VORFALL-LAGEBILD

Cybersecurity-Incident bei Ahold Delhaize: Distributionszentren gestört, leere Regale bei Albert Heijn

Stand 27.10.2026 14:50 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Bei Ahold ist keine Kühlanlage ausgefallen, sondern die IT, und weil Bestellung, Lager und Lieferung daran hängen, standen nach Stunden die Lager still.

2. Abschalten und binnen 24 Stunden das NCSC informieren war richtig (CC1, ICS Incident Response), teuer wird es, wenn die Logistik ohne zentrale IT gar nicht weiterarbeiten kann (CC2, Defensible Architecture).

3. Wer Angriffsverkehr früh sieht, kann rechtzeitig abschalten (CC3, Monitoring), und mit KI schaffen das heute auch kleine Teams, wenn sie sich auf die fünf SANS Critical Controls konzentrieren.

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
Ahold Delhaize bestätigt ein Sicherheitsproblem („security issue“) im eigenen Netzwerk. Zum Schutz („to help protect them“) wurden einige Systeme offline genommen.	100 %	100 %	bestätigt
Die Systeme sind seit Sonntagnachmittag, 11.10.2026, offline. Albert Heijn sprach zuerst von einem „IT-Incident“ und später von einem „Cybersecurity-Incident“. Einen Hack hat das Unternehmen nicht bestätigt.	100 %	50 %	präzisiert
CEO Margaret Versteden-van Duijn kann noch nicht sagen, ob Angreifer in die IT eingedrungen sind, weil die Untersuchung noch läuft.	100 %	40 %	offen
Laut niederländischer Polizei ist bisher keine Straftat festgestellt. Ein Hack ist damit aber nicht ausgeschlossen.	100 %	15 %	widerlegt
Der Konzern hat externe Cybersecurity-Experten hinzugezogen und arbeitet nach eigener Aussage mit den zuständigen Behörden zusammen. Welche Behörden das sind, sagt er nicht.	100 %	70 %	präzisiert
Bisher hat sich keine Ransomware-Gruppe zu dem Angriff bekannt. Der Konzern lässt offen, ob Systeme verschlüsselt wurden.	100 %	90 %	bestätigt
Ein Sprecher von Ahold Delhaize sagte Reuters, es gebe keinen Grund, einen Zusammenhang mit dem Angriff auf französische Supermärkte zu sehen.	100 %	75 %	offen
Ein externer Angreifer hatte Zugriff auf Konzernsysteme. Eine reine technische Störung ist es nicht.	75 %	85 %	präzisiert

Frühere Aussage	vorher	jetzt	Status
Dahinter stecken finanziell motivierte Kriminelle, etwa mit Ransomware oder Datenerpressung.	55 %	45 %	offen
Der Konzern hat eine Schwachstelle selbst entdeckt und nur vorsorglich abgeschaltet, ohne dass Angreifer tief im Netz waren.	15 %	5 %	widerlegt
Der Fall hängt direkt mit dem Danfoss-Kühlanlagen-Angriff in Frankreich zusammen.	10 %	7 %	offen
Websites, Apps, Kundenservice und Online-Lieferungen von Albert Heijn, Etos und Gall & Gall fallen aus. Online-Bestellungen werden bis auf Weiteres nicht ausgeliefert. Die Kassen funktionieren.	100 %	90 %	präzisiert
Laut CEO stehen einige Distributionszentren von Albert Heijn komplett still, weil Systeme vorsorglich abgeschaltet wurden. Wie viele große Zentren es in den Niederlanden insgesamt gibt, ist widersprüchlich: A und B zitieren NOS mit sieben, B zitiert außerdem DutchNews mit sechs.	100 %	85 %	präzisiert
Laut einer E-Mail an einen Lieferanten, über die RTL Z berichtet, lief nur noch das Zentrum in Zaandam. Albert Heijn hat das nicht bestätigt.	100 %	50 %	offen
Knapp werden vor allem Frischwaren wie Obst und Gemüse. Haltbare Produkte, Brot und Tiefkühlware sollen besser verfügbar bleiben.	100 %	90 %	bestätigt
Die elektronischen Preisschilder zeigten veraltete Aktionspreise. Persönliche Rabatte über Bonuskarte und App funktionieren nicht.	100 %	90 %	bestätigt
Belgien: Das DC Tilburg ist betroffen, deshalb werden die belgischen AH-Filialen aus anderen Zentren beliefert. Delhaize-Filialleiter können keine Bestellungen aufgeben. Die Zentrale beliefert sie auf Basis früherer Bestellungen, und externe Lieferanten sind ausnahmsweise erlaubt.	100 %	60 %	offen
USA: Die Websites bzw. das Online-Geschäft von Food Lion, Giant Food, Stop & Shop, Hannaford und The Giant Company sind offline, die Filialen haben geöffnet. Die Ketten betreiben über 2.000 Filialen in 23 Bundesstaaten.	100 %	85 %	präzisiert
Bei Stop & Shop hatten Mitarbeitende Probleme mit Dienstplänen und Gehaltsabrechnung.	100 %	60 %	präzisiert
Die Aktie schloss am 12.10. bei 31,38 € und damit 3,15 % unter dem Eröffnungskurs.	100 %	60 %	offen
In der grenznahen AH-Filiale in Vaals bei Aachen waren die Regale bei einem Besuch der Aachener Zeitung zunächst gut gefüllt, in anderen niederländischen Filialen teils leer.	100 %	100 %	bestätigt

