' bij Albert Heijn. *NOS Nieuws*. <https://nos.nl/artikel/2634644-geen-bezorging-en-verkeerde-winkelprijzen-na-cyberveiligheidsincident-bij-albert-heijn> (Gepubliceerd 7.56 uur, aangepast 11.38 uur. Over Delhaize in België verwijst de NOS naar VRT Nieuws; die pagina is niet geopend.)
10. Goldschmidt, B. (2026, 12 oktober). 'Security issue' reported at Ahold Delhaize. *Progressive Grocer*. <https://progressivegrocer.com/security-issue-reported-ahold-delhaize>
11. Redactie Security.nl. (2026, 12 oktober). Albert Heijn getroffen door cybersecurity-incident: geen bezorging boodschappen. *Security.NL*. <https://www.security.nl/posting/957095/Albert+Heijn+getroffen+door+cybersecurity-incident%3A+geen+bezorging+boodschappen> (Gepubliceerd 9.42 uur, laatst bijgewerkt 14.04 uur. Meldt dat Albert Heijn het persbericht heeft aangepast en nu ook van een cybersecurity incident spreekt.)
12. NL Times. (2026, 12 oktober). "Cybersecurity incident:" Hack may be behind outage at Albert Heijn. *NL Times*. <https://nltimes.nl/2026/10/12/cybersecurity-incident-hack-may-behind-outage-albert-heijn> (Gepubliceerd 14.30 uur. Noemt een update van de verklaring van Albert Heijn om 11.30 uur.)
13. Albert Heijn. (z.d.). *Storing - Albert Heijn* [Webpagina]. <https://www.ah.nl/> (Geraadpleegd op de avond van 12 oktober 2026. De pagina meldt dat de website niet werkt.)
14. Bakker, P. (2026, 12 oktober). AH-netwerk offline wegens IT-veiligheidsprobleem. *De Orkaan*. <https://www.deorkaan.nl/ah-netwerk-offline-wegens-it-veiligheidsprobleem/> (Lokale nieuwssite, gebaseerd op mededelingen van Ahold Delhaize en de webwinkels. De waarschuwing aan medewerkers staat in een update; de oorspronkelijke tekst daarvan is niet gelezen.)
15. De Telegraaf. (2026, 12 oktober). Albert Heijn, Etos en Gall & Gall getroffen door 'it-incident': geen bezorging online bestelde boodschappen. *De Telegraaf*. <https://www.telegraaf.nl/binnenland/albert-heijn-etos-en-gall-gall-getroffen-door-it-incident-geen-bezorging-online-bestelde-boodschappen/162925204.html> (Gepubliceerd 7.45 uur; de pagina toont de bijgewerkte tekst. Gelezen via Google Nieuws.)
16. Autoriteit Persoonsgegevens. (z.d.). *Zo meldt u een datalek*. <https://autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/zo-meldt-u-een-datalek> (Tekst aangepast in juni 2026. Noemt de termijn van 72 uur na kennisname.)
17. NOS. (2026, 12 oktober). Cyberaanval treft Franse supermarkten, koelsystemen op 50 graden gezet. *NOS Nieuws*. <https://nos.nl/artikel/2634691-cyberaanval-treft-franse-supermarkten-koelsystemen-op-50-graden-gezet> (Gepubliceerd 15.20 uur; bericht van AFP.)
18. Gatlan, S. (2026, 12 oktober). Cyberattack shuts down refrigerators at French supermarkets. *BleepingComputer*. <https://www.bleepingcomputer.com/news/security/cyberattack-shuts-down-refrigerators-at-french-supermarkets/> (Noemt Danfoss-regelaars en een eerdere CISA-waarschuwing over CVE-2025-41450. Zegt dat er geen bewijs is voor een verband met Ahold Delhaize.)
