BRANDEFENSE COUNTRY REPORT · DENMARK 2026

Brandefense Denmark Cyber Threat Landscape Report 2026

Identity, shared data and service continuity in a connected economy

Odin by Brandefense
Research window: 1 January–22 November 2026
Version 1.0 · Public Research Edition · TLP:CLEAR · 8–22 November 2026

37 of 250
selected domains had a credential listed for sale when checked

6
case dossiers separating advertisements, provenance and access claims

29
Danish ransomware listings in the research window

3
separate concerns: institution systems, customer fraud and shared-service continuity

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Denmark's digital and institutional context	10
03	Selected-domain exposure and validation priorities	14
04	Underground activity: what the retained posts establish	21
05	Incidents and campaigns	34
06	Hacktivism, DDoS and connected systems	54
07	Actors, campaigns and evidence relationships	62
08	Fraud after data exposure	71
09	Banking and payment-service dependencies	76
10	Regulation and the national response	80
11	Outlook: conditional decisions through the next quarter	86
12	Action plan: owners and completion evidence	90
A	Appendix A. Scope and evidence boundaries	97
B	Appendix B. Evidence-card register	100
C	Appendix C. Sources	102
D	Appendix D. Glossary	106
	About this report	108

Board and executives	01 05 11 12
CISO and service owners	03 04 05 09 12
SOC and intelligence teams	04 06 07 B
Fraud and customer operations	05 08 09
Legal, privacy and communications	05 06 10 12

About this edition

Prepared with AI assistance. Evidence populations, attribution and limitations remain beside the findings.

Denmark's documented incidents connect identity, suppliers, historical records and essential services. Defenders need separate decisions about access, copied information, continuity and customer harm.

29

Denmark-associated ransomware listings; criminal claims [S2]

19

claimant labels in that listing population; not unique operators [S2]

37 / 250

selected domains with a credential listed for sale when checked [S3]

4

decisions for leaders, linked to accountable owners

Contents and reading routes

Chapter	Question
1 Executive summary	Which decisions deserve leadership attention first?
2 Context	Which Danish operating conditions change those decisions?
3 Selected-domain exposure	What can owners validate, and which observations are unavailable?
4 Underground activity	What do the retained advertisements and posts establish?
5 Incidents and campaigns	What did organisations and authorities actually confirm?
6 Hacktivism, DDoS and connected systems	How do public claims differ from operational effects?
7 Actors and relationships	Which source supports each attribution or association?
8 Fraud after exposure	How can copied information cause a second incident?
9 Banking and payments	How do customer, institution and supplier risks differ?
10 Regulation	Which scope, recipient and reporting clock apply?
11 Outlook	Which conditional scenarios justify preparation?
12 Action plan	Who acts, and what demonstrates completion?
Appendices A–D	Evidence boundaries, card register, sources and definitions

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which findings justify immediate decisions for Danish organisations?

29

ransomware listings in the requested window, each recording a claim

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Denmark's disclosures show how identity systems, historical records and shared suppliers connect security incidents to daily work. November updates add legacy-system access, booking-related fraud and service interruptions. Ransompedia records 29 Danish listings under 19 claimant labels. These claims are separate from confirmed disclosures and exposure observations. Validate identity evidence, test supplier-dependent services and give customers a known route to verify suspicious contact.

This report combines retained Brandefense underground evidence and ransomware listings with source-verified public disclosures, official warnings and legal texts. Posts, offers, listing claims, people notified and domain associations remain different populations. They are not added into a national attack total. [S1][S2][S3]

The requested observation window is 1 January–22 November 2026 by post time. Public cases use the dates stated in their sources, distinguishing intrusion, detection, disclosure and later updates. The 8–22 November view highlights recent developments without relabelling earlier intrusions as new attacks.

1. Identity infrastructure deserves scrutiny beyond the password. DTU's published chronology describes a guest account, subsequent remote access, administrative privileges and extraction. KU describes a separate identity-data incident. AU, a Danish university, describes attempted password changes that did not succeed. These are different propositions, requiring different containment and communication decisions. [S12][S13][S14][S53]

2. A supplier event can require several customer decisions. Dental-service, publishing and hospitality notices concern different dependencies. One supplier incident can produce several customer disclosures. Each customer must establish its own data scope, service state and reporting responsibilities before deciding what to restore or tell affected people. [S18][S45][S49][S50]

3. Copied information can outlast technical containment. Datatilsynet's CPR advice explains how familiar personal information can support convincing fraud. Hospitality notices describe fraudulent payment requests using booking details. Closing an access route does not establish that copied information has disappeared. Customer protection belongs in the incident response. [S16][S18]

4. November's maritime incident needs a bounded account. Maersk confirmed unauthorised access and extraction from a local legacy system. It reported no indication of impact on other or integrated customer systems and anticipated no customer operational disruption. The actor identity, advertised quantity and ransom demand remain separate claims in reporting. [S10][S11]

5. Extortion labels support broad preparation rather than one-actor assumptions. The 29 retained listings carry 19 labels. Eight use Thegentlemen, three Settra and two Qilin; sixteen other labels have one each. The partial 2026 window differs from the full-year 2025 total of 27. Neither population establishes confirmed intrusions, encryption or loss. [S2]

Four decisions for leaders

1. **Give identity alerts an accountable route.** Obtain relevant observations, confirm ownership and validity, investigate sessions and recovery paths where warranted, and retain the disposition (§3, §12).
2. **Test the service and its supplier dependency.** Identify the business function, data custodian, affected interface and fallback. Require evidence for reconnection, with a named business owner (§5, §9).
3. **Protect people after a data notice.** Give staff and customers an independent verification route for payment, account recovery and identity-document requests. Preserve reports of later misuse (§8).
4. **Exercise the right reporting clocks.** Establish the legal entity, scope, awareness time, classification and recipients. Treat NIS2, GDPR and DORA as distinct assessments sharing one factual chronology (§10).

The year in numbers

29

Denmark-associated ransomware listings in the requested window

WHAT IT DOES NOT MEASURE

Confirmed intrusions or unique victims

19

Claimant labels attached to those listings

WHAT IT DOES NOT MEASURE

Unique people, operators or affiliates

27

Denmark-associated listings for all of 2025

WHAT IT DOES NOT MEASURE

A matched-period baseline

8 / 3 / 2

Listings under Thegentlemen / Settra / Qilin

WHAT IT DOES NOT MEASURE

Verified success or a common access route

250

Selected candidate domains across ten groups

WHAT IT DOES NOT MEASURE

Independent legal entities or national prevalence

525,000

Approximate users in KU's affected database scope

WHAT IT DOES NOT MEASURE

Confirmed fraudulent use or active student population

More than 200,000

Users potentially affected in DTU's latest notice

WHAT IT DOES NOT MEASURE

A verified count of records downloaded

4,071

Responses in the official business-security study, collected in 2025

WHAT IT DOES NOT MEASURE

A 2026 incident count

[S2][S3][S5][S12][S13]

Credentials were listed for sale for 37 of the 250 selected domains when checked. The national Atlas headline is 45/100 (B). At least 141,187 device associations and 2,039,476 credential-record associations require separate validation. These overlapping signals do not establish confirmed intrusions. Passive-control results remain unavailable. [S3]

KEY TAKEAWAYS

01

Separate advertisements, listing claims and confirmed disclosures before deciding on action.

02

Connect identity, supplier and customer-protection owners in the same response.

03

Require working continuity and reporting evidence, with explicit ownership of missing inputs.

Report map

Twelve chapters, five reader routes. Follow the decision you own; evidence limits travel with the findings.

Board and executives	Fund priorities and test essential services	01 05 11 12
CISO and service owners	Validate relevant exposure and dependencies	03 04 05 09 12
SOC and intelligence teams	Distinguish observation, claim and attribution	04 06 07 B
Fraud and customer operations	Prevent harm after information exposure	05 08 09
Legal, privacy and communications	Apply the correct scope and clock	05 06 10 12

The evidence labels are **observation**, **actor claim**, **official confirmation** and **analyst inference**. An observed advertisement remains a claim about the advertised material. A confirmed incident can leave its actor, entry route and full data scope unresolved.

Chapter	What the reader should leave with
Context	A service and reporting map rather than an assumed single authority
Exposure	Dated exposure observations, the national Atlas headline and accountable validation
Underground activity	Traceable examples with no assumed sale, freshness or successful access
Public incidents	Separate timelines for detection, disclosure and response
Availability and actors	Source-specific attribution and distinct operational consequences
Fraud and banking	Customer, institution and supplier decisions kept separate
Regulation	Entity-specific notification decisions and documented awareness
Outlook and action	Conditional triggers, accountable owners and completion evidence

CHAPTER 02

Denmark's digital and institutional context

02

THIS CHAPTER ANSWERS

Which operating conditions change the decisions Danish organisations need to make?

4,071

company responses underlying the official business-security study, collected in 2025

2.1 A recent publication can describe an earlier population 11

2.2 The former CFCS and the national CSIRT have distinct roles 11

2.3 Digital identity creates responsibilities beyond the sign-in page 12

2.4 Political framing is a source claim, not an attribution shortcut 12

2.5 Keep the populations separate 13

CHAPTER 02

Denmark's digital and institutional context

IN SHORT

Denmark's public disclosures connect identity, shared data, suppliers and everyday service delivery. Official publications use different windows and responsibilities. A November assessment can describe last year's survey, while a recent regulator decision can concern an older intrusion. These distinctions change both priorities and reporting obligations. Map the service, data, legal entity and competent contact before an incident starts.

2.1 A recent publication can describe an earlier population

SAMSIK published Digital Security in Businesses 2026 on 6 November. It describes responses collected in 2025 from 4,071 companies with at least ten employees. Its headline says four in ten SMEs lack basic security measures. That is survey context, not a measured 2026 intrusion rate. [S5]

The practical question is whether a control works in the organisation's actual workflows. A password policy does not show how support staff authorise recovery. A backup record does not show whether a dependent service can operate while restoration proceeds. A supplier contract does not establish who can stop an export.

The report therefore treats security and continuity as connected responsibilities. An account can remain technically valid after its owner leaves. A legacy system can retain business data after an acquisition. A public website can fail while operational systems continue. Chapters 5 and 6 distinguish these states using the relevant disclosures.

This is an analytical interpretation of the documented cases. It does not assert that every Danish organisation shares the same systems, control gaps or attack path. Leaders should use the cases to choose validation questions for their own services.

2.2 The former CFCS and the national CSIRT have distinct roles

SAMSIK's March 2025 notice states that the Centre for Cyber Security became part of Styrelsen for Samfundssikkerhed. It explains why older CFCS material and current SAMSIK publications appear together. That institutional change does not make every technical or statutory function a SAMSIK responsibility. [S6]

FE's page, updated on 2 October 2026, identifies its situation centre as performing the national CSIRT function for NIS2. SAMSIK's NIS2 guidance separately describes sector authorities' supervisory role. Incident plans must distinguish advice, technical coordination, statutory reporting and criminal investigation. [S7][S28]

Purpose	Relevant route	Evidence to retain
Cybersecurity guidance	SAMSIK and the applicable sector authority	Scope determination and advice received
NIS2 incident coordination	Competent authority and FE's CSIRT through the prescribed route	Submission, chronology and updates
Personal-data breach assessment	Datatilsynet	Risk assessment, notification decision and receipt
Financial ICT incident	Finanstilsynet under the applicable regime	Classification and staged reports
Suspected crime	Police and the relevant cybercrime function	Preserved evidence and reporting record

These routes can concern one event without becoming interchangeable. A regulator may need a legal assessment before a technical investigation is complete. Police may require evidence that the business would otherwise overwrite during restoration. Assign an owner to each purpose rather than assuming one contact resolves every duty.

2.3 Digital identity creates responsibilities beyond the sign-in page

The university and register cases in Chapter 5 concern different populations and kinds of data. Their shared lesson is that identity infrastructure also holds historical relationships. Records can include former students, applicants, staff, contacts and people who no longer use a service.

The information-security owner should establish which identities still grant access. The data owner should establish why historical records remain. Customer operations should know how a genuine warning reaches the affected person. These are separate questions even where one platform holds all the information.

A familiar name, address or identifier can make a fraudulent contact convincing. Datatilsynet's CPR advice warns that knowledge of personal information does not establish a caller's identity. The response should therefore include an independent verification route rather than relying on how much a caller already knows. [S16]

2.4 Political framing is a source claim, not an attribution shortcut

PET, FE and SAMSIK published an election-related threat assessment in February. Its descriptions of foreign influence are the agencies' assessments. They do not establish that a particular outage changed an election outcome, or that every politically framed post had state direction. [S9]

This report takes no position on Greenland, Russia, NATO, Israel/Gaza, religion, Quran-burning incidents, elections or government decisions. Where such issues appear in a source, only the attribution needed to understand the cyber evidence is retained. An actor's language or chosen slogan does not establish nationality or sponsorship.

A defender can prepare for politically framed availability claims without endorsing the claimant's account. The trigger is relevant activity against the organisation or its dependencies, supported by a dated source. It is not an assumption that a public decision caused an attack.

2.5 Keep the populations separate

Posts, extortion listings, public disclosures, regulator decisions and exposure associations answer different questions. They cannot be added into a national attack total. A regulator's decision may describe an earlier event. A supplier notice may affect many customers without establishing separate intrusions at each one.

The same caution applies to country comparisons. Swedish, Norwegian, German and Dutch listing observations share the reporting window, but their economies and source visibility differ. Chapter 7 uses them to describe the retained listing population. It does not estimate relative national security or control effectiveness.

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

KEY TAKEAWAYS

01

Read the observation period as well as the publication date.

02

Separate SAMSIK guidance, FE technical coordination and sector reporting duties.

03

Verify the relevant service and identity evidence before interpreting political framing.

CHAPTER 03

Selected-domain exposure and validation priorities

THIS CHAPTER ANSWERS

Which observed exposure signals need an accountable response?

37 of 250

selected domains had a credential listed for sale when checked

3.1 Universe card 15

3.2 The national Atlas headline describes this portfolio 16

3.3 Devices and credential records need different validation 17

3.4 Give different observations different owners 19

3.5 Passive controls need their own denominator 20

CHAPTER 03

Selected-domain exposure and validation priorities

IN SHORT

Credentials were listed for sale for 37 of the 250 selected organisation domains when checked. The portfolio's national Atlas headline is 45/100 (B). The observations include at least 141,187 device associations and 2,039,476 credential-record associations. They describe overlapping external signals, not confirmed intrusions or unique people. Passive-control results remain unavailable. Validate current accounts, investigate employee-device associations and assign the relevant service or data owner.

3.1 Universe card

Item	Definition
Selected population	250 organisation-related domains across ten groups, with 25 entries per group
Selection	Public-service, commercial and systemic relevance; not an official top-company ranking
Unit	A selected domain associated with an institution, operating brand or group
Independence	Brands, subsidiaries, shared operators and subdomains can overlap
Ownership	Domain resolution does not establish current legal ownership or service responsibility
Exposure snapshot	Device, credential, document and current-listing observations read on 22 November 2026
Other periods	Annual mention context to 18 November 2026; similar-name context from 19 October to 18 November 2026
Passive results	No complete mail-policy, DNS, certificate or web-control dataset available

[S3]

The observed denominator is 250 selected domains. It does not establish 250 independent legal entities or national prevalence. Ownership and service responsibility require confirmation before an observation is assigned to an organisation. Related services and group brands can share records.

A current advertisement is a reason to validate the relevant account. It does not establish a completed sale, working credentials or unauthorised access to an organisation's internal systems. Historical records and the dates of their observation must remain distinct.

3.2 The national Atlas headline describes this portfolio

The national Atlas headline is 45/100 (B). Higher values indicate greater observed exposure in the selected portfolio. The headline supports validation priorities. It is not a breach percentage, incident probability, control certification or security ranking of Denmark. [S3]

45/100 (B)

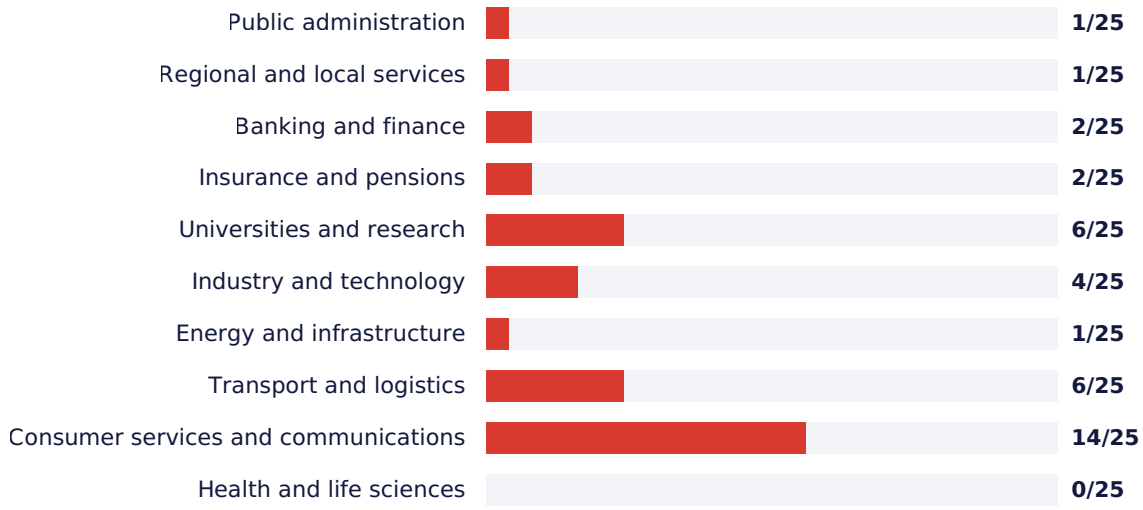
national Atlas headline for the selected 250-domain portfolio [S3]

Only the national Atlas rating is published. The sector rows show signal counts and observed denominators. Banking and finance includes financial services and infrastructure; it is not a complete register of licensed banks or card issuers.

Selected group	Domains	Domains with current credential offers	Documents	Similar names
Public administration	25	1	73	4,039
Regional and local services	25	1	64	1,167
Banking and finance	25	2	22	13,991
Insurance and pensions	25	2	35	1,388
Universities and research	25	6	57	7,175
Industry and technology	25	4	267	476
Energy and infrastructure	25	1	6	6,486
Transport and logistics	25	6	413	483
Consumer services and communications	25	14	564	25,357
Health and life sciences	25	0	18	816
ALL	250	37	1,519	61,378

[S3]

Current-listing observations have a defined selected-domain denominator



Current credential listings by sector (coral). Each denominator is 25 selected domains; current access or a completed sale is not established. Source: Odin by Brandefense, 250 selected domains, exposure snapshot 22 November 2026 [S3]. Associations can overlap and include historical records; they are not unique people or confirmed intrusions.

The document total records associations, not a count of confidential files or confirmed disclosures. Similar-name observations do not establish malicious registration, brand impersonation or phishing. Owners must establish relevance and actual abuse before requesting action.

These categories can overlap within a domain and across domains. Their totals cannot be added to estimate unique incidents, people, accounts or artefacts. A sector with no observed listing has no confirmed clean-security finding.