Frühere Aussage	vorher	jetzt	Status
Laut Konzern gibt es derzeit keinen Hinweis darauf, dass Kunden- oder Mitarbeiterdaten gestohlen wurden. Die Untersuchung läuft.	100 %	100 %	bestätigt
Die Engpässe betreffen vor allem Frischware und halten an, bis die Distributionszentren wieder voll laufen. Das dürfte noch einige Tage dauern.	unbekannt (Vorgabe abgeschnitten) %	85 %	bestätigt

Neu seit dem letzten Stand

• 19.10.: Konzern bestätigt „malicious actions of others“, Meldung an das NCSC binnen 24 h, Anzeige bei der Polizei

• 23.10.: Polizei bestätigt ein strafrechtliches Ermittlungsverfahren

• 13.10. (NOS): Angriffsverkehr über Server in den USA, Polen, Moldau und der Türkei, laut anonymen Quellen

• 14.10.: Distributionszentren wieder in Betrieb, 15.10. Frischware wieder geliefert

• 19./20.10.: Websites und Apps in NL, BE und USA wieder online

• 23.10.: Heimlieferung mit einem Drittel der Kapazität, volle Kapazität erwartet ab 28.10.

• 20.10.: Fachleute schätzen den Umsatzausfall auf 120 bis 150 Mio. Euro

• Weiterhin kein Bekennerschreiben; Konzern sagt nichts zur Verschlüsselung

• t-online erwähnt keine Fernmanipulation von Kühlgeräten (der Widerspruch ist damit geklärt: dafür gibt es keine Quelle)

Wissensstand



■ Wissen 56 % ■ Wahrscheinlich 20 % ■ Nicht bekannt 24 %

Zu Ablauf, Folgen und Wiederherstellung ist der Stand gut belegt (Konzernmitteilungen, Polizei, NOS, NL Times); zu Täter, Einfallstor, Ransomware und Datenabfluss gibt es keine belastbaren Angaben.

1. Was ist passiert, und warum?

WISSEN

• Ahold Delhaize hat verdächtige Aktivität in seiner IT-Infrastruktur entdeckt, externe Experten geholt und Systeme vorsorglich abgeschaltet. Laut Untersuchung gehen die Vorgänge auf „malicious actions of others“ zurück. (100 %)

[https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident/]

• Albert Heijn sprach zuerst von einem „IT-Incident“, später von einem „Cybersecurity-Incident“, und hat das Wort Cyberangriff zunächst vermieden. (100 %)

[https://nltimes.nl/2026/10/16/albert-heijn-hasnt-reported-hack-police-grocery-deliveries-least-sunday]

