BRANDEFENSE COUNTRY REPORT · DENMARK 2026

Brandefense Rapport om Danmarks cybertrusselslandskab 2026

Identitet, fælles data og driftskontinuitet i en forbundet økonomi

Odin by Brandefense

Undersøgelsesperiode: 1. januar–22. november 2026

Version 1.0 · Offentlig forskningsudgave · TLP:CLEAR · 8.–22. november 2026

37 af 250

udvalgte domæner havde legitimationsoplysninger annonceret til salg ved kontrollen

6

sager, der skelner mellem annoncer, dataenes oprindelse og påstået adgang

29

danske ransomwareopslag i undersøgelsesperioden

3

særskilte forhold: institutionssystemer, kundesvindel og kontinuitet i fælles tjenester

INDHOLD

Indhold

Translated with AI

Denne udgave er oversat med AI fra den engelske originaltekst. Ved forskelle har den engelske udgave forrang.

01	Sammenfatning	05
	Rapportkort	09
02	Danmarks digitale og institutionelle kontekst	10
03	Eksponering af udvalgte domæner og valideringsprioriteter	14
04	Aktivitet i undergrundsmiljøer: Hvad de bevarede opslag viser	21
05	Hændelser og kampagner	35
06	Hacktivisme, DDoS og forbundne systemer	56
07	Aktører, kampagner og evidensforbindelser	64
08	Svindel efter dataeksponering	73
09	Bankers og betalingstjenesters afhængigheder	78
10	Regulering og den nationale indsats	82
11	Udsigter: betingede beslutninger i næste kvartal	88
12	Handlingsplan: ansvar og afslutningsdokumentation	93
A	Bilag A. Omfang og evidensgrænser	101
B	Bilag B. Evidenskortregister	104
C	Bilag C. Kilder	106
D	Bilag D. Ordliste	110
	Om rapporten	112

Bestyrelse og direktion	01 05 11 12
CISO og tjenesteansvarlige	03 04 05 09 12
SOC- og efterretningsteams	04 06 07 B
Svindelbekæmpelse og kundeservice	05 08 09
Jura, databeskyttelse og kommunikation	05 06 10 12

Om denne udgave

Oversat med AI. Ved forskelle mellem udgaverne har den engelske udgave forrang.

Udarbejdet med AI-assistance. Datagrundlag, tilskrivning og begrænsninger fremgår ved resultaterne.

Danmarks dokumenterede hændelser forbinder identitet, leverandører, historiske oplysninger og væsentlige tjenester. Sikkerhedsansvarlige skal træffe særskilte beslutninger om adgang, kopierede oplysninger, fortsat drift og skade på kunder.

29

ransomwareopslag knyttet til Danmark; kriminelle påstande [S2]

19

aktørbetegnelser i denne samling af opslag; ikke unikke operatører [S2]

37 / 250

udvalgte domæner med legitimationsoplysninger annonceret til salg ved kontrollen [S3]

4

beslutninger for ledelsen med ansvarlige ejere

Indhold og læseveje

Kapitel	Spørgsmål
1 Sammenfatning	Hvilke beslutninger kræver først ledelsens opmærksomhed?
2 Kontekst	Hvilke danske driftsforhold ændrer disse beslutninger?
3 Eksponering af udvalgte domæner	Hvad kan de ansvarlige validere, og hvilke observationer mangler?
4 Aktivitet i kriminelle miljøer	Hvad dokumenterer de bevarede annoncer og opslag?
5 Hændelser og kampagner	Hvad bekræftede organisationer og myndigheder faktisk?
6 Hacktivisme, DDoS og forbundne systemer	Hvordan adskiller offentlige påstande sig fra driftsmæssige følger?
7 Aktører og forbindelser	Hvilken kilde understøtter hver tilskrivning eller forbindelse?
8 Svindel efter eksponering	Hvordan kan kopierede oplysninger føre til en ny hændelse?
9 Banker og betalinger	Hvordan adskiller kunde-, institutions- og leverandørrisici sig?
10 Regulering	Hvilket anvendelsesområde, hvilken modtager og hvilken frist gælder?
11 Udsigter	Hvilke betingede scenarier begrunder forberedelse?
12 Handlingsplan	Hvem handler, og hvad dokumenterer afslutningen?
Bilag A–D	Evidensgrænser, kortregister, kilder og definitioner

KAPITEL 01

Sammenfatning

01

DETTE KAPITEL BESVARER

Hvilke resultater begrunder øjeblikkelige beslutninger for danske organisationer?

29

ransomwareopslag i den ønskede periode, hvert med en påstand

Fire beslutninger for ledelsen 07

Året i tal 07

KAPITEL 01

Sammenfatning

KORT FORTALT

Danske offentliggørelser viser, hvordan identitetssystemer, historiske oplysninger og fælles leverandører forbinder sikkerhedshændelser med daglig drift. Novemberopdateringer tilføjer adgang til ældre systemer, bookingrelateret svindel og driftsafbrydelser. Ransompedia registrerer 29 danske opslag under 19 aktørbetegnelser. Påstandene er adskilt fra bekræftede offentliggørelser og eksponeringsobservationer. Validér identitetsrelateret evidens, afprøv leverandørafhængige tjenester, og giv kunder en kendt kanal til at kontrollere mistænkelige henvendelser.

Rapporten kombinerer bevaret Brandefense-materiale fra kriminelle miljøer og ransomwareopslag med kildeverificerede offentliggørelser, myndighedsadvarsler og lovtekster. Opslag, tilbud, påstande, underrettede personer og domænerelationer er forskellige populationer. De lægges ikke sammen til et nationalt antal angreb. [S1][S2][S3]

Den ønskede observationsperiode er 1. januar–22. november 2026 efter opslagstidspunkt. Offentlige sager bruger kildernes datoer og skelner mellem indtrængen, opdagelse, offentliggørelse og senere opdateringer. Oversigten for 8.–22. november fremhæver nye oplysninger uden at omdøbe tidligere indtrængen til nye angreb.

1. Identitetsinfrastruktur kræver kontrol ud over adgangskoden. DTU's offentliggjorte tidslinje beskriver en gæstekonto, efterfølgende fjernadgang, administratorrettigheder og dataudtræk. KU beskriver en særskilt hændelse med identitetsdata. AU, et dansk universitet, beskriver forsøg på adgangskodeændringer, som ikke lykkedes. Det er forskellige forhold, som kræver forskellige beslutninger om inddæmning og kommunikation. [S12][S13][S14][S53]

2. En leverandørhændelse kan kræve flere kundebeslutninger. Meddelelser inden for tandpleje, udgivervirksomhed og hotelbranchen vedrører forskellige afhængigheder. Én leverandørhændelse kan føre til flere kunders offentliggørelser. Hver kunde skal fastslå sit datamæssige omfang, sin driftsstatus og sine indberetningspligter, før genopretning eller underretning besluttes. [S18][S45][S49][S50]

3. Kopierede oplysninger kan bestå efter den tekniske inddæmning. Datatilsynets CPR-råd forklarer, hvordan kendte personoplysninger kan understøtte overbevisende svindel. Meddelelser fra hotelbranchen beskriver falske betalingsanmodninger med bookingoplysninger. Lukning af en adgangsvej dokumenterer ikke, at kopierede oplysninger er forsvundet. Kundebeskyttelse hører til i hændelseshåndteringen. [S16][S18]

4. Novembers maritime hændelse kræver en afgrænset beskrivelse. Maersk bekræftede uautoriseret adgang og dataudtræk fra et lokalt ældre system. Virksomheden oplyste, at intet tydede på påvirkning af andre systemer eller integrerede kundesystemer, og forventede ingen afbrydelse af kundernes drift. Aktøridentitet, annonceret datamængde og løsesum er særskilte påstande i omtalen. [S10][S11]

5. Afpresningsbetegnelser understøtter bred forberedelse frem for antagelser om én aktør. De 29 bevarede opslag har 19 betegnelser. Otte bruger Thegentlemen, tre Settra og to Qilin; seksten andre har ét hver. Den delvise 2026-periode adskiller sig fra de 27 for hele 2025. Ingen af populationerne dokumenterer bekræftet indtrængen, kryptering eller tab. [S2]

Fire beslutninger for ledelsen

1. **Giv identitetsalarmer en ansvarlig modtager.** Modtag relevante observationer, bekræft ejerskab og gyldighed, undersøg sessioner og gendannelsesveje efter behov, og gem afgørelsen (§3, §12).
2. **Afprøv tjenesten og dens leverandørafhængighed.** Identificér forretningsfunktion, dataansvarlig, berørt grænseflade og alternativ drift. Kræv dokumentation for gentilslutning med en navngiven forretningsansvarlig (§5, §9).
3. **Beskyt mennesker efter en datameddelelse.** Giv ansatte og kunder en uafhængig kontrolkanal for anmodninger om betaling, kontogendannelse og identitetsdokumenter. Gem indberetninger om senere misbrug (§8).
4. **Afprøv de rette indberetningsfrister.** Fastslå juridisk enhed, omfang, kendskabstidspunkt, klassifikation og modtagere. Behandl NIS2, GDPR og DORA som særskilte vurderinger med én fælles faktuel tidslinje (§10).

Året i tal

29
Ransomwareopslag knyttet til Danmark i den ønskede periode

HVAD DET IKKE MÅLER
Bekræftet indtrængen eller unikke ofre

19
Aktørbetegnelser knyttet til disse opslag

HVAD DET IKKE MÅLER
Unikke personer, operatører eller tilknyttede aktører

27
Opslag knyttet til Danmark for hele 2025

HVAD DET IKKE MÅLER
Et sammenligningsgrundlag for samme periode

8 / 3 / 2
Opslag under Thegentlemen / Settra / Qilin

HVAD DET IKKE MÅLER
Bekræftet succes eller en fælles adgangsvej

250
Udvalgte kandidatdomæner i ti grupper

HVAD DET IKKE MÅLER
Selvstændige juridiske enheder eller national udbredelse

525.000
Omtrentligt antal brugere i KU's berørte database

HVAD DET IKKE MÅLER
Bekræftet svigagtig brug eller antal aktive studerende

Mere end 200.000
Potentielt berørte brugere i DTU's seneste meddelelse

HVAD DET IKKE MÅLER
Et verificeret antal downloadede registreringer

4.071
Besvarelser i den officielle undersøgelse af virksomheders sikkerhed, indsamlet i 2025

HVAD DET IKKE MÅLER
Et antal hændelser i 2026

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

Legitimationsoplysninger blev annonceret til salg for 37 af de 250 udvalgte domæner ved kontrollen. Den nationale Atlas-vurdering er 45/100 (B). Mindst 141.187 enhedsrelationer og 2.039.476 relationer til legitimationsposter kræver særskilt validering. De overlappende signaler dokumenterer ikke bekræftede indtrængninger. Passive kontrolresultater mangler fortsat. [S3]

HOVEDPOINTER

01

Adskil annoncer, påstande i opslag og bekræftede offentliggørelser før handling.

02

Forbind de ansvarlige for identitet, leverandører og kundebeskyttelse i samme indsats.

03

Kræv fungerende kontinuitets- og indberetningsdokumentation med tydeligt ansvar for manglende input.

Rapportkort

Tolv kapitler, fem læseveje. Følg den beslutning, du ejer; evidensgrænserne følger resultaterne.

Bestyrelse og direktion	Finansier prioriteter og afprøv væsentlige tjenester	Gå til 1 5 11 12
CISO og tjenesteansvarlige	Validér relevant eksponering og afhængigheder	Gå til 3 4 5 9 12
SOC- og efterretningsteams	Skeln mellem observation, påstand og tilskrivning	Gå til 4 6 7 Bilag B
Svindelbekæmpelse og kundeservice	Forebyg skade efter eksponering af oplysninger	Gå til 5 8 9
Jura, databeskyttelse og kommunikation	Anvend det rette omfang og den rette frist	Gå til 5 6 10 12

Evidensbetegnelserne er **observation**, **aktørpåstand**, **officiel bekræftelse** og **analytikerslutning**. En observeret annonce er fortsat en påstand om det annoncerede materiale. En bekræftet hændelse kan efterlade aktør, adgangsvej og fuldt dataomfang uafklaret.

Kapitel	Hvad læseren bør få med
Kontekst	Et kort over tjenester og indberetninger frem for en antaget enkelt myndighed
Eksponering	Daterede eksponeringsobservationer, national Atlas-vurdering og ansvarlig validering
Kriminelle miljøer	Sporbare eksempler uden antaget salg, aktualitet eller vellykket adgang
Offentlige hændelser	Særskilte tidslinjer for opdagelse, offentliggørelse og håndtering
Tilgængelighed og aktører	Kildespecifik tilskrivning og forskellige driftsmæssige følger
Svindel og banker	Særskilte beslutninger for kunde, institution og leverandør
Regulering	Enhedsspecifikke underretningsbeslutninger og dokumenteret kendskab
Udsigter og handling	Betingede udløsere, ansvarlige ejere og dokumentation for afslutning

KAPITEL 02

Danmarks digitale og institutionelle kontekst

02

DETTE KAPITEL BESVARER

Hvilke driftsforhold ændrer de beslutninger, danske organisationer skal træffe?

4.071

virksomhedsbesvarelser bag den officielle undersøgelse af virksomheders sikkerhed, indsamlet i 2025

2.1 En nyere publikation kan beskrive en tidligere population 11

2.2 Det tidligere CFCS og den nationale CSIRT har forskellige roller 11

2.3 Digital identitet skaber ansvar ud over loginsiden 12

2.4 Politisk indramning er en kildepåstand, ikke en genvej til tilskrivning 12

2.5 Hold populationerne adskilt 13

KAPITEL 02

Danmarks digitale og institutionelle kontekst

KORT FORTALT

Danske offentliggørelser forbinder identitet, fælles data, leverandører og daglig levering af tjenester. Officielle publikationer bruger forskellige perioder og ansvarsområder. En novembervurdering kan beskrive sidste års undersøgelse, mens en nyere tilsynsafgørelse kan vedrøre tidligere indtrængen. Forskellene ændrer både prioriteter og indberetningspligter. Kortlæg tjeneste, data, juridisk enhed og kompetent kontakt, før en hændelse begynder.

2.1 En nyere publikation kan beskrive en tidligere population

SAMSIK offentliggjorde Digital sikkerhed i virksomheder 2026 den 6. november. Den beskriver svar indsamlet i 2025 fra 4.071 virksomheder med mindst ti ansatte. Hovedbudskabet er, at fire ud af ti SMV'er mangler grundlæggende sikkerhedsforanstaltninger. Det er undersøgelseskontekst, ikke en målt indtrængningsrate for 2026. [S5]

Det praktiske spørgsmål er, om en kontrol virker i organisationens faktiske arbejdsgange. En adgangskodepolitik viser ikke, hvordan support godkender gendannelse. En sikkerhedskopi viser ikke, om en afhængig tjeneste kan fungere under genopretning. En leverandøraftale fastslår ikke, hvem der kan stoppe et dataudtræk.

Rapporten behandler derfor sikkerhed og fortsat drift som forbundne ansvarsområder. En konto kan forblive teknisk gyldig efter ejerens fratrædelse. Et ældre system kan beholde forretningsdata efter et opkøb. Et offentligt websted kan svigte, mens driftssystemer fortsætter. Kapitel 5 og 6 skelner mellem tilstandene med de relevante offentliggørelser.