3.3 Devices and credential records need different validation

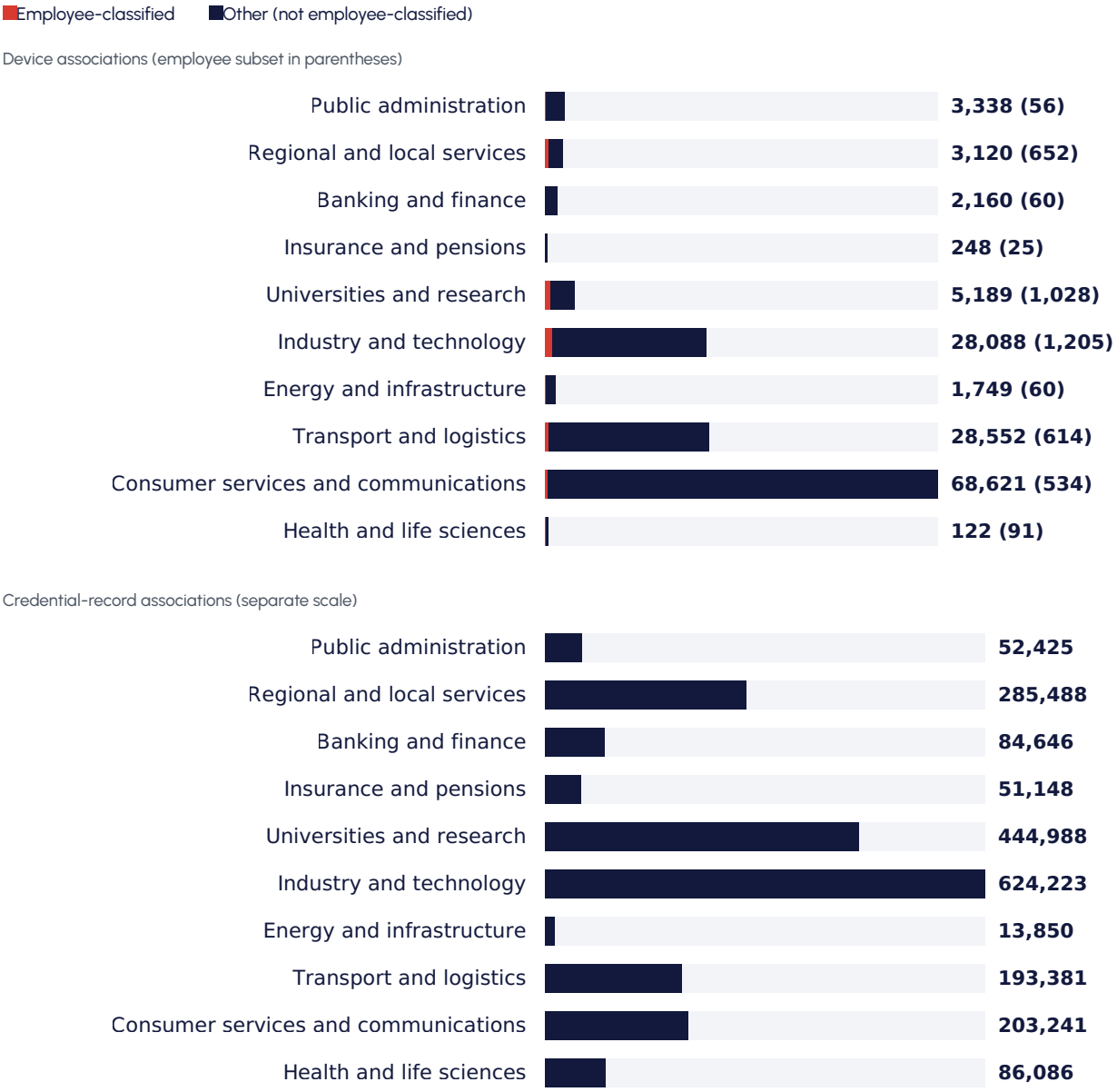
The snapshot contains at least 141,187 device associations, including 4,325 employee-device associations. It also contains 2,039,476 credential-record associations. These populations can overlap and do not establish unique people or currently valid accounts. [S3]

Selected group	Devices, at least	Employee devices	Credential records
Public administration	3,338	56	52,425
Regional and local services	3,120	652	285,488
Banking and finance	2,160	60	84,646
Insurance and pensions	248	25	51,148
Universities and research	5,189	1,028	444,988
Industry and technology	28,088	1,205	624,223

Selected group	Devices, at least	Employee devices	Credential records
Energy and infrastructure	1,749	60	13,850
Transport and logistics	28,552	614	193,381
Consumer services and communications	68,621	534	203,241
Health and life sciences	122	91	86,086
ALL	141,187	4,325	2,039,476

[S3]

Device and credential associations require separate ownership decisions



Source: Odin by Brandefense, 250 selected domains, exposure snapshot 22 November 2026 [S3]. Associations can overlap and include historical records; they are not unique people or confirmed intrusions.

A device associated with a customer-facing service is not automatically an endpoint operated by that service. An employee association also needs verification against asset and account records. A credential associated with a domain does not establish that the organisation's own infrastructure was its source.

Credential records may be historical, repeated or associated with several domains. Check current account status, previous remediation and relevant sessions before choosing disruptive action. An old record can concern a valid account; a recent advertisement can repeat obsolete material.

3.4 Give different observations different owners

The response model connects the measured signals to internal validation. Its actions are recommendations, rather than findings that any selected organisation lacked a particular control.

Observation received	First validation	Accountable owner	Completion evidence
Current credential offer	Confirm account ownership, freshness and access scope	Identity and incident response	Recorded disposition and justified containment
Employee-device association	Identify the endpoint and relevant sessions	Endpoint security and identity	Investigation outcome and session review
Other device association	Establish the service relationship and affected owner	Service and customer operations	Correct routing without assumed employee ownership
Historical credential record	Check account status and earlier remediation	Identity and data owner	Validated status and control action
Similar domain name	Establish actual abuse and brand relationship	Brand protection and legal	Abuse decision and proportionate response
Document observation	Confirm sensitivity, provenance and authority to share	Data owner and legal	Exposure assessment and corrective action
Mail-policy gap	Confirm intended sending services and policy	Messaging owner	Verified delivery and policy behaviour

If an offer concerns an owned account, establish which systems it can reach. Investigate session, recovery and privilege changes alongside the password. A password reset alone does not answer whether another access route was changed.

Each alert needs a disposition: relevant and current, historical and remediated, unrelated, or unresolved. Record the evidence and owner for that decision. An unresolved alert requires a follow-up date rather than an assumed successful closure.

3.5 Passive controls need their own denominator

The missing passive dataset means this edition cannot state a Danish DMARC enforcement rate, certificate-validity rate or hygiene index. It also cannot treat missing observations as absent controls. No conclusion about the security of an individual candidate follows from this absence.

An authorised owner can review its own mail, DNS and web controls against the intended service design. Test legitimate sending and recovery arrangements as part of the review. A visible policy does not by itself establish that every business system uses it correctly.

Exposure observations and passive controls answer different questions. A portfolio headline cannot replace validation of an organisation's individual observations. Nor can a public incident disclosure establish which externally observed records are currently relevant.

KEY TAKEAWAYS

01

Validate accounts associated with the 37 domains with current credential offers.

02

Route employee and other device associations to their correct owners.

03

Keep the national Atlas headline separate from unavailable passive-control results.

CHAPTER 04

Underground activity: what the retained posts establish

THIS CHAPTER ANSWERS

Which underground observations warrant validation without becoming unverified incident counts?

6

case dossiers separating advertisements, provenance and access claims

4.1 Universe card 22
4.2 Volume, venues and language associations 23
4.3 Case dossiers 25
4.4 Vendor claims do not establish customer intrusions 32
4.5 Relays and replies do not independently corroborate a claim 32
4.6 What the cases change for defenders 33

CHAPTER 04

Underground activity: what the retained posts establish

IN SHORT

The retained forum material contains credential-list advertisements, customer-data allegations, development-system claims and a regional access offer. Their evidential value differs. A hidden download, a field header and a seller's assurance do not establish usable access or a new intrusion. Repeated titles and short replies can keep an old allegation visible. Validate the relevant account, system and data proposition before choosing a response.

4.1 Universe card

Item	Meaning
Window	1 January–22 November 2026, by post time
Recent activity	8–22 November 2026, separated from earlier context
Retained posts	4,116 distinct messages; 557 forum records; overlapping country associations
Unit	A retained message, including advertisements, replies, relays and unrelated material
Country association	A country label or reference does not establish targeting or a Danish victim
Case population	Six selected dossiers, each tied to a public evidence card
Underlying claims	Account validity, data provenance, access and transactions remain unverified unless separately stated
Relationships	Repeated wording supports an advertising association, not a shared operator or identical underlying file

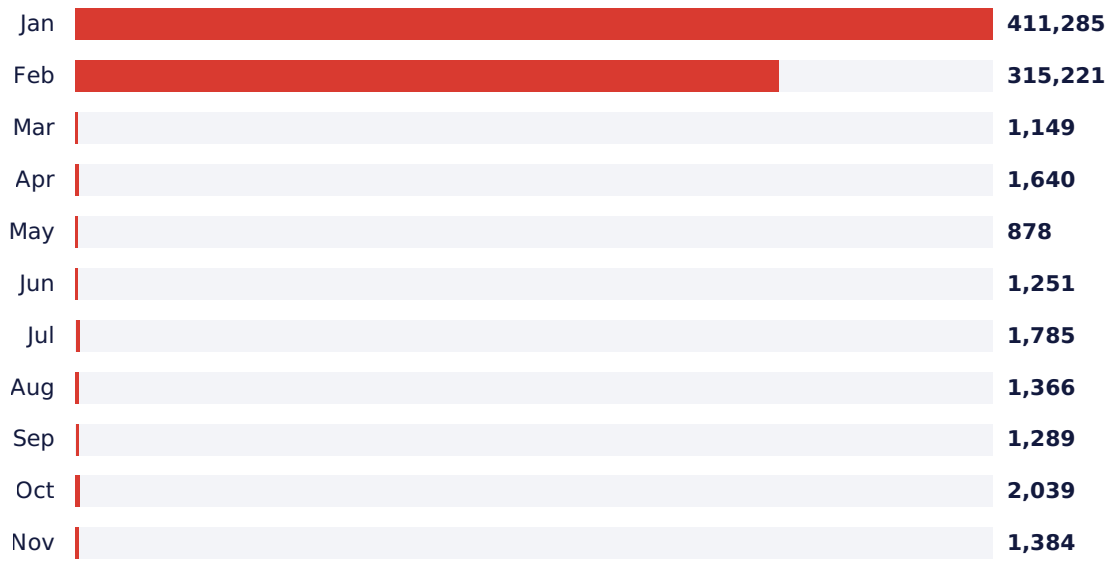
[S1]

The six dossiers address different validation questions. They are not six confirmed intrusions and cannot be added to ransomware listings. A post can describe an old dataset, commercially compiled information, a hidden download or a service available in many countries. The relevant fact is what the retained message actually says.

4.2 Volume, venues and language associations

The monthly country-associated series contains 739,287 post records. January and February account for 726,506, or 98.3%. These are messages carrying a country association, rather than verified Danish targeting or a national incident count. [S1]

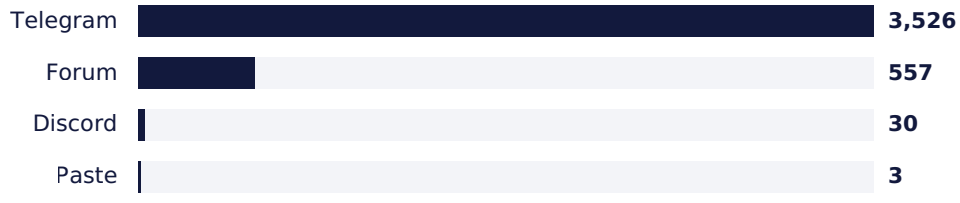
Most country-associated records fall in January and February



Source: Odin by Brandefense, retained Denmark-associated posts, 1 January–22 November 2026; November partial [S1]. Country-tagged monthly records and the 4,116-message reading corpus are different populations; neither measures confirmed incidents.

The retained reading corpus contains 4,116 distinct messages. It includes 557 forum records and 3,738 records carrying the Danish country label. These populations overlap. They are not added together and are not the same population as the monthly series. [S1]

The reading corpus spans several venues

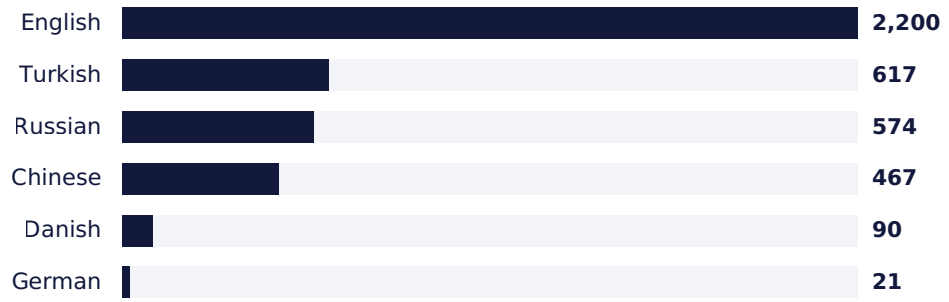


Source: Odin by Brandefense, retained Denmark-associated posts, 1 January–22 November 2026; November partial [S1]. Country-tagged monthly records and the 4,116-message reading corpus are different populations; neither measures confirmed incidents.

Retained venue	Messages	Meaning
Telegram	3,526	Retained messages, including promotional material and claims
Forum	557	Retained advertisements, replies, discussions and relays
Discord	30	Retained messages in the reading corpus
Paste	3	Retained pasted material
ALL	4,116	Distinct messages across these venues

The early-period material includes repeated promotions referring to many countries, including Denmark. Its volume does not demonstrate that attacks on Danish organisations declined afterwards. Message mix and source visibility differ; publication counts are not a measure of successful intrusion. [S1]

Selected language labels describe messages, not actor nationality



Selected language associations can overlap; not an exhaustive distribution or actor nationality. Source: Odin by Brandefense, retained Denmark-associated posts, 1 January–22 November 2026; November partial [S1]. Country-tagged monthly records and the 4,116-message reading corpus are different populations; neither measures confirmed incidents.

English, Turkish, Russian, Chinese, Danish and German labels appear in the retained corpus. A message can have more than one language association. The chart shows selected labels rather than an exhaustive language partition. A language label does not establish the poster's location, nationality or state connection. [S1]

The conclusions rest on the retained material. Neither the reading corpus nor the selected dossiers support an estimate of all Danish advertisements, active sellers, criminal revenue or confirmed incidents.

4.3 Case dossiers

A

CASE A

A new post date does not establish fresh credentials

Evidence card B01 | 2 Jul 2026 | Forum post | Identity records

Claim unverified

CLAIM	A country-labelled advertisement describes an email-and-password list and calls it fresh. The advertised quantity is the poster's statement. The selected July record retains a February date in its title and body. [S1]
CHRONOLOGY	An earlier February record contains matching wording. A July-dated record repeats that dated description, and a short reply adds thanks without validating the material. The dates describe the messages, rather than when any account information was obtained.
WHAT WE CAN ESTABLISH	The same dated advertising description appears in the retained material at different times. This supports a repeated-advertising association. It does not establish that both downloads contain an identical file or that the poster obtained the records personally.
ALTERNATIVES	The material could be historical, previously remediated, repackaged or incorrectly labelled. A later message could also refer to an updated file without explaining the change. The advertisement alone does not resolve those alternatives.
LIMITS	Neither working accounts nor unique people are established. An advertised line count is not a victim count. The freshness label and the message's publication date cannot replace account-level validation.
RESPONSE	If an alert concerns an owned account, confirm its current status and prior remediation. Review relevant access and sessions before choosing containment. Record the evidence supporting the disposition rather than treating every repeated title as another incident.

Bottom line

Validate account freshness before treating repeated advertising as a new incident.

Evidence card B01 — 2 Jul 2026

thejackal101 | Forum post | Forum | EN

ORIGINAL

Database: Denmark Type: Email : Password Date: [6/FEB/2026] Combo: [34 K++]

Note. The advertised quantity and freshness label are the poster's statements. A short reply on the same date adds no validation.

Held

A July-dated record with a February-labelled credential-list advertisement; an earlier February record has matching wording.

Not established

Freshness, valid accounts, unique people, contents of the hidden download or a new intrusion.

CASE B

B ■ Financial-customer fields do not establish bank-system access

Claim unverified

Evidence card B02 | 12 Sep 2026 | Forum post | Financial services

CLAIM	A September advertisement alleges a financial-services customer dataset associated with Denmark. It lists contact, identity and financial-profile fields and asks 800 dollars. That is an asking price, not evidence of a completed transaction. [S1]
CHRONOLOGY	The retained post is dated 12 September. It does not establish when the underlying information was created or acquired. No separate collection date, access event or sale is confirmed by this message.
WHAT WE CAN ESTABLISH	An advertisement and its field descriptions were present. The claimed organisation and identifying description are withheld. Descriptive text about a financial business does not establish that the business supplied, lost or verified the offered records.
ALTERNATIVES	The offer could concern historical leads, a third-party dataset, commercially assembled information or a false association. A record can describe a prospective customer without representing an active account. These possibilities require different owners and responses.
LIMITS	No current account, balance, access to banking systems or customer-loss total is established. The field labels do not demonstrate the authenticity of the records beneath them. The seller's price does not measure the value of the alleged dataset.

RESPONSE	Route a relevant signal to the data owner, fraud team and incident lead. Establish provenance and affected relationships through authorised evidence. Prepare a verification route for suspicious contacts if genuine exposure is confirmed.

Bottom line

Customer-themed fields do not establish bank-system access.

Evidence card B02 — 12 Sep 2026

K0d3x | Forum post | Forum | EN

ORIGINAL

Denmark / [financial-services organisation] / [customer data] [...] For sale: 800$

Note. The organisation name and identifying description are withheld. Do not infer the advertised data came from a current intrusion.

Held

An advertisement with contact, identity and financial-profile field labels and an asking price.

Not established

Authenticity, current accounts, the named organisation's involvement, a sale or access to banking systems.

CASE C

C

Community profile headers are an allegation, not a verified dataset

Claim unverified

Evidence card B03 | 14 Oct 2026 | Forum post | Online services

CLAIM	An October post alleges data from a Danish online community. Its body presents user-table headers, including account and profile fields. The poster describes the material as a current data incident. That description remains the poster's claim. [S1]
CHRONOLOGY	The retained message is dated 14 October and labels the alleged data with the same month. This temporal wording does not establish the date of access, the age of the records or the time any information became publicly available.
WHAT WE CAN ESTABLISH	The post contains table-field descriptions and a claim about their source. No personal sample rows or target identifiers are published here. Headers can describe a database structure without demonstrating the number or authenticity of its records.
ALTERNATIVES	A historical database, a template, a copied schema or an inaccurate attribution could produce similar field descriptions. Two sets of headers do not by themselves establish two intrusions or separate victim populations.

LIMITS	Working passwords, affected-person counts and a confirmed incident at the alleged target are not established. Profile fields may be sensitive, but their presence in a claimed schema does not prove that the corresponding personal information was accessed.
RESPONSE	If the claim relates to an owned service, preserve relevant logs and validate the affected data categories. Check account recovery and historical retention. Notify people according to the established facts and applicable duties, rather than the claimant's most specific allegation.

Bottom line

Table headers do not establish authentic personal records.

Evidence card B03 — 14 Oct 2026

MrData · Forum post · Forum · EN

ORIGINAL

Country: Denmark Date: Oct 2026 [...] Table_Name: [redacted]

Note. The platform name, domain, contact identifiers and detailed profile field list are withheld. Headers are not proof of the underlying records.

Held

A community-data allegation accompanied by user-table field headers.

Not established

Authentic records, valid passwords, number of people affected, or a confirmed incident at the claimed target.

CASE D

D

Development-system allegations require separate account and key checks

Claim unverified

Evidence card B04 · 24 Aug 2026 · Forum post · Technology services

CLAIM	An August advertisement alleges access-related material from a development environment. It describes employee account records and refers to signing and development credentials. Those references are assertions in the post, not independently verified working secrets. [S1]
CHRONOLOGY	The retained material includes two August messages and a September message with closely matching descriptions. Different posters repeat the allegation. This supports an association between the advertisements, without identifying the first source or a common operator.

WHAT WE CAN ESTABLISH	The allegation, a user-table sample and references to keys appear in the stored messages. The public card removes personal rows, target information and contact details. A sample description cannot establish the present reach of an account or the validity of a key.
ALTERNATIVES	The posts could share copied advertising, historical material or the same unverified source. Similar wording does not establish that an underlying file is identical, that a sale occurred or that any software release was changed.
LIMITS	No code modification, downstream customer access or successful use of credentials is established. Administrative account access, signing authority and the ability to publish a release are distinct propositions. Each needs evidence from the relevant owner.
RESPONSE	For a relevant owned environment, review accounts, signing authority and release permissions separately. Preserve build and access evidence before remediation changes it. Choose credential or key action according to validated exposure, and document the reason for each decision.

Bottom line

Validate accounts, signing authority and release permissions separately.

Evidence card B04 — 24 Aug 2026

Bitcoins | Forum post | Forum | EN

ORIGINAL

Table Contents: [redacted] [...] Azure signing keys leaked, VCS Credentials SSH key + SVN.