• Laut anonymen Quellen aus der Security-Branche hat Albert Heijn verdächtigen Angriffsverkehr gesehen und Systeme abgeschaltet, damit die Angreifer nicht tiefer eindringen. Dabei wurden Server in den USA, Polen, Moldau und der Türkei genutzt; über den Standort der Täter sagt das nichts. (100 %)

[https://nos.nl/artikel/2634805-albert-heijn-zag-verkeer-hackers-aanval-via-meerdere-buitenlandse-servers]

• Das niederländische NCSC wurde binnen 24 Stunden informiert. Am 19.10. hat der Konzern Anzeige bei der niederländischen Polizei erstattet. (100 %)

[https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident/]

• Die Polizei hat ein strafrechtliches Ermittlungsverfahren eingeleitet und äußert sich nicht zu laufenden Ermittlungen. (100 %)

[https://nltimes.nl/2026/10/23/police-investigate-cyberattack-albert-heijn-works-restore-full-deliveries]

• Bekannt hat sich bisher keine Gruppe. Ob Geräte verschlüsselt wurden, wollte ein Sprecher nicht sagen. (100 %)

[https://www.bleepingcomputer.com/news/security/ahold-delhaize-cyberattack-affects-services-across-us-and-europe/]

NICHT BEKANNT

• Wer hinter dem Angriff steckt

• Wie die Angreifer hineingekommen sind

• Ob Ransomware eingesetzt oder Lösegeld gefordert wurde

• Ob ein Zusammenhang mit den Angriffen auf Kühlanlagen in Frankreich besteht (keine Quelle belegt einen)

WAHRSCHEINLICH (Einschätzung)

• Angreifer hatten tatsächlich Zugriff auf Konzernsysteme, es war keine reine technische Störung. (85 %) – Der Konzern bestätigt „malicious actions of others“, NOS-Quellen sprechen von Angriffsverkehr, Anzeige und Ermittlungen laufen. Wie tief der Zugriff ging, ist nicht bestätigt.

• Dahinter stehen finanziell motivierte Kriminelle (Ransomware oder Datenerpressung). (45 %) – Das ist das häufigste Muster bei Händlern (Ahold USA 2024, M&S/Co-op 2025). Nach mehr als zwei Wochen gibt es aber weder ein Bekennerschreiben noch einen Eintrag auf einer Leak-Site.

• Der Fall hängt direkt mit den Angriffen auf Danfoss-Kühlanlagen in Frankreich zusammen. (7 %) – Getroffen wurden andere Ziele (Konzern-IT hier, Kühlregler im Internet dort). Laut Berichten sieht Ahold keinen Grund für einen Zusammenhang, und keine Quelle meldet manipulierte Kühlgeräte bei Albert Heijn.

2. Was ist die Auswirkung?

WISSEN

• Betroffen waren die Websites und Apps der meisten Marken in Europa und den USA. Die Filialen blieben die ganze Zeit offen. (100 %)

[https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident/]

• Mehrere Distributionszentren von Albert Heijn standen still, Regale blieben leer. Lieferanten konnten ab Sonntag nicht anliefern. (100 %)

[https://nos.nl/artikel/2634968-opstarten-systemen-ah-betekent-niet-dat-alles-meteen-weer-werkt-kan-weken-duren]

• Am 14.10. fehlte laut ANP vor allem Obst und Gemüse. Elektronische Preisschilder zeigten falsche Preise. (100 %)

[https://nltimes.nl/2026/10/14/albert-heijn-recovery-underway-cyberattack-damage-likely-tops-eu10-million]

• Abgeschaltet wurden auch das Treueprogramm und die Bonuskarte. Heimlieferungen fielen fast zwei Wochen lang aus. (100 %)

[https://nltimes.nl/2026/10/16/albert-heijn-hasnt-reported-hack-police-grocery-deliveries-least-sunday]

• Die US-Marken von Ahold Delhaize USA hatten mindestens acht Tage lang keine Websites und Apps. (100 %) [https://www.grocerydive.com/news/ahold-delhaize-adusa-cybersecurity-update/833414/]