Dette er en analytisk fortolkning af de dokumenterede sager. Den hævder ikke, at alle danske organisationer har samme systemer, kontrolmangler eller angrebsvej. Ledelsen bør bruge sagerne til at vælge valideringsspørgsmål for egne tjenester.

2.2 Det tidligere CFCS og den nationale CSIRT har forskellige roller

SAMSIK's meddelelse fra marts 2025 siger, at Center for Cybersikkerhed blev en del af Styrelsen for Samfundssikkerhed. Det forklarer, hvorfor ældre CFCS-materiale optræder sammen med aktuelle SAMSIK-publikationer. Ændringen gør ikke enhver teknisk eller lovbestemt funktion til SAMSIK's ansvar. [S6]

FE's side, opdateret den 2. oktober 2026, angiver, at situationscenteret varetager den nationale CSIRT-funktion for NIS2. SAMSIK's NIS2-vejledning beskriver særskilt sektormyndighedernes tilsynsrolle. Hændelsesplaner skal skelne mellem rådgivning, teknisk koordinering, lovpligtig indberetning og efterforskning. [S7][S28]

Formål	Relevant kanal	Dokumentation
Cybersikkerhedsrådgivning	SAMSIK og relevant sektormyndighed	Vurderet anvendelsesområde og modtaget rådgivning
NIS2-hændelseskoordinering	Kompetent myndighed og FE's CSIRT via foreskrevet kanal	Indsendelse, tidslinje og opdateringer
Vurdering af persondatabrud	Datatilsynet	Risikovurdering, underretningsbeslutning og kvittering
Finansiel IKT-hændelse	Finanstilsynet under relevant regelsæt	Klassifikation og trinvise rapporter
Mistanke om kriminalitet	Politiet og relevant cyberkriminalitets-funktion	Bevaret evidens og anmeldelsesdoku-mentation

Kanalerne kan vedrøre samme hændelse uden at være udskiftelige. Et tilsyn kan behøve en juridisk vurdering, før en teknisk undersøgelse er afsluttet. Politiet kan behøve materiale, som ellers overskrives under genopretning. Udpeg en ansvarlig for hvert formål frem for at antage, at én kontakt løser alle pligter.

2.3 Digital identitet skaber ansvar ud over loginsiden

Universitets- og registersagerne i kapitel 5 vedrører forskellige populationer og datatyper. Den fælles lære er, at identitetsinfrastruktur også indeholder historiske relationer. Registreringer kan omfatte tidligere studerende, ansøgere, ansatte, kontaktpersoner og mennesker, som ikke længere bruger tjenesten.

Den informationssikkerhedsansvarlige bør fastslå, hvilke identiteter der stadig giver adgang. Den dataansvarlige bør fastslå, hvorfor historiske oplysninger bevares. Kundeservice bør vide, hvordan en ægte advarsel når den berørte. Spørgsmålene er forskellige, selv når én platform indeholder alle oplysninger.

Et kendt navn, en adresse eller en identifikator kan gøre svindel overbevisende. Datatilsynets CPR-råd advarer om, at kendskab til personoplysninger ikke bekræfter en opkalders identitet. Indsatsen bør derfor omfatte en uafhængig kontrolkanal frem for at stole på opkalderens viden. [S16]

2.4 Politisk indramning er en kildepåstand, ikke en genvej til tilskrivning

PET, FE og SAMSIK offentliggjorde en valgrelateret trusselsvurdering i februar. Beskrivelserne af udenlandsk påvirkning er myndighedernes vurderinger. De dokumenterer ikke, at en bestemt afbrydelse ændrede et valgresultat, eller at ethvert politisk indrammet opslag var statsstyret. [S9]

Rapporten tager ikke stilling til Grønland, Rusland, NATO, Israel/Gaza, religion, koranafbrændinger, valg eller regeringsbeslutninger. Hvor emnerne optræder i en kilde, bevares kun den tilskrivning, der er nødvendig for at forstå cybermaterialet. En aktørs sprog eller slogan dokumenterer ikke nationalitet eller støtte.

Sikkerhedsansvarlige kan forberede sig på politisk indrammede tilgængelighedspåstande uden at tilslutte sig aktørens forklaring. Udløseren er relevant aktivitet mod organisationen eller dens afhængigheder, understøttet af en dateret kilde. Den er ikke en antagelse om, at en offentlig beslutning forårsagede et angreb.

2.5 Hold populationerne adskilt

Opslag, afpresningspåstande, offentliggørelser, tilsynsafgørelser og eksponeringsrelationer besvarer forskellige spørgsmål. De kan ikke lægges sammen til et nationalt antal angreb. En tilsynsafgørelse kan beskrive en tidligere hændelse. En leverandørmeddelelse kan berøre mange kunder uden at dokumentere særskilt indtrængen hos hver.

Det samme gælder landesammenligninger. Svenske, norske, tyske og nederlandske opslag har samme undersøgelsesperiode, men økonomier og kildedækning er forskellige. Kapitel 7 bruger dem til at beskrive den bevarede samling. Det estimerer ikke landenes relative sikkerhed eller kontrollernes virkning.

Sammenligningslandene er udelukkende valgt som eksempler for at give kontekst; de indebærer ingen rangordning eller politisk vurdering.

HOVEDPOINTER

01

Læs observationsperioden sammen med udgivelsesdatoen.

02

Adskil SAMSIK's rådgivning, FE's tekniske koordinering og sektorernes indberetningspligter.

03

Verificér relevant tjeneste- og identitetsevidens, før politisk indramning fortolkes.

KAPITEL 03

Eksponering af udvalgte domæner og valideringsprioriteter

03

DETTE KAPITEL BESVARER

Hvilke observerede eksponeringssignaler kræver en ansvarlig indsats?

37 af 250

udvalgte domæner havde legitimationsoplysninger annonceret til salg ved kontrollen

3.1 Populationskort 15

3.2 Den nationale Atlas-vurdering beskriver denne portefølje 16

3.3 Enheder og legitimationsposter kræver forskellig validering 17

3.4 Giv forskellige observationer forskellige ansvarlige 19

3.5 Passive kontroller kræver deres egen nævner 19

KAPITEL 03

Eksponering af udvalgte domæner og valideringsprioriteter

KORT FORTALT

Legitimationsoplysninger blev annonceret til salg for 37 af de 250 udvalgte organisationsdomæner ved kontrollen. Porteføljens nationale Atlas-vurdering er 45/100 (B). Observationerne omfatter mindst 141.187 enhedsrelationer og 2.039.476 relationer til legitimationsposter. De beskriver overlappende eksterne signaler, ikke bekræftede indtrængninger eller unikke personer. Passive kontrolresultater mangler fortsat. Validér aktuelle konti, undersøg relationer til medarbejderenheder, og udpeg den relevante tjeneste- eller dataansvarlige.

3.1 Populationskort

Punkt	Definition
Udvalgt population	250 organisationsrelaterede domæner i ti grupper med 25 poster pr. gruppe
Udvælgelse	Relevans for offentlige tjenester, erhverv og samfund; ingen officiel rangliste over store virksomheder
Enhed	Et udvalgt domæne tilknyttet en institution, et driftsbrand eller en koncern
Uafhængighed	Brands, datterselskaber, fælles operatører og underdomæner kan overlappe
Ejerskab	Domæneopløsning fastslår ikke aktuelt juridisk ejerskab eller tjenesteansvar
Eksponeringsøjebliksbillede	Observationer af enheder, legitimationsposter, dokumenter og aktuelle tilbud læst 22. november 2026
Andre perioder	Årlig omtale frem til 18. november 2026; lignende navne fra 19. oktober til 18. november 2026
Passive resultater	Intet fuldstændigt datasæt om mailpolitikker, DNS, certifikater eller webkontroller

[S3]

Den observerede nævner er 250 udvalgte domæner. Den fastslår ikke 250 selvstændige juridiske enheder eller national udbredelse. Ejerskab og tjenesteansvar skal bekræftes, før en observation henføres til en organisation. Relaterede tjenester og koncernbrands kan dele poster.

En aktuel annonce giver grund til at validere den relevante konto. Den dokumenterer ikke gennemført salg, fungerende legitimationsoplysninger eller uautoriseret adgang til organisationens interne systemer. Historiske poster og observationstidspunkter skal holdes adskilt.

3.2 Den nationale Atlas-vurdering beskriver denne portefølje

Den nationale Atlas-vurdering er 45/100 (B). Højere værdier angiver større observeret eksponering i den udvalgte portefølje. Vurderingen understøtter valideringsprioriteter. Den er ikke en brudprocent, hændelsessandsynlighed, kontrolcertificering eller sikkerhedsrangliste for Danmark. [S3]

45/100 (B)

national Atlas-vurdering for den udvalgte portefølje med 250 domæner [S3]

Kun den nationale Atlas-vurdering offentliggøres. Sektorrækkerne viser signaltællinger og observerede nævnere. Bank og finans omfatter finansielle tjenester og infrastruktur; gruppen er ikke et fuldstændigt register over banker med tilladelse eller kortudstedere.

Udvalgt gruppe	Domæner	Domæner med aktuelle legitimationstilbud	Dokumenter	Lignende navne
Offentlig administration	25	1	73	4.039
Regionale og lokale tjenester	25	1	64	1.167
Bank og finans	25	2	22	13.991
Forsikring og pension	25	2	35	1.388
Universiteter og forskning	25	6	57	7.175
Industri og teknologi	25	4	267	476
Energi og infrastruktur	25	1	6	6.486
Transport og logistik	25	6	413	483
Forbrugertjenester og kommunikation	25	14	564	25.357
Sundhed og biovidenskab	25	0	18	816
ALLE	250	37	1.519	61.378

[S3]

Aktuelle tilbudsobservationer har en defineret nævner af udvalgte domæner



Aktuelle legitimationstilbud efter sektor (koral). Hver nævner er 25 udvalgte domæner; aktuel adgang eller gennemført salg er ikke fastslået. Kilde: Odin by Brandefense, 250 udvalgte domæner, eksponeringsøjebliksbillede 22. november 2026 [S3]. Relationer kan overlappe og omfatte historiske poster; de er ikke unikke personer eller bekræftede indtrængninger.

Dokumenttallet registrerer relationer, ikke fortrolige filer eller bekræftede offentliggørelser. Observationer af lignende navne dokumenterer ikke ondsindet registrering, brandefterligning eller phishing. De ansvarlige skal fastslå relevans og faktisk misbrug før anmodning om indgreb.

Kategorierne kan overlappe inden for og på tværs af domæner. Tallene kan ikke lægges sammen til et estimat over unikke hændelser, personer, konti eller artefakter. En sektor uden observerede tilbud har ingen bekræftet vurdering af sikker drift.

3.3 Enheder og legitimationsposter kræver forskellig validering

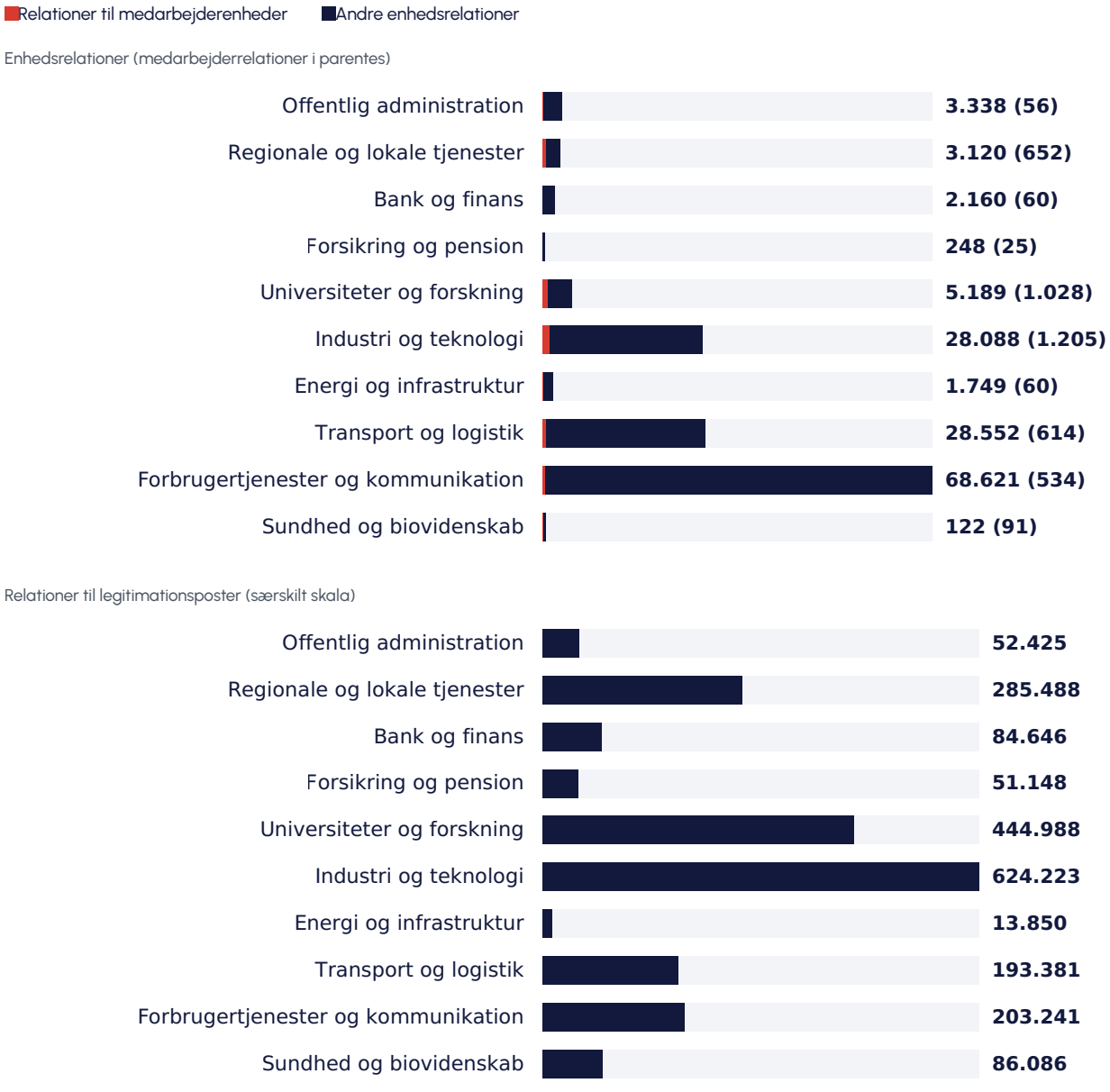
Øjebliksbilledet indeholder mindst 141.187 enhedsrelationer, herunder 4.325 relationer til medarbejderenheder. Det indeholder også 2.039.476 relationer til legitimationsposter. Populationerne kan overlappe og fastslår ikke unikke personer eller aktuelt gyldige konti. [S3]

Udvalgt gruppe	Enheder, mindst	Medarbejderenheder	Legitimationsposter
Offentlig administration	3.338	56	52.425
Regionale og lokale tjenester	3.120	652	285.488
Bank og finans	2.160	60	84.646
Forsikring og pension	248	25	51.148
Universiteter og forskning	5.189	1.028	444.988
Industri og teknologi	28.088	1.205	624.223
Energi og infrastruktur	1.749	60	13.850

Udvalgt gruppe	Enheder, mindst	Medarbejderenheder	Legitimationsposter
Transport og logistik	28.552	614	193.381
Forbrugertjenester og kommunikation	68.621	534	203.241
Sundhed og biovidenskab	122	91	86.086
ALLE	141.187	4.325	2.039.476

[S3]

Enheds- og legitimationsrelationer kræver særskilte beslutninger om ansvar



Kilde: Odin by Brandefense, 250 udvalgte domæner, eksponeringsøjebliksbillede 22. november 2026 [S3]. Relationer kan overlappe og omfatte historiske poster; de er ikke unikke personer eller bekræftede indtrængninger.