Note. The quote records the poster's claim. No keys, personal sample rows or target identifiers are published.

Held

A development-system allegation that includes a user-table sample and references to keys; later records repeat the allegation.

Not established

That any credential or signing key works, that code was changed, or that the different posters share an operator.

E

CASE E

A regional access offer has explicit country and reach limits

Evidence card B05 | 5 Nov 2026 | Forum post | Business services

Claim unverified

CLAIM	A November offer describes privileged access to build and database systems at a Nordic business. Its author also states exclusions, including no domain-administrator access and no customer or business-application data. Those exclusions belong beside the broader access claim. [S1]

CHRONOLOGY	The retained post is dated 5 November, before the recent-activity window. It is relevant context for supplier and development-system planning. Its publication does not establish when access began or whether it remained available at this report's cut-off.
WHAT WE CAN ESTABLISH	The seller advertised privileges and described their claimed scope. The country association extends beyond Denmark. This report therefore treats the offer as a regional validation example, rather than a confirmed Danish incident.
ALTERNATIVES	The offer could contain genuine, stale, overstated or fabricated access. The seller's technical descriptions and assurances do not resolve these alternatives. A reference to customer-related infrastructure does not establish access to the customers themselves.
LIMITS	No sale, working login, downstream system access or operational effect is established. Revenue and detailed environment counts are withheld to avoid identifying the claimed target. The claim does not establish a software vulnerability or a particular entry route.
RESPONSE	A relevant service owner should validate administrative accounts, build permissions and deployment relationships. Supplier oversight should identify who can suspend access and what evidence permits reconnection. Do not warn downstream customers as confirmed victims solely because an advertisement mentions customer environments.

Bottom line

A regional access claim does not establish Danish targeting or downstream impact.

Evidence card B05 — 5 Nov 2026

marlowfinch42 | Forum post | Forum | EN

ORIGINAL

TeamCity SYSTEM_ADMIN at [an organisation]. [...] Not included: no domain admin, no customer or ERP data

Note. Country associations are broader than Denmark. The seller's own exclusions must stay attached to the access claim; the targeted business is not named.

Held
An access offer describing build and database privileges at a Nordic business.

Not established
Denmark-specific targeting, working access, customer-system access, a completed sale or any downstream effect.

CASE F

F

Directory-themed contact data is not proof of theft

Evidence card B06 | 4 Jan 2026 | Forum post | Commercial contact data

Claim unverified

CLAIM	A January advertisement offers business-directory-themed information for Denmark and another country. It describes business, contact and location fields and offers examples on request. The advertised quantity is not a verified count of affected organisations or people. [S1]
CHRONOLOGY	The retained message is dated 4 January. It provides no independently supported acquisition date or incident chronology. An offer at the start of the year does not establish that the underlying information was newly obtained in that year.
WHAT WE CAN ESTABLISH	The message advertises a dataset and describes its purported fields. It does not demonstrate exclusive possession or a completed sale. The named service and identifying quantity are withheld because the allegation lacks separate confirmation.
ALTERNATIVES	Public directory information, commercial compilation, repackaged leads or an inaccurate description could account for the offer. Even authentic contact details would not by themselves establish unauthorised access to the organisations described in them.
LIMITS	No verified breach, valid individual record or incident population follows from the advertisement. The country reference describes the claimed dataset, rather than a demonstrated attack on every organisation represented.
RESPONSE	Assess relevant information against lawful public availability, provenance and actual sensitivity. Fraud teams should consider how verified contact data could support impersonation. Do not treat a business-directory offer as evidence that each listed business needs intrusion containment.

Bottom line

Directory-themed information does not establish intrusion at the businesses described.

Evidence card B06 4 Jan 2026

selluk Forum post Forum EN

ORIGINAL

this databases DENMARK contains [advertised quantity] LINES [...] PROFFS AND EXAMPLE ON DEMAND.

Note. The publisher/service identity and detailed quantity are withheld. Public or commercially compiled directory information is an alternative to stolen data.

Held
A business-directory-themed data offer describing contact and business fields for Denmark and another country.

Not established
Provenance, exclusivity, a verified breach, valid contact details or a sale.

4.4 Vendor claims do not establish customer intrusions

A 9 April forum advertisement alleges an earlier vendor incident and offers employee contact records associated with customer companies, including Danish firms. A repeated advertisement does not establish the records' provenance or a separate intrusion at each customer. It also does not establish currently valid credentials or access to customer systems. [S3]

Another advertisement markets a platform dataset as a leak. The offered material does not establish a Danish affected population, the records' provenance or access to the platform's internal systems. [S3]

These observations belong to the separate organisation-associated post context. They are outside the reading-corpus figures above. Relevant customers should verify the vendor relationship, affected information and current account evidence through authorised channels.

4.5 Relays and replies do not independently corroborate a claim

The retained forum material also contains news relays about public incidents and law-enforcement activity. A relay can help locate the original statement, but it does not become an independent investigation because it appears on another platform. Public confirmation belongs to the source that actually supplies it. [S1]

Short replies require similar caution. A message saying thanks, asking whether a link works or repeating a thread title does not establish a fresh offer, purchase or successful download. Several records can describe one allegation without representing several incidents.

The same limit applies to repeated advertisements under different aliases. Shared wording supports the narrow advertising association. Common control, operator identity, dataset identity and completed transfers require additional concrete evidence. No such relationship is inferred merely to connect the cases into one criminal network.

4.6 What the cases change for defenders

Observation	Decision supported	Decision not yet supported
A dated credential advertisement	Check owned accounts and earlier remediation	Count working credentials or new intrusions
Customer-data field descriptions	Assess provenance and possible misuse	Confirm internal bank access
Community user-table headers	Validate account and data scope	Infer authentic personal records or affected-person totals
Development-system allegations	Review accounts, keys and release permissions separately	Declare downstream software or customers affected
A regional build-system offer	Validate relevant supplier dependencies	Assign the event specifically to Denmark
A directory-themed data offer	Assess sensitivity and fraud implications	Treat every represented business as breached

These are conditional response choices. The organisation first needs a relevant alert and enough ownership information to route it. A documented historical or inaccurate association can be a valid closure outcome. Where evidence remains unresolved, retain the uncertainty and the owner responsible for the next validation step.

KEY TAKEAWAYS

01

A message date and a freshness label do not establish a new intrusion.

02

Validate accounts, data provenance and downstream reach as separate propositions.

03

Repeated titles, relays and replies cannot substitute for independent confirmation.

CHAPTER 05

Incidents and campaigns

05

THIS CHAPTER ANSWERS

What did Danish organisations and authorities confirm, and what remains unresolved?

20

public-source dossiers with distinct evidence and impact boundaries

5.1 What the confirmed cases change 35
5.2 Education, research and identity administration 36
5.3 Public services, regulated information and customer records 39
5.4 Contractors, acquired systems and external platforms 43
Other reported hospitality notice 50
5.5 Recent activity: 8 to 22 November 2026 51
5.6 Decisions to take from these cases 52
5.7 Current vulnerabilities: applicability before attribution 52

CHAPTER 05

Incidents and campaigns

IN SHORT

Denmark's public incidents show several distinct routes to disruption and personal-data exposure. Identity administration, test environments, inherited systems and external service providers recur across otherwise different organisations. Recent notices also show why a recovery announcement needs its own date: a service can reopen while the investigation continues. Treat a public claim, an official notification and a confirmed service impact as separate facts. Exercise account recovery, supplier containment and customer communication together.

5.1 What the confirmed cases change

The cases below separate the organisation's account from claims made elsewhere. A notification can establish unauthorised access without establishing the attacker's identity, the complete data volume or subsequent misuse. Conversely, an absence of observed misuse does not undo confirmed access. Each boundary affects the response a defender should choose.

The concentration of public disclosures in September, October and November should not be read as an attack rate. Some notices describe earlier access; others document precautionary action or a regulator's later decision. The date attached to an event must say what happened on that date. Counts of potentially affected people also belong to individual cases and cannot be added into a national total.

Three distinctions matter operationally. An attempted password change is different from a successful account takeover. Access to a local legacy system is different from compromise of a whole corporate estate. Exposure of customer contact details is different from access to payment systems. The cases give defenders concrete reasons to preserve these distinctions in incident reporting.

5.2 Education, research and identity administration

CASE G

DTU's identity compromise extended beyond the initial account

DTU

confirmed

CONFIRMED	DTU's chronology starts with access to a guest identity on 15 September. It describes intercepted password resets, attacker enrolment of an authentication factor, remote access and later administrative permissions. DTU detected the incident on 20 September. Its 19 November update said more than 200,000 current or former users might be affected and that the response was complete. [S13][S53]
BOUNDARY	The notification population does not establish that every person's information was extracted. Scope changed as DTU investigated, so the latest notice matters more than the first estimate. [S13]
INTERPRETATION	Recovery channels and enrolment permissions deserve the same attention as the primary login. An additional authentication factor offers limited protection if an intruder can enrol one through an affected recovery path.
RESPONSE	The identity owner should review reset events, factor registration and privileged changes together, then revoke untrusted sessions and credentials across connected services.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

Account restoration should include an explicit check for identities created during the incident. Removing the first affected account may leave another route open. A useful exercise asks the team to reconstruct who approved each new factor and permission. The help desk should have a clear escalation route when a plausible recovery request conflicts with the account's usual behaviour.

CASE H

H

The University of Copenhagen's test environment carried production consequences

confirmed

University of Copenhagen

CONFIRMED	The University of Copenhagen detected unauthorised access on 20 October. Its notice described a configuration error in a test environment containing a user database of about 525,000 people. The database's last synchronisation was 13 January 2026. Fields varied by person and included encrypted civil registration numbers; relevant decryption material was also affected. [S12]
BOUNDARY	The university said the affected database did not contain private home addresses or health information. A later precautionary shutdown was initially reported as another attack, then corrected on 27 October. It should not be counted twice. [S12][S54]
INTERPRETATION	A non-production label does not reduce the sensitivity of copied identity data. Encryption also needs a separate assessment of where the keys or decryption material reside.
RESPONSE	The application owner should remove unnecessary personal data from test systems and isolate secrets from the datasets they protect.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

Incident communication should distinguish the age of a database from the age of the intrusion. A January synchronisation does not date the attack to January. Recovery decisions also need to consider access cards and other physical credentials when those fields appear in the affected system. The responsible teams should agree on replacement criteria before a breach requires an urgent decision.

CASE I

I

AU separated server access from unsuccessful password changes

confirmed

AU

CONFIRMED	AU reported unauthorised server access detected on 19 October. It said attempts to access or change passwords for approximately 1,700 users were unsuccessful. Its public account described containment and no current indication that confidential or sensitive information had leaked. [S14]
BOUNDARY	The account establishes server compromise and attempted account activity. It does not establish 1,700 successful account takeovers or a confirmed disclosure of sensitive records. [S14]

INTERPRETATION	A blocked action remains useful evidence of attacker intent. It should inform the investigation without becoming a successful-impact statistic.
RESPONSE	The infrastructure and identity teams should reconcile server activity with authentication logs and investigate the attempted password changes as a connected sequence.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

The practical question is which control interrupted the sequence and whether that control operates elsewhere. Defenders should preserve the evidence needed to answer it before routine rebuilding removes useful context. Communications should identify what remains under investigation while stating the observed protection clearly. This gives users a reason to follow instructions without implying that every attempted action succeeded.

J

CASE J

A college disclosure brought older access into November

Publicly reported service

reported

REPORTED	Danish reporting on 11 November described an education provider notifying approximately 44,000 current or former students and course participants. The report quoted its IT leadership and described personal information including identity and contact fields. It placed the start of access in March. [S48]
BOUNDARY	November is the disclosure date in this account. It should not become the assumed intrusion date, and a notification count is not evidence of identity fraud. [S48]
INTERPRETATION	Long retention periods can make an institution's former users a substantial part of its notification burden. Current enrolment alone is a poor guide to the people a response team may need to reach.
RESPONSE	The education provider's data owner should maintain a practicable notification route for former users and review why historical records remain accessible to active applications.

Bottom line

Validate the reported chronology, data and service scope before choosing the response.

An exercise should include records whose owners no longer use the institution's email service. The team needs a lawful, reliable way to contact them and a clear explanation of which advice applies. Identity verification for incoming enquiries should avoid collecting another unnecessary copy of sensitive information. The objective is to help affected people without creating an additional database during the response.

5.3 Public services, regulated information and customer records

CASE K

K

CPR access abused a legitimate access route

CPR

confirmed

CONFIRMED	The responsible ministry disclosed extensive unauthorised access to CPR information on 5 October. Irregularities concerned September and were discovered on the evening of 2 October. The ministry described abuse of a private company's legitimate search access, affecting information concerning approximately 8.8 million registered people. Access was stopped and the matter referred to the relevant authorities. [S15]
BOUNDARY	The population includes deceased people and people who have emigrated. It is not a count of living Danish residents. Protected names and addresses were excluded, and the notice did not identify the perpetrator. [S15]
INTERPRETATION	An authorised interface can become the route for unauthorised use. Access governance needs to assess the behaviour of entitled customers as well as outsiders.
RESPONSE	Register and service owners should review search volumes, purpose restrictions and escalation routes for abnormal use by otherwise legitimate accounts.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

Response planning should allow an operator to suspend a suspect customer quickly while preserving evidence and essential service delivery. Contracts should make investigative cooperation practical. Affected people also need advice matched to the disclosed fields. The scale of a register does not justify describing every record as an active person or implying that unrelated credentials were exposed.

CASE L

L

Mobile customer enquiries required a careful population boundary

Publicly reported service

confirmed

CONFIRMED	The mobile operator 3 disclosed a customer-information incident on 23 October. It said an affected application interface had been blocked and that names and address information might have been accessible. Its updates described investigation and customer communication. [S47]
BOUNDARY	A population of around 400,000 was under investigation. This was not confirmation that every customer in that population had data accessed. The company's account also distinguished this incident from the separate PHP vulnerability reports. [S47]
INTERPRETATION	An interface can expose customer information even when the main customer portal remains available. The permission model around individual queries needs direct scrutiny.
RESPONSE	The service owner should test object-level access controls and check whether one customer's session can retrieve another customer's records.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

Containment is easier when an interface can be disabled independently of essential customer functions. The team should also establish which logs can distinguish a possible exposure from an actual retrieval. That evidence supports more precise notifications. Customer support should have a short, consistent explanation of the affected fields and should never request an account password to discuss the incident.

CASE M

M

A dental supplier incident reached municipal residents

Lejre Municipality

confirmed

CONFIRMED	Lejre Municipality announced on 18 May that approximately 23,000 current or former residents would receive information about a supplier security breach. Its account concerned a dental service supplier and possible disclosure of names, addresses and civil registration numbers, with some telephone and email details. Children and parents were among those covered. [S45]
BOUNDARY	The notification population is not proof that every record was extracted. The notice's information fields do not justify adding a claim that treatment records were exposed. [S45]

INTERPRETATION	The customer's notification duty can remain substantial even when the technical incident occurs at a supplier. Families may receive notices concerning several people and need an intelligible explanation.
RESPONSE	Municipal service owners should agree notification responsibilities and data inventories with processors before an incident, including arrangements for children and former service users.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

The contract owner should be able to identify which local datasets the supplier holds without waiting for a commercial relationship review. A useful rehearsal asks the supplier for an affected-customer file and checks whether it can be reconciled with local records. Duplicate or confusing notices can undermine trust. One coordinated explanation should state the information involved and the action available to each recipient.

CASE N

N

A hospital building network carried staff information

Publicly reported service

confirmed

CONFIRMED	An August hospital notice described an attack on a local building network on 1 August. It said patient treatment was unaffected. Possible access concerned cardholder information, including staff identity and employment details. Approximately 7,600 current employees were notified, alongside other relevant cardholders. [S46]
BOUNDARY	The employee figure does not include every other cardholder. The notice does not establish exposure of patient records or interruption of clinical treatment. [S46]
INTERPRETATION	Building services can hold sensitive staff records while remaining outside the systems most visibly associated with healthcare. Their information inventory should be part of hospital incident planning.
RESPONSE	Facilities, security and IT owners should assess the personal data and credentials held in access-control systems and test separation from clinical services.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

The continuity plan should explain how staff enter restricted areas if electronic access is unavailable or credentials require replacement. That plan must preserve patient safety and appropriate access control at the same time. Supplier support arrangements also deserve a practical test. The hospital should know who can make an emergency configuration change and how that action will be recorded.

CASE O

Novo Nordisk distinguished copied data from core operations

confirmed

Novo Nordisk

CONFIRMED	Novo Nordisk said on 11 June that unauthorised access affected a limited part of its internal IT environment. Some non-public and personal data had been copied externally. The company described temporary shutdowns of some internal systems while stating that core business operations were unaffected. [S44]
BOUNDARY	Criminal claims concerning the incident do not establish a verified data volume, payment demand or complete scope. The company's public statement supports the narrower access and copying finding. [S44]
INTERPRETATION	Selective shutdown can support containment without implying that the entire enterprise has stopped. Accurate scope language helps operational teams prioritise their response.
RESPONSE	The incident lead should identify the affected business processes and data owners, then make containment decisions against those dependencies rather than the corporate name alone.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

Exercises should require separate answers for manufacturing continuity, employee systems and sensitive business information. A single red or green status for the whole company hides useful distinctions. Communications should identify which operations remain available and which staff processes require temporary alternatives. Investigators should preserve evidence of data movement even when restoration of the affected service is straightforward.

5.4 Contractors, acquired systems and external platforms

P

CASE P

A major construction contractor reported affected personal data

Femern Link Contractors

confirmed

CONFIRMED	Femern Link Contractors said it discovered a cyber incident on 11 October. Its 27 October update described affected systems containing personal data, isolation of servers and notification of potentially affected people. External specialists supported its investigation. [S20]
BOUNDARY	The update did not establish an attacker identity or a final quantity of affected information. It also does not support treating the incident as a confirmed compromise of tunnel control or construction equipment. [S20]
INTERPRETATION	A strategically important project can suffer an administrative information incident without evidence of an operational technology intrusion. Response requirements still extend across employers, contractors and suppliers.
RESPONSE	The project security owner should map personal-data responsibilities across contracting parties and ensure each party can receive a timely, consistent incident notification.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

Joint projects need a shared communications route before an event. The prime contractor, project owner and specialist suppliers may hold different parts of the same picture. An exercise should ask who decides whether work continues and what evidence supports that decision. It should also establish how potentially affected workers receive advice when their employer is a subcontractor.

Q

CASE Q

A supplier incident affected older public-service attachments

Publicly reported service

confirmed incident; access unknown

CONFIRMED	A public complaints body disclosed a supplier incident involving activity between 17 and 23 October. Its notice concerned attachments submitted through an earlier website during a defined period. Approximately 730 people were contacted. The current website and the actual complaint forms were outside the affected scope described in the notice. [S17]

BOUNDARY	The body could not establish whether the files had been accessed or downloaded, but could not rule it out. A possible confidentiality breach must not become a confirmed publication claim. [S17]
INTERPRETATION	Website replacement does not automatically retire the data held by the previous service. Old attachments can remain relevant after the visible application has changed.
RESPONSE	The website owner should verify deletion, migration and access arrangements for retired services, including backups and supplier-held attachments.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

The closure checklist for a replaced application should name the person responsible for its remaining data. That responsibility should survive the end of the hosting contract. During an incident, support teams need enough information to identify the affected submission period accurately. They should avoid telling all past complainants that their material was involved when the notice describes a narrower set.

R

CASE R

Maersk's inherited system needed a bounded account

Maersk

confirmed access; actor claim separate

CONFIRMED	Maersk disclosed on 11 November that a local legacy IT system from an earlier acquisition had experienced unauthorised access and data extraction. It reported no indication of impact on other systems or customer and partner interfaces. It did not anticipate disruption to customer operations. [S10]
BOUNDARY	Public reporting relayed a criminal group's data-theft and extortion claims. These remain separate from the company's account. The disclosure does not establish encryption of Maersk's global estate or disruption of shipping operations. [S10][S11]
INTERPRETATION	Acquisition integration should include an explicit decision about inherited systems, their data and their connections. A locally contained asset can still create a material disclosure obligation.
RESPONSE	The acquisition and security owners should identify retained legacy services, restrict their access and agree a retirement or support plan with a named business owner.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

An acquired system needs a current answer to three questions: who uses it, what information it retains and how it connects to the group. The incident plan should be able to isolate it without guesswork about those dependencies. Communications should describe the actual system boundary. A familiar corporate name should not turn a local finding into an unsupported global outage narrative.