19. Luimstra, J., & Louws, B. (2026, 12 oktober). Website en app Albert Heijn plat door 'cybersecurityincident': 'Waarschijnlijk een hack'. *AD*. <https://www.ad.nl/binnenland/website-en-app-albert-heijn-plat-door-cybersecurityincident-waarschijnlijk-een-hack~aa4cbd47/> (Gepubliceerd 12.18 uur, laatste update 18.07 uur. Gelezen via Google Nieuws. Bevat uitspraken van securitydeskundigen; hun namen zijn hier niet overgenomen.)
20. Toulas, B. (2025, 17 april). Ahold Delhaize confirms data theft after INC ransomware claims attack. *BleepingComputer*. <https://www.bleepingcomputer.com/news/security/ahold-delhaize-confirms-data-theft-after-inc-ransomware-claims-attack/>

21. Gatlan, S. (2025, 27 juni). Retail giant Ahold Delhaize says data breach affects 2.2 million people. *BleepingComputer*. <https://www.bleepingcomputer.com/news/security/retail-giant-ahold-delhaize-says-data-breach-affects-22-million-people/> (Noemt toegang op 6 november 2024 en 2.242.521 getroffen mensen, volgens een melding bij de procureur-generaal van Maine.)
22. Verlaan, D. (2025, 23 oktober). Medewerkers Albert Heijn opnieuw slachtoffer hack: paspoorten en personeelsdossiers op straat. *RTL Nieuws*. <https://www.rtl.nl/nieuws/binnenland/artikel/5535056/grootste-franchisenemer-ah-gehackt-paspoorten-en>
23. Afgeleid (gedeelde of centrale systemen). Redenering: (1) het uitvalbeeld beslaat verschillende merken (Albert Heijn, Etos, Gall & Gall), verschillende landen (Nederland, Delhaize in België en Amerikaanse merken) en veel soorten systemen (websites, apps, klantenservice, logistiek, schapkaartjes, spaarsysteem en distributiecentra), allemaal binnen dezelfde dag (zie noot 1, noot 9, noot 10 en noot 3); (2) Ahold Delhaize spreekt in het persbericht van een beveiligingsprobleem binnen het eigen netwerk, niet van één merk (zie noot 2); (3) volgens de mail aan leveranciers werkt nog maar één distributiecentrum (zie noot 4). Dat past bij systemen of verbindingen die door meerdere merken worden gedeeld, of die uit voorzorg zijn losgekoppeld. Het bewijst niet dat de aanvallers overal aanwezig waren: het bedrijf kan ook meer hebben uitgezet dan nodig. Een deskundige zei tegen het AD dat het meer op een hack van het interne netwerk lijkt dan op een aanval via één toepassing (zie noot 19). Welke systemen gedeeld zijn, is niet bekend.
24. Geen techniek toegekend voor stap 8 (en stap 7). De uitval komt volgens Albert Heijn door het preventief uitzetten van systemen door het bedrijf zelf (zie noot 1). Dat is een reactie, geen techniek van de aanvallers, en ATT&CK beschrijft alleen wat aanvallers doen. Zou later blijken dat de aanvallers bestanden hebben versleuteld of vernietigd, dan zijn T1486 Data Encrypted for Impact of T1485 Data Destruction de kandidaten. Dat is nu niet bekend (zie stap 5 en noot 33).
25. Autoriteit Persoonsgegevens. (z.d.). *Datalek door ransomware*. <https://autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-door-ransomware>
26. Ellison, J., & Whitehouse, O. (2025, 4 mei). *Incidents impacting retailers – recommendations from the NCSC* [Blogbericht]. National Cyber Security Centre. <https://www.ncsc.gov.uk/blog-post/incidents-impacting-retailers>
27. Koenis, C. (2026, 8 augustus). Supermarkten zijn slecht voorbereid op crisissituaties: 'Vrij snel chaos'. *RTL Nieuws*. <https://www.rtl.nl/nieuws/binnenland/artikel/5635383/supermarkten-zijn-slecht-voorbereid-op-crisissituaties> (Aangepast op 14 augustus 2026. Bevat uitspraken van een onderzoeker van Instituut Clingendael, van de branchevereniging CBL en van de staatssecretaris van Landbouw.)