En enhed tilknyttet en kundevendt tjeneste er ikke automatisk et endepunkt drevet af tjenesten. En medarbejderrelation skal også kontrolleres mod aktiv- og kontoregistre. En legitimationspost tilknyttet et domæne dokumenterer ikke, at organisationens egen infrastruktur var kilden.

Legitimationsposter kan være historiske, gentagne eller tilknyttet flere domæner. Kontrollér aktuel kontostatus, tidligere afhjælpning og relevante sessioner før forstyrrende indgreb. En gammel post kan vedrøre en gyldig konto; en ny annonce kan gentage forældet materiale.

3.4 Giv forskellige observationer forskellige ansvarlige

Indsatsmodellen forbinder de målte signaler med intern validering. Handlingerne er anbefalinger, ikke konstateringer af, at en udvalgt organisation manglede en bestemt kontrol.

Modtaget observation	Første validering	Ansvarlig	Bevis for afslutning
Aktuelt tilbud om legitimationsoplysninger	Bekræft kontoejerskab, aktualitet og adgangsomfang	Identitet og hændelseshåndtering	Registreret vurdering og begrundet inddæmning
Relation til medarbejderenhed	Identificér endepunktet og relevante sessioner	Endepunktssikkerhed og identitet	Undersøgelsesresultat og sessionsgennemgang
Anden enhedsrelation	Fastslå tjenesteforholdet og den berørte ansvarlige	Tjeneste- og kundedrift	Korrekt placering uden antaget medarbejderejerskab
Historisk legitimationspost	Kontrollér kontostatus og tidligere afhjælpning	Identitet og dataansvarlig	Valideret status og kontrolhandling
Lignende domænenavn	Fastslå faktisk misbrug og brandforhold	Brandbeskyttelse og jura	Afgørelse om misbrug og passende indsats
Dokumentobservation	Bekræft følsomhed, oprindelse og delingsret	Dataansvarlig og jura	Eksponeringsvurdering og afhjælpning
Hul i mailpolitik	Bekræft tilsigtede afsendertjenester og politik	Mailansvarlig	Kontrolleret levering og politikadfærd

Hvis et tilbud vedrører en konto i eget miljø, skal det fastslås, hvilke systemer den kan nå. Undersøg sessioner, gendannelse og rettighedsændringer sammen med adgangskoden. Et adgangskodeskift alene besvarer ikke, om en anden adgangsvej blev ændret.

Hver alarm kræver en vurdering: relevant og aktuel, historisk og afhjulpet, uvedkommende eller uafklaret. Registrér evidensen og den ansvarlige for beslutningen. En uafklaret alarm kræver en opfølgningsdato frem for en antaget vellykket afslutning.

3.5 Passive kontroller kræver deres egen nævner

Det manglende passive datasæt betyder, at denne udgave ikke kan angive dansk DMARC-håndhævelse, certifikatgyldighed eller et hygiejneindeks. Manglende observationer kan heller ikke tolkes som manglende kontroller. Fraværet understøtter ingen konklusion om et enkelt kandidatdomænes sikkerhed.

En autoriseret ansvarlig kan gennemgå egne mail-, DNS- og webkontroller mod det tilsigtede tjenestedesign. Test legitim afsendelse og gendannelse som del af gennemgangen. En synlig politik fastslår ikke i sig selv, at alle forretningssystemer bruger den korrekt.

Eksponeringsobservationer og passive kontroller besvarer forskellige spørgsmål. En porteføljevurdering kan ikke erstatte validering af en organisations egne observationer. En offentlig hændelsesmeddelelse kan heller ikke fastslå, hvilke eksternt observerede poster der er aktuelle.

HOVEDPOINTER

01

Validér konti knyttet til de 37 domæner med aktuelle legitimationstilbud.

02

Send medarbejder- og andre enhedsrelationer til de rette ansvarlige.

03

Hold den nationale Atlas-vurdering adskilt fra utilgængelige passive kontrolresultater.

KAPITEL 04

Aktivitet i undergrundsmiljøer: Hvad de bevarede opslag viser

DETTE KAPITEL BESVARER

Hvilke observationer fra undergrundsmiljøer bør undersøges uden at blive til ubekræftede hændelsestal?

6

sager, der skelner mellem annoncer, dataenes oprindelse og påstået adgang

4.1 Datagrundlag 22
4.2 Omfang, platforme og sprogtilknytning 23
4.3 Sager 25
4.4 Leverandørpåstande fastslår ikke indtrængen hos kunder 32
4.5 Videreformidling og svar bekræfter ikke en påstand uafhængigt 33
4.6 Hvad sagerne betyder for forsvarsindsatsen 33

KAPITEL 04

Aktivitet i undergrundsmiljøer: Hvad de bevarede opslag viser

KORT FORTALT

Det bevarede forummateriale indeholder annoncer for loginoplysninger, påstande om kundedata og udviklingssystemer samt et regionalt adgangstilbud. Bevisværdien varierer. En skjult download, en felt-overskrift og sælgerens forsikringer dokumenterer ikke brugbar adgang eller et nyt indbrud. Gentagne overskrifter og korte svar kan holde en gammel påstand synlig. Undersøg den relevante konto, det relevante system og påstanden om data, før I vælger en indsats.

4.1 Datagrundlag

Punkt	Betydning
Periode	1. januar–22. november 2026 efter opslagstidspunkt
Nyere aktivitet	8.–22. november 2026, adskilt fra tidligere kontekst
Bevarede opslag	4.116 forskellige beskeder; 557 forumposter; overlappende landstilknytning
Enhed	En bevaret besked, herunder annoncer, svar, videreformidling og irrelevant materiale
Landetilknytning	En landemærkning eller omtale dokumenterer ikke målretning eller et dansk offer
Sagsgrundlag	Seks udvalgte sager, hver knyttet til et offentligt evidenskort
Underliggende påstande	Kontoers gyldighed, dataenes oprindelse, adgang og handler er ubekræftede, medmindre andet fremgår
Relationer	Gentagen ordlyd understøtter en annoncerelation, ikke en fælles operatør eller en identisk underliggende fil

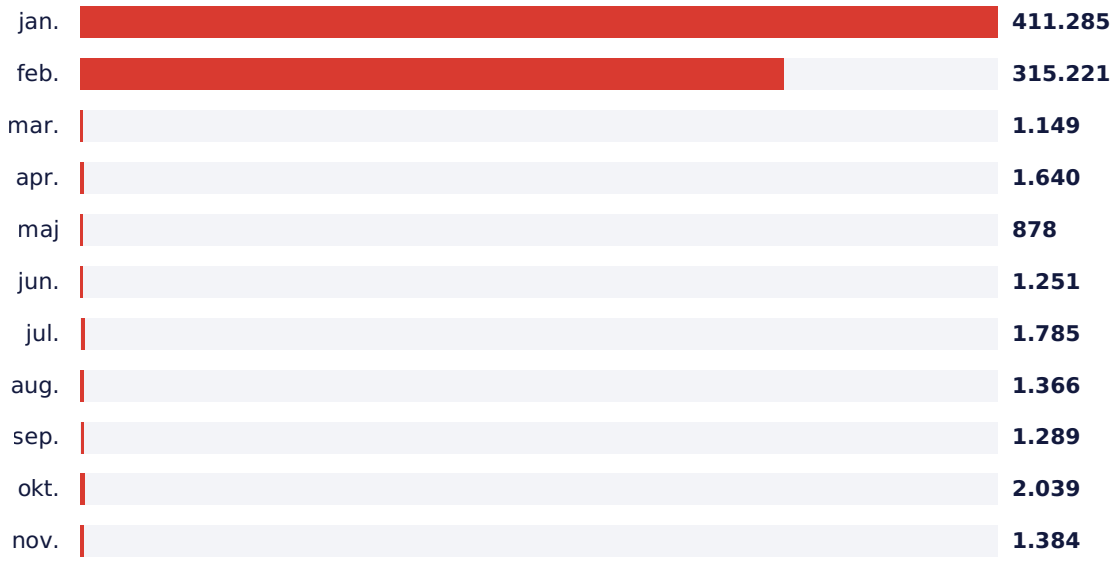
[S1]

De seks sager handler om forskellige spørgsmål, som bør undersøges. De er ikke seks bekræftede indbrud og kan ikke lægges sammen med ransomware-listninger. Et opslag kan beskrive et gammelt datasæt, kommercielt indsamlede oplysninger, en skjult download eller en tjeneste i mange lande. Det afgørende er, hvad den bevarede besked faktisk siger.

4.2 Omfang, platforme og sprogtilknytning

Den månedlige serie med landstilknytning indeholder 739.287 opslagsposter. Januar og februar står for 726.506, svarende til 98,3 %. Det er beskeder med en landstilknytning, ikke verificeret målretning mod Danmark eller et nationalt antal hændelser. [S1]

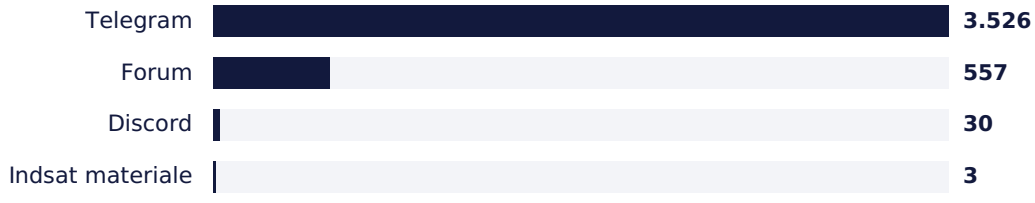
De fleste landstilknyttede poster stammer fra januar og februar



Kilde: Odin by Brandefense, bevarede Danmarkstilknyttede opslag, 1. januar–22. november 2026; november er ufuldstændig [S1]. Månedlige landemærkede poster og læsekorpussets 4.116 beskeder er forskellige populationer; ingen af dem måler bekræftede hændelser.

Det bevarede læsekorpus indeholder 4.116 forskellige beskeder. Det omfatter 557 forumposter og 3.738 poster med dansk landemærkning. Grupperne overlapper. De lægges ikke sammen og er ikke samme population som den månedlige serie. [S1]

Læsekorpusset dækker flere platforme

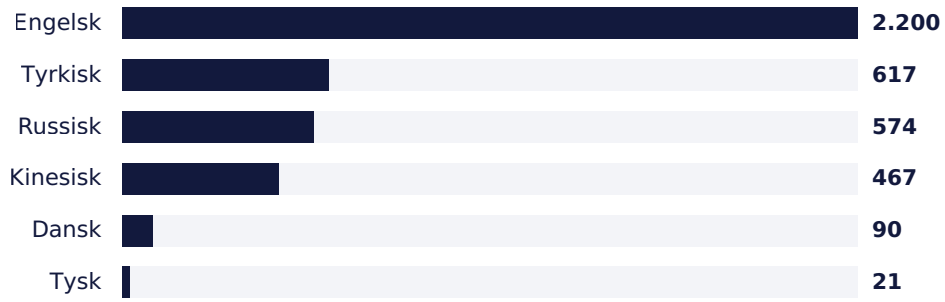


Kilde: Odin by Brandefense, bevarede Danmarkstilknyttede opslag, 1. januar–22. november 2026; november er ufuldstændig [S1]. Månedlige landemærkede poster og læsekorpussets 4.116 beskeder er forskellige populationer; ingen af dem måler bekræftede hændelser.

Bevaret platform	Beskeder	Betydning
Telegram	3.526	Bevarede beskeder, herunder reklame-materiale og påstande
Forum	557	Bevarede annoncer, svar, diskussioner og nyhedsvideregivelser
Discord	30	Bevarede beskeder i læsekorpusset
Paste	3	Bevaret indsat materiale
ALLE	4.116	Forskellige beskeder på tværs af platformene

Materialet fra årets første del omfatter gentagne reklamer, der henviser til mange lande, herunder Danmark. Omfanget fastslår ikke, at angreb mod danske organisationer efterfølgende faldt. Beskedernes sammensætning og kildernes synlighed varierer; antallet af opslag måler ikke vellykkede indtrængninger. [S1]

Udvalgte sprogmærkninger beskriver beskeder, ikke aktørernes nationalitet



Udvalgte sprogtilknytninger kan overlappe; ikke en udtømmende fordeling eller aktørernes nationalitet. Kilde: Odin by Brandefense, bevarede Danmarkstilknyttede opslag, 1. januar–22. november 2026; november er ufuldstændig [S1]. Månedlige landemærkede poster og læsekorpussets 4.116 beskeder er forskellige populationer; ingen af dem måler bekræftede hændelser.

Mærkninger for engelsk, tyrkisk, russisk, kinesisk, dansk og tysk forekommer i det bevarede korpus. En besked kan have flere sprogtilknytninger. Figuren viser udvalgte mærkninger frem for en udtømmende opdeling efter sprog. En sprogmærkning fastslår ikke afsenderens placering, nationalitet eller forbindelse til en stat. [S1]

Konklusionerne bygger på det bevarede materiale. Hverken læsekorpusset eller de udvalgte sager giver grundlag for at anslå alle danske annoncer, aktive sælgere, kriminelle indtægter eller bekræftede hændelser.

4.3 Sager

SAG A

A

En ny opslagsdato dokumenterer ikke friske loginoplysninger

Påstand ubekræftet

Evidenskort B01 | 2 jul. 2026 | Forumopslag | Identitetsoplysninger

PÅSTAND	En landemærket annonce beskriver en liste med mailadresser og adgangskoder og kalder den frisk. Den annoncerede mængde er afsenderens oplysning. Den udvalgte juli-post bevarer en februardato i overskrift og brødtekst. [S1]
FORLØB	En tidligere februar-post indeholder tilsvarende ordlyd. En post dateret i juli gentager denne daterede beskrivelse, og et kort svar tilføjer en tak uden at kontrollere materialet. Datoerne beskriver beskederne, ikke tidspunktet for indsamling af kontooplysninger.
HVAD VI KAN FASTSLÅ	Den samme daterede annoncebeskrivelse optræder på forskellige tidspunkter i det bevarede materiale. Det understøtter en relation mellem gentagne annoncer. Det dokumenterer ikke, at begge downloads indeholder en identisk fil, eller at afsenderen selv har indsamlet oplysningerne.
ANDRE FORKLARINGER	Materialet kan være historisk, tidligere håndteret, ompakket eller forkert mærket. En senere besked kan også henvise til en opdateret fil uden at forklare ændringen. Annoncen alene afklarer ikke disse muligheder.
BEGRÆNSNINGER	Hverken fungerende konti eller unikke personer er dokumenteret. Et annonceret linjetal er ikke et antal ofre. Mærkningen som frisk og opslagets dato kan ikke erstatte kontrol af den enkelte konto.
HANDLING	Hvis en advarsel vedrører en konto, I ejer, skal I kontrollere dens aktuelle status og tidligere afhjælpning. Gennemgå relevant adgang og aktive sessioner, før I vælger inddæmning. Dokumentér afgørelsen frem for at tælle hver gentagen overskrift som en ny hændelse.