CASE S

S

Hotel reservation information supported convincing payment fraud

Techotel

confirmed leak; fraud outcome unquantified

CONFIRMED	Techotel's public incident log described a reservation-information leak recognised on 7 November. Its November updates discussed investigation, customer assistance and continued suspicious messages. A 19 November entry referred to renewed leakage on 15 and 16 November. Later updates said the leak had been closed, while warning that previously copied information could still be used. [S18]
BOUNDARY	Public reporting described fraudulent WhatsApp payment requests using booking context. A convincing message is not evidence that every recipient paid, or that hotel payment systems were affected. [S18]
INTERPRETATION	Accurate reservation details can make an external fraud attempt look like an ordinary part of a hotel stay. Technical containment does not invalidate the attacker's existing copy.
RESPONSE	Hotels should warn guests through established channels and require staff to verify changes to payment instructions independently of the incoming message.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

The reservations team needs a standard response for a guest who receives a payment request. It should state how the hotel takes payment and how the guest can verify a request using a trusted contact route. Staff should preserve examples for investigation without forwarding exposed guest information widely. The warning should remain available after the immediate technical repair.

CASE T

T

One print supplier incident generated several customer notices

Publicly reported service

confirmed customer notices

CONFIRMED	November notices from two organisations described an incident at a shared print and distribution supplier. One distinguished approximately 75,000 print recipients from unaffected digital subscribers. Another described copied contact and subscription information, while excluding civil registration numbers and payment-card details from its affected dataset. [S49][S50]
BOUNDARY	These are customer-specific accounts of a supplier chain. Their populations should not be added without establishing overlap, and one customer's exclusions should not be applied to another customer's data. [S49][S50]
INTERPRETATION	Routine fulfilment services can accumulate valuable contact information across many organisations. A supplier incident may produce several public disclosures without representing several independent intrusions.
RESPONSE	Subscription and communications owners should minimise fulfilment exports and agree rapid, customer-specific incident reporting with distribution providers.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

Data minimisation should follow the actual delivery requirement. A supplier preparing postal labels does not necessarily need all fields held by the customer relationship system. The contract owner should also agree how data is deleted after each production cycle. During an incident, each customer needs its own field-level scope so that notifications remain accurate and relevant.

CASE U

U

BrickLink reopened, then returned to precautionary shutdown

BrickLink

confirmed shutdown; later data impact unknown

CONFIRMED	BrickLink's notices and public coverage described an earlier November interruption followed by reopening. Its subsequent official notice said renewed unusual activity on 19 November led it to take the platform offline again. The service remained under that shutdown at the cut-off. [S19]

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

Brickset's 12 November coverage of BrickLink's earlier statement reported access to usernames, IP addresses and a very small number of email addresses. It said no passwords or financial information were accessed. That scope concerns the earlier interruption; data consequences of the 19 November shutdown remained unresolved. [S61]

- **Boundary.** A precautionary shutdown establishes an availability impact and an investigation. It does not establish a new confirmed theft of payment information. A planned reopening date is a forecast, not a completed recovery event. [S19]
- **Interpretation.** Reopening is a decision point within an incident response. Continued monitoring and clear rollback criteria are needed even after a platform appears ready to resume service.
- **Response.** Marketplace operators should agree reopening criteria, monitor for recurrence and maintain an accessible status channel that does not depend on the affected platform.

Customers and sellers also need guidance about pending transactions and unexpected emails during downtime. The incident team should separate ordinary automated messages from requests that require verification. Repeated updates should retain a clear chronology so readers can distinguish the initial interruption, restoration and renewed precaution. This reduces the risk that an old notice is mistaken for the current service state.

CASE V

V

A provider warning did not establish customer data theft

Publicly reported service

supplier incident; customer compromise unestablished

CONFIRMED	A membership service's public update described a 16 November incident at its web-platform provider. It said the matter was handled that day and that analysis continued. The notice reported no indication that the membership service's website data had been affected. [S51]
BOUNDARY	The size of an organisation's membership is not an affected-person count. A supplier vulnerability or security incident does not establish that every customer, or this customer, suffered data extraction. [S51]
INTERPRETATION	A precautionary supplier notice deserves action even when there is no confirmed customer breach. The response should follow the customer's actual exposure and evidence.
RESPONSE	The application owner should obtain the supplier's incident timeline, confirm the affected component and version, and document the basis for its own customer-impact assessment.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

The supplier questionnaire should ask for the distinction between remediation and forensic conclusions. A patch can close a route without resolving whether it was used. The customer should keep appropriate monitoring active while that question remains open. External updates should explain the present finding accurately, without converting the provider's whole customer base into a victim population.

CASE W

W

A specialist information service found earlier access during review

Publicly reported service

confirmed

CONFIRMED	A specialist public information service disclosed on 4 November that a review had identified unauthorised access on 22 October. It described a downloaded user list concerning approximately 5,000 registered users. The fields included contact details, encrypted passwords and an occupational licence identifier. [S52]
BOUNDARY	The notice concerned the user administration of a particular service. It does not establish disruption of the wider operational functions associated with the organisation's sector. [S52]
INTERPRETATION	A later vulnerability warning can uncover an earlier incident. Discovery, access and public disclosure therefore need separate dates even when the response is prompt after discovery.
RESPONSE	The service owner should review historical access after a relevant warning, reset affected credentials and give users clear advice about reuse of the same password elsewhere.

Bottom line

Validate the confirmed account, data and service scope before choosing the response.

Specialist portals should be included in the organisation's application inventory even when their user population is relatively small. Their records may contain identifiers uncommon in general customer systems. Security teams should assess those fields directly instead of applying a generic contact-data label. The response should also ensure that affected users can reach reliable guidance without logging into the affected service.

CASE X

X

A browser dependency could alter payment destinations

Browser dependency

Official account: scope limits retained

CONFIRMED	Adform's August update dates malicious activity to 26–27 July. It says the removed code could replace cryptocurrency wallet addresses while an affected webpage was open. The company reported no further distribution after containment on 27 July. [S66]

BOUNDARY	Adform said the code was not designed to install software or persist on the device. Its later assessment could not exclude disclosure of limited browsing information on affected HTTP pages. It reported no evidence of transmission of account credentials or webpage contents. [S66]
INTERPRETATION	A third-party script can affect the browser's displayed destination even when the site's own application remains available. A clean endpoint finding alone does not answer what happened while a page was open.
RESPONSE	Website owners should identify the relevant dependency and affected period, follow the provider's incident guidance and help users verify relevant transaction destinations.

Bottom line

Separate service continuity, data scope and evidence of actual misuse.

Adform's statement and technical reporting do not establish a Danish visitor total, a verified loss figure or an actor identity. [S66][S67]

For an exercise, ask the web owner to identify which third-party services can change what a visitor sees. Then test who can suspend that dependency, communicate the affected period and verify safe return. Treat data disclosure, altered payment information and installed software as separate investigation questions.

Y

CASE Y

A retailer kept customer services running through an internal incident

Retail services

Official account scope limits retained

CONFIRMED	A department-store chain's 21 October statement says unauthorised activity detected on 18 October affected internal functions. Some stores initially used more manual working arrangements. The stores, checkout services and webshop continued operating. [S68]
BOUNDARY	The company was still establishing which customer, employee and partner information might be affected. It said customer payment-card information was outside the affected systems. Continued trading does not establish that every internal process was unaffected. [S68]
INTERPRETATION	Continuity should be measured against the business task. A working checkout can coexist with affected administrative systems and an unresolved personal-data investigation.
RESPONSE	Retail service owners should test minimum trading arrangements, staff instructions and reconciliation while internal systems are restricted.

Bottom line

Separate service continuity, data scope and evidence of actual misuse.

An exercise should make the distinction visible to management. Ask which customer tasks continue, which staff tasks need temporary alternatives and who checks transactions afterwards. Keep the operational status and the data-scope assessment separate in customer communications.

CASE Z

Z

A travel-information service separated email exposure from booking systems

Travel information

Official account scope limits retained

CONFIRMED	Travelmarket's official notice describes an incident detected on 15 January involving databases used for price alerts and newsletters. It says the accessible user information consisted of email addresses. [S69]
REPORTED	February technical reporting separately reports a January ransomware incident at the company. [S70]
BOUNDARY	The company says it does not hold users' bank, payment or booking information. Those arrangements belong to the travel provider used for the booking. An incident at the comparison service does not establish exposure at every travel company it references. [S69]
INTERPRETATION	A service's commercial relationship to a journey is different from custody of the passenger's booking and payment data. Response scope should follow the actual data flow.
RESPONSE	Travel and comparison-service owners should maintain a clear data inventory and explain which provider can answer each customer's incident question.

Bottom line

Separate service continuity, data scope and evidence of actual misuse.

The data owner should verify the affected contact lists and provide a route for suspicious messages using the company's name. The infrastructure owner should test restoration against the required customer service. Neither exercise needs to assume that the press account of the intrusion is complete.

Other reported hospitality notice

A 3 November press report quotes a restaurant's customer email about unauthorised access to email addresses at its reservation supplier. It gives no affected-person total and says payment and password exposure had not been reported. This remains a press-reported customer notice, with the organisations unnamed here. It is not evidence that the restaurant's own systems were accessed. [S71]

5.5 Recent activity: 8 to 22 November 2026

The period combines new disclosures, continuing investigations, recovery updates and enforcement activity. It should not be presented as a list of newly begun intrusions. The dates below identify the relevant public event.

Date	Date kind	Development	Defender relevance
9 November	Regulatory decision	A data-retention decision concerned access to a vehicle retailer in December 2024, discovered in January 2025. It is a recent decision about an older incident. [S23]	Review deletion schedules and prove that old records are removed.
11 November	Company disclosure	Maersk reported unauthorised access and extraction from a local inherited system. [S10]	Include acquired and legacy applications in incident ownership.
11 November	Public report	An education provider's notice concerned access reported to have begun in March. [S48]	Separate access, discovery and notification dates.
12 November	Police action announced	Danish police described removal of malicious code from 681 websites in Denmark and abroad during an international operation. [S24]	Treat this as disruption activity, not 681 Danish breach victims.
12–13 November	Customer disclosures	Organisations published notices concerning a print supplier incident. [S49][S50]	Ask suppliers for customer-specific datasets and impact boundaries.
16 November	Supplier incident date	A web-platform customer described a provider incident without evidence that its own website data had been affected. [S51]	Establish exposure before assigning an affected-person count.
19 November	Recovery update	DTU said its response was complete. [S13]	Validate restored identity controls and retain lessons from the full sequence.
19 November	Precautionary shutdown	BrickLink took its platform offline after renewed unusual activity. [S19]	Use explicit reopening and rollback criteria.
19–22 November	Continuing updates	Techotel addressed renewed leakage and the persistence of booking-related fraud risks after containment. [S18]	Keep guest verification advice active after repair.

The police operation is significant because it concerns removal of infrastructure used to deliver malicious code. Its mixed national and international website population prevents a Denmark-only victim count. Likewise, the retailer decision belongs in governance learning, while its underlying attack remains outside this report's incident window. Neither item should inflate a November intrusion total. [S23][S24]

5.6 Decisions to take from these cases

The first priority is to make identity recovery defensible. Reset channels, new authentication factors and changes in privilege need linked monitoring and a clear owner. This applies to guests and former users as well as employees. A response exercise should require the team to find secondary access created after the first compromise.

The second priority is to know where retained information lives. Test databases, retired websites, building systems and fulfilment exports all need an accountable owner. Their sensitivity follows their content. The organisation should be able to describe that content without waiting for an incident to force a reconstruction of old contracts and migrations.

The third priority is to make supplier response usable. A supplier's general statement is a starting point. Customers need their own affected fields, relevant dates and service dependencies. Contracts and exercises should make those answers available quickly. Notifications should distinguish a supplier incident from a confirmed compromise of the customer's systems.

Finally, recovery communication needs continuing attention. A reopened service can close again, and copied information can support fraud after the original route is repaired. Keep the status page current, explain what changed and give affected users one dependable verification route. Assign an owner for that communication through the end of the incident.

5.7 Current vulnerabilities: applicability before attribution

Two November advisories deserve an immediate applicability check. They describe product vulnerabilities, not evidence that Danish organisations were targeted or affected. Keep patch verification separate from investigation of possible earlier access.

Apache's advisory records CVE-2026-119618 in the HTTP/2 module. The affected upstream HTTP Server releases are 2.4.55–2.4.70; version 2.4.71 was released on 11 November. The NVD record identifies the same affected range. [S34][S35]

DKCERT's 12 November warning says HTTP/2 must be enabled and recommends prompt updating. Distribution packages can use their own versions and security updates. Validate the vendor's package status instead of deciding solely from the displayed upstream version. [S36]

Broadcom's 19 November advisory, updated on 20 November, records CVE-2026-123890 as a vCenter Directory Service authentication bypass. It requires network access to vCenter and lists no workaround. The NVD entry and vendor matrix concern the product issue; neither establishes Danish exploitation. [S37][S38]

Mandiant reported exploitation of this vCenter vulnerability in early September 2026. This does not establish exploitation in Denmark. Include that history when assessing possible earlier access. [S72]

The table identifies the relevant affected branches and remediation references.

Issue and component	Affected scope	Fixed release or route
CVE-2026-119618, Apache HTTP Server	Upstream 2.4.55–2.4.70 with HTTP/2 enabled	2.4.71; vendor package update where applicable
CVE-2026-123890, vCenter 9.1.x	Before the relevant fix	9.1.1.0200
CVE-2026-123890, vCenter 9.0.x	Before the relevant fix	9.0.2.0200
CVE-2026-123890, vCenter 8.0	Before the relevant fix	8.0 U3m
CVE-2026-123890, vCenter 7.0	Listed affected in the Broadcom matrix [S38]	Extended-support customers should contact Broadcom Support
CVE-2026-123890, packaged VMware stacks	Relevant VCF and Telco Cloud deployments in the matrix	Follow the product-specific response matrix and linked guidance

[S34][S36][S38]

The infrastructure owner should identify applicable deployments, confirm the supported remediation path and apply the update promptly. Service owners should agree recovery checks and validate that the expected build is running after the change.

Record an explicit earlier-access investigation decision. A successful update establishes the new patch state; it does not establish whether the earlier vulnerable period was free of intrusion. Preserve relevant evidence through the authorised incident process when signs warrant investigation.

Security should report three outcomes separately: systems requiring remediation, systems with verified fixes and systems needing further investigation. An unknown asset owner or unsupported branch requires an accountable exception and a resolution date.

KEY TAKEAWAYS

01

Match each response to the confirmed account, data and service scope.

02

Separate supplier events, customer notices and precautionary actions when counting incidents.

03

Preserve the distinction between intrusion, disclosure and recovery dates.

CHAPTER 06

Hacktivism, DDoS and connected systems

06

THIS CHAPTER ANSWERS

What distinguishes a disruption claim from verified service impact or a change to a physical process?

3

separate questions: availability, data access and physical impact

6.1 Timeline of claims, reporting and official assessments 55
6.2 A claim about a website needs a service answer 56
6.3 Direct announcements retain their claim limits 56
6.4 Later claims require separate evidence 57
6.5 Camera access and cooling controls need different checks 59
6.6 Threat assessments guide preparation, not retrospective counting 60
6.7 Evidence of readiness 61

CHAPTER 06

Hacktivism, DDoS and connected systems

IN SHORT

Denmark's public record contains DDoS claims, bounded outage confirmations and warnings about connected equipment. These describe different events. An inaccessible website does not establish access to internal systems, while a camera image does not establish control of an industrial process. November's cooling notices also leave Danish impact and responsibility unresolved. Verify service status, preserve local evidence and give technical, operational and communications decisions separate owners.

6.1 Timeline of claims, reporting and official assessments

The timeline distinguishes public assessments from incident confirmations. A warning date is not the date of a newly established intrusion.

13 Jan 2026	**SAMSIK** Warns about claims involving Danish surveillance cameras and urges equipment-security review [S40]
28 Jan 2026	**inteid** Published claims concerning Danish public-facing services; coalition association is self-described [S1]
2 Feb 2026	**inteid** Published a further service-related claim; outcome and operator attribution unverified [S1]
18 Feb 2026	**TjekDet** Reports a January–February DDoS campaign, with differing official accounts of service impact [S41]
27 Feb 2026	**PET, FE and SAMSIK** Publish an election-related foreign-influence threat assessment; this is not an election-outcome finding [S9]
10 Mar 2026	**SAMSIK** Assesses a high DDoS threat and calls for preparation across internet-facing services [S8]
30 Jun 2026	**SAMSIK** Warns of a heightened destructive threat, including data-wiping and operational-control risks [S42]
24 Sep 2026	**SAMSIK** Raises its destructive-cyberattack threat assessment from medium to high [S43]
2 Nov 2026	**SAMSIK** Investigates whether Danish businesses are affected by European cooling-system attacks [S25]
5 Nov 2026	**SAMSIK** Says it cannot confirm or deny the role of two groups claiming the cooling attacks [S26]

6.2 A claim about a website needs a service answer

TjekDet's February reporting describes nearly 40 websites in a campaign. Its quoted official responses differ: some services experienced outages, while others remained available to Danish users or handled the attempt without an outage. [S41]

The same reporting includes a court-service account limiting the incident to website overload, without access to underlying systems. A transport-service response separately says travel and customer data were unaffected. These are bounded statements about particular services. [S41]

Those accounts do not support 40 confirmed outages, a common intrusion route or a total for affected citizens. A claim can concern one public page while the essential service follows a different technical path.

SAMSIK's 10 March guidance broadens the preparation question beyond websites. It includes underlying internet-facing services and recommends provider agreements, updated equipment, monitoring and an exercised response plan. Its assessment of a high threat is the agency's, not an incident count. [S8]

For a service owner, the practical measure is the legitimate task. Can a person obtain information, complete a booking or reach support? Record which task failed, for whom, for how long and through which alternative route.

6.3 Direct announcements retain their claim limits

The retained material includes announcements dated 28 January and 2 February under the alias inteid. The January post describes participation in a coalition called Russian Legion. That is the author's self-description, not this report's finding about common control, nationality or state direction. [S1]

The posts refer to Danish organisations' public-facing services. Target names, identifying descriptions and service links are withheld. Their references do not establish access to operational systems, data theft or physical-process effects. A description of an organisation's business is not evidence that its business operations stopped.

The February message alleges activity against a public-facing service. A separate public chronology can establish what the organisation or a journalist reported about availability. Even a matching date does not establish that this poster caused the reported outage or that the records describe the same technical event. [S1]

Evidence card B07 28 Jan 2026

inteid Channel post Telegram RU

ORIGINAL

наносим удары по инфраструктуре Дании

TRANSLATION

We are striking Denmark's infrastructure.

Note. The post presents a coalition association as the author's self-description. Its target references concern public-facing services; no national infrastructure outcome is verified.

Held
An actor announcement alleging activity against Danish organisations and citing availability-check links.

Not established
A verified outage, data access, physical-process effect, common operator or Russian-state direction.

Evidence card B08 2 Feb 2026

inteid Channel post Telegram RU

ORIGINAL

Удар по сайту [организации]

TRANSLATION

A strike against [an organisation]'s website.

Note. The organisation name, identifying role and service links are withheld. A separate press chronology can inform the availability assessment but does not identify the operator.

Held
A further actor announcement referring to a Danish public-facing service.

Not established
Confirmed service disruption, backend access, data loss, or attribution of an independently reported outage to this poster.

Keep three observations separate: an actor published a claim, a service was observed unavailable, and an organisation confirmed its own incident scope. These propositions can support different actions. Relevant claims justify checking owned services and mitigation readiness; confirmed internal evidence determines containment and recovery.

The retained announcements do not corroborate their own escalation threats. This report omits political ultimatums and rhetorical slogans. It does not infer follow-through, a shared operator or state sponsorship from the coalition label.