• Laut Konzern gibt es bisher keinen Hinweis, dass sensible Daten von Kunden, Mitarbeitenden oder Partnern abgeflossen sind. Die Untersuchung läuft. (100 %)

[https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident/]

• Fachleute schätzen den Umsatzausfall auf 120 bis 150 Mio. Euro (Sloot für RTL Z: etwa 150 Mio.; Hemmes: etwa 120 Mio.). Albert Heijn selbst nennt keine Zahl. (100 %)

[https://nltimes.nl/2026/10/20/cyberattack-attempt-cost-albert-heijn-eu150-million-experts-say]

• In der Filiale in Vaals bei Aachen waren die Regale zunächst gut gefüllt, in anderen niederländischen Filialen teils leer. (100 %) [https://aachen.t-online.de/region/aachen/id_101479088/cyberangriff-auf-albert-heijn-leere-regale-in-den-niederlanden.html]

NICHT BEKANNT

• Ob doch Daten abgeflossen sind (Untersuchung läuft)

• Wie viele Distributionszentren genau stillstanden

• Der tatsächliche Schaden einschließlich Wiederherstellung und Incident Response

WAHRSCHEINLICH (Einschätzung)

• Die Versorgung der Bevölkerung war zu keinem Zeitpunkt ernsthaft gefährdet. Die Kundschaft ist zu Jumbo, Lidl, Aldi und Plus ausgewichen. (80 %) – Die Filialen blieben offen, Konkurrenten meldeten mehr Kundschaft (NL Times 16.10.), die Lücken bestanden einige Tage und betrafen vor allem Frischware.

• Später wird doch ein Abfluss von Daten bekannt. (30 %) – Beim Ahold-Vorfall 2024 und bei Co-op 2025 kam ein Datenabfluss erst später heraus. Diesmal verneint der Konzern ihn wiederholt, und niemand hat sich bekannt.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

• Am 13.10. begann ein kontrollierter Neustart einzelner Systeme. (100 %)
[https://newsroom.aholddelhaize.com/update-on-ahold-delhaizes-cybersecurity-incident/]

• Albert Heijn rechnete damit, dass alle Distributionszentren im Laufe des 14.10. wieder arbeiten. Haltbare Ware wurde seit dem 13.10. wieder geliefert. (100 %)
[https://nltimes.nl/2026/10/14/albert-heijn-recovery-underway-cyberattack-damage-likely-tops-eu10-million]

• Stand 19.10. waren die Website und App von Albert Heijn sowie die Websites von Etos und Gall & Gall wieder online, der belgische Onlinehandel lief voll. (100 %)
[https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident/]

• Die US-Seiten und -Apps waren am 20.10. wieder online. (100 %)
[https://www.grocerydive.com/news/ahold-delhaize-adusa-cybersecurity-update/833414/]

• Die Heimlieferung lief am 23.10. mit etwa einem Drittel der Kapazität wieder an. Volle Kapazität erwartet Albert Heijn ab Mittwoch (28.10.). (100 %)
[https://nltimes.nl/2026/10/23/police-investigate-cyberattack-albert-heijn-works-restore-full-deliveries]

• Logistikprofessor Jan Fransoo rechnet mit mehreren Wochen bis zur vollen Erholung. Er vermutet, dass die Bestandsdaten nicht stimmen und von Hand nachgezählt werden müssen. (100 %)
[https://nos.nl/artikel/2634968-opstarten-systemen-ah-betekent-niet-dat-alles-meteen-weer-werkt-kan-weken-duren]

NICHT BEKANNT

• Welche internen Systeme (ERP, Lagerverwaltung, Kassen-Backend) wieder voll laufen

• Ob die Lieferkapazität am 28.10. tatsächlich wieder normal war (dazu gab es bei Redaktionsschluss noch keinen Beleg)

WAHRSCHEINLICH (Einschätzung)