Konklusion

Kontrollér kontoers aktualitet, før gentagen annoncering behandles som en ny hændelse.

Evidenskort B01 2 jul. 2026

thejackal101 Forumopslag Forum EN

ORIGINALTEKST

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

OVERSÆTTELSE

Database: Danmark Type: Mail : Adgangskode Dato: [6/FEB/2026] Liste: [34 K++]

Bemærkning. Den annoncerede mængde og mærkningen som frisk er afsenderens oplysninger. Et kort svar samme dag tilføjer ingen bekræftelse.

Dokumenteret
En juli-dateret post med en februar-mærket annonce for loginoplysninger; en tidligere februar-post har tilsvarende ordlyd.

Ikke fastslået
Friskhed, gyldige konti, unikke personer, indholdet af den skjulte download eller et nyt indbrud.

SAG B

B

Felter om finansielle kunder dokumenterer ikke adgang til banksystemer

Påstand ubekræftet

Evidenskort B02 12 sep. 2026 Forumopslag Finansielle tjenester

PÅSTAND	En september-annonce påstår at tilbyde et finansielt kundedatasæt med tilknytning til Danmark. Den nævner kontakt-, identitets- og økonomiske profilfelter og kræver 800 dollars. Det er en udbudspris, ikke dokumentation for en gennemført handel. [S1]
FORLØB	Det bevarede opslag er dateret 12. september. Det dokumenterer ikke, hvornår de underliggende oplysninger blev oprettet eller indsamlet. Beskeden bekræfter ingen særskilt indsamlingsdato, adgangshændelse eller handel.
HVAD VI KAN FASTSLÅ	En annonce og dens feltbeskrivelser var til stede. Den påståede organisations navn og identificerende beskrivelse er udeladt. Beskrivende tekst om en finansiel virksomhed dokumenterer ikke, at virksomheden har leveret, mistet eller kontrolleret de tilbudte oplysninger.
ANDRE FORKLARINGER	Tilbuddet kan vedrøre historiske kundeemner, et tredjepartsdatasæt, kommercielt sammenstillede oplysninger eller en falsk tilknytning. En registrering kan beskrive en mulig kunde uden at repræsentere en aktiv konto. Mulighederne kræver forskellige ansvarlige og indsatser.
BEGRÆNSNINGER	Ingen aktuel konto, saldo, adgang til banksystemer eller samlet kundetab er dokumenteret. Feltbetegnelserne beviser ikke ægtheden af de underliggende registreringer. Sælgerens pris måler ikke det påståede datasæts værdi.

HANDLING

Send et relevant signal til dataejeren, svindelteamet og hændelseslederen. Fastslå oprindelse og berørte relationer gennem autoriseret dokumentation. Forbered en kontrolkanal til mistænkelige henvendelser, hvis en reel eksponering bekræftes.

Konklusion

Felter om kunder dokumenterer ikke adgang til banksystemer.

Evidenskort B02 — 12 sep. 2026

K0d3x | Forumopslag | Forum | EN

ORIGINALTEKST

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

OVERSÆTTELSE

Danmark / [finansiel organisation] / [kundedata] [...] Til salg: 800$

Bemærkning. Organisationens navn og identificerende beskrivelse er udeladt. Det kan ikke udledes, at de annoncerede data stammer fra et aktuelt indbrud.

Dokumenteret
En annonce med betegnelser for kontakt-, identitets- og økonomiske profilfelter samt en udbudspris.

Ikke fastslået
Ægthed, aktuelle konti, den nævnte organisations involvering, en handel eller adgang til banksystemer.

C

SAG C

Profilfelter fra et netfællesskab er en påstand, ikke et verificeret datasæt

Påstand ubekræftet

Evidenskort B03 | 14 okt. 2026 | Forumopslag | Onlinetjenester

PÅSTAND

Et oktober-opslag påstår at indeholde data fra et dansk netfællesskab. Brødteksten viser overskrifter fra brugertabeller, herunder konto- og profilfelter. Afsenderen beskriver materialet som en aktuel datahændelse. Den beskrivelse er fortsat afsenderens påstand. [S1]

FORLØB

Den bevarede besked er dateret 14. oktober og mærker de påståede data med samme måned. Det dokumenterer ikke adgangsdatoen, registreringernes alder eller tidspunktet, hvor oplysninger eventuelt blev offentligt tilgængelige.

HVAD VI KAN FASTSLÅ

Opslaget indeholder beskrivelser af tabelfelter og en påstand om deres kilde. Ingen personrækker eller målidentifikatorer offentliggøres her. Overskrifter kan beskrive en databases struktur uden at dokumentere antallet eller ægtheden af registreringerne.

ANDRE FORKLARINGER	En historisk database, en skabelon, et kopieret skema eller en forkert tilskrivning kan give tilsvarende feltbeskrivelser. To sæt overskrifter dokumenterer ikke i sig selv to indbrud eller adskilte grupper af ofre.
BEGRÆNSNINGER	Fungerende adgangskoder, antal berørte personer og en bekræftet hændelse hos det påståede mål er ikke dokumenteret. Profilfelter kan være følsomme, men deres tilstedeværelse i et påstået skema beviser ikke adgang til de tilsvarende personoplysninger.
HANDLING	Hvis påstanden vedrører en tjeneste, I ejer, skal I bevare relevante logs og undersøge de berørte datakategorier. Kontrollér kontogendannelse og historisk opbevaring. Underret personer efter dokumenterede forhold og gældende pligter frem for afsenderens mest specifikke påstand.

Konklusion

Tabeloverskrifter dokumenterer ikke ægte personrækker.

Evidenskort B03 — 14 okt. 2026

MrData | Forumopslag | Forum | EN

ORIGINALTEKST

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

OVERSÆTTELSE

Land: Danmark Dato: Oct 2026 [...] Tabelnavn: [udeladt]

Bemærkning. Platformens navn, domæne, kontaktidentifikatorer og detaljerede profilfelter er udeladt. Overskrifter beviser ikke de underliggende registreringer.

Dokumenteret

En påstand om data fra et netfællesskab ledsaget af overskrifter fra brugertabeller.

Ikke fastslået

Ægte registreringer, gyldige adgangskoder, antal berørte personer eller en bekræftet hændelse hos det påståede mål.

D

SAG D

Påstande om udviklingssystemer kræver særskilt kontrol af konti og nøgler

Påstand ubekræftet

Evidenskort B04 | 24 aug. 2026 | Forumopslag | Teknologitjenester

PÅSTAND	En august-annonce påstår at tilbyde adgangsrelateret materiale fra et udviklingsmiljø. Den beskriver medarbejderkonti og henviser til signerings- og udviklingsoplysninger. Henvisningerne er påstande i opslaget, ikke uafhængigt bekræftede, brugbare loginoplysninger eller nøgler. [S1]

FORLØB	Det bevarede materiale omfatter to august-beskeder og en september-besked med meget ens beskrivelser. Forskellige afsendere gentager påstanden. Det understøtter en relation mellem annoncerne uden at identificere den første kilde eller en fælles operatør.
HVAD VI KAN FASTSLÅ	Påstanden, en brugertabelprøve og henvisninger til nøgler fremgår af de lagrede beskeder. Det offentlige kort udelader personrækker, måloplysninger og kontaktoplysninger. En prøvebeskrivelse dokumenterer ikke en kontos aktuelle rækkevidde eller en nøgles gyldighed.
ANDRE FORKLARINGER	Opslagene kan bygge på kopieret annoncering, historisk materiale eller samme ubekræftede kilde. Ens ordlyd dokumenterer ikke en identisk underliggende fil, en gennemført handel eller ændring af en softwareudgivelse.
BEGRÆNSNINGER	Ingen kodeændring, adgang til efterfølgende kunder eller vellykket brug af loginoplysninger er dokumenteret. Administrativ kontoadgang, signeringsbeføjelser og mulighed for at offentliggøre en udgivelse er forskellige påstande. Hver kræver dokumentation fra den relevante ejer.
HANDLING	Gennemgå konti, signeringsbeføjelser og udgivelsesrettigheder særskilt i et relevant miljø, I ejer. Bevar dokumentation fra softwarebygning og adgang før afhjælpning ændrer den. Vælg indsatser for loginoplysninger og nøgler efter verificeret eksponering, og dokumentér begrundelsen.

Konklusion

Undersøg konti, signeringsbeføjelser og udgivelsesrettigheder særskilt.

Evidenskort B04 — 24 aug. 2026

Bitcoins | Forumopslag | Forum | EN

ORIGINALTEKST

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

OVERSÆTTELSE

Tabelindhold: [udeladt] [...] Azure-signeringsnøgler lækket, VCS-loginoplysninger SSH-nøgle + SVN.

Bemærkning. Citatet gengiver afsenderens påstand. Ingen nøgler, personrækker fra prøven eller målidentifikatorer offentliggøres.

Dokumenteret
En påstand om et udviklingssystem med en brugertabelprøve og henvisninger til nøgler; senere poster gentager påstanden.

Ikke fastslået
At loginoplysninger eller signeringsnøgler fungerer, at kode er ændret, eller at afsenderne deler en operatør.

SAG E

E

Et regionalt adgangstilbud har udtrykkelige begrænsninger for land og rækkevidde

Påstand ubekræftet

Evidenskort B05 | 5 nov. 2026 | Forumopslag | Erhvervstjenester

PÅSTAND	Et november-tilbud beskriver privilegeret adgang til systemer for softwarebygning og databaser i en nordisk virksomhed. Afsenderen angiver også undtagelser, herunder ingen domæneadministratoradgang og ingen kunde- eller forretningsapplikationsdata. Disse begrænsninger skal følge den bredere adgangspåstand. [S1]
FORLØB	Det bevarede opslag er dateret 5. november, før perioden for nyere aktivitet. Det giver relevant kontekst for planlægning omkring leverandører og udviklingssystemer. Offentliggørelsen dokumenterer ikke, hvornår adgang begyndte, eller om den stadig fandtes ved rapportens skæringsdato.
HVAD VI KAN FASTSLÅ	Sælgeren annoncerede privilegier og beskrev deres påståede omfang. Landetilknytningen omfatter mere end Danmark. Rapporten behandler derfor tilbuddet som et regionalt undersøgelseseksempel frem for en bekræftet dansk hændelse.
ANDRE FORKLARINGER	Tilbuddet kan indeholde reel, forældet, overdrevet eller opdigtet adgang. Sælgerens tekniske beskrivelser og forsikringer afklarer ikke mulighederne. En henvisning til kunderelateret infrastruktur dokumenterer ikke adgang til kunderne selv.
BEGRÆNSNINGER	Ingen handel, fungerende login, adgang til efterfølgende systemer eller driftsvirkning er dokumenteret. Omsætning og detaljerede miljøtal er udeladt for at beskytte det påståede måls identitet. Påstanden dokumenterer ikke en softwaresårbarhed eller en bestemt adgangsvej.
HANDLING	En relevant tjenesteejer bør undersøge administrative konti, rettigheder til softwarebygning og udrulningsrelationer. Leverandørstyringen bør fastslå, hvem der kan lukke adgang, og hvilken dokumentation der tillader genåbning. Omtal ikke kunder som bekræftede ofre alene på grund af en annonces omtale af kundemiljøer.

Konklusion

En regional adgangspåstand dokumenterer ikke dansk målretning eller efterfølgende virkning.

Evidenskort B05 5 nov. 2026

marlowfinch42 Forumopslag Forum EN

ORIGINALTEKST

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

OVERSÆTTELSE

TeamCity SYSTEM_ADMIN hos [en organisation]. [...] Ikke omfattet: ingen domæneadministrator, ingen kunde- eller ERP-data

Bemærkning. Landetilknytningen er bredere end Danmark. Sælgerens egne undtagelser skal følge adgangspåstanden; den påståede virksomhed navngives ikke.

Dokumenteret
Et adgangstilbud, der beskriver privilegier til softwarebygning og databaser i en nordisk virksomhed.

Ikke fastslået
Målretning specifikt mod Danmark, fungerende adgang, adgang til kundesystemer, en gennemført handel eller efterfølgende virkning.

F

SAG F

Kontaktdata med katalogtema er ikke bevis for tyveri

Evidenskort B06 4 jan. 2026 Forumopslag Kommercielle kontaktdata

Påstand ubekræftet

PÅSTAND	En januar-annonce tilbyder oplysninger med erhvervskatalogtema for Danmark og et andet land. Den beskriver virksomheds-, kontakt- og lokationsfelter og tilbyder eksempler på forespørgsel. Den annoncerede mængde er ikke et verificeret antal berørte organisationer eller personer. [S1]
FORLØB	Den bevarede besked er dateret 4. januar. Den giver ingen uafhængigt dokumenteret indsamlingsdato eller hændelsestidslinje. Et tilbud ved årets begyndelse dokumenterer ikke, at de underliggende oplysninger blev indsamlet i det år.
HVAD VI KAN FASTSLÅ	Beskeden annoncerer et datasæt og beskriver dets påståede felter. Den dokumenterer ikke eksklusiv besiddelse eller en gennemført handel. Den nævnte tjeneste og identificerende mængde er udeladt, fordi påstanden mangler særskilt bekræftelse.
ANDRE FORKLARINGER	Offentlige katalogoplysninger, kommerciel sammenstilling, ompakkede kundeemner eller en forkert beskrivelse kan forklare tilbuddet. Selv ægte kontaktoplysninger dokumenterer ikke i sig selv uautoriseret adgang til de organisationer, de beskriver.

BEGRÆNSNINGER	Annoncen dokumenterer ingen verificeret datasikkerhedshændelse, gyldig enkeltregistrering eller hændelsespopulation. Landehenvisningen beskriver det påståede datasæt frem for et dokumenteret angreb mod hver repræsenteret organisation.
HANDLING	Vurder relevante oplysninger ud fra lovlig offentlig tilgængelighed, oprindelse og faktisk følsomhed. Svindelteamet bør overveje, hvordan verificerede kontaktdata kan bruges til identitetsmisbrug. Behandl ikke et erhvervskatalogtilbud som bevis for, at hver virksomhed har behov for at inddæmme et indbrud.

Konklusion

Kataloglignende oplysninger dokumenterer ikke indbrud hos de beskrevne virksomheder.

Evidenskort B06 — 4 jan. 2026

selluk | Forumopslag | Forum | EN

ORIGINALTEKST

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

OVERSÆTTELSE

denne database DANMARK indeholder [annonceret mængde] LINJER [...] BEVISER OG EKSEMPEL PÅ FORESPØRGSEL.

Bemærkning. Udgiverens eller tjenestens identitet og den detaljerede mængde er udeladt. Offentlige eller kommercielt sammenstillede katalogoplysninger er et alternativ til stjålne data.

Dokumenteret
Et datatilbud med erhvervskatalogtema, der beskriver kontakt- og virksomhedsfelter for Danmark og et andet land.

Ikke fastslået
Oprindelse, eksklusivitet, et verificeret indbrud, gyldige kontaktoplysninger eller en handel.