The organisation-associated post context records further public-service website allegations dated 28 January and 6 April. A 3 February message also alleges internal-network, communications, design and customer-data access across public and commercial services. Those assertions remain uncorroborated. External reachability checks do not establish internal access, information loss or a common operator. [S3]

6.4 Later claims require separate evidence

Posts dated 23, 26, 27 and 28 March carry the signature NoName057(16). They allege website disruption across Danish public services and commercial organisations, including energy-sector websites. Their availability-check links remain part of the claimant's presentation. They do not establish outage duration, internal access or effects on energy supply. Spanish-language versions repeat several announcements; repetition does not add an independent witness. [S1]

One 23 March announcement refers to services in Greenland. That is the source's stated target geography. This report does not infer a position on Greenland's status, a common incident across all named services, or election interference from the post's political framing.

A separate English-language post on 28 September carries the same signature. It alleges access to an industrial control panel in Denmark and readable settings and logs. It further alleges that settings were changed and processes stopped. This is a claimed process effect, distinct from the March website claims. The retained post does not establish asset ownership, successful changes, a physical interruption or who controlled the system. The shared signature does not establish a common operator. [S1]

Evidence card B09 26 Mar 2026

NoName057(16) (posting signature) Channel post Telegram RU

ORIGINAL

DDoS-приветы получают [...] от нас сайты Дании

TRANSLATION

Danish websites are receiving DDoS greetings [...] from us.

Note. The post carries the signature NoName057(16). Target identifiers and availability-check links are withheld.

Held
A signed announcement alleging website disruption in Denmark.

Not established
Independently verified availability, outage duration, internal access, energy-supply effects, state direction or a common operator.

Evidence card B10 28 Sep 2026

NoName057(16) (posting signature) Channel post Telegram EN

ORIGINAL

We intervened a little, changed the settings and stopped the processes.

Note. The quote is an allegation in an English-language post. Target-identifying equipment details and links are withheld. The signature is not verified operator identity.

Held
A post alleging access to a Danish industrial control panel, readable settings and logs, changed settings and stopped processes.

Not established
Asset ownership, actual access, successful changes, a physical interruption, Danish intrusion, state direction or common control with the March posters.

For an operator, the September allegation warrants checking remote access, configuration-change records and process alarms against its own evidence. It does not justify announcing a confirmed operational-technology incident or attributing an interruption to the poster.

NoName057(16)

Posting signature; not verified operator identity

Signature attached to retained claims | No state direction or operator linkage established

IN DENMARK, 2026

23–28 March
Website-availability claims in retained posts

28 September
Separate industrial-control allegation in an English-language post

CLAIMED TARGETS

Source-described public-facing services, a control panel and an equipment vendor; identities withheld

3 November
Additional vendor, process and credential allegations; unverified effects

SEEN IN PUBLIC REPORTING

[S1] Own data: retained posts carry this visible posting signature; asserted effects remain unverified.

[S3] Own data: a November post carries the same visible signature; asserted process effects and credential provenance remain unverified.

OUR ASSESSMENT

The retained posts establish publication of claims. March availability claims, a separately source-labelled Greenland reference and the September process allegation remain distinct. A repeated signature does not establish common control, a confirmed intrusion or a physical effect. November material adds vendor, process and credential allegations without corroborating their effects or provenance.

CONFIDENCE
High for publication and the visible signature; asserted technical effects unverified

6.5 Camera access and cooling controls need different checks

SAMSIK's 13 January notice concerns groups claiming access to Danish camera images. The agency describes the groups as pro-Russian and recommends strengthening credentials, updating equipment and disabling unused functions. The political label remains the agency's assessment. [S40]

Do not treat a published image as a complete account of access. The operator needs to establish the equipment, account, capture time and exposure relevant to its own installation. Avoid circulating images that identify uninvolved people or locations.

The November cooling notices require a different response. On 2 November, SAMSIK said it was establishing whether Danish companies were affected. It recommended reviewing direct internet access, security updates and restrictions that preserve critical functions. [S25]

On 5 November, SAMSIK said two groups had claimed responsibility. The agency could neither confirm nor deny their involvement and considered it too early to determine their role. Repetition of the claims does not remove that uncertainty. [S26]

A post dated 3 November carries the NoName057(16) signature and alleges website disruption, refrigeration-system effects and credential exposure associated with an equipment vendor. The retained post does not establish process interruption, credential provenance or a verified internal intrusion. Language variants do not provide independent corroboration. [S3]

This allegation is separate from the agency statements. Neither the post nor its external reachability links establish which Danish installations, if any, experienced a physical effect. The report does not infer that the official investigation confirms this particular vendor allegation.

The following panel keeps each decision tied to the evidence it needs.

Question	Claim or reporting	Official boundary	Defender decision
Website impact	Campaign reporting describes many named websites [S41]	Quoted responses distinguish outages from contained attempts [S41]	Test the actual user task and record its duration
Camera access	Groups claim access to images [S40]	SAMSIK advises equipment review; no complete affected population is supplied [S40]	Validate the installation and restrict unsafe access
Danish cooling impact	Attacks are reported elsewhere in Europe [S25]	SAMSIK is establishing whether Danish businesses are affected [S25]	Check local readings and authorised maintenance records
Cooling attribution	Two groups claim responsibility [S26]	SAMSIK cannot confirm or deny their role [S26]	Contain verified exposure without assigning an unconfirmed actor

A facilities owner and an IT owner should agree who can restrict remote maintenance. The equipment contractor should explain how local control and emergency servicing continue. Check physical readings before describing spoilage, safety consequences or process manipulation.

6.6 Threat assessments guide preparation, not retrospective counting

SAMSIK's June warning identifies an increased destructive threat, including data-wiping and manipulation of operational technology. Its September assessment raises the threat level to high and judges it likely that Russia will attempt destructive cyberattacks against Denmark. Those are the agency's attributed judgements. [S42][S43]

They justify reviewing recovery and control dependencies. They do not establish that every Danish outage was destructive, that every claimant acted for a state or that the November cooling claims share an operator.

The February election assessment by PET, FE and SAMSIK also discusses foreign-influence risks and limited cyberattacks. It is a prospective assessment. This report draws no conclusion about an election result or any political decision from it. [S9]

Apply the same response discipline to any politically framed claim. Confirm the service facts, avoid repeating slogans and say which questions remain unresolved. An organisation can explain an outage without endorsing the claimant's account of its cause.

6.7 Evidence of readiness

Rehearse a public-service interruption and a separate connected-equipment incident. The exercises should use different technical and business owners. A successful website fallback does not demonstrate safe local control of equipment.

Control	Owner	Completion evidence
Service availability	Digital service and network teams	Failed user task reproduced and fallback demonstrated
Remote equipment access	Facilities and authorised contractor	Access ownership confirmed and safe restriction tested
Physical continuity	Operations	Local readings, escalation route and recovery criteria recorded
Public update	Communications and incident lead	Approved factual statement with a next-update time

KEY TAKEAWAYS

01

Verify legitimate service impact before repeating a disruption claim.

02

Keep camera access, website overload and physical-process changes separate.

03

Exercise safe remote-access restriction and a workable service fallback.

CHAPTER 07

Actors, campaigns and evidence relationships

07

THIS CHAPTER ANSWERS

Which actor associations are supported, and which conclusions would exceed the evidence?

29

Danish ransomware listings in the research window

7.1 A map of evidence relationships 63
7.2 Ransomware listings and regional context 65
7.3 The leading labels do not describe one criminal chain 66
7.4 WhiteArmor: a reported claim and a narrower company statement 68
7.5 Official assessments are not an incident attribution matrix 69
7.6 Operation Endgame and the boundary of disruption 69
7.7 What an actor name should change 70

CHAPTER 07

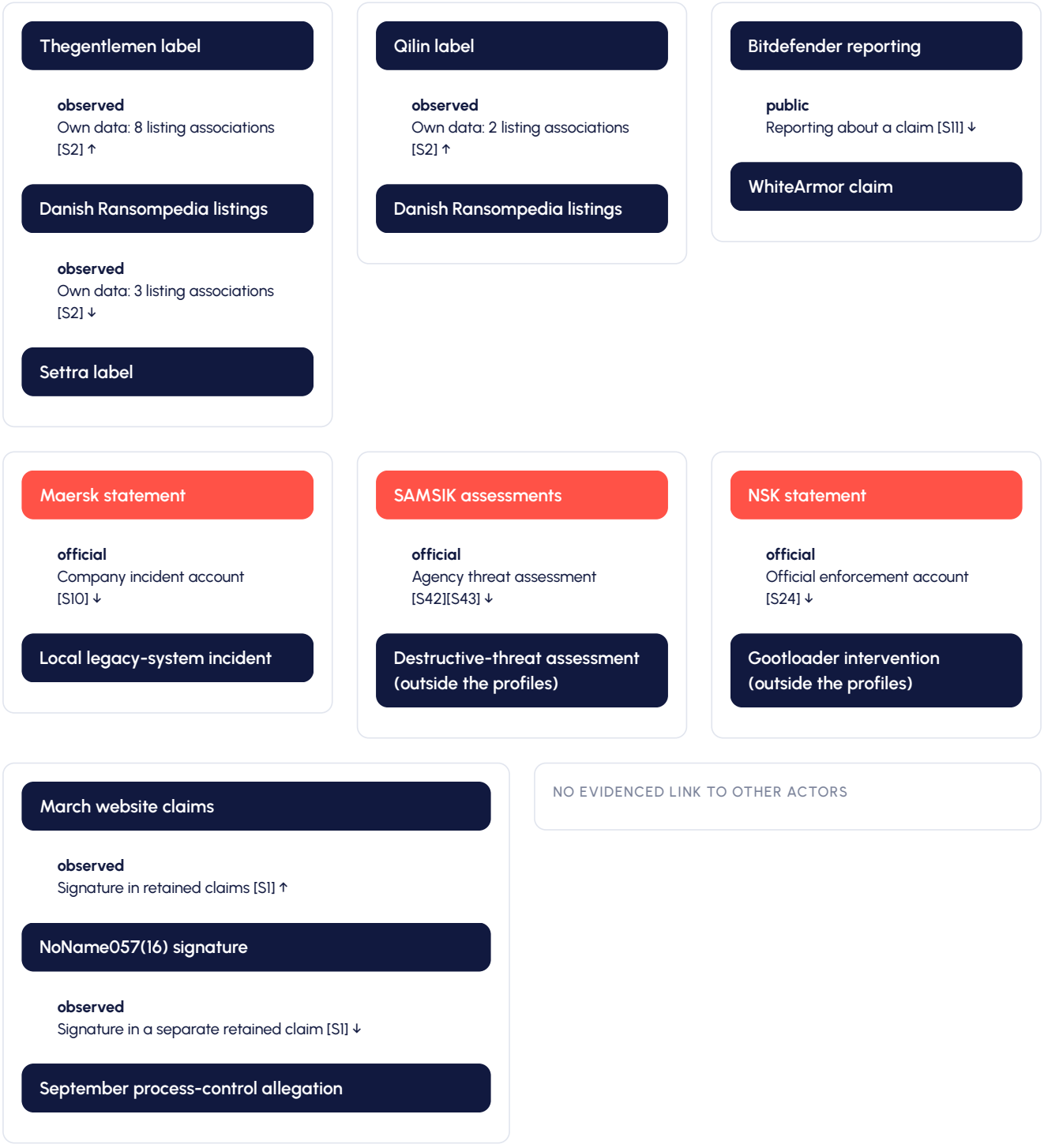
Actors, campaigns and evidence relationships

IN SHORT

Ransompedia records 29 Danish listings under 19 labels. These are criminal assertions, separate from confirmed incidents and state-threat assessments. WhiteArmor's reported claim about Maersk also exceeds the company's bounded public statement. Official enforcement reporting describes another part of the criminal environment. Use the relationship map to preserve those source boundaries, then prioritise verified exposure, service recovery and the specific accounts involved.

7.1 A map of evidence relationships

Own post Relay Official statement Public reporting Our observation



The map is an analytical model of source relationships. Each edge identifies an own-data observation, an attributed assessment or public reporting. It does not establish cooperation, shared infrastructure or common operators among the displayed groups.

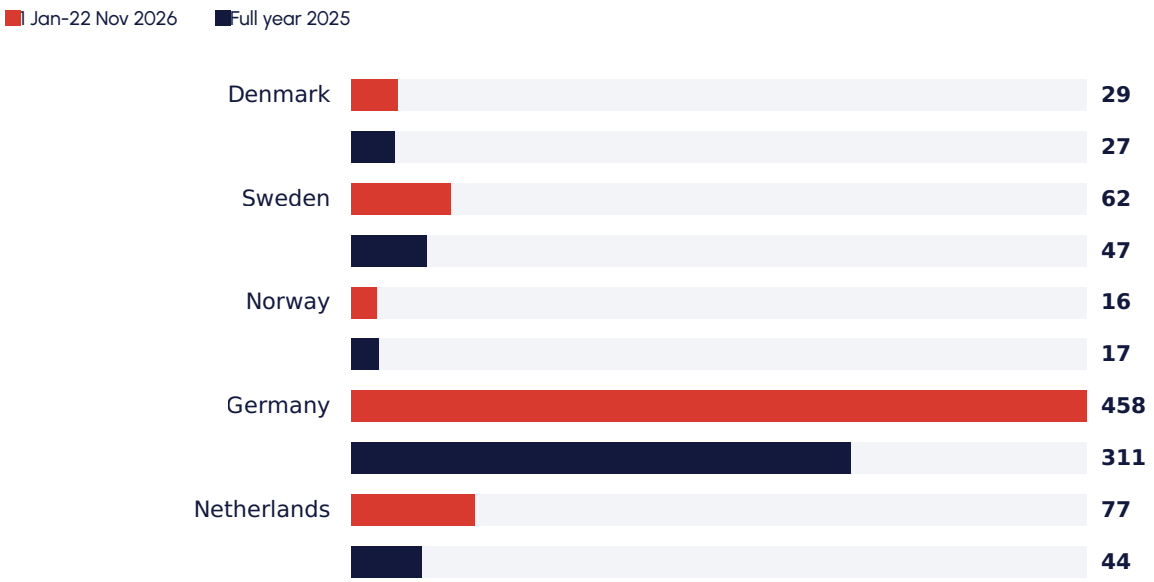
A Ransompedia edge records a listing association in Brandefense's own data. A vendor report about an actor's claim is a different relationship from a company's incident confirmation. The map keeps these edges separate. [S2][S10][S11]

The same distinction applies to official warnings. An agency's assessment of a state threat does not attribute every incident in the report to that state. No language, alias or political reference establishes nationality or state direction here.

7.2 Ransomware listings and regional context

Ransompedia records 29 Danish listings from 1 January to 22 November 2026, compared with 27 during all of 2025. The periods differ. This is a comparison of listing populations, not a matched-period growth rate. [S2]

Danish listings sit within a wider regional extortion population



Source: Brandefense Ransompedia, 1 January-22 November 2026 versus full-year 2025 [S2]. Unequal periods, different source visibility and economies; not matched-period growth or a national security ranking.

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Country	Research-window listings	What the count describes
Denmark	29	Listings carrying the Danish country label
Sweden	62	Listings carrying the Swedish country label
Norway	16	Listings carrying the Norwegian country label
Germany	458	Listings carrying the German country label
Netherlands	77	Listings carrying the Dutch country label

All figures concern the same research window. Economic scale, reporting and source visibility differ. These totals do not rank national risk, control quality or the likelihood that an individual organisation will experience an incident. [S2]

A listing does not establish encryption, data authenticity, financial loss, a completed payment or a unique victim. Related brands and repeated claims can also complicate interpretation. Use relevant listings to trigger validation through authorised organisational records.

A 22 November message in the retained posts relays an additional LockBit5 listing claim. It belongs to the post corpus, not the 29-listing Ransompedia snapshot. It is not added to that total or treated as another confirmed intrusion. [S1][S2]

7.3 The leading labels do not describe one criminal chain

Thegentlemen accounts for eight Danish listings, Settra for three and Qilin for two. Together they account for 13 of 29, or 44.8%. Sixteen further labels have one listing each. [S2]

The larger share still leaves more than half of the listing population outside those three labels. Recovery planning should therefore address extortion mechanisms and dependencies, rather than assuming one named group will define the next event.

Thegentlemen

Extortion listing label | No state or political attribution assessed

IN DENMARK, 2026

1 January–22 November
8 Danish listings in the Ransompedia snapshot

CLAIMED TARGETS

Organisations described by the listings; identities withheld

SEEN IN PUBLIC REPORTING

[S2] Own data: Ransompedia records 8 Danish listings under this label.

OUR ASSESSMENT

The listing association supports validation, recovery and disclosure readiness. It does not establish encryption, data authenticity, a common affiliate, an entry path or a completed payment.

CONFIDENCE
High for the retained listing count; underlying incident assertions remain claims

Settra

Extortion listing label | No state or political attribution assessed

IN DENMARK, 2026

1 January–22 November

3 Danish listings in the Ransompedia snapshot

CLAIMED TARGETS

Organisations described by the listings; identities withheld

SEEN IN PUBLIC REPORTING

[S2] Own data: Ransompedia records 3 Danish listings under this label.

OUR ASSESSMENT

The listing association supports validation, recovery and disclosure readiness. It does not establish encryption, data authenticity, a common affiliate, an entry path or a completed payment.

CONFIDENCE

High for the retained listing count; underlying incident assertions remain claims

Qilin

Extortion listing label | No state or political attribution assessed

IN DENMARK, 2026

1 January–22 November

2 Danish listings in the Ransompedia snapshot

CLAIMED TARGETS

Organisations described by the listings; identities withheld

SEEN IN PUBLIC REPORTING

[S2] Own data: Ransompedia records 2 Danish listings under this label.

OUR ASSESSMENT

The listing association supports validation, recovery and disclosure readiness. It does not establish encryption, data authenticity, a common affiliate, an entry path or a completed payment.

CONFIDENCE

High for the retained listing count; underlying incident assertions remain claims

A listing label can be useful for finding the relevant assertion. It does not identify an affiliate, show an entry path or demonstrate that every incident under that label used the same tools.

The defensive sequence starts with the organisation's own evidence. Establish whether the asserted data or account belongs to the organisation, whether access is current and whether containment is required. Preserve the distinction between an old record and an active session.

Recovery and disclosure readiness can proceed while attribution remains unresolved. Service owners can test restoration and privacy teams can assess data risks without waiting for the identity of the person behind a listing.

7.4 WhiteArmor: a reported claim and a narrower company statement

Bitdefender's 12 November article reports that WhiteArmor claimed responsibility for a Maersk incident and made an extortion demand. Those details are attributed reporting about the group's assertion. They are not company-confirmed actor attribution. [S11]

The WhiteArmor label also appears once among the 29 Ransompedia listings; that listing is a claim, not company confirmation. [S2]

Maersk's 11 November statement confirms unauthorised access and data extraction involving a local legacy system inherited from an earlier acquisition. Its initial findings suggested no sensitive-information disclosure and no indication of impact on other integrated systems. [S10]

The company also said it did not anticipate disruption to customer operations. That dated assessment should not become a claim that every aspect of the investigation was final. It neither confirms the claimant's complete account nor establishes the contents of the advertised material. [S10][S11]

WhiteArmor

Extortion listing label and vendor-reported claim | No state or political attribution established

IN DENMARK, 2026

11 November
Maersk publishes a bounded incident statement [S10]

12 November
Bitdefender reports WhiteArmor claiming responsibility [S11]

CLAIMED TARGETS

A reported claim about Maersk; no wider victim list inferred

SEEN IN PUBLIC REPORTING

[S2] Own data: Ransompedia records one Danish listing under this label; the listing is a claim, not company confirmation.

[S11] Bitdefender reports the group's claim and demand; Maersk did not confirm the claimant's complete account.

[S10] Maersk confirms access and extraction involving a local legacy system, with the stated limits.

OUR ASSESSMENT

Keep the reported actor claim separate from the company-confirmed system incident. Validate acquired-system ownership, relevant identities and customer communications through authorised records.

CONFIDENCE

High for the existence of the published accounts; actor responsibility not independently established

For an organisation with acquired systems, the useful question is ownership. Identify who maintains the system, which identities still reach it and what information it holds. A legacy label alone does not establish neglect or a specific technical failure.

Fraud teams should also prepare for approaches that cite a genuine public incident. Verify consequential requests through a known contact route. A message mentioning the incident does not establish that its sender holds stolen data or represents the affected company.