• Die Nacharbeit im Hintergrund (Härtung, Forensik, Neuaufbau von Identitäten) zieht sich noch Wochen bis Monate. (75 %) – Das ist bei Vorfällen dieser Größe so üblich (M&S brauchte 2025 Monate). Der Konzern nennt keine Details.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

• Die Distributionszentren standen still, weil IT-Systeme vorsorglich abgeschaltet waren. Nach etwa drei Tagen liefen sie wieder. (100 %)
[https://nltimes.nl/2026/10/16/albert-heijn-hasnt-reported-hack-police-grocery-deliveries-least-sunday]

• Weder Konzern noch Medien berichten von physischen Schäden an Anlagen, Fördertechnik oder Kühlung. (100 %) [https://aachen.t-online.de/region/aachen/id_101479088/cyberangriff-auf-albert-heijn-leere-regale-in-den-niederlanden.html]

NICHT BEKANNT

• Ob Lagerautomatisierung oder OT-Systeme in den Zentren selbst betroffen waren oder nur durch die fehlende IT stillstanden

WAHRSCHEINLICH (Einschätzung)

• Die Zentren standen wegen der Abhängigkeit von der IT still (Bestellungen, Lagerverwaltung), nicht weil Anlagen manipuliert wurden. (80 %) – Die Zentren liefen nach etwa drei Tagen wieder, schneller als nach einem echten Schaden an der Anlage. Nach NOS ist die Steuerung stark automatisiert und hängt an den Daten aus der IT.

5. Wie viele solcher Ziele gibt es?

WISSEN

• Ahold Delhaize betreibt 9.551 Filialen mit über 384.000 Beschäftigten und hat 77 Mio. Kunden pro Woche in den USA, Europa und Indonesien. (100 %)
[https://www.bleepingcomputer.com/news/security/ahold-delhaize-cyberattack-affects-services-across-us-and-europe/]

• Fast zeitgleich wurden in Frankreich laut Finanzminister rund 700 von 10.000 Supermärkten über Fernwartungsmodule für Kühlanlagen (Danfoss, Copeland) angegriffen. (100 %) [https://www.clickondetroit.com/business/2026/10/13/cyberattack-targeting-refrigeration-systems-hits-700-supermarkets-french-government-says/]

• Das BSI warnt Betreiber kleiner vernetzter Anlagen (Kühlung, Wechselrichter, Windräder, Trinkwasser). heise fand in Deutschland nur wenige potenziell verwundbare Systeme, der Lebensmittelhandelsverband kennt keine betroffenen Märkte. (100 %)
[https://www.heise.de/news/BSI-gemahnt-auch-Betreiber-kleiner-vernetzter-Anlagen-11487069.html]

• Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 148369 gesamt (DNP3 34441, OMRON FINS 25856, ProConOS 17136, EtherNet/IP 16235, Siemens S7 8060, OPC UA 5613) (100 %)

NICHT BEKANNT

• Wie viele Händler in DACH dieselbe zentrale Logistik-IT ohne Notbetrieb haben

WAHRSCHEINLICH (Einschätzung)

• Jeder große Lebensmittelhändler mit zentraler, automatisierter Logistik kann von einem IT-Ausfall dieser Art ähnlich getroffen werden. (70 %) – Bei M&S und Co-op 2025 und bei Bakker Logistiek 2021 lief es nach demselben Muster: Zentrale Systeme fallen aus, und wenige Tage später sind die Regale leer.

6. Kann das wieder passieren?

WISSEN

• Ahold Delhaize USA wurde schon im November 2024 angegriffen. Betroffen waren Apotheken und Onlinehandel, INC Ransom hat sich später zu dem Angriff bekannt. (100 %)
[https://www.foxnews.com/tech/major-us-grocery-chains-hit-cybersecurity-incident]

• Das BSI hält nach dem Fall Frankreich Nachahmer-Angriffe für möglich. (100 %)
[https://www.heise.de/news/BSI-gemahnt-auch-Betreiber-kleiner-vernetzter-Anlagen-11487069.html]

NICHT BEKANNT

• Ob die Ursache dieses Vorfalls schon vollständig beseitigt ist

WAHRSCHEINLICH (Einschätzung)

• Große Lebensmittelhändler werden in den nächsten zwölf Monaten erneut Ziel von Angriffen, die den Betrieb stören. (75 %) – Seit 2024 gibt es eine dichte Folge solcher Fälle (Ahold 2024, M&S/Co-op 2025, Ahold 2026), und Händler stehen unter hohem Zeitdruck, was sie für Erpresser interessant macht.