4.4 Leverandørpåstande fastslår ikke indtrængen hos kunder

En forumannonce fra 9. april hævder en tidligere leverandørhændelse og tilbyder medarbejderkontaktoplysninger knyttet til kundevirksomheder, herunder danske firmaer. En gentaget annonce dokumenterer ikke oplysningernes oprindelse eller særskilt indtrængen hos hver kunde. Den fastslår heller ikke aktuelt gyldige legitimationsoplysninger eller adgang til kundesystemer. [S3]

En anden annonce markedsfører et platformsdatasæt som en datalækage. Det tilbudte materiale fastslår ikke en dansk berørt population, oplysningernes oprindelse eller adgang til platformens interne systemer. [S3]

Observationerne tilhører den særskilte organisationsrelaterede opslagkontekst. De indgår ikke i tallene for læsekorpusset ovenfor. Relevante kunder bør verificere leverandørforholdet, de berørte oplysninger og aktuel kontoevidens gennem autoriserede kanaler.

4.5 Videreformidling og svar bekræfter ikke en påstand uafhængigt

Det bevarede forummateriale indeholder også videreformidlede nyheder om offentligt kendte hændelser og politiindsatser. En sådan besked kan hjælpe med at finde den oprindelige udtalelse. Den bliver ikke en uafhængig undersøgelse ved at optræde på en anden platform. Offentlig bekræftelse tilhører den kilde, som faktisk giver den. [S1]

Korte svar kræver samme forsigtighed. En tak, et spørgsmål om et fungerende link eller en gentaget trådoverskrift dokumenterer ikke et nyt tilbud, et køb eller en vellykket download. Flere registreringer kan beskrive én påstand uden at repræsentere flere hændelser.

Det samme gælder gentagne annoncer under forskellige aliasser. Ens ordlyd understøtter den snævre annoncerelation. Fælles kontrol, operatøridentitet, identiske datasæt og gennemførte overførsler kræver yderligere konkret dokumentation. Rapporten udleder ikke sådanne relationer blot for at forbinde sagerne i ét kriminelt netværk.

4.6 Hvad sagerne betyder for forsvarsindsatsen

Observation	Beslutning med støtte	Beslutning uden tilstrækkelig støtte
En dateret annonce for loginoplysninger	Kontrollér egne konti og tidligere afhjælpning	Tæl fungerende loginoplysninger eller nye indbrud
Feltbeskrivelser om kundedata	Vurder oprindelse og mulig misbrug	Bekræft intern bankadgang
Overskrifter fra et netfællesskabs brugertabel	Undersøg konto- og dataomfang	Udled ægte personrækker eller antal berørte personer
Påstande om udviklingssystemer	Undersøg konti, nøgler og udgivelsesrettigheder særskilt	Erklær efterfølgende software eller kunder berørt
Et regionalt tilbud om adgang til systemer for softwarebygning	Undersøg relevante leverandørafhængigheder	Henfør hændelsen specifikt til Danmark
Et datatilbud med katalogtema	Vurder følsomhed og svindelrisiko	Behandl hver repræsenteret virksomhed som udsat for indbrud

Dette er betingede indsatsvalg. Organisationen har først brug for en relevant advarsel og tilstrækkelige ejerskabsoplysninger til at sende den videre. En dokumenteret historisk eller forkert tilknytning kan være et gyldigt afslutningsresultat. Hvis dokumentationen fortsat er uafklaret, skal usikkerheden og den ansvarlige for næste undersøgelsestrin bevares.

HOVEDPOINTER

01

En beskeddato og mærkning som frisk dokumenterer ikke et nyt indbrud.

02

Undersøg konti, dataenes oprindelse og rækkevidden til andre systemer som særskilte påstande.

03

Gentagne overskrifter, videreformidling og svar kan ikke erstatte uafhængig bekræftelse.

KAPITEL 05

Hændelser og kampagner

05

DETTE KAPITEL BESVARER

Hvad bekræftede danske organisationer og myndigheder, og hvad er stadig uafklaret?

20

sagsbeskrivelser fra offentlige kilder med særskilte afgrænsninger af dokumentation og påvirkning

5.1 Hvad de bekræftede sager betyder 36
5.2 Uddannelse, forskning og identitetsadministration 37
5.3 Offentlige tjenester, regulerede oplysninger og kundedata 40
5.4 Entreprenører, overtagne systemer og eksterne platforme 44
En anden omtalt meddelelse i restaurationsbranchen 52
5.5 Seneste aktivitet: 8. til 22. november 2026 52
5.6 Beslutninger på baggrund af sagerne 53
5.7 Aktuelle sårbarheder: afklar relevans før tilskrivning 54

KAPITEL 05

Hændelser og kampagner

KORT FORTALT

De offentligt beskrevne hændelser i Danmark viser flere veje til driftsforstyrrelser og eksponering af personoplysninger. Identitetsadministration, testmiljøer, overtagne systemer og eksterne leverandører går igen på tværs af forskellige organisationer. De seneste meddelelser viser også, hvorfor genåbning skal have sin egen dato: En tjeneste kan genåbne, mens undersøgelsen fortsætter. Skeln mellem en offentlig påstand, en officiel meddelelse og en bekræftet driftspåvirkning. Øv gendannelse af konti, begrænsning af leverandørhændelser og kundekommunikation samlet.

5.1 Hvad de bekræftede sager betyder

Sagerne nedenfor skelner mellem organisationens redegørelse og påstande fra andre. En meddelelse kan bekræfte uautoriseret adgang uden at fastslå angriberens identitet, den samlede datamængde eller senere misbrug. Omvendt ophæver fravær af observeret misbrug ikke en bekræftet adgang. Hver afgrænsning har betydning for den indsats, sikkerhedsansvarlige bør vælge.

De mange offentliggørelser i september, oktober og november bør ikke læses som et mål for angrebshyppigheden. Nogle meddelelser beskriver tidligere adgang. Andre dokumenterer en forholdsregel eller en senere myndighedsafgørelse. Datoen for en hændelse skal vise, hvad der skete den dag. Antal potentielt berørte personer hører også til de enkelte sager og kan ikke lægges sammen til et nationalt tal.

Tre skel er vigtige i praksis. Et forsøg på at ændre en adgangskode er noget andet end en overtaget konto. Adgang til et lokalt, ældre system er noget andet end kompromittering af hele virksomhedens it-miljø. Eksponering af kunders kontaktoplysninger er noget andet end adgang til betalingssystemer. Sagerne giver konkrete grunde til at fastholde disse skel i hændelsesrapporteringen.

5.2 Uddannelse, forskning og identitetsadministration

SAG G

G DTU's identitetskompromittering rakte ud over den første konto

bekræftet

DTU

BEKRÆFTET	DTU's tidslinje begynder med adgang til en gæsteidentitet den 15. september. Den beskriver opsnappede nulstillinger af adgangskoder, angriberens registrering af en godkendelsesfaktor, fjernadgang og senere administrative rettigheder. DTU opdagede hændelsen den 20. september. Opdateringen den 19. november oplyste, at over 200.000 nuværende eller tidligere brugere kunne være berørt, og at indsatsen var afsluttet. [S13][S53]
AFGRÆNSNING	Antallet af personer omfattet af orienteringen bekræfter ikke, at hver persons oplysninger blev hentet ud. Omfanget ændrede sig under DTU's undersøgelse. Derfor vejer den seneste meddelelse tungere end det første skøn. [S13]
VURDERING	Kanaler til kontogendannelse og rettigheder til at registrere godkendelsesfaktorer kræver samme opmærksomhed som selve loginfunktionen. En ekstra faktor beskytter kun i begrænset omfang, hvis en angriber kan registrere sin egen gennem en berørt gendannelsesvej.
HANDLING	Den identitetsansvarlige bør gennemgå nulstillinger, faktorregistreringer og privilegerede ændringer samlet. Derefter bør uvedkommende sessioner og legitimationsoplysninger tilbagekaldes på tværs af tilknyttede tjenester.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Gendannelse af konti bør omfatte en særskilt kontrol af identiteter oprettet under hændelsen. Fjernelse af den første berørte konto kan efterlade en anden adgangsvej. En nyttig øvelse beder teamet rekonstruere, hvem der godkendte hver ny faktor og rettighed. Helpdesken bør have en klar eskalationsvej, når en plausibel gendannelsesanmodning afviger fra kontoens sædvanlige adfærd.

SAG H

H ■ Københavns Universitets testmiljø fik følger uden for test

Københavns Universitet

bekræftet

BEKRÆFTET	Københavns Universitet opdagede uautoriseret adgang den 20. oktober. Meddelelsen beskrev en konfigurationsfejl i et testmiljø med en brugerdatabase på omkring 525.000 personer. Databasen var senest synkroniseret den 13. januar 2026. Oplysningerne varierede fra person til person og omfattede krypterede CPR-numre. Relevant dekrypteringsmateriale var også berørt. [S12]
AFGRÆNSNING	Universitetet oplyste, at databasen hverken indeholdt private bopælsadresser eller helbredsoplysninger. En senere nedlukning som forholdsregel blev først omtalt som endnu et angreb. Det blev rettet den 27. oktober og bør ikke tælles to gange. [S12][S54]
VURDERING	Betegnelsen testmiljø gør ikke kopierede identitetsoplysninger mindre følsomme. Kryptering kræver også en særskilt vurdering af, hvor nøgler eller dekrypteringsmateriale opbevares.
HANDLING	Den applikationsansvarlige bør fjerne unødvendige personoplysninger fra testsystemer og adskille hemmeligheder fra de datasæt, de beskytter.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Kommunikation om hændelsen bør skelne mellem databasens alder og tidspunktet for indbruddet. En synkronisering i januar daterer ikke angrebet til januar. Beslutninger om genopretning skal også omfatte adgangskort og andre fysiske legitimationsmidler, når sådanne felter findes i det berørte system. De ansvarlige teams bør aftale kriterier for udskiftning, før et brud kræver en hurtig beslutning.

SAG I

I ■ AU skelnede mellem serveradgang og mislykkede kodeændringer

AU

bekræftet

BEKRÆFTET	AU oplyste om uautoriseret serveradgang, som blev opdaget den 19. oktober. Forsøg på at tilgå eller ændre adgangskoder for omkring 1.700 brugere var ifølge universitetet mislykkedes. Den offentlige redegørelse beskrev inddæmning og ingen aktuelle tegn på læk af fortrolige eller følsomme oplysninger. [S14]

AFGRÆNSNING	Redegørelsen bekræfter kompromittering af en server og forsøg på kontoaktivitet. Den bekræfter ikke 1.700 overtagne konti eller videregivelse af følsomme oplysninger. [S14]
VURDERING	En blokeret handling er stadig nyttig viden om angriberens hensigt. Den bør indgå i undersøgelsen uden at blive til et tal for gennemført skade.
HANDLING	Infrastruktur- og identitetsteams bør sammenholde serveraktivitet med godkendelseslogge og undersøge de forsøgte kodeændringer som et sammenhængende forløb.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Det praktiske spørgsmål er, hvilken kontrol der brød forløbet, og om den samme kontrol bruges andre steder. Sikkerhedsansvarlige bør bevare dokumentationen, før rutinemæssig genopbygning fjerner nyttig kontekst. Kommunikationen bør tydeliggøre den observerede beskyttelse og de forhold, der stadig undersøges. Det giver brugerne grund til at følge vejledningen uden at antyde, at alle forsøg lykkedes.

J

SAG J

En uddannelsesinstitutions novembermeddelelse handlede om tidligere adgang

omtalt

Offentligt omtalt tjeneste

OMTALT	Danske medier beskrev den 11. november, at en uddannelsesinstitution orienterede omkring 44.000 nuværende eller tidligere studerende og kursister. Omtalen citerede institutionens it-ledelse og beskrev personoplysninger, herunder identitets- og kontaktoplysninger. Adgangen skulle være begyndt i marts. [S48]
AFGRÆNSNING	November er offentliggørelsesdatoen i denne redegørelse. Den bør ikke antages at være datoen for indbruddet. Antallet af orienterede personer er heller ikke dokumentation for identitetssvindel. [S48]
VURDERING	Lange opbevaringsperioder kan gøre tidligere brugere til en væsentlig del af institutionens orienteringsopgave. Det aktuelle antal studerende siger kun lidt om, hvem et beredskab kan få behov for at kontakte.
HANDLING	Institutionens dataansvarlige bør sikre en praktisk kontaktvej til tidligere brugere og undersøge, hvorfor aktive applikationer fortsat har adgang til historiske oplysninger.

Konklusion

Kontrollér det omtalte forløb samt data- og tjenesteomfanget, før indsatsen vælges.

En øvelse bør omfatte personer, som ikke længere bruger institutionens e-mailtjeneste. Teamet har brug for en lovlig og pålidelig kontaktvej og en klar forklaring af, hvilke råd der gælder. Identitetskontrol ved henvendelser bør undgå endnu en unødvendig kopi af følsomme oplysninger. Målet er at hjælpe de berørte uden at oprette en ekstra database under indsatsen.

5.3 Offentlige tjenester, regulerede oplysninger og kundedata

K

SAG K

CPR-adgang misbrugte en legitim adgangsvej

CPR

bekræftet

BEKRÆFTET	Det ansvarlige ministerium offentliggjorde omfattende uautoriseret adgang til CPR-oplysninger den 5. oktober. Uregelmæssighederne vedrørte september og blev opdaget om aftenen den 2. oktober. Ministeriet beskrev misbrug af en privat virksomheds legitime søgeadgang. Det berørte oplysninger om omkring 8,8 millioner registrerede personer. Adgangen blev stoppet, og sagen blev overgivet til de relevante myndigheder. [S15]
AFGRÆNSNING	Gruppen omfatter afdøde og udvandrede personer. Tallet angiver ikke antallet af nulevende indbyggere i Danmark. Beskyttede navne og adresser var undtaget, og meddelelsen identificerede ikke gerningspersonen. [S15]
VURDERING	En autoriseret grænseflade kan blive vejen til uautoriseret brug. Adgangsstyringen skal vurdere adfærden hos kunder med adgangsrettigheder såvel som hos udefrakommende.
HANDLING	Register- og tjenesteansvarlige bør gennemgå søgemængder, formålsbegrænsninger og eskalationsveje ved unormal brug fra ellers legitime konti.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Beredskabet bør gøre det muligt hurtigt at suspendere en mistænkelig kunde og samtidig bevare dokumentation og nødvendige tjenester. Kontrakter bør gøre samarbejde om undersøgelsen praktisk muligt. De berørte har også brug for råd, der passer til de eksponerede oplysninger. Et stort register berettiger ikke til at beskrive hver post som en nulevende person eller antyde eksponering af uvedkommende adgangsoplysninger.

SAG L

L Mobilkundernes oplysninger krævede en præcis afgrænsning

bekræftet

Offentligt omtalt tjeneste

BEKRÆFTET	Mobiloperatøren 3 offentliggjorde en hændelse med kundeoplysninger den 23. oktober. Virksomheden oplyste, at en berørt applikationsgrænseflade var blokeret, og at navne og adresseoplysninger muligvis havde været tilgængelige. Opdateringerne beskrev undersøgelse og kundekommunikation. [S47]
AFGRÆNSNING	En gruppe på omkring 400.000 indgik i undersøgelsen. Det bekræftede ikke adgang til oplysninger om hver kunde i gruppen. Virksomhedens redegørelse adskilte også hændelsen fra de særskilte omtaler af en PHP-sårbarhed. [S47]
VURDERING	En grænseflade kan eksponere kundeoplysninger, selv om den primære kundeportal er tilgængelig. Rettighedsmodellen omkring de enkelte forespørgsler kræver en direkte kontrol.
HANDLING	Den tjenesteansvarlige bør teste adgangskontrol for de enkelte dataobjekter og kontrollere, om én kundes session kan hente en anden kundes oplysninger.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Inddæmning bliver lettere, når en grænseflade kan deaktiveres uafhængigt af nødvendige kundefunktioner. Teamet bør også fastslå, hvilke logge der kan skelne mellem mulig eksponering og faktisk hentning. Den dokumentation understøtter mere præcise orienteringer. Kundeservice bør have en kort, ensartet forklaring af de berørte oplysninger og må aldrig bede om kontoens adgangskode for at tale om hændelsen.