7.5 Official assessments are not an incident attribution matrix

SAMSIK's June and September destructive-threat assessments describe the agency's judgement about state-related risk. The September publication raises its assessment from medium to high. Their defensive relevance is continuity and recovery preparation, with attribution remaining source-specific. [S42][S43]

The January camera warning and November cooling notices are different strands. The latter expressly leaves the claiming groups' involvement unresolved. Similar political language does not connect a camera claim, a DDoS campaign and a cooling-system event. [S40][S26]

No verified country-specific technique mapping supports assigning a Danish MITRE ATT&CK matrix to these strands here. Product vulnerabilities and general actor descriptions cannot supply the missing incident evidence. Review the assets and behaviours actually described by each source.

For the SOC, an asset-specific task is more useful than an unsupported actor profile. Check relevant sign-ins, account privileges, administrative changes and recovery records against the organisation's actual architecture. Escalate confirmed anomalies through the incident owner.

7.6 Operation Endgame and the boundary of disruption

NSK's 12 November statement describes an international action against Gootloader. Authorities removed malicious code from 681 WordPress sites in Denmark and abroad. The operation also involved 218 domains and 14 servers abroad. [S24]

These figures concern different infrastructure populations. They are not 681 Danish victims, 681 completed ransomware incidents or a count of losses prevented. The authority describes the action as part of Operation Endgame. [S24]

NSK assessed that stolen passwords had enabled access to the websites. Its recommendations include reviewing administrator accounts, changing passwords, enabling multifactor authentication and updating the website software. That entry-route assessment belongs to NSK. [S24]

An affected site owner still needs to establish account control and inspect the application state. Removal of one malicious component does not establish that every earlier access path or exposed credential has been addressed.

A business receiving an enforcement-related notice should preserve the notice and assign a response owner. Establish which asset the notice concerns, what action was completed and what remains the organisation's responsibility. Record the follow-up evidence rather than assuming the operation closes the incident.

7.7 What an actor name should change

Use a name to locate evidence and authoritative guidance. Use validated technical facts to select containment and recovery actions. Attribution can remain unresolved while a current account or unsafe remote connection receives an urgent response.

Leadership should ask for the proposition, source and decision together. "A listing exists", "the company confirmed access" and "an agency assesses a threat" support different conclusions. Keeping those statements distinct protects both operational judgement and public communication.

KEY TAKEAWAYS

01

Treat listing labels as evidence associations, not verified incident outcomes.

02

Keep company confirmation separate from a reported actor claim.

03

Follow enforcement notices with asset-specific validation and recovery evidence.

CHAPTER 08

Fraud after data exposure

THIS CHAPTER ANSWERS

How can an information incident become a second incident for customers and staff?

3

decisions: verify the contact, the requested action and the receiving destination

8.1 Familiar information is not identity proof 72

8.2 Hotel and booking information can support targeted payment messages 72

8.3 Retention changes the possible harm 73

8.4 Advertising is not a measure of the fraud economy 73

8.5 Payment-card observations 74

8.6 A usable customer-protection workflow 74

CHAPTER 08

Fraud after data exposure

IN SHORT

Data exposure can make a fraudulent message more convincing without giving the sender legitimate authority. Danish notices describe this risk through personal identifiers, hotel bookings and supplier relationships. The protective response needs customer operations alongside security. Give people an independent verification route, interrupt suspicious payment changes and preserve reports that show how the fraud reached them.

8.1 Familiar information is not identity proof

Datatilsynet's advice following the CPR case separates exposure from proven misuse. It warns that a sender can know a person's name and address while still being fraudulent. That matters for organisations whose support staff regularly authenticate people through biographical questions. [S16]

The defensive consequence is a planning judgement. Review which questions a caller can answer using information already disclosed publicly or supplied to another service. An emergency process should not accept the same information as both the reason for concern and the proof that the caller is genuine.

Separate three decisions. First, establish who is contacting the organisation. Second, establish whether that person is authorised to request the action. Third, verify the account, destination or device receiving the result. A genuine supplier contact can still have an incorrect payment destination in a message.

An incident warning also needs an independent path. Direct customers to a route they can find themselves, using existing service materials. A warning that asks people to follow an unfamiliar link can resemble the fraud it is meant to prevent. Customer operations should test the message with people outside the incident team.

8.2 Hotel and booking information can support targeted payment messages

The hospitality-software notices in Chapter 5 connect a data incident with fraudulent communications. The important distinction is between closing a leak and removing every copy already obtained. A provider's containment update cannot establish that every recipient of copied information has deleted it. [S18]

A hotel should ask which reservations, customer contacts and payment instructions are implicated. It should provide a clear route for guests who receive a new payment demand. A supplier should give customers enough scope information to make that warning useful, without distributing unnecessary personal data.

Fraud and customer-service teams should share a disposition process. Preserve the message and transaction reference through authorised channels, check whether payment was attempted and tell the customer how to obtain assistance. Do not ask the customer to forward sensitive documents to an improvised mailbox.

8.3 Retention changes the possible harm

Datatilsynet's November decision concerns an earlier malicious intrusion at a vehicle retailer. It says more than 48,000 people were affected and that records concerning between 25,000 and 30,000 people should already have been deleted. Unauthorised access occurred on 30 December 2024 and was discovered on 5 January 2025; the decision is recent regulatory learning. [S22][S23]

The lesson is not that every stored record will be misused. It is that retention and deletion affect the population potentially harmed by an incident. The data owner must check whether the organisation still needs each category, and whether the implemented deletion process reaches legacy storage.

A policy and an automatic deletion function can coexist with an unmanaged archive. Completion therefore requires evidence from the actual storage locations, including inherited systems. Ask the owner to demonstrate a representative deletion and explain any lawful exception. Keep the justification and validation result in the control record.

8.4 Advertising is not a measure of the fraud economy

Underground offers can advertise identities, accounts or access. An asking price does not establish a sale, a usable account or the size of a national market. A country name in a sales menu does not establish that the seller holds working material for that country.

Chapter 4 records the retained evidence and proposition limits. This chapter does not convert those advertisements into fraud losses or customer counts. A relevant advertisement creates a validation task for the organisation; confirmed misuse requires separate evidence.

A fraud team can still use the distinction operationally. Track the claimed material, the internal evidence checked, the customer harm established and the action taken. Leave unknown fields explicitly unknown. This lets the team update the case without turning an initial claim into a confirmed event by repetition.

Danish-language offers require separate validation. A message dated 26 April addresses Danish readers and advertises compensation of 8–15k. It lists adulthood, a bank account, a payment-service account and identification as requirements. The message does not establish the currency, work performed, account control, a completed payment or criminal purpose. [S1]

This is a recruitment observation, not a confirmed money-mule case or an earnings figure. The relevant defensive question is whether someone is being asked to transfer funds, disclose credentials or hand over account control. Establish the requested action and its authorisation before assigning a fraud conclusion.

Separate messages advertise bulk SMS directed at Denmark, including custom sender identification and possible tests. Their wording establishes a marketed service, not verified delivery, a successful phishing campaign or unlawful use. The report withholds service names and contacts. [S1]

For defenders, familiar sender text should not substitute for an independent verification route. Assess an actual suspicious message, destination or account event through the organisation's fraud process. Do not turn a provider's advertising claim into an observed capability or a national fraud-volume estimate.

8.5 Payment-card observations

SCOPE OF THE CARD FIGURES

The figures describe payment-card records in the retained post corpus. They do not measure national card exposure, card theft or fraud loss.

The retained corpus contains 43 Denmark-associated payment-card records. These observations do not establish active cards, issuer losses or the total number of Danish cards exposed. [S4]

The card observations and their bounded denominator are recorded with the data summary. They do not support issuer market shares, active-card totals or a Danish loss estimate. An advertised status is the poster's statement, not a payment-network verification. [S4]

Account, card and endpoint evidence remain different populations. A customer may appear in more than one source, while an observed record can be historical. Issuers and payment-service providers should apply their own transaction and account evidence before deciding on disruptive customer action.

8.6 A usable customer-protection workflow

Trigger	First decision	Owner	Evidence of completion
Relevant data notice	Identify affected customer groups and possible misuse	Privacy and customer operations	Approved scope and plain warning
Unexpected payment request	Verify the request through a known route	Finance and customer support	Recorded verification before transfer
Account-recovery request after exposure	Check identity and authority independently	Identity and fraud operations	Recovery decision and session review
Reported attempted scam	Preserve the contact and assess actual harm	Fraud and incident response	Case disposition and customer guidance
Legacy storage found	Establish need, retention rule and deletion reach	Data owner	Documented retention decision and tested deletion

These are recommended controls, rather than claims that each affected organisation lacked them. Choose the action against the information and harm established in the particular incident.

KEY TAKEAWAYS

01

Personal knowledge can make a scam credible without establishing the sender's identity.

02

Closing a leak does not erase copied information.

03

Connect retention, customer warnings and payment verification to named owners.

CHAPTER 09

Banking and payment-service dependencies

09

THIS CHAPTER ANSWERS

Which financial-service decisions follow from exposure observations and confirmed supervision findings?

3

separate concerns: institution systems, customer fraud and shared-service continuity

9.1 Define which relationship the evidence concerns 77
9.2 Issuer domains keep their population boundary 77
9.3 Continuity findings need business ownership 78
9.4 Supplier exit must be an operational capability 78
9.5 DORA reporting is not the privacy reporting clock 78
9.6 Customer communications are part of payment security 79
9.7 Questions for the next governance meeting 79

CHAPTER 09

Banking and payment-service dependencies

IN SHORT

Financial institutions, customers and payment suppliers can be affected in different ways. A service interruption does not establish stolen card data, while a customer scam does not establish access to a bank's internal systems. The exposure view separates institution, issuer and customer-related observations. Use the official supervision findings to test continuity, supplier exits and reporting ownership, then validate relevant account and fraud alerts against internal evidence.

9.1 Define which relationship the evidence concerns

The selected banking and finance cell contains 25 candidate domains. It includes financial services and infrastructure. It is not a complete register of Danish licensed banks, a card-issuer population or a basis for comparing individual institutions. The dated exposure snapshot supplies device, credential and listing observations for this selected group. [S3]

Keep institutional access separate from customer-side fraud. An advertisement referring to a bank can concern customer accounts, a payment intermediary, a historical list or an unverified claim. None of those possibilities alone establishes an intrusion into the institution's production environment.

The same distinction applies to device observations. A financial-service domain can appear in material associated with customers as well as staff. Establish the account, endpoint and business relationship before assigning the alert. Do not label all non-employee associations as verified customer devices.

Relationship	Evidence that answers the question	Decision supported
Institution's internal systems	Authorised logs, incident evidence and relevant supplier records	Containment and operational recovery
Customer account or payment	Account ownership, transaction and verified contact evidence	Fraud intervention and customer support
Payment-service supplier	Provider scope, affected functions and continuity evidence	Fallback, reconnection and reporting
Historical account record	Current validity and earlier remediation	Proportionate account action

9.2 Issuer domains keep their population boundary

Eight of the 25 selected banking and finance domains belong to card issuers. This issuer population is not a census of Danish banks. These issuer domains have 539 non-employee device associations and 47 employee-device associations. Current credential listings concern one of these issuer domains. [S3]

The same view contains 7 card-to-issuer associations from the retained posts. These associations are distinct from the national retained total of 43 card records. They do not establish active cards, completed fraud or access to a bank's internal systems. Other card records are not assigned to a selected issuer. [S3][S4]

Identity, endpoint and fraud teams should validate their own evidence separately. A shared domain association does not establish that device material and a payment-card record describe the same person or incident. No issuer identity or issuer rating is published.

9.3 Continuity findings need business ownership

Finanstilsynet's July inspection statement describes weaknesses in a payment-service provider's ICT risk management, contingency arrangements and third-party controls. It considers those weaknesses relevant to the severity of two incidents, one in 2025 and one in May 2026. The statement does not establish ransomware or theft of payment-card data. [S21]

Its practical relevance extends beyond security operations. A restoration target must relate to the business function, and a continuity plan must show how that function continues during recovery. A successful infrastructure restart is not the same as restored payment service for every dependent customer.

The provider and each dependent institution should know who declares service restoration, who approves reconnection and who checks reconciliation. These are recommendations drawn from the supervisory findings. They are not claims that every institution sharing a supplier has the same weakness.

9.4 Supplier exit must be an operational capability

The same inspection identifies untested exit plans for critical or important suppliers. A contract termination right alone does not demonstrate that a service can move while operations continue. Dependency owners should identify the data, interfaces, specialist staff and authorisations needed for a workable exit. [S21]

Choose an exercise with a realistic business constraint. For example, assume a supplier is technically reachable but cannot provide reliable evidence about a data export. The institution must decide which functions can continue, what compensating controls apply and what evidence permits a return to normal operation.

Record unresolved dependencies rather than declaring the exercise successful because a meeting occurred. Completion evidence should show the alternative service, the people who can operate it and the reconciliation needed afterwards. A supplier assurance can inform the decision without replacing the institution's own assessment.

9.5 DORA reporting is not the privacy reporting clock

Finanstilsynet's reporting page describes initial, intermediate and final reports for major ICT incidents. It directs covered entities to the prescribed form and explains that estimates should be used where exact initial or intermediate figures are unavailable. This supports timely reporting while the investigation continues. [S31]

A personal-data incident can also require a separate GDPR assessment. The reportable population, awareness time and responsible legal entity may differ. Chapter 10 sets out the relevant clocks and exceptions. Do not copy a single 72-hour rule into every procedure.

Finanstilsynet's September insurance and pension survey calls for stronger management oversight, documented risk arrangements, skills and tested continuity. Its findings concern selected firms studied between October 2025 and March 2026. They do not measure all financial organisations' security at this cut-off. [S33]

9.6 Customer communications are part of payment security

A data incident can generate requests for a new payment destination, extra identity documents or an urgent account reset. Staff should verify both the request and the destination through an existing route. Suspicious messages should enter the fraud case process even if the underlying IT incident is already contained.

Where customers are affected, explain what the institution knows, what remains unresolved and what action is appropriate. Avoid saying that a password reset solves every kind of exposed personal information. Conversely, do not imply confirmed financial loss merely because identifying records were accessed.

9.7 Questions for the next governance meeting

Question	Accountable function	Evidence to request
Can a critical payment function continue during recovery?	Operations and technology	Demonstrated fallback and reconciliation
Can we obtain timely supplier scope information?	Third-party risk	Contracted contact and exercised notice
Can customers verify a genuine warning independently?	Fraud and customer operations	Tested communication route
Can we classify and report an ICT incident promptly?	Compliance and incident response	Timed exercise with staged reports
Can we explain every relevant account alert?	Identity and security	Owned disposition register after alert receipt

KEY TAKEAWAYS

01

Distinguish bank-system access, customer fraud and supplier interruption.

02

Test the business function and supplier exit, not only the technical restart.

03

Keep DORA and personal-data reporting decisions in the same factual chronology with separate assessments.

CHAPTER 10

Regulation and the national response

THIS CHAPTER ANSWERS

Which duties apply, who receives the report and what evidence should the incident owner preserve?

1 July 2025

commencement of Denmark's NIS 2 Act

10.1 Start with the entity and the service 81
10.2 Registration and incident reporting need separate owners 82
10.3 The NIS 2 sequence follows awareness 82
10.4 Personal-data reporting asks a different question 83
10.5 Financial ICT incidents have their own clocks 83
10.6 Supervision should change operational evidence 84
10.7 Fines and territorial scope need precise wording 84
10.8 Rehearse a reporting decision 84

CHAPTER 10

Regulation and the national response

IN SHORT

Denmark's NIS 2 Act already applies. Personal-data breaches and major financial ICT incidents have separate tests and reporting clocks. Registration, technical response and notification are different tasks. A supplier's message can require several decisions without establishing several intrusions. Establish the applicable entity and sector, preserve awareness and classification times, and rehearse the reporting route with an accountable owner and alternate.

This chapter supports incident planning, not an entity-specific legal determination. Legal and compliance owners should check the applicable law, sector rules and facts before deciding what to report.

10.1 Start with the entity and the service

The NIS 2 Act became applicable on 1 July 2025. SAMSIK's guidance identifies separate implementation for energy, telecommunications and finance. A shared business group can therefore need more than one applicability assessment. [S27][S28]

The report's sector labels do not determine legal scope. Assess the relevant legal entity, activities, size and any special inclusion or exclusion. A selected domain in Chapter 3 does not establish that its operator is an essential or important entity. [S28]

Create an applicability record.

Question	Owner	Evidence to retain
Which entity provides the affected service?	Legal and service owner	Entity, activity and contractual responsibility
Which information or operation is affected?	Incident lead	Known impact and unresolved scope
Which sector framework applies?	Compliance	Applicable text and competent authority
Who decides and submits?	CISO and legal	Named reporter, alternate and approval route

The Act contains exclusions for specified sector arrangements and equivalent EU requirements. National-security, defence, public-security and law-enforcement provisions also matter. Education or public ownership alone does not settle applicability. [S27]

A supplier outside the Act can face contractual security requirements. SAMSIK links that distinction to the security of the customer's supply chain. Separate the supplier's legal status from its customer's dependency. [S28]

10.2 Registration and incident reporting need separate owners

SAMSIK's registration guidance gives 1 October 2025 as the original deadline. An entity entering scope later must register within two weeks. Changes to submitted information generally require an updated submission within three months. [S29]

The guidance uses the national business reporting service. It distinguishes DORA entities from this registration obligation. It also explains that the selected sectors determine which competent authorities receive the submission. [S29]

Test access before an incident. The nominated reporter should know how to reach the relevant form, authenticate and obtain a receipt. An alternate should be able to continue.

SAMSIK's FAQ distinguishes sector supervision from incident handling. Sector authorities supervise their own areas; FE handles incident reports as the national CSIRT. Those functions should appear separately in the response plan. [S28]

10.3 The NIS 2 sequence follows awareness

Section 12 concerns significant incidents, including serious operational disruption, financial loss or substantial harm to others. Section 13 supplies the reporting sequence. The maximum periods do not replace the duty to report without undue delay. [S27]

Stage	General maximum	Record needed
Early warning	24 hours after awareness	Awareness time and initial assessment
Incident notification	72 hours after awareness	Severity, impact and available evidence
Interim update	On CSIRT request	Current status and changed facts
Final report	One month after notification	Cause, impact and response account

Trust-service providers have a 24-hour notification maximum. If the incident continues, the Act requires a status report followed by a final report within one month after handling. A single universal deadline would miss those exceptions. [S27]

Keep the source of each time visible. A security alert, a supplier's discovery and the organisation's awareness may be different moments. Record what was known, who assessed it and when the assessment changed.

Maintain one chronology and separate reporting decisions within it. Later updates can correct scope while preserving the first notice.

10.4 Personal-data reporting asks a different question

Datatilsynet's guidance distinguishes reporting to the authority from communicating with affected people. The controller reports without undue delay and, where feasible, within 72 hours of awareness, unless risk to people's rights and freedoms is unlikely. [S30]

A processor informs the controller without undue delay. The controller retains responsibility for its decision. Available information can be reported first and supplemented promptly; a late report needs reasons. The 72-hour period also runs during weekends and holidays. [S30]

Communication to affected people is required where high risk is likely, subject to the applicable exceptions. It must be prompt and understandable; it does not have a separate universal 72-hour deadline. Document all breaches and the reasons for reporting or withholding notification. [S30]

For a supplier event, ask which records the organisation entrusted to the service. Establish whose information is involved, what protection applied and what people can do now. A provider's restoration notice does not answer those questions.

Customer operations should receive an approved description of the established facts and a route for suspicious approaches. Privacy review and practical support should proceed together, while unconfirmed data quantities remain qualified.