Lage

Am Sonntagnachmittag, 11.10.2026, hat Ahold Delhaize verdächtige Aktivität in der eigenen IT entdeckt und vorsorglich Systeme abgeschaltet. Websites, Apps und Lieferdienste in Europa und den USA fielen aus, mehrere Distributionszentren von Albert Heijn standen still, und in den Niederlanden blieben Regale leer. Nach eigener Untersuchung geht der Vorfall auf „malicious actions of others“ zurück. Der Konzern hat das NCSC binnen 24 Stunden informiert und am 19.10. Anzeige erstattet, die Polizei ermittelt. Die Distributionszentren laufen seit 14.10. wieder, die Websites sind zurück, die Heimlieferung soll bis etwa 28.10. wieder voll laufen. Täter, Einfallstor und eine mögliche Verschlüsselung sind weiter unbekannt.

Angriff	Angriff durch Dritte auf die IT-Infrastruktur („malicious actions of others“). Daraufhin wurden vorsorglich Websites, Apps, Treueprogramm, Lieferdienste und Systeme für die Distributionszentren abgeschaltet.
Wann / Status	Entdeckt am Sonntagnachmittag, 11.10.2026 · eingedämmt

Täter	unbekannt, kein Bekennerschreiben bekannt – unbekannt
Betreiber / Branche	Ahold Delhaize (Albert Heijn, Etos, Gall & Gall, Delhaize, Ahold Delhaize USA mit Food Lion, Hannaford, Stop & Shop, Giant) · Lebensmitteleinzelhandel
Anlage / Alter	IT-Infrastruktur, E-Commerce, Distributionszentren mit automatisierter Logistik ·
Region	Niederlande, Belgien, Mittel- und Südosteuropa, USA
Auswirkungen	Die Filialen hatten durchgehend offen. Etwa vom 12. bis 15.10. fehlte in vielen niederländischen Filialen Frischware, die Kundschaft wich zu Wettbewerbern aus. Rund zwei Wochen gab es keine Heimlieferung. Nach Angaben des Konzerns fehlt bisher jeder Hinweis auf abgeflossene Daten. Eine Gefahr für die Versorgung ist nicht belegt. In Deutschland ist nur die Grenzregion indirekt betroffen.
Behörden	Niederländisches NCSC (gemeldet binnen 24 h), niederländische Polizei (Anzeige 19.10., Ermittlungsverfahren bestätigt 23.10.), laut Konzern weitere Regulierer. In Deutschland nicht beteiligt; das BSI äußert sich nur zum Fall Frankreich.
Regulatorik	In den Niederlanden setzt die Cyberbeveiligingswet NIS2 um (Stb. 2026, 187). Laut Sekundärquellen gilt sie seit 15.08.2026 (https://www.aaff.nl/artikelen/de-nis2-richtlijn-per-15-augustus-dit-moet-je-als-ondernemer-weten) . Lebensmittel sind ein NIS2-Sektor, ob reiner Einzelhandel darunter fällt, ist aber umstritten (Konsultationsstellungnahme: https://internetconsultatie.nl/cyberbeveiligingsbesluit/reactie/276554/bestand). Ob Ahold als NIS2-Einrichtung gemeldet hat, ist offen; die Meldung binnen 24 h an das NCSC entspricht aber der NIS2-Frühwarnfrist. Für Datenschutzvorfälle gilt die DSGVO (72 h). In Deutschland gilt das NIS2-Umsetzungsgesetz für Lebensmittel-Großhandel und -Produktion. Ab Dezember 2027 bringt der CRA strengere Pflichten für Hersteller vernetzter Geräte wie Kühlregler (heise).