SAG M

M En hændelse hos en tandleverandør nåede kommunens borgere

bekræftet

Lejre Kommune

BEKRÆFTET	Lejre Kommune meddelte den 18. maj, at omkring 23.000 nuværende eller tidligere borgere ville modtage information om et sikkerhedsbrud hos en leverandør. Redegørelsen vedrørte en leverandør til tandplejen og mulig videregivelse af navne, adresser og CPR-numre samt visse telefonnumre og e-mailadresser. Børn og forældre var omfattet. [S45]
AFGRÆNSNING	Antallet af orienterede personer beviser ikke, at alle oplysninger blev hentet ud. De oplyste datafelter giver ikke grundlag for at tilføje en påstand om eksponerede behandlingsoplysninger. [S45]

VURDERING	Kundens orienteringsopgave kan være omfattende, selv om den tekniske hændelse sker hos en leverandør. Familier kan modtage breve om flere personer og har brug for en forståelig forklaring.
HANDLING	Kommunale tjenesteansvarlige bør aftale orienteringsansvar og dataforteg-nelser med databehandlere før en hændelse. Aftalen bør også omfatte børn og tidligere brugere.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Den kontraktansvarlige bør kunne identificere leverandørens lokale datasæt uden at afvente en gennemgang af det kommercielle samarbejde. En nyttig øvelse beder leverandøren om en liste over berørte kunder og kontrollerer, om den kan afstemmes med lokale oplysninger. Dobbelte eller uklare meddelelser kan svække tilliden. Én koordineret forklaring bør beskrive oplysningerne og den handling, hver modtager kan foretage.

SAG N

N ■ Et hospitals bygningsnetværk indeholdt medarbejderoplysninger

bekræftet

Offentligt omtalt tjeneste

BEKRÆFTET	Et hospital beskrev i august et angreb på et lokalt bygningsnetværk den 1. august. Patientbehandlingen var ifølge meddelelsen upåvirket. Mulig adgang vedrørte kortholderoplysninger, herunder medarbejderes identitets- og ansættelsesoplysninger. Omkring 7.600 nuværende medarbejdere blev orienteret sammen med andre relevante kortholdere. [S46]
AFGRÆNSNING	Medarbejdertallet omfatter ikke alle andre kortholdere. Meddelelsen bekræfter hverken eksponering af patientjournaler eller afbrydelse af klinisk behandling. [S46]
VURDERING	Bygningssystemer kan indeholde følsomme medarbejderoplysninger uden at høre til de systemer, der tydeligst forbindes med sundhedsvæsenet. Deres datafortegnelse bør indgå i hospitalets hændelsesberedskab.
HANDLING	Bygnings-, sikrings- og it-ansvarlige bør vurdere personoplysninger og legiti-mationsmidler i adgangskontrolsystemer og teste adskillelsen fra kliniske tje-nester.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Beredskabsplanen bør forklare, hvordan medarbejdere kommer ind i afspærrede områder, hvis elektronisk adgang svigter, eller adgangsmidler skal udskiftes. Planen skal sikre både patientsikkerhed og passende adgangskontrol. Leverandørens supportaftaler bør også testes i praksis. Hospitalet bør vide, hvem der kan foretage en akut konfigurationsændring, og hvordan ændringen registreres.

SAG O

Novo Nordisk skelnede mellem kopierede data og kernedrift

bekræftet

Novo Nordisk

BEKRÆFTET	Novo Nordisk oplyste den 11. juni, at uautoriseret adgang berørte en begrænset del af virksomhedens interne it-miljø. Nogle ikke-offentlige oplysninger og personoplysninger var kopieret ud. Virksomheden beskrev midlertidig nedlukning af visse interne systemer og oplyste samtidig, at kerneaktiviteterne var upåvirkede. [S44]
AFGRÆNSNING	Kriminelles påstande om hændelsen fastslår ikke en verificeret datamængde, et betalingskrav eller det fulde omfang. Virksomhedens meddelelse understøtter den snævrere konklusion om adgang og kopiering. [S44]
VURDERING	En afgrænset nedlukning kan understøtte inddæmning uden at betyde, at hele virksomheden er standset. Præcist sprog om omfanget hjælper driftsteams med at prioritere indsatsen.
HANDLING	Den hændelsesansvarlige bør identificere berørte forretningsprocesser og dataejere. Beslutninger om inddæmning bør bygge på disse afhængigheder frem for virksomhedens navn alene.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Øvelser bør kræve særskilte svar om produktionskontinuitet, medarbejdersystemer og følsomme forretningsoplysninger. Én samlet rød eller grøn status for virksomheden skjuler nyttige forskelle. Kommunikationen bør vise, hvilke aktiviteter der fortsætter, og hvilke medarbejderprocesser der kræver midlertidige alternativer. Undersøgere bør bevare dokumentation for databevægelser, selv når det er ligetil at genetablere den berørte tjeneste.

5.4 Entreprenører, overtagne systemer og eksterne platforme

P

SAG P

En stor entreprenør oplyste om berørte personoplysninger

Femern Link Contractors

bekræftet

BEKRÆFTET	Femern Link Contractors oplyste, at virksomheden opdagede en cyberhændelse den 11. oktober. Opdateringen den 27. oktober beskrev berørte systemer med personoplysninger, isolering af servere og orientering af potentielt berørte personer. Eksterne specialister bistod undersøgelsen. [S20]
AFGRÆNSNING	Opdateringen fastslog ikke angriberens identitet eller en endelig mængde berørte oplysninger. Den giver heller ikke grundlag for at beskrive hændelsen som en bekræftet kompromittering af tunnelstyring eller entreprenørmateriel. [S20]
VURDERING	Et strategisk vigtigt projekt kan opleve en hændelse med administrative oplysninger uden dokumentation for indbrud i operationel teknologi. Indsatsen stiller stadig krav på tværs af arbejdsgivere, entreprenører og leverandører.
HANDLING	Projektets sikkerhedsansvarlige bør kortlægge ansvaret for personoplysninger på tværs af kontraktparter og sikre, at hver part kan modtage en rettidig, ensartet hændelsesmeddelelse.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Fælles projekter har brug for en fælles kommunikationsvej før en hændelse. Hovedentreprenøren, projektejeren og specialleverandørerne kan kende forskellige dele af det samlede billede. En øvelse bør afklare, hvem der beslutter, om arbejdet fortsætter, og hvilken dokumentation beslutningen bygger på. Den bør også afklare, hvordan potentielt berørte medarbejdere får råd, når deres arbejdsgiver er underentreprenør.

SAG Q

Q ■ En leverandørhændelse berørte ældre bilag til en offentlig tjeneste

Offentligt omtalt tjeneste

bekræftet hændelse; adgang uafklaret

BEKRÆFTET	En offentlig klageinstans oplyste om en leverandørhændelse med aktivitet mellem den 17. og 23. oktober. Meddelelsen vedrørte bilag indsendt gennem en tidligere hjemmeside i en afgrænset periode. Omkring 730 personer blev kontaktet. Den nuværende hjemmeside og selve klageformularerne lå uden for det beskrevne berørte område. [S17]
AFGRÆNSNING	Instansen kunne ikke fastslå, om filerne var tilgået eller downloadet, men kunne heller ikke udelukke det. En mulig krænkelse af fortroligheden må ikke blive til en påstand om bekræftet offentliggørelse. [S17]
VURDERING	Udskiftning af en hjemmeside fjerner ikke automatisk data hos den tidligere tjeneste. Gamle bilag kan fortsat være relevante, efter at den synlige applikation er skiftet.
HANDLING	Den hjemmesideansvarlige bør kontrollere sletning, flytning og adgangsforhold for udfasede tjenester, herunder sikkerhedskopier og bilag hos leverandøren.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Tjeklisten ved lukning af en erstattet applikation bør navngive den ansvarlige for de resterende data. Ansvaret bør bestå efter hostingkontraktens ophør. Under en hændelse har supportteams brug for nok information til præcist at identificere den berørte indsendelsesperiode. De bør undgå at fortælle alle tidligere klagere, at deres materiale var omfattet, når meddelelsen beskriver en snævrere gruppe.

SAG R

R ■ Maersks overtagne system krævede en afgrænset redegørelse

Maersk

bekræftet adgang; aktørpåstand særskilt

BEKRÆFTET	Maersk oplyste den 11. november, at et lokalt, ældre it-system fra et tidligere opkøb havde været udsat for uautoriseret adgang og udtræk af data. Virksomheden så ingen tegn på påvirkning af andre systemer eller kunde- og partnergrænseflader. Den forventede ikke forstyrrelser af kundernes drift. [S10]

AFGRÆNSNING	Offentlig omtale viderebragte en kriminel gruppes påstande om datatyveri og afpresning. De står adskilt fra virksomhedens redegørelse. Meddelelsen bekræfter ikke kryptering af Maersks globale it-miljø eller forstyrrelse af søtransporten. [S10][S11]
VURDERING	Integration efter opkøb bør omfatte en udtrykkelig beslutning om overtagne systemer, deres data og forbindelser. Et lokalt afgrænset system kan stadig medføre en væsentlig oplysningspligt.
HANDLING	Opkøbs- og sikkerhedsansvarlige bør identificere bevarede, ældre tjenester, begrænse adgangen og aftale udfasning eller support med en navngiven forretningsansvarlig.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Et overtaget system kræver aktuelle svar på tre spørgsmål: Hvem bruger det, hvilke oplysninger opbevarer det, og hvordan er det forbundet med koncernen? Beredskabet bør kunne isolere det uden gæt om disse afhængigheder. Kommunikationen bør beskrive den faktiske systemgrænse. Et velkendt virksomhedsnavn bør ikke gøre et lokalt fund til en udokumenteret fortælling om globalt driftsstop.

S

SAG S

Hotelreservationer gjorde falske betalingskrav troværdige

Techotel

bekræftet læk; svindeludfald ikke opgjort

BEKRÆFTET	Techotels offentlige hændelseslog beskrev en læk af reservationsoplysninger, som blev erkendt den 7. november. Opdateringerne i november omtalte undersøgelse, kundehjælp og fortsatte mistænkelige beskeder. En opdatering den 19. november henviste til fornyet læk den 15. og 16. november. Senere opdateringer oplyste, at lækken var lukket, men advarede om fortsat brug af tidligere kopierede oplysninger. [S18]
AFGRÆNSNING	Offentlig omtale beskrev falske betalingskrav på WhatsApp med oplysninger fra reservationer. En overbevisende besked beviser hverken, at alle modtagere betalte, eller at hotellernes betalingssystemer var påvirket. [S18]
VURDERING	Korrekte reservationsoplysninger kan få et eksternt svindelforsøg til at ligne en almindelig del af et hotelophold. Teknisk inddæmning gør ikke angriberens eksisterende kopi ubrugelig.
HANDLING	Hoteller bør advare gæster gennem kendte kanaler og kræve, at medarbejdere kontrollerer ændrede betalingsinstruktioner uafhængigt af den indgående besked.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Reservationsmedarbejdere har brug for et standardsvar til gæster, der modtager et betalingskrav. Det bør forklare, hvordan hotellet modtager betaling, og hvordan gæsten kan kontrollere et krav gennem en betroet kontaktvej. Medarbejdere bør bevare eksempler til undersøgelsen uden at videresende eksponerede gæsteoplysninger bredt. Advarslen bør fortsat være tilgængelig efter den umiddelbare tekniske reparation.

T

SAG T

Én printleverandørhændelse førte til flere kundemeddelelser

Offentligt omtalt tjeneste

bekræftede kundemeddelelser

BEKRÆFTET	To organisationers novembermeddelelser beskrev en hændelse hos en fælles print- og distributionsleverandør. Den ene skelnede mellem omkring 75.000 modtagere af tryksager og upåvirkede digitale abonnenter. Den anden beskrev kopierede kontakt- og abonnementsoplysninger, men udelukkede CPR-numre og betalingskortoplysninger fra sit berørte datasæt. [S49][S50]
AFGRÆNSNING	Det er kundespecifikke redegørelser om en leverandørkæde. Antallene bør ikke lægges sammen, før eventuelt overlap er fastslået. Én kundes undtagelser bør heller ikke overføres til en anden kundes data. [S49][S50]
VURDERING	Almindelige distributionsydelser kan samle værdifulde kontaktoplysninger fra mange organisationer. En leverandørhændelse kan føre til flere offentlige meddelelser uden at være flere uafhængige indbrud.
HANDLING	Abonnements- og kommunikationsansvarlige bør minimere dataudtræk til distribution og aftale hurtig, kundespecifik hændelsesrapportering med leverandørerne.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Dataminimering bør følge det faktiske leveringsbehov. En leverandør, der udarbejder adresselabels, behøver ikke nødvendigvis alle felter fra kundesystemet. Den kontraktansvarlige bør også aftale sletning efter hver produktionsrunde. Under en hændelse har hver kunde brug for sit eget overblik over de berørte datafelter, så orienteringen forbliver præcis og relevant.

SAG U

U

BrickLink genåbnede og lukkede derefter igen som forholdsregel

BrickLink

bekræftet nedlukning; senere datapåvirkning uafklaret

BEKRÆFTET

BrickLinks meddelelser og offentlig omtale beskrev en tidligere afbrydelse i november efterfulgt af genåbning. En senere officiel meddelelse oplyste, at fornyet usædvanlig aktivitet den 19. november fik platformen til at lukke igen. Tjenesten var fortsat lukket ved skæringsdatoen. [S19]

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Bricksets omtale den 12. november af BrickLinks tidligere meddelelse beskrev adgang til brugernavne, IP-adresser og et meget lille antal e-mailadresser. Ifølge omtalen var der ikke adgang til adgangskoder eller finansielle oplysninger. Afgrænsningen vedrører den tidligere afbrydelse; datafølgerne af nedlukningen den 19. november var fortsat uafklarede. [S61]

- **Afgrænsning.** En nedlukning som forholdsregel bekræfter påvirket tilgængelighed og en undersøgelse. Den bekræfter ikke et nyt tyveri af betalingsoplysninger. En planlagt genåbningsdato er en forventning, ikke en afsluttet genopretning. [S19]
- **Vurdering.** Genåbning er et beslutningspunkt i hændelseshåndteringen. Fortsat overvågning og klare kriterier for at lukke igen er nødvendige, selv når platformen ser klar ud til at genoptage driften.
- **Handling.** Markedspladsoperatører bør aftale genåbningskriterier, overvåge gentagelser og opretholde en tilgængelig statuskanal, som er uafhængig af den berørte platform.

Kunder og sælgere har også brug for vejledning om igangværende handler og uventede e-mails under nedetid. Hændelsesteamet bør skelne almindelige automatiske beskeder fra anmodninger, der kræver kontrol. Løbende opdateringer bør bevare en klar tidslinje for den første afbrydelse, genopretningen og den nye forholdsregel. Det mindsker risikoen for at forveksle en gammel meddelelse med den aktuelle driftsstatus.

SAG V

V

En leverandøradvarsel bekræftede ikke tyveri af kundedata

Offentligt omtalt tjeneste

leverandørhændelse; kompromittering hos kunden ikke fastslået

BEKRÆFTET

En medlemsorganisations opdatering beskrev en hændelse den 16. november hos leverandøren af dens webplatform. Sagen var ifølge meddelelsen håndteret samme dag, mens analysen fortsatte. Der var ingen tegn på påvirkning af data fra medlemsorganisationens hjemmeside. [S51]

AFGRÆNSNING	En organisations medlemstal er ikke et antal berørte personer. En sårbarhed eller sikkerhedshændelse hos en leverandør bekræfter ikke dataudtræk hos alle kunder eller hos denne kunde. [S51]
VURDERING	En forebyggende leverandørmeddelelse kræver handling, selv når et kundebrud ikke er bekræftet. Indsatsen bør følge kundens faktiske eksponering og dokumentation.
HANDLING	Den applikationsansvarlige bør indhente leverandørens tidslinje, bekræfte den berørte komponent og version og dokumentere grundlaget for sin egen vurdering af kundepåvirkningen.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Spørgsmålene til leverandøren bør skelne mellem udbedring og tekniske undersøgelsesresultater. En rettelse kan lukke en adgangsvej uden at afklare, om den blev brugt. Kunden bør opretholde passende overvågning, mens spørgsmålet står åbent. Eksterne opdateringer bør præcist forklare det aktuelle fund uden at gøre hele leverandørens kundebase til en gruppe ofre.

W

SAG W

En specialiseret informationstjeneste fandt tidligere adgang ved gennemgang

bekræftet

Offentligt omtalt tjeneste

BEKRÆFTET	En specialiseret offentlig informationstjeneste oplyste den 4. november, at en gennemgang havde fundet uautoriseret adgang den 22. oktober. Meddelelsen beskrev en downloadet brugerliste med omkring 5.000 registrerede brugere. Felterne omfattede kontaktoplysninger, krypterede adgangskoder og et erhvervsrelateret licensnummer. [S52]
AFGRÆNSNING	Meddelelsen vedrørte brugeradministrationen for en bestemt tjeneste. Den bekræfter ikke forstyrrelse af de bredere driftsfunktioner, som forbindes med organisationens sektor. [S52]
VURDERING	En senere sårbarhedsadvarsel kan afdække en tidligere hændelse. Opdagelse, adgang og offentliggørelse kræver derfor særskilte datoer, selv når indsatsen følger hurtigt efter opdagelsen.
HANDLING	Den tjenesteansvarlige bør gennemgå historisk adgang efter en relevant advarsel, nulstille berørte adgangskoder og give brugerne klare råd om genbrug af samme kode andre steder.

Konklusion

Kontrollér den bekræftede afgrænsning af konto, data og tjeneste, før indsatsen vælges.

Specialportaler bør indgå i organisationens applikationsfortegnelse, selv når brugergruppen er forholdsvis lille. Oplysningerne kan omfatte identifikatorer, som er usædvanlige i almindelige kundesystemer. Sikkerhedsteams bør vurdere felterne direkte frem for at bruge den generelle betegnelse kontaktoplysninger. Indsatsen bør også sikre, at berørte brugere kan finde pålidelig vejledning uden at logge ind på den berørte tjeneste.

X

SAG X

En browserafhængighed kunne ændre betalingsmodtagere

Browserafhængighed

Officiel redegørelse med afgrænsning

BEKRÆFTET	Adforms augustopdatering daterer den skadelige aktivitet til den 26.–27. juli. Den fjernede kode kunne ifølge virksomheden erstatte adresser på kryptovalutategnebøger, mens en berørt hjemmeside var åben. Virksomheden oplyste, at der ikke skete yderligere spredning efter inddæmningen den 27. juli. [S66]
AFGRÆNSNING	Adform oplyste, at koden ikke var udviklet til at installere software eller forblive på enheden. Den senere vurdering kunne ikke udelukke videregivelse af begrænsede browsingoplysninger på berørte HTTP-sider. Virksomheden havde ingen dokumentation for overførsel af kontoers legitimationsoplysninger eller hjemmesidernes indhold. [S66]
VURDERING	Et tredjepartsscript kan påvirke den viste betalingsdestination i browseren, selv når hjemmesidens egen applikation er tilgængelig. Et rent resultat fra enhedskontrollen besvarer ikke alene, hvad der skete, mens siden var åben.
HANDLING	Hjemmesideejere bør identificere den relevante afhængighed og berørte periode, følge leverandørens hændelsesvejledning og hjælpe brugere med at kontrollere relevante transaktionsmodtagere.

Konklusion

Adskil fortsat drift, dataomfang og belæg for faktisk misbrug.

Adforms redegørelse og teknisk omtale fastslår ikke et antal danske besøgende, et verificeret tab eller en angriberidentitet. [S66][S67]

Bed i en øvelse den hjemmesideansvarlige identificere de tredjepartstjenester, der kan ændre det, en besøgende ser. Test derefter, hvem der kan deaktivere afhængigheden, kommunikere den berørte periode og kontrollere en sikker genstart. Behandl videregivelse af data, ændrede betalingsoplysninger og installeret software som særskilte undersøgelsesspørgsmål.

SAG Y

Y

En detailkæde holdt kundebetjeningen i gang under en intern hændelse

Detailhandel

Officiel redegørelse med afgrænsning

BEKRÆFTET	En stormagasinkædes meddelelse den 21. oktober oplyser, at uautoriseret aktivitet opdaget den 18. oktober påvirkede interne funktioner. Nogle butikker brugte i begyndelsen mere manuelle arbejdsgange. Butikker, kassefunktioner og webshop fortsatte driften. [S68]
AFGRÆNSNING	Virksomheden var stadig ved at fastslå, hvilke kunde-, medarbejder- og partneroplysninger der kunne være berørt. Ifølge virksomheden lå kundernes betalingskortoplysninger uden for de berørte systemer. Fortsat handel bekræfter ikke, at alle interne processer var upåvirkede. [S68]
VURDERING	Kontinuitet bør måles ud fra forretningsopgaven. En fungerende kasse kan eksistere samtidig med påvirkede administrative systemer og en uafklaret undersøgelse af personoplysninger.
HANDLING	Ansvarlige for detailtjenester bør teste minimumsløsninger for handel, medarbejderinstruktioner og afstemning, mens adgangen til interne systemer er begrænset.

Konklusion

Adskil fortsat drift, dataomfang og belæg for faktisk misbrug.

En øvelse bør gøre forskellen tydelig for ledelsen. Spørg, hvilke kundeopgaver der fortsætter, hvilke medarbejderopgaver der kræver midlertidige alternativer, og hvem der efterfølgende kontrollerer transaktionerne. Hold driftsstatus og vurderingen af dataomfang adskilt i kundekommunikationen.

SAG Z

Z

En rejseinformationstjeneste skelnede mellem e-maileksponering og bookingsystemer

Rejseinformation

Officiel redegørelse med afgrænsning

BEKRÆFTET	Travelmarkets officielle meddelelse beskriver en hændelse opdaget den 15. januar, som vedrørte databaser til prisalarmer og nyhedsbreve. Ifølge meddelelsen bestod de tilgængelige brugeroplysninger af e-mailadresser. [S69]
OMTALT	Teknisk omtale i februar omtaler særskilt en ransomwarehændelse hos virksomheden i januar. [S70]

AFGRÆNSNING	Virksomheden oplyser, at den ikke opbevarer brugernes bank-, betalings- eller bookingoplysninger. De forhold hører til hos den rejseudbyder, som bookingen blev foretaget hos. En hændelse hos sammenligningstjenesten bekræfter ikke eksponering hos alle de rejseselskaber, den henviser til. [S69]
VURDERING	En tjenestes kommercielle forbindelse til en rejse er noget andet end opbevaring af passagerens booking- og betalingsoplysninger. Indsatsens omfang bør følge den faktiske datastrøm.
HANDLING	Ansvarlige for rejse- og sammenligningstjenester bør vedligeholde en klar datafortegnelse og forklare, hvilken udbyder der kan besvare hver kundes spørgsmål om hændelsen.

Konklusion

Adskil fortsat drift, dataomfang og belæg for faktisk misbrug.

Den dataansvarlige bør kontrollere de berørte kontaktlister og stille en kontaktvej til rådighed for mistænkelige beskeder, der bruger virksomhedens navn. Den infrastrukturansvarlige bør teste genopretning mod den nødvendige kundeservice. Ingen af øvelserne kræver, at man antager, at presseomtalen af indbruddet er fuldstændig.

En anden omtalt meddelelse i restaurationsbranchen

En presseartikel den 3. november citerer en restaurants kundemail om uautoriseret adgang til e-mailadresser hos dens reservationsleverandør. Den angiver intet antal berørte personer og oplyser, at eksponering af betalingsoplysninger og adgangskoder ikke var rapporteret. Dette er fortsat en kundemeddelelse gengivet i pressen, og organisationerne navngives ikke her. Den dokumenterer ikke adgang til restaurantens egne systemer. [S71]

5.5 Seneste aktivitet: 8. til 22. november 2026

Perioden omfatter nye offentliggørelser, fortsatte undersøgelser, genopretningsopdateringer og myndighedsindsatser. Den bør ikke fremstilles som en liste over indbrud, der netop er begyndt. Datoerne nedenfor angiver den relevante offentlige begivenhed.

Dato	Datotype	Udvikling	Betydning for sikkerhedsarbejdet
9. november	Myndighedsafgørelse	En afgørelse om opbevaring af data vedrørte adgang hos en bilforhandler i december 2024, opdaget i januar 2025. Det er en ny afgørelse om en ældre hændelse. [S23]	Gennemgå slettefrister og dokumentér, at gamle oplysninger fjernes.

Dato	Datotype	Udvikling	Betydning for sikkerhedsarbejdet
11. november	Virksomhedsmeddelelse	Maersk oplyste om uautoriseret adgang og dataudtræk fra et lokalt, overtaget system. [S10]	Medtag overtagne og ældre applikationer i hændelsesansvaret.
11. november	Medieomtale	En uddannelsesinstitutions meddelelse vedrørte adgang, der ifølge omtalen begyndte i marts. [S48]	Skeln mellem datoer for adgang, opdagelse og orientering.
12. november	Politiindsats offentliggjort	Dansk politi beskrev fjernelse af skadelig kode fra 681 hjemmesider i Danmark og udlandet under en international operation. [S24]	Behandl det som en indsats mod infrastrukturen, ikke som 681 danske ofre for databrud.
12.–13. november	Kundemeddelelser	Organisationer offentliggjorde meddelelser om en hændelse hos en printleverandør. [S49][S50]	Bed leverandører om kundespecifikke datasæt og afgrænsninger af påvirkningen.
16. november	Dato for leverandørhændelse	En webplatformkunde beskrev en leverandørhændelse uden dokumentation for påvirkning af egne hjemmesidedata. [S51]	Fastslå eksponeringen, før et antal berørte personer angives.
19. november	Genopretningsopdatering	DTU oplyste, at indsatsen var afsluttet. [S13]	Kontrollér gendannede identitetskontroller, og fasthold læring fra hele forløbet.
19. november	Forebyggende nedlukning	BrickLink tog platformen offline efter fornyet usædvanlig aktivitet. [S19]	Brug udtrykkelige kriterier for genåbning og ny nedlukning.
19.–22. november	Fortsatte opdateringer	Techotel beskrev fornyet læk og fortsat risiko for reservationsbaseret svindel efter inddæmning. [S18]	Oprethold gæsternes kontrolvejledning efter reparationen.

Politioperationen er væsentlig, fordi den vedrører fjernelse af infrastruktur brugt til at levere skadelig kode. Blandingen af danske og udenlandske hjemmesider forhindrer et rent dansk offertal. Tilsvarende hører forhandlerafgørelsen til læring om styring, mens selve angrebet ligger uden for rapportens hændelsesperiode. Ingen af delene bør øge et tal for indbrud i november. [S23][S24]

5.6 Beslutninger på baggrund af sagerne

Første prioritet er at gøre identitetsgendannelse sikker og kontrollerbar. Nulstillingskanaler, nye godkendelsesfaktorer og rettighedsændringer kræver sammenhængende overvågning og en klar ansvarlig. Det gælder både gæster, tidligere brugere og medarbejdere. En beredskabsøvelse bør kræve, at teamet finder yderligere adgang, som blev oprettet efter den første kompromittering.

Anden prioritet er at vide, hvor opbevarede oplysninger findes. Testdatabaser, udfasede hjemmesider, bygningssystemer og distributionsudtræk skal alle have en ansvarlig ejer. Følsomheden følger indholdet. Organisationen bør kunne beskrive indholdet uden at vente på, at en hændelse tvinger den til at rekonstruere gamle kontrakter og dataflytninger.

Tredje prioritet er at gøre leverandørberedskabet anvendeligt. En generel leverandørerklæring er et udgangspunkt. Kunder har brug for deres egne berørte datafelter, relevante datoer og tjenesteafhængigheder. Kontrakter og øvelser bør sikre hurtige svar. Orienteringer bør skelne mellem en leverandørhændelse og en bekræftet kompromittering af kundens systemer.

Endelig kræver genopretningskommunikation fortsat opmærksomhed. En genåbnet tjeneste kan lukke igen, og kopierede oplysninger kan understøtte svindel, efter at den oprindelige adgangsvej er repareret. Hold statussiden opdateret, forklar ændringerne, og giv berørte brugere én pålidelig kontrolvej. Udpeg en ansvarlig for kommunikationen frem til hændelsens afslutning.

5.7 Aktuelle sårbarheder: afklar relevans før tilskrivning

To advarsler fra november kræver en hurtig kontrol af, om systemerne er berørt. De beskriver produktsårbarheder og dokumenterer ikke, at danske organisationer blev angrebet eller påvirket. Hold kontrol af rettelser adskilt fra undersøgelse af mulig tidligere adgang.

Apaches advarsel beskriver CVE-2026-119618 i HTTP/2-modulet. De berørte upstream-versioner af HTTP Server er 2.4.55–2.4.70. Version 2.4.71 blev frigivet den 11. november. NVD-registreringen angiver samme berørte versionsinterval. [S34][S35]

DKCERT's advarsel den 12. november siger, at HTTP/2 skal være aktiveret, og anbefaler hurtig opdatering. Distributionspakker kan have egne versioner og sikkerhedsopdateringer. Kontrollér leverandørens pakkestatus frem for udelukkende at vurdere den viste upstream-version. [S36]

Broadcoms advarsel den 19. november, opdateret den 20. november, beskriver CVE-2026-123890 som omgåelse af godkendelse i vCenter Directory Service. Den kræver netværksadgang til vCenter og angiver ingen midlertidig omgåelsesløsning. NVD-registreringen og leverandørens matrix vedrører produktfejlen. Ingen af dem dokumenterer udnyttelse i Danmark. [S37][S38]

Mandiant rapporterede udnyttelse af denne vCenter-sårbarhed i begyndelsen af september 2026. Det dokumenterer ikke udnyttelse i Danmark. Medtag denne historik i vurderingen af mulig tidligere adgang. [S72]

Tabellen viser de relevante berørte versionsgrene og henvisninger til udbedring.

Sårbarhed og komponent	Berørt område	Rettet version eller fremgangsmåde
CVE-2026-119618, Apache HTTP Server	Upstream 2.4.55–2.4.70 med HTTP/2 aktiveret	2.4.71; leverandørens pakkeopdatering, hvor det er relevant
CVE-2026-123890, vCenter 9.1.x	Før den relevante rettelse	9.1.1.0200
CVE-2026-123890, vCenter 9.0.x	Før den relevante rettelse	9.0.2.0200
CVE-2026-123890, vCenter 8.0	Før den relevante rettelse	8.0 U3m
CVE-2026-123890, vCenter 7.0	Angivet som berørt i Broadcoms matrix [S38]	Kunder med udvidet support bør kontakte Broadcom Support
CVE-2026-123890, samlede VMware-platforme	Relevante VCF- og Telco Cloud-installationer i matricen	Følg den produktspecifikke responsmatrix og tilknyttede vejledning

[S34][S36][S38]

Den infrastrukturansvarlige bør identificere relevante installationer, bekræfte den understøttede udbedringsvej og opdatere hurtigt. Tjenesteansvarlige bør aftale genopretningskontroller og efter ændringen bekræfte, at den forventede build kører.

Registrér en udtrykkelig beslutning om undersøgelse af tidligere adgang. En vellykket opdatering bekræfter den nye rettelsesstatus. Den fastslår ikke, om den tidligere sårbare periode var fri for indbrud. Bevar relevant dokumentation gennem den godkendte hændelsesproces, når tegn giver grund til undersøgelse.

Sikkerhedsfunktionen bør rapportere tre resultater særskilt: systemer, der kræver udbedring, systemer med verificerede rettelser og systemer, der kræver yderligere undersøgelse. En ukendt systemejer eller en ikke-understøttet versionsgren kræver en ansvarligt godkendt undtagelse og en afklaringsdato.

HOVEDPOINTER

01

Tilpas hver indsats til den bekræftede redegørelse og afgrænsningen af data og tjenester.

02

Skeln mellem leverandørhændelser, kundemeddelelser og forholdsregler, når hændelser tælles.

03

Bevar skellet mellem datoer for indbrud, offentliggørelse og genopretning.

KAPITEL 06

Hacktivisme, DDoS og forbundne systemer

06

DETTE KAPITEL BESVARER

Hvad adskiller en påstand om afbrydelse fra verificeret tjenestepåvirkning eller ændring af en fysisk proces?

3

særskilte spørgsmål: tilgængelighed, dataadgang og fysisk påvirkning

6.1 Tidslinje for påstande, omtale og officielle vurderinger 57
6.2 En webstedspåstand kræver svar om tjenesten 58
6.3 Direkte meddelelser bevarer deres begrænsninger som påstande 58
6.4 Senere påstande kræver særskilt dokumentation 59
6.5 Kameraadgang og kølestyring kræver forskellige kontroller 61
6.6 Trusselsvurderinger vejleder forberedelse, ikke efterfølgende optælling 62
6.7 Dokumentation for beredskab 63

KAPITEL 06

Hacktivisme, DDoS og forbundne systemer

KORT FORTALT

Det offentlige danske materiale indeholder DDoS-påstande, afgrænsede bekræftelser af afbrydelser og advarsler om forbundet udstyr. De beskriver forskellige hændelser. Et utilgængeligt websted dokumenterer ikke adgang til interne systemer, og et kamerabillede dokumenterer ikke styring af en industriproces. Novembers kølemeddelelser efterlader også dansk påvirkning og ansvar uafklaret. Verificér driftsstatus, bevar lokal evidens, og giv tekniske, driftsmæssige og kommunikative beslutninger særskilte ansvarlige.

6.1 Tidslinje for påstande, omtale og officielle vurderinger

Tidslinjen skelner mellem offentlige vurderinger og hændelsesbekræftelser. En advarselsdato er ikke datoen for en ny dokumenteret indtrængen.

13 jan. 2026	**SAMSIK** Advarer om påstande vedrørende danske overvågningskameraer og opfordrer til sikkerhedsgennemgang af udstyret [S40]
28 jan. 2026	**inteid** Offentliggjorde påstande om danske offentligt tilgængelige tjenester; koalitionstilknytningen er selvbeskrevet [S1]
2 feb. 2026	**inteid** Offentliggjorde endnu en tjenestepåstand; virkning og operatørtilskrivning er ubekræftede [S1]
18 feb. 2026	**TjekDet** Omtaler en DDoS-kampagne i januar–februar med forskellige officielle beskrivelser af tjenestepåvirkningen [S41]
27 feb. 2026	**PET, FE og SAMSIK** Offentliggør en valgrelateret vurdering af udenlandsk påvirkning; ingen konklusion om valgresultatet [S9]
10 mar. 2026	**SAMSIK** Vurderer DDoS-truslen som høj og anbefaler forberedelse på tværs af internetvendte tjenester [S8]
30 jun. 2026	**SAMSIK** Advarer om en skærpet destruktiv trussel, herunder datasletning og risici for operationel styring [S42]
24 sep. 2026	**SAMSIK** Hæver vurderingen af truslen fra destruktive cyberangreb fra middel til høj [S43]
2 nov. 2026	**SAMSIK** Undersøger, om danske virksomheder er berørt af europæiske kølesystemangreb [S25]
5 nov. 2026	**SAMSIK**

Siger, at styrelsen hverken kan be- eller afkræfte rollen for to grupper, der hævder ansvar for køleangrebene [S26]

6.2 En webstedspåstand kræver svar om tjenesten

TjekDets februaromtale beskriver næsten 40 websteder i en kampagne. De citerede officielle svar er forskellige: nogle tjenester havde afbrydelser, mens andre forblev tilgængelige for danske brugere eller håndterede forsøget uden nedetid. [S41]

Omtalen indeholder også en retslig tjenestes beskrivelse, som afgrænser hændelsen til overbelastning af webstedet uden adgang til bagvedliggende systemer. Et særskilt svar fra en transporttjeneste siger, at rejser og kundedata var upåvirkede. Det er afgrænsede udsagn om bestemte tjenester. [S41]

Beskrivelserne understøtter ikke 40 bekræftede afbrydelser, en fælles indtrængningsvej eller et samlet antal berørte borgere. En påstand kan vedrøre én offentlig side, mens den væsentlige tjeneste følger en anden teknisk vej.

SAMSIK's vejledning fra 10. marts udvider forberedelsen ud over websteder. Den omfatter bagvedliggende internetvendte tjenester og anbefaler leverandøraftaler, opdateret udstyr, overvågning og en afprøvet beredskabsplan. Vurderingen af høj trussel er styrelsens, ikke en hændelsesoptælling. [S8]

For en tjenesteansvarlig er den praktiske målestok brugerens legitime opgave. Kan personen finde information, gennemføre en booking eller nå support? Registrér, hvilken opgave der svigtede, for hvem, hvor længe og via hvilken alternativ kanal.

6.3 Direkte meddelelser bevarer deres begrænsninger som påstande

Det bevarede materiale omfatter meddelelser dateret 28. januar og 2. februar under aliasset inteid. Januar-opslaget beskriver deltagelse i en koalition kaldet Russian Legion. Det er afsenderens egen beskrivelse, ikke rapportens konklusion om fælles kontrol, nationalitet eller statslig styring. [S1]

Opslagene henviser til danske organisationers offentligt tilgængelige tjenester. Målnavne, identificerende beskrivelser og tjenestelinks er udeladt. Henvisningerne dokumenterer ikke adgang til systemer, der understøtter driften, datatyveri eller fysiske procesvirkninger. En beskrivelse af en organisations forretning beviser ikke, at driften blev afbrudt.

Februar-beskeden påstår aktivitet mod en offentligt tilgængelig tjeneste. En særskilt offentlig tidslinje kan dokumentere, hvad organisationen eller en journalist rapporterede om tilgængeligheden. Selv samme dato beviser ikke, at afsenderen forårsagede det rapporterede nedbrud, eller at registreringerne beskriver samme tekniske hændelse. [S1]

Evidenskort B07 28 jan. 2026

inteid Kanalopslag Telegram RU

ORIGINALTEKST

наносим удары по инфраструктуре Дании

OVERSÆTTELSE

Vi angriber Danmarks infrastruktur.

Bemærkning. Opslaget angiver en koalitionstilknytning som afsenderens egen beskrivelse. Målhenvisningerne vedrører offentligt tilgængelige tjenester; ingen virkning på national infrastruktur er verificeret.

Dokumenteret
En aktørmeddelelse, som påstår aktivitet mod danske organisationer og henviser til links med tilgængelighedskontrol.

Ikke fastslået
Et verificeret nedbrud, dataadgang, fysisk procesvirkning, en fælles operatør eller styring fra den russiske stat.

Evidenskort B08 2 feb. 2026

inteid Kanalopslag Telegram RU

ORIGINALTEKST

Удар по сайту [организации]

OVERSÆTTELSE

Et angreb mod [en organisations] hjemmeside.

Bemærkning. Organisationens navn, identificerende rolle og tjenestelinks er udeladt. En særskilt pressetidslinje kan belyse tilgængeligheden, men identificerer ikke operatøren.

Dokumenteret
Endnu en aktørmeddelelse med henvisning til en dansk, offentligt tilgængelig tjeneste.

Ikke fastslået
Bekræftet driftsforstyrrelse, adgang til bagvedliggende systemer, datatab eller tilskrivning af et særskilt rapporteret nedbrud til denne afsender.

Hold tre observationer adskilt: En aktør offentliggjorde en påstand, en tjeneste blev observeret utilgængelig, og en organisation bekræftede sit eget hændelsesomfang. Påstandene kan understøtte forskellige handlinger. Relevante påstande begrunder kontrol af egne tjenester og beredskab; bekræftet intern dokumentation afgør inddæmning og genopretning.

De bevarede meddelelser bekræfter ikke deres egne trusler om optrapning. Rapporten udelader politiske ultimatummer og retoriske slogans. Den udleder ikke gennemførelse, en fælles operatør eller støtte fra en stat af koalitionsnavnet.

Den organisationsrelaterede opslagkontekst registrerer yderligere påstande om offentlige websteder dateret 28. januar og 6. april. En besked fra 3. februar hævder også adgang til interne netværk, kommunikation, design og kundedata på tværs af offentlige og kommercielle tjenester. Påstandene er fortsat ubekræftede. Eksterne tilgængelighedstjek dokumenterer ikke intern adgang, informationstab eller en fælles operatør. [S3]

6.4 Senere påstande kræver særskilt dokumentation

Opslag fra 23., 26., 27. og 28. marts bærer signaturen NoName057(16). De hævder at have forstyrret hjemmesider for danske offentlige tjenester og virksomheder, herunder hjemmesider i energisektoren. Links til tilgængelighedstjek er en del af afsenderens fremstilling. De dokumenterer ikke nedetidens varighed, intern adgang eller påvirkning af energiforsyningen. Spanske versioner gentager flere meddelelser; gentagelse giver ikke et uafhængigt vidne. [S1]

En meddelelse fra 23. marts omtaler tjenester i Grønland. Det er kildens angivne målområde. Rapporten tager ikke stilling til Grønlands status og udleder hverken en fælles hændelse på tværs af tjenesterne eller valgpåvirkning af opslagets politiske fremstilling.

Et særskilt engelsksproget opslag fra 28. september bærer samme signatur. Det hævder adgang til et industrielt kontrolpanel i Danmark samt læsbare indstillinger og logfiler. Det hævder desuden, at indstillinger blev ændret, og processer standset. Dette er en påstand om procespåvirkning, adskilt fra påstandene om hjemmesider i marts. Det gemte opslag dokumenterer ikke anlæggets ejer, gennemførte ændringer, en fysisk driftsafbrydelse eller hvem der styrede systemet. Samme signatur dokumenterer ikke samme operatør. [S1]

Evidenskort B09 — 26 mar. 2026

NoName057(16) (signatur i opslaget) | Kanalopslag | Telegram | RU

ORIGINALTEKST

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

OVERSÆTTELSE

Danske hjemmesider modtager DDoS-hilsner [...] fra os.

Bemærkning. Opslaget bærer signaturen NoName057(16). Målidentifikatorer og links til tilgængelighedstjek er udeladt.

Dokumenteret
En signeret meddelelse med påstand om forstyrrelser af hjemmesider i Danmark.

Ikke fastslået
Uafhængigt bekræftet tilgængelighed, nedetidens varighed, intern adgang, påvirkning af energiforsyning, styring fra en stat eller fælles operatør.

Evidenskort B10 — 28 sep. 2026

NoName057(16) (signatur i opslaget) | Kanalopslag | Telegram | EN

ORIGINALTEKST

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

OVERSÆTTELSE

Vi greb lidt ind, ændrede indstillingerne og standsede processerne.

Bemærkning. Citatet er en påstand i et engelsksproget opslag. Identificerende udstyrsdetaljer og links er udeladt. Signaturen er ikke en bekræftet operatøridentitet.

Dokumenteret
Et opslag med påstand om adgang til et dansk industrielt kontrolpanel, læsbare indstillinger og logfiler, ændrede indstillinger og standsede processer.

Ikke fastslået
Anlæggets ejer, faktisk adgang, gennemførte ændringer, fysisk driftsafbrydelse, et indbrud i Danmark, styring fra en stat eller fælles kontrol med afsenderne i marts.

For en driftsansvarlig giver septemberpåstanden grund til at kontrollere fjernadgang, registrerede konfigurationsændringer og procesalarmer i egne data. Den giver ikke grundlag for at melde en bekræftet hændelse i industrielle systemer eller tilskrive afsenderen en driftsafbrydelse.

NoName057(16)

Signatur i opslag; ikke bekræftet operatøridentitet

Signatur knyttet til gemte påstande | Ingen styring fra en stat eller operatørsammenhæng fastslået

I DANMARK, 2026

23.–28. marts
Påstande om hjemmesiders tilgængelighed i gemte opslag

PÅSTÅEDE MÅL

Kildebeskrevne offentligt tilgængelige tjenester, et kontrolpanel og en udstyrsleverandør; identiteter udeladt

28. september
Særskilt påstand om industriel styring i et engelsksproget opslag

3. november
Yderligere leverandør-, proces- og legitimationspåstande; ubekræftede virkninger

I OFFENTLIG OMTALE

[S1] Egne data: bevarede opslag bærer denne synlige signatur; de hævdede virkninger er ubekræftede.

[S3] Egne belæg: et novemberopslag bærer samme synlige signatur; hævdede procesvirkninger og legitimationsoplysningernes oprindelse er ubekræftede.

VORES VURDERING

De gemte opslag dokumenterer offentliggjorte påstande. Marts-påstande om tilgængelighed, en særskilt kildeangivet Grønlandshenvisning og septemberpåstanden om processer holdes adskilt. Gentagen signatur dokumenterer ikke fælles kontrol, et bekræftet indbrud eller en fysisk virkning. Novembermateriale tilføjer leverandør-, proces- og legitimationspåstande uden at bekræfte virkninger eller oprindelse.

SIKKERHED I VURDERINGEN
Høj for offentliggørelsen og den synlige signatur; påståede tekniske virkninger ubekræftede

6.5 Kameraadgang og kølestyring kræver forskellige kontroller