10.5 Financial ICT incidents have their own clocks

Finanstilsynet's DORA guidance requires in-scope financial entities to report major ICT incidents through the designated financial-sector route. The sequence includes initial, intermediate and final reporting, with a route for reclassification. [S31]

The detailed deadlines come from Article 5 of Delegated Regulation 2025/301. Preserve both awareness and major-classification times. They start different parts of the sequence. [S32]

Stage	Requirement
Initial notification	As early as possible; within four hours of major classification and no later than 24 hours after awareness
Late major classification	If classification occurs after 24 hours, notify within four hours of classification
Intermediate report	Within 72 hours after initial notification; update promptly and when regular activities recover
Final report	Within one month after the intermediate report or its latest update

If a deadline cannot be met, inform the authority without undue delay, no later than that deadline, and explain why. The calendar allowance can move a weekend or holiday deadline to noon next working day. [S32]

That allowance excludes initial and intermediate reports from credit institutions, central counterparties, trading venues and other NIS 2 essential or important financial entities. Their final reports are not excluded by that provision. [S32]

Supervisors can also disapply the allowance for initial and intermediate reports from other significant or systemic entities, after notifying them. Keep any such decision with the entity's reporting instructions. [S32]

Finanstilsynet provides an alternative contact route when technical problems prevent the initial submission. Establish that route before the normal reporting service becomes unavailable. Preserve the submission and the acknowledgement separately. [S31]

10.6 Supervision should change operational evidence

Finanstilsynet's 23 September publication reports an examination of selected insurance and pension companies conducted between October 2025 and March 2026. It identifies improvements needed in management oversight, documented risk frameworks, skills and tested operational preparedness. [S33]

The authority requested action plans where significant deficiencies were identified. These findings concern the examined population. They do not establish that every Danish financial institution has the same deficiency or suffered an intrusion. [S33]

The practical response is to connect governance records to a service test. A board should be able to see which critical service was exercised, what failed and who owns the repair. A policy approval is a different form of evidence.

For a material supplier, ask the business owner to demonstrate a workable fallback. Record how identity, communications and customer support continue if the supplier cannot provide timely updates.

10.7 Fines and territorial scope need precise wording

Section 32 provides for fines for specified violations and permits criminal liability for legal persons. It does not state numerical fine bands in that section. Fine exposure requires the applicable Danish framework and case-specific legal assessment. [S27]

Section 34 states that the Act does not apply to the Faroe Islands and Greenland, while allowing separate activation by royal order. Organisations operating there should establish the applicable local legal position. [S27]

10.8 Rehearse a reporting decision

Use a supplier notice describing possible access to customer records while an important service is interrupted. Give the exercise team incomplete information and a later correction. This tests decisions under uncertainty without assuming the provider's first estimate is final.

Exercise decision	Accountable owner	Completion evidence
Identify entity and sector duties	Legal and compliance	Written applicability decision
Preserve awareness and classification	Incident lead	Dated chronology with reasons
Prepare the relevant notifications	Reporter and alternate	Completed exercise forms and receipt route
Explain practical customer risks	Privacy and customer operations	Approved notice and support instructions
Continue the essential service	Business and supplier owners	Demonstrated fallback and recovery criteria

Close the exercise with the unresolved questions, responsible owners and target dates. Test the alternate reporter and independent communications route. Leadership should receive the evidence of completed actions, alongside any accepted exception.

KEY TAKEAWAYS

01

Establish entity and sector scope before selecting a reporting route.

02

Preserve awareness, classification, notifications and reasons in one chronology.

03

Rehearse reporting and service continuity with an owner and alternate.

CHAPTER 11

Outlook: conditional decisions through the next quarter

11

THIS CHAPTER ANSWERS

Which preparations follow from the evidence without predicting a national attack count?

4

planning scenarios with explicit triggers and closure evidence

11.1 Key judgements and their limits 87
11.2 Scenario A: a supplier notice arrives before complete scope 88
11.3 Scenario B: an account advertisement matches a live identity 88
11.4 Scenario C: a website claim coincides with an equipment alert 88
11.5 Scenario D: copied information supports a convincing scam 89
11.6 What this report does not forecast 89

CHAPTER 11

Outlook: conditional decisions through the next quarter

IN SHORT

The evidence supports preparation for identity misuse, supplier disruption, follow-up fraud and connected-system incidents. It does not establish their future frequency or a common operator. Each scenario below has a trigger that changes the response. Assign the decision owner now, then test the relevant dependency with evidence from your own environment.

11.1 Key judgements and their limits

Confidence attaches to a proposition. A confirmed disclosure can leave the actor or entry route unresolved. A high-confidence listing count can contain unverified underlying allegations. The table separates those meanings rather than assigning one credibility label to an entire actor.

Judgement	Confidence and basis	Limit	Evidence that changes it
Identity and historical records deserve separate control reviews	High for relevance of the documented university and register disclosures	No national incident rate or common entry route established	Confirmed scope, internal access history and retention validation
Supplier information can affect continuity and customer protection at the same time	High for relevance of the hospitality and other supplier notices	Different customers may have different effects	Tenant-specific scope and demonstrated safe restoration
Extortion preparation should not depend on one actor label	High for the 19 labels in the retained 29-listing population	Listing labels do not identify unique operators	Confirmed intrusion mechanism or linked incident evidence
Public availability claims do not settle physical impact	High for the distinction in official guidance and cooling statements	A later investigation may establish a different scope	Operational logs and a dated official finding
Portfolio signals require validation by the relevant owner	High for the dated domain observations	The Atlas headline describes a selected portfolio; passive controls remain unavailable	Active-account evidence, managed-asset ownership and service context

[S1][S2][S3][S10][S12][S13][S15][S18][S25][S26]

The most useful management question is whether a new fact changes an action. A new group alias may change an intelligence note without changing recovery priorities. Confirmed use of a privileged account changes containment. A customer receiving a fraudulent payment message changes the customer-protection response even if the original system is restored.

11.2 Scenario A: a supplier notice arrives before complete scope

Planning assumption. A critical supplier reports unauthorised access and cannot yet identify every affected customer. Your service depends on an interface operated by that supplier.

Trigger. A notice identifies your tenant, account, integration or data category, or internal evidence links the event to your environment. A generic country mention alone does not meet this trigger.

Decision. The service owner and incident lead assess continued operation, temporary restrictions and evidence needed for reconnection. Privacy and compliance assess their own reporting duties using the facts available. Customer operations prepares a warning if the known data can support fraud.

Closure evidence. Record affected interfaces, the supplier's scope statement, relevant internal observations, fallback performance and the approval to restore normal operation. Restoration closes an availability question; it does not prove that copied information disappeared.

Alternative explanation. A supplier can suspend a service as a precaution without confirming customer data access. Keep the precautionary action and the confirmed exposure scope separate in communications.

11.3 Scenario B: an account advertisement matches a live identity

Planning assumption. The organisation receives a credential offer relevant to an account it owns. The post is new, but the underlying material may be old.

Trigger. Identity staff confirm the account, access scope and evidence requiring action. The post's date alone does not establish credential freshness or successful use.

Decision. Identity and incident response choose proportionate containment, including session and recovery review where warranted. The endpoint team investigates associated devices when the evidence identifies them. Customer operations receives any separately validated customer-account concerns.

Closure evidence. Preserve the alert, ownership check, validity assessment, access investigation and justified remediation. If the organisation lacks a usable alert source, record the dependency and obtain the input before measuring disposition coverage.

Alternative explanation. The advertisement may repeat previously remediated data or mislabel a shared service. A documented false or historical association is a valid outcome when supported by evidence.

11.4 Scenario C: a website claim coincides with an equipment alert

Planning assumption. An actor claims disruption while an operational team receives an alarm from connected equipment. Their timing overlaps, but a common cause is unknown.

Trigger. The operational owner observes an unauthorised state change, remote session or configuration change, or receives a relevant official warning. A screenshot of an unavailable website does not establish this trigger.

Decision. The operational owner checks safe operation and can isolate remote administration through an authorised procedure. Security preserves relevant logs. Communications distinguishes public-service availability, data access and physical-process effects.

Closure evidence. Retain the equipment state, approved configuration, remote-access review, safety decision and tested recovery. State the cause as unresolved until the investigation supports one. Do not assign a state actor from the claimant's language or political slogan.

Alternative explanation. An ordinary equipment fault and a separate availability claim can occur together. This possibility must remain open until the evidence links them.

11.5 Scenario D: copied information supports a convincing scam

Planning assumption. After a supplier or register notice, a customer reports a message containing familiar personal or booking details and a request for payment.

Trigger. Customer operations receives an actual message, attempted transaction or independently verifiable report. General concern after a news article is a reason to explain the verification route, not proof of fraud loss.

Decision. Fraud staff verify the destination, preserve the contact and establish whether money or account access is at risk. Privacy staff connects the event to the earlier scope only where the evidence supports that relationship.

Closure evidence. Record the customer's protected route, transaction disposition, communication issued and any service-control change. Avoid treating a technical restoration notice as a reason to close reports of later misuse.

Alternative explanation. A scam can use information from another source. Matching biographical details alone does not establish which incident supplied them.

11.6 What this report does not forecast

The post and listing populations do not support a future Danish incident count, an attack probability, financial loss or a market-size estimate. The selected portfolio does not establish national prevalence. Political events are not treated as causes of attacks without evidence supporting that proposition.

A new official finding, verified account use or supplier-specific scope can change these judgements. Update the incident record and action owner when it does. Preserve the earlier uncertainty rather than rewriting the original claim as if it had always been confirmed.

KEY TAKEAWAYS

01

Use conditional scenarios to choose actions, not to imply predicted incident volumes.

02

Define the evidence that changes containment, reporting or customer protection.

03

Keep alternatives open until the relevant service and account evidence resolves them.

CHAPTER 12

Action plan: owners and completion evidence

12

THIS CHAPTER ANSWERS

What should leaders require in the next 30, 60 and 90 days?

4

workstreams: identity, suppliers, continuity and reporting

12.1 The 30/60/90 plan 91
12.2 Identity and SOC teams 93
12.3 Service and operational owners 93
12.4 Privacy, legal and communications 93
12.5 Fraud, customer operations and finance 94
12.6 A management scorecard that can be evidenced 94
12.7 How Brandefense can help 95

CHAPTER 12

Action plan: owners and completion evidence

IN SHORT

Start by establishing usable alerts, service ownership and incident contacts. Then test account recovery, supplier scope and business continuity through realistic exercises. Evidence of completion should show a working decision, not only a policy or meeting. Active threats and urgent exposed vulnerabilities require immediate action; the improvement plan is not permission to wait. Assign each workstream an owner and require the evidence below.

12.1 The 30/60/90 plan

The lanes sequence programme improvements. Any confirmed active misuse, safety concern or urgent applicable vulnerability overrides this schedule. The incident lead should record the immediate action and its justification.

1Days 1–30

Establish relevant external alerts and a disposition route

OWNER	COMPLETION EVIDENCE
CISO and intelligence lead	First alert received, ownership assigned and response tested

Map critical services to identity, data and supplier dependencies

OWNER	COMPLETION EVIDENCE
Service owners and technology	Approved service map with fallback and contacts

Reconcile privileged, inactive and emergency access

OWNER	COMPLETION EVIDENCE
Identity and system owners	Access decisions and tested emergency recovery

Verify applicable reporting routes and substitute decision makers

OWNER	COMPLETION EVIDENCE
Legal, privacy and compliance	Entity-specific route map and accessible contact record

Review inherited systems and historical personal-data stores

OWNER	COMPLETION EVIDENCE
Data and technology owners	Retention purpose, owner and deletion exceptions recorded

2Days 31–60

Exercise a supplier notice with incomplete scope

OWNER

Incident response and third-party risk

COMPLETION EVIDENCE

Timed scope request, service decision and notification assessment

Restore one critical service while its normal dependency is unavailable

OWNER

Operations and recovery

COMPLETION EVIDENCE

Demonstrated fallback, safe restoration and reconciliation

Test account recovery against a convincing impersonation

OWNER

Identity and fraud

COMPLETION EVIDENCE

Impersonation refused and legitimate user restored through approved route

Test customer warnings and payment-change verification

OWNER

Customer operations and finance

COMPLETION EVIDENCE

Warning understood and destination independently checked

3Days 61–90

Exercise connected-equipment isolation with its operational owner

OWNER

Operations and security

COMPLETION EVIDENCE

Safe isolation, preserved evidence and authorised return to service

Demonstrate supplier exit for a critical dependency

OWNER

Procurement, operations and technology

COMPLETION EVIDENCE

Alternative service, data access and reconciliation demonstrated

Review alert dispositions after usable observations arrive

OWNER

Security and identity

COMPLETION EVIDENCE

Evidence-backed decisions and unresolved-input ownership

Report residual risk and overdue dependencies to management

OWNER

CISO and accountable executives

COMPLETION EVIDENCE

Accepted risk, funded action and named closure date

12.2 Identity and SOC teams

Establish the input. Agree which assets and accounts are covered by external alerts, where they arrive and who accepts them. Confirm that escalation works outside normal working hours. If no observation arrives, treat coverage as untested rather than claiming perfect validation.

Check the proposition. Separate an advertised credential, a valid account, a successful sign-in and confirmed data access. Each requires different evidence. Preserve the alert and internal findings so that later updates do not overwrite the original uncertainty.

Review recovery and sessions. Where the evidence warrants containment, inspect account recovery, privileged changes and active sessions alongside password action. Establish the endpoint owner before isolating a device. Historical material should be checked against earlier remediation.

Prioritise applicable urgent weaknesses. Identify the installed product and relevant configuration, use vendor guidance and record the corrected version or mitigation. Check for earlier access where the advisory or internal evidence warrants it. A successful update and an intrusion investigation answer different questions.

12.3 Service and operational owners

Define minimum service. Identify what must continue while the normal identity, booking, payment or administrative system is unavailable. A technical recovery target should connect to that business requirement. Test the fallback with the people who will operate it.

Control reconnection. State who can restore a supplier interface and what evidence they require. A supplier saying it is online does not automatically establish that your data scope is resolved. Record any temporary restriction and its business consequence.

Protect connected equipment. Maintain an ownership and remote-access record for controls affecting physical processes. Exercise safe isolation with the operational specialist. Do not infer physical impact from an unavailable public website or an actor's assertion.

12.4 Privacy, legal and communications

Preserve the chronology. Record detection, awareness, classification, containment, disclosure and update times separately. Explain which time starts each applicable reporting duty. Do not delay a required initial notice merely because every affected record is not yet counted.

Write to established facts. Distinguish unauthorised access, copied data, disrupted services and unverified extortion assertions. Attribute an actor label to the source that makes it. Say what remains unresolved and give the next update time.

Use proportionate public detail. Explain what people need to do without publishing unnecessary identifiers or repeating the claimant's rhetoric. A useful warning gives a known contact route, relevant protective action and a clear statement of its limits.

12.5 Fraud, customer operations and finance

Verify requests and destinations. Require a known route for changed payment instructions, account recovery and requests for identity documents. A caller's knowledge of names, booking details or addresses does not establish authority.

Keep reports open after restoration. Copied information can remain useful for scams. Give customers a route to report suspicious contacts and assess actual attempted or completed harm. Connect the report to an earlier incident only when the evidence supports the link.

Test understandable warnings. Ask a person outside the incident team to follow the warning and locate the verification route. Remove unnecessary jargon. A warning should reduce risky decisions without asking the recipient to trust an unfamiliar contact.

12.6 A management scorecard that can be evidenced

Management question	Target by day 90	Evidence to inspect
Are relevant alerts reaching an owner?	A working route with a first tested receipt	Alert and escalation record
Can we explain actions on relevant identity signals?	Each received material alert has a disposition or an owned dependency	Case register and validation evidence
Can critical services continue through a supplier outage?	Exercised fallback for the prioritised service	Business demonstration and reconciliation
Can we meet the applicable reporting duties?	Entity-specific exercise completed with corrections closed	Timed chronology and submission drafts
Can customers verify a genuine request?	Known route tested with customer operations	Communication test and fraud workflow
Do legacy records have an accountable owner?	Prioritised stores reviewed and exceptions approved	Retention decision and deletion validation

These are proposed governance targets, not measured results for Danish organisations. Management should choose the priority service and accept any residual dependency explicitly. The objective is a decision that can be demonstrated during an incident.

12.7 How Brandefense can help

Brandefense offers threat intelligence, dark-web monitoring and external attack-surface capabilities. A useful demonstration should follow one owned asset from an external observation through validation, assignment and closure. Ask how the alert reaches the team and which evidence supports the decision. [S39]

The report does not promise that a tool prevents every incident or that an advertisement establishes access. The operating value depends on relevant coverage, accountable owners and a response process that distinguishes claims from confirmed findings.

Request a Brandefense demonstration.

KEY TAKEAWAYS

01

Establish usable inputs and accountable owners before measuring response performance.

02

Test the service, recovery route and supplier decision with business participants.

03

Require evidence of closure while treating active threats and urgent weaknesses immediately.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Scope and evidence boundaries · Appendix B. Evidence-card register · Appendix C. Sources · Appendix D. Glossary

76
sources

Appendix A. Scope and evidence boundaries 97
Appendix B. Evidence-card register 100
Appendix C. Sources 102
Appendix D. Glossary 106

Appendix A. Scope and evidence boundaries

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

A.1 Window and date meanings

The report's requested window is 1 January–22 November 2026 by post time. Recent activity covers 8–22 November 2026. Public incident dates follow the source: occurrence, detection, disclosure and later updates are distinguished. A publication during the recent window does not establish a new intrusion during that window.

The research uses retained underground posts, public extortion listings, a selected domain portfolio, official notices, organisational disclosures and supporting press or technical reporting. Each population has a separate unit. Their totals cannot be added to produce a national incident count. [S1][S2][S3]

The public-source record includes material in Danish, English, Russian and Turkish. Source availability and archive coverage differ. The report does not certify the absence of incidents in a month, at a selected organisation or on a service that has no confirmed disclosure.

A.2 Posts, advertisements and case dossiers

A post is a retained message. It may contain an advertisement, a reply, a news relay, an actor claim, a country reference or unrelated material. A country association does not establish targeting, the location of the underlying system or the nationality of the poster. [S1]

The six underground dossiers are selected examples that support different validation decisions. They are not a representative sample of Danish incidents or criminal activity. Several messages can concern one allegation. Similar wording supports an advertising association without establishing identical files, a completed transaction or common control.

Authentic excerpts retain bracketed redactions. They describe what a poster said, with the date and venue recorded beside the card. The report does not publish working credentials, personal rows, criminal contact details or identifiers of unconfirmed targets. A quotation does not turn the underlying allegation into a confirmed event.

A public disclosure and a post about that disclosure can describe the same event. A news relay does not independently corroborate the report it repeats. Likewise, a short reply does not establish a purchase or a successful download. Claims remain bounded when they appear in summaries, cards, tables and recommendations.

A.3 Extortion listings and peers

Ransompedia's dated snapshot contains Denmark-associated listings and the four peer populations for Sweden, Norway, Germany and the Netherlands. Listing dates fall within the requested window. The previous-year figures cover all of 2025, so they are not matched-period baselines. [S2]

A listing records a criminal assertion. It does not establish encryption, exfiltration, payment, financial loss or the exact date an intrusion began. Country and industry labels describe the listing population. They are not legal ownership findings or nationally representative sector samples.

Group labels do not identify unique operators. Several labels may involve overlapping people or services, but that relationship is not inferred without concrete evidence. No country ranking, population-adjusted attack probability or measure of control effectiveness follows from the peer figures.

A.4 Selected-domain portfolio and exposure observations

The selected portfolio contains 250 candidate domains in ten groups of 25. Selection reflects service and sector relevance. It is not an official top-company list or a probability sample. Brands, subsidiaries and shared services can overlap, and a domain does not necessarily represent an independent legal entity. [S3]

Atlas supplies the national headline of 45/100 (B) for the selected portfolio. Credentials were listed for sale for 37 of 250 domains when checked. Sector tables publish signal counts only. No organisation or sector rating is published. Device and credential associations can overlap and do not establish current account validity. [S3]

Device, credential, document and current-listing observations were read on 22 November 2026. Annual mention observations were read on 23 November 2026 and end on 18 November 2026. Similar-name context covers 19 October–18 November 2026. Passive-control observations remain unavailable, so no hygiene index or mail-policy finding is published. Domain resolution alone does not validate ownership or establish a security condition.

The validation workflow connects observations to accountable internal checks. It identifies the first check, owner and completion evidence for an observation if one is received. A reader should obtain relevant alerts and confirm the service relationship before deciding on remediation or notification.