28. Voorstel van de schrijver van deze case, gebaseerd op algemene richtlijnen (zie noot 30, noot 26, noot 31, noot 29 en noot 25). Geen bron bevestigt dit voor Ahold Delhaize en het is niet bekend welke maatregelen het bedrijf al had.
29. Nationaal Cyber Security Centrum. (z.d.). *Kies je authenticatiemiddel op basis van het risico*. <https://www.ncsc.nl/multifactor-authenticatie/kies-je-authenticatiemiddel-op-basis-van-het-risico> (Het NCSC adviseert passkeys en noemt ze bestand tegen phishing.)
30. Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency, & Multi-State Information Sharing and Analysis Center. (2023, september). *#StopRansomware Guide*. CISA. <https://www.cisa.gov/stopransomware/ransomware-guide> (Bevat deel 1, preventie, en deel 2, een responschecklist. Gelezen op 12 oktober 2026.)
31. James L. (2019, 13 augustus). *Offline backups in an online world* [Blogbericht]. National Cyber Security Centre. <https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world>
32. Verjans, B. (2026, 12 oktober). Cyberincident bij Ahold Delhaize: systemen van Delhaize en Albert Heijn deels offline. *KMO partners*. <https://www.kmo.partners/2026/10/12/cyberincident-ahold-delhaize-delhaize-albert-heijn-systemen-offline/> (Raadt leveranciers aan alert te zijn op berichten die het incident gebruiken om gegevens, betalingen of nieuwe rekeningnummers te vragen.)
33. MITRE. (2026, 5 augustus). *Enterprise ATT&CK, release 19.2* [Gegevensbestand]. GitHub, mitre-attack/attack-stix-data. <https://raw.githubusercontent.com/mitre-attack/attack-stix-data/master/enterprise-attack/enterprise-attack.json> (Gebruikt om te controleren dat de genoemde ID's bestaan en niet zijn ingetrokken.)
34. Deze lijst is geen reconstructie. Redenering: de technieken komen uit algemene richtlijnen over ransomware en afpersing en uit de eerste uitspraken van deskundigen. CISA groepeerde preventie naar veelvoorkomende ingangen: gestolen inloggegevens, phishing, misbruik van kwetsbare software of externe toegang, en derden (zie noot 30). Het Britse NCSC noemde bij aanvallen op winkels in 2025 misbruik van legitieme toegang en mogelijke misleiding van de helpdesk (zie noot 26). De Autoriteit Persoonsgegevens noemt phishing, niet bijgewerkte software en inbraak in het netwerk (zie noot 25). Deskundigen noemden ransomware en afpersing mogelijk, zonder bewijs (zie noot 19 en noot 4). Voor Ahold Delhaize bevestigt geen bron één van deze technieken. De waarschuwing aan medewerkers (zie noot 14) kan een voorzorg zijn. De technieken zijn gecontroleerd in ATT&CK v19.2 (zie noot 33).
35. Ahold Delhaize. (2024, 8 november). *Ahold Delhaize statement on Ahold Delhaize USA cybersecurity issue* [Persbericht]. Ahold Delhaize Newsroom. <https://newsroom.aholddelhaize.com/ahold-delhaize-statement-on-ahold-delhaize-usa-cybersecurity-issue/> (Het bedrijf zegt hierin externe cybersecurityexperts te hebben ingeschakeld en de politie te hebben ingelicht.)
36. BNR Redactie. (2026, 12 oktober). 'Cyberaanval bij Albert Heijn raakt bevoorrading winkels, vrees voor lege schappen'. *BNR Nieuwsradio*. <https://www.bnr.nl/nieuws/ondernemen-werk/10613299/cyberaanval-bij-albert-heijn-raakt-bevoorrading-winkels-vrees-voor-lege-schappen> (Gepubliceerd 17.03 uur, aangepast 18.10 uur. Gelezen via Google Nieuws.)
37. Nationaal Cyber Security Centrum. (z.d.). *Ransomware: weerbaar tegen ransomware-aanvallen*. <https://www.ncsc.nl/ransomware>