Angriffsvektor

Noch nicht bekannt – Hypothesen (Einschätzung):

• HYPOTHESE: Ausgenutzte Schwachstelle in einem Edge Device (VPN, Firewall, Gateway) oder einem Dienst, der aus dem Internet erreichbar ist (mittel): Bei großen Konzernen 2025/2026 war das einer der häufigsten Einstiege (Citrix NetScaler, Ivanti, Fortinet). Belegt ist für diesen Fall nichts.

• HYPOTHESE: Social Engineering gegen den IT-Helpdesk oder Übernahme von Identitäten (mittel): So liefen 2025 die Angriffe auf M&S und Co-op, die ebenfalls zu leeren Regalen führten (https://www.helpnetsecurity.com/2025/05/05/uk-retailers-under-cyber-attack-co-op-member-data-compromised/).

• HYPOTHESE: Gestohlene Zugangsdaten (Infostealer, Initial Access Broker, Credential Stuffing) (mittel): Bei großen Konzernen mit vielen Konten ist das ein gängiger Weg. Laut NOS wurde Infrastruktur in mehreren Ländern genutzt, was zu gekauftem oder gemietetem Zugang passt, aber nichts beweist.

• HYPOTHESE: Zugang über einen Dienstleister oder Lieferanten (gering): In der Logistik ist das ein bekannter Weg (Bakker Logistiek 2021). Bisher deutet keine Quelle auf einen Dritten als Einfallstor hin.

Zeitleiste

11.10.2026 nachmittags Verdächtige Aktivität entdeckt, Systeme vorsorglich abgeschaltet, Website/App/Kundendienst offline – bestätigt
[https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident/]

12.10.2026 Erste Mitteilung des Konzerns zu einem „cybersecurity issue“ – bestätigt
[https://newsroom.aholddelhaize.com/update-on-ahold-delhaizes-cybersecurity-incident/]

13.10.2026 Kontrollierter Neustart einzelner Systeme. NOS berichtet über Angriffsverkehr über Server in vier Ländern. Leere Regale, falsche Preisschilder – berichtet
[https://nos.nl/artikel/2634805-albert-heijn-zag-verkeer-hackers-aanval-via-meerdere-buitenlandse-servers]

13.10.2026 BSI gibt eine Empfehlung für Betreiber kleiner vernetzter Anlagen heraus (Anlass ist Frankreich) – berichtet
[https://www.heise.de/news/BSI-gemahnt-auch-Betreiber-kleiner-vernetzter-Anlagen-11487069.html]

14.10.2026 Albert Heijn erwartet alle Distributionszentren im Tagesverlauf wieder in Betrieb – berichtet [https://nltimes.nl/2026/10/14/albert-heijn-recovery-underway-cyberattack-damage-likely-tops-eu10-million]

15.10.2026 Polizei: noch keine Anzeige, deshalb keine Ermittlungen. Frischware wird wieder geliefert – berichtet
[https://nltimes.nl/2026/10/16/albert-heijn-hasnt-reported-hack-police-grocery-deliveries-least-sunday]

19.10.2026 Konzern bestätigt „malicious actions of others“ und erstattet Anzeige. Website/App von AH, Etos und Gall & Gall wieder online – bestätigt
[https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident/]

20.10.2026 Websites und Apps der US-Marken wieder online – berichtet
[https://www.grocerydive.com/news/ahold-delhaize-adusa-cybersecurity-update/833414/]

23.10.2026 Polizei bestätigt Ermittlungsverfahren. Heimlieferung startet mit etwa einem Drittel der Kapazität – berichtet
[https://nltimes.nl/2026/10/23/police-investigate-cyberattack-albert-heijn-works-restore-full-deliveries]

Vergleichsfälle

• Ahold Delhaize USA (Stop & Shop, Hannaford u. a.) (2024): Derselbe Konzern war schon einmal betroffen, und erst Monate später hat sich INC Ransom zu dem Angriff bekannt.
[https://www.foxnews.com/tech/major-us-grocery-chains-hit-cybersecurity-incident]

• Marks & Spencer und Co-op (UK) (2025): Angreifer kamen über Social Engineering am Helpdesk hinein, und die Abschaltung der Bestellsysteme führte zu wochenlangen Lücken im Regal.
[https://www.helpnetsecurity.com/2025/05/05/uk-retailers-under-cyber-attack-co-op-member-data-compromised/]

• Bakker Logistiek (NL), Käsemangel bei Albert Heijn (2021): Ransomware bei einem einzigen Logistikdienstleister hat die Lagerautomatisierung gestoppt; dank eines guten Backups lief nach wenigen Tagen alles wieder. [https://www.bitdefender.com/blog/hotforsecurity/ransomware-attack-causes-supermarket-cheese-shortage-in-the-netherlands]

• Kühlanlagen in rund 700 französischen Supermärkten (Danfoss, Copeland) (2026): Kühlregler mit veralteter Firmware, die aus dem Internet erreichbar waren, wurden massenhaft manipuliert; ein anderes Ziel als bei Ahold, aber dieselbe Branche zur selben Zeit. [https://www.clickondetroit.com/business/2026/10/13/cyberattack-targeting-refrigeration-systems-hits-700-supermarkets-french-government-says/]

Begriffe einfach erklärt

OT: Operational Technology ist die Technik, die Maschinen und Anlagen steuert, etwa Förderbänder im Lager oder Kühlanlagen.

Distributionszentrum: Ein großes Zentrallager, aus dem die Filialen einer Region täglich beliefert werden.

Ransomware: Schadsoftware, die Daten verschlüsselt, damit die Täter Lösegeld erpressen können.

NCSC: Das Nationale Cyber Security Centrum der Niederlande, vergleichbar mit dem BSI.

Incident Response: Die geplante Reaktion auf einen Sicherheitsvorfall: erkennen, eindämmen, aufräumen, wieder hochfahren.

NIS2: EU-Richtlinie, die wichtige Unternehmen zu Cybersicherheit und schnellen Meldungen von Vorfällen verpflichtet.

Früherer Stand: Erstmeldung (13.10.2026 15:38)

Wissen 46 % · wahrscheinlich 23 % · nicht bekannt 31 %

Ahold Delhaize hat seit Sonntagnachmittag, 11.10.2026, wegen eines „security issue within its network“ vorsorglich Systeme abgeschaltet. Ausgefallen sind Websites, Apps, Online-Lieferungen, Kundenservice und Kundenbindungsprogramme in den Niederlanden, in Belgien und in den USA. Mehrere Distributionszentren von Albert Heijn stehen ganz oder teilweise still. Deshalb fehlt in Filialen vor allem Frischware. Seit dem 13.10. fährt der Konzern einzelne Systeme kontrolliert wieder hoch, einen Zeitplan nennt er nicht. Ein Hack ist nicht bestätigt, Experten halten ihn aber für sehr wahrscheinlich. Täter, Angriffsvektor und die Frage, ob Ransomware im Spiel ist, sind offen. Laut Reuters sieht der Konzern keinen Grund für einen Zusammenhang mit dem Kühlanlagen-Angriff auf Danfoss-Regler in Frankreich.

Früherer Stand: Nach 24 Stunden (14.10.2026 15:58)

Wissen 47 % · wahrscheinlich 24 % · nicht bekannt 29 %

Seit Sonntagnachmittag, 11.10.2026, hat Ahold Delhaize wegen eines Sicherheitsproblems im eigenen Netzwerk vorsorglich Systeme abgeschaltet. Mehrere Distributionszentren von Albert Heijn standen deshalb still. In den Niederlanden blieben Regale teils leer, auch Delhaize in Belgien war betroffen, und Websites, Apps und Online-Dienste in Europa und den USA waren offline. Seit dem 13.10. fährt der Konzern die Systeme kontrolliert wieder hoch. Am 14.10. sollen alle Distributionszentren wieder laufen. Täter, Angriffsweg und eine mögliche Verschlüsselung sind offiziell weiter unbekannt. Belege für einen Datenabfluss gibt es laut Konzern bisher nicht.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.