The organisation-associated post context is a separate evidence population from the Chapter 4 reading corpus and the payment-card observations. It supplies dated allegations, not additional confirmed incidents. Its records are not added to the reading-corpus figures or ransomware-listing totals. [S3]

In c03, `orgs_listed_for_sale_now` counts selected domains with current credential offers. It does not count independent organisations, advertisements or organisations offered for sale.

A.5 Public confirmation and attribution

Official confirmation attaches to the proposition actually stated by the organisation or authority. It can establish access while leaving the actor, entry route, amount copied or operational impact unresolved. A supplier's confirmation does not establish identical effects at every customer.

An organisation is named only where official confirmation and broad public reporting support the incident description. Other cases use general service or sector labels. When a source identifies a withheld target, the public reference protects that identity as well as the narrative. Victim-owned source addresses are omitted.

State attribution remains the cited authority's assessment. Language, political framing, geography or an alias does not establish nationality, sponsorship or common control. The relationship map records source relationships; it does not imply that otherwise unconnected actors cooperate.

A.6 Payment-card scope

SCOPE OF THE CARD FIGURES

The figures describe payment-card records in the retained post corpus. They do not measure national card exposure, card theft or fraud loss.

Observed records, advertised statuses and asking prices do not establish active cards, completed purchases or issuer losses. Card, account and device observations remain separate populations. No national fraud-market estimate is derived from them. [S4]

A.7 Confidence and decisions

Evidence label	What it supports	Principal limit
Observation	The retained source contains the stated message or record	Underlying contents and consequences can remain unverified
Actor claim	A poster or listing asserts the described activity	Successful access, provenance and loss need separate evidence
Official confirmation	The issuing organisation or authority confirms the stated scope	Its account can be provisional or leave attribution unresolved
Analyst inference	A reasoned interpretation or planning consequence	Alternatives and the evidence that changes it remain explicit

Confidence is attached to a proposition, not a person or group. The recommended action should match the established evidence. A validated historical or inaccurate association can justify closure, while unresolved evidence needs an owner and a next validation step.

Appendix B. Evidence-card register

The cards record selected retained advertisements. Their dates are message dates, and their aliases identify posting labels rather than verified people. Cards B01–B06 appear with Chapter 4 dossiers; the remaining cards appear with Chapter 6 claims. [S1]

Card	Date	Venue	Alias	Language	Dossier
B01	2026-07-02	Forum	thejackal101	English	A: repeated credential description
B02	2026-09-12	Forum	K0d3x	English	B: financial-customer allegation
B03	2026-10-14	Forum	MrData	English	C: community-data allegation
B04	2026-08-24	Forum	Bitcoins	English	D: development-system allegation
B05	2026-11-05	Forum	marlowfinch42	English	E: regional build-system offer
B06	2026-01-04	Forum	selluk	English	F: directory-themed offer
B07	2026-01-28	Telegram	inteid	RU	Chapter 6 claim
B08	2026-02-02	Telegram	inteid	RU	Chapter 6 claim
B09	2026-03-26	Telegram	NoName057(16) (posting signature)	RU	Chapter 6 claim
B10	2026-09-28	Telegram	NoName057(16) (posting signature)	EN	Chapter 6 claim

Named public cases and supporting coverage

The following source pairs support public naming for the specific incident description. They do not clear unrelated allegations or identify unconfirmed downstream victims.

Public case	Official account	Supporting reporting
DTU	[S13][S53]	[S55]
University of Copenhagen	[S12]	[S56]
AU	[S14]	[S57]
CPR incident	[S15]	[S58]

Public case	Official account	Supporting reporting
Mobile operator 3	[S47]	[S65]
Lejre Municipality	[S45]	[S63]
Novo Nordisk	[S44]	[S64]
Femern Link Contractors	[S20]	[S59]
Maersk	[S10]	[S11]
Techotel	[S18]	[S60]
BrickLink	[S19]	[S61]
Adform	[S66]	[S67]
Travelmarket	[S69]	[S70]

Appendix C. Sources

S1: Odin by Brandefense. Retained Denmark-associated underground posts, 1 January–22 November 2026. Own-source evidence; no public address. Verified on 23 November 2026.

S2: Ransompedia. Denmark and four regional peer listing snapshot, 1 January–22 November 2026. Own-source evidence; no public address. Verified on 23 November 2026.

S3: Odin by Brandefense. Selected Danish domain portfolio, Atlas exposure observations and organisation-associated post context. Own-source evidence; no public address. Verified on 23 November 2026.

S4: Odin by Brandefense. Payment-card observations in the retained post corpus. Own-source evidence; no public address. Verified on 23 November 2026.

S5: SAMSIK. Digital sikkerhed i virksomheder 2026. https://samsik.dk/publikation/digital-sikkerhed-i-virksomheder-2026/ Verified on 24 November 2026.

S6: SAMSIK. SAMSIK/CFCS transition. https://samsik.dk/artikler/2025/03/center-for-cybersikkerhed-er-en-del-af-styrelsen-for-samfundssikkerhed/ Verified on 23 November 2026.

S7: FE. FE current cyber role. https://www.fe-ddis.dk/da/arbejdsomrade-a/Cybertruslen/ Verified on 23 November 2026.

S8: SAMSIK. DDoS-angreb: Hvad er det, og hvordan beskytter man sig mod dem?. https://samsik.dk/artikler/2026/03/ddos-angreb-hvad-er-det-og-hvordan-beskytter-man-sig-mod-dem/ Verified on 23 November 2026.

S9: PET, FE and SAMSIK. Fremmede stater kan forsøge at påvirke folketingsvalget. https://samsik.dk/artikler/2026/02/fremmede-stater-kan-forsoege-at-paavirke-folketingsvalget/ Verified on 23 November 2026.

S10: Maersk. Maersk official incident. https://www.maersk.com/news/articles/2026/11/11/it-security-incident Verified on 23 November 2026.

S11: Bitdefender. Maersk WhiteArmor claim coverage. https://www.bitdefender.com/en-us/blog/hotforsecurity/whitearmor-gang-cyberattack-maersk Verified on 23 November 2026.

S12: University of Copenhagen. KU incident and FAQ. https://www.ku.dk/orientering-om-bruddet-paa-persondatasikkerheden Verified on 23 November 2026.

S13: Technical University of Denmark. DTU incident latest update. https://dtu.dk/english/about/contact/it-information Verified on 23 November 2026.

S14: AU. AU official incident notice. https://medarbejdere.au.dk/nyheder/nyhed/artikel/au-har-vaeret-udsat-for-hackerangreb Verified on 24 November 2026.

S15: Ministry responsible for the population-register notice. CPR unauthorised access statement. https://fudm.dk/aktuelt/pressemeddelelser/2026/oktober/omfattende-uautoriseret-adgang-til-borgeres-cpr-oplysninger/ Verified on 23 November 2026.

S16: Datatilsynet. CPR-sagen: Det kan du gøre, hvis du er bekymret for dine personoplysninger. https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2026/okt/cpr-sagen-det-kan-du-goere-hvis-du-er-bekymret-for-dine-personoplysninger Verified on 23 November 2026.

S17: Public-sector body. Supplier-related personal-data notice, 30 October; update 4 November 2026. Article URL withheld; source notice read. Verified on 23 November 2026.

S18: Techotel. Techotel operational log. https://techotel.dk/operation/?page=target Verified on 23 November 2026.

S19: BrickLink. BrickLink latest official recovery. https://maintenance.bricklink.com/recovery.html Verified on 23 November 2026.

S20: Femern Link Contractors. FLC official update. https://femernlinkcontractors.com/update-on-the-cyber-incident/ Verified on 23 November 2026.

S21: Finanstilsynet. Payment-service provider IT inspection, 10 July 2026. https://www.finanstilsynet.dk/ (article URL withheld) Verified on 23 November 2026.

S22: Datatilsynet. Autoforhandler får alvorlig kritik for manglende sletning: announcement. https://www.datatilsynet.dk/ (article URL withheld) Verified on 23 November 2026.

S23: Datatilsynet. Datatilsynet vehicle-retailer decision. https://www.datatilsynet.dk/ (article URL withheld) Verified on 23 November 2026.

S24: NSK. NSK Gootloader intervention. https://politi.dk/national-enhed-for-saerlig-kriminalitet/nyhedsliste/skadelig-kode-fjernet-fra-over-600-hjemmesider/2026/11/12 Verified on 23 November 2026.

S25: SAMSIK. SAMSIK cooling advisory. https://samsik.dk/artikler/2026/11/styrelsen-for-samfundssikkerhed-foelger-sagen-om-cyberangreb-mod-koele-og-frysesystemer-i-europa/ Verified on 23 November 2026.

S26: SAMSIK. SAMSIK cooling actor caution. https://samsik.dk/artikler/2026/11/samsik-opmaerksom-pa-pro-russiske-hackergrupper-tager-ansvar-for-cyberangreb/ Verified on 23 November 2026.

S27: Retsinformation. NIS2 statutory text. https://www.retsinformation.dk/eli/lta/2025/434/pdf Verified on 23 November 2026.

S28: SAMSIK. Spørgsmål og svar om NIS 2. https://samsik.dk/nis2/faq/ Verified on 23 November 2026.

S29: SAMSIK. Registrering af enheder efter NIS 2-loven. https://samsik.dk/nis2/registrering-nis2/ Verified on 23 November 2026.

S30: Datatilsynet. Kort fortalt: Håndtering af brud på persondatasikkerheden. https://cdn.datatilsynet.dk/datatilsynet/Media/639292218536950571/kort-fortalt_haandtering-af-brud-paa-persondatasikkerheden.pdf Verified on 23 November 2026.

S31: Finanstilsynet. DORA incident reporting. https://www.finanstilsynet.dk/finansielle-temaer/tilsyn-med-ikt-og-datasikkerhed/indberetning-af-ikt-relaterede-haendelser-i-henhold-til-dora Verified on 23 November 2026.

S32: European Commission. Delegated Regulation (EU) 2025/301, Article 5. https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng Verified on 23 November 2026.

S33: Finanstilsynet. Finanstilsynet DORA findings. https://www.finanstilsynet.dk/nyheder-og-presse/nyheder-og-pressemeddelelser/2026/sep/undersoegelse-af-forsikrings-og-pensionssektorens-implementering-af-dora-forordningen Verified on 23 November 2026.

S34: Apache Software Foundation. Apache HTTP Server 2.4 security advisories. https://httpd.apache.org/security/vulnerabilities_24.html Verified on 23 November 2026.

S35: NVD. CVE-2026-119618 record. https://nvd.nist.gov/vuln/detail/CVE-2026-119618 Verified on 23 November 2026.

S36: DKCERT. Apache HTTP/2 warning, 12 November 2026. https://cert.dk/news/2026-11-12/Kritisk-Apache-HTTP2-saarbarhed-giver-mulighed-for-fjernafvikling-af-kode Verified on 23 November 2026.

S37: NVD. CVE-2026-123890 record. https://nvd.nist.gov/vuln/detail/CVE-2026-123890 Verified on 23 November 2026.

S38: Broadcom. VMSA-2026-0009.1, response matrix. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/VMSA-2026-0009--VMware-vCenter--Tools--and-SDDC-Manager-updates-address-multiple-vulnerabilities--CVE-2026-123890--CVE-2026-123891--CVE-2026-123892--CVE-2026-123893--CVE-2026-123894-/39495 Verified on 24 November 2026.

S39: Brandefense. Platform demonstration. https://brandefense.io/request-a-demo/ Verified on 23 November 2026.

S40: SAMSIK. SAMSIK camera warning. https://samsik.dk/artikler/2026/01/opfordring-husk-sikkerheden-paa-overvaagningskameraer/ Verified on 23 November 2026.

S41: TjekDet. DDoS campaign primary journalism. https://www.tjekdet.dk/indsigt/danske-virksomheder-og-myndigheder-udsat-omfattende-hackerangreb Verified on 23 November 2026.

S42: SAMSIK. SAMSIK June destructive warning. https://samsik.dk/publikation/skaerpet-trussel-fra-destruktive-cyberangreb/ Verified on 23 November 2026.

S43: SAMSIK. SAMSIK September high threat. https://samsik.dk/publikation/destruktive-cyberangreb-september-2026/ Verified on 24 November 2026.

S44: Official issuer. Novo Nordisk official incident. https://www.novonordisk.com/content/nncorp/global/en/news-and-media/news-and-ir-materials/news-details.html?id=916571 Verified on 23 November 2026.

S45: Official issuer. Lejre official dental-supplier notice. https://lejre.dk/alle-nyheder/2026/maj/brud-paa-datasikkerheden-brev-paa-vej-til-beroerte-borgere Verified on 23 November 2026.

S46: Regional health authority. Hospital building-network incident notice. Article URL withheld; source notice read. Verified on 23 November 2026.

S47: Official issuer. 3 Denmark official notice. https://via.ritzau.dk/pressemeddelelse/15244429/3-undersoger-sikkerhedshaendelse-med-kundeoplysninger?publisherId=13561616 Verified on 24 November 2026.

S48: Press publisher. Education-provider incident report quoting institutional leadership. https://presse-fotos.dk/ (article URL withheld) Verified on 23 November 2026.

S49: Publishing customer. Print-distribution supplier incident: customer notice, 12 November. Article URL withheld; source notice read. Verified on 23 November 2026.

S50: Subscriber organisation. Print-distribution supplier incident: customer notice, 13 November. Article URL withheld; source notice read. Verified on 23 November 2026.

S51: Membership-service organisation. Web-platform provider incident and customer-impact boundary. Article URL withheld; source notice read. Verified on 23 November 2026.

S52: Specialist public information service. User-administration incident notice, 4 November. Article URL withheld; source notice read. Verified on 23 November 2026.

S53: Official issuer. DTU attack chronology. https://dtu.dk/english/about/contact/it-information/timeline-of-the-cyberattack Verified on 23 November 2026.

S54: Press publisher. KU second-attack correction. https://ni.dk/ni-news/id/1fac113d-1481-48d1-b6d3-2505eeef8180/K%C3%B8benhavns-Universitet-var-alligevel-ikke-udsat-for-nyt-cyberangreb Verified on 23 November 2026.

S55: Ritzau. DTU national-wire press. https://www.dkteknikogmiljoe.dk/ritzau/359ff96b-88ab-44f6-bd48-4a7f1312c07a Verified on 23 November 2026.

S56: TechRadar. KU broad press. https://www.techradar.com/pro/security/over-525-000-hit-in-massive-university-of-copenhagen-data-breach Verified on 23 November 2026.

S57: Ritzau. AU Ritzau coverage. https://ni.dk/ni-news/id/01f6c003-4349-46fe-a1f8-ba2ba8342961/ Verified on 24 November 2026.

S58: ITPro. CPR incident coverage. https://www.itpro.com/security/data-breaches/danish-data-breach-everything-we-know-about-the-cyber-attack-that-hit-8-8m-danes Verified on 23 November 2026.

S59: Tunnelling Journal. FLC industry press. https://tunnellingjournal.com/cyber-incident-hits-fehmarnbelt-tunnel-contractor/ Verified on 23 November 2026.

S60: Forbrugerpenge. Techotel follow-on fraud. https://forbrugerpenge.dk/spar-penge/hotelgaester-falske-betalingskrav-whatsapp-datalaek/ Verified on 23 November 2026.

S61: Brickset. BrickLink back online, 12 November 2026. https://brickset.com/article/136115/bricklink-back-online Verified on 23 November 2026.

S62: IETF. RFC 9989: Domain-Based Message Authentication, Reporting, and Conformance (DMARC). https://datatracker.ietf.org/doc/html/rfc9989 Verified on 23 November 2026.

S63: DK Nyt. Lejre public coverage. https://www.dknyt.dk/artikel/data-fra-23-000-borgere-i-lejre-kan-vaere-hacket Verified on 23 November 2026.

S64: Reuters / Cinco Días. Novo Nordisk Reuters report republication. https://cincodias.elpais.com/companias/2026-06-17/novo-nordisk-sufre-un-ciberataque-por-un-grupo-de-hackers-que-pide-215-millones-por-los-datos-robados.html Verified on 23 November 2026.

S65: Press publisher. Mobile provider national-wire coverage. https://www.dknyt.dk/ritzau/5d07abc3-2dd0-48c9-a1cf-d55e5f7fbdf3 Verified on 23 November 2026.

S66: Adform. Security incident: update 5 August, timings added 7 August 2026. https://site.adform.com/resources/newsroom/security-incident-company-update Verified on 23 November 2026.

S67: SANS NewsBites. Adform incident coverage, issue 58, 7 August 2026. https://www.sans.org/newsletters/newsbites/xxviii-58 Verified on 23 November 2026.

S68: Company statement via Ritzau. Department-store internal IT incident and continuing customer operations, 21 October 2026. https://via.ritzau.dk/ (article URL withheld) Verified on 23 November 2026.

S69: Travelmarket. Information om säkerhetsincident hos Travelmarket. https://www.travelmarket.se/blog/sakerhetsincident-travelmarket/ Verified on 23 November 2026.

S70: Digi.no / Version2. Travelmarket incident reporting, 14 February 2026. https://www.digi.no/hacking/beryktet-hackergruppe-snublet-i-krypteringen/2946179 Verified on 24 November 2026.

S71: Nyhed24. Restaurant customer notice concerning a reservation supplier, 3 November 2026. https://nyhed24.dk/ (article URL withheld) Verified on 23 November 2026.

S72: Mandiant. ARMORY CASTLE Exploits vSphere, 20 November 2026. https://cloud.google.com/blog/topics/threat-intelligence/armory-castle-exploits-vsphere Verified on 23 November 2026.

Appendix D. Glossary

Term	Plain meaning
Account recovery	The authorised process for restoring legitimate access after a problem
Authentication	Checking an identity before granting access
Authentication bypass	A flaw allowing an unauthorised party to avoid an intended identity check [S37]
Awareness time	When the relevant entity knows enough about an incident to begin the applicable assessment
Build system	A service that prepares software for testing or release
CFCS	Centre for Cyber Security, whose former responsibilities were divided between current functions [S6][S7]
Claimant label	The name attached to a criminal assertion; it does not identify a verified person
Combolist	A combined list of account names and passwords from different sources
CPR	Denmark's civil registration system; an identifier is not proof of a caller's authority [S16]
CSIRT	A computer-security incident response team; FE performs the Danish national NIS2 function [S7]
Data controller	The party deciding why and how personal information is processed
Data processor	A party processing personal information on a controller's behalf
Data retention	Keeping information for a justified purpose and period, followed by appropriate deletion
DDoS	Distributed traffic intended to overwhelm an online service [S8]
DMARC	Email policy and reporting connecting sender-domain alignment with authentication results [S62]
DORA	EU rules for digital operational resilience of covered financial entities [S31][S32]
Endpoint	A device or system at the edge of a managed environment
Extortion listing	A criminal publication asserting a claim about an organisation
FE	Forsvarets Efterretningstjeneste, with the cyber functions described in its current guidance [S7]

Term	Plain meaning
GDPR	EU data-protection framework, including separate breach-reporting and communication duties [S30]
IAM	Identity and access management: administering accounts and the permissions they receive
ICT	Information and communication technology
MFA	Authentication that requires more than one type of factor
NIS2	EU cybersecurity directive implemented through national obligations for in-scope entities [S27]
OT	Technology monitoring or controlling physical processes
Phishing	Deceptive contact intended to obtain information or induce an unsafe action
Ransompedia	Brandefense's ransomware-listing source; listings record claims
SAMSIK	Styrelsen for Samfundssikkerhed, the Danish Resilience Agency [S6]
Session	A period of authenticated access that can need separate review after account concerns
Signing key	Cryptographic material used to create digital signatures that support checks of content origin and integrity
Smishing	Phishing delivered through text messages
Supplier exit	Moving away from a supplier while preserving the required service
TLP:CLEAR	Information may be shared without restriction, subject to other applicable duties
VPN	A controlled network connection used to reach services remotely

About this report

Prepared by Odin by Brandefense for security leadership, service owners, incident responders, fraud teams, privacy officers and communications teams. Version 1.0 covers the requested window of 1 January–22 November 2026, with recent activity shown for 8–22 November.

The findings distinguish retained observations, actor claims, official confirmation and analyst inference. The report's selected portfolio does not estimate national prevalence. Missing observations remain unavailable rather than implying zero exposure.

The Danish edition is translated from the English master. The English edition prevails where meanings differ.

© 2026 Brandefense. All rights reserved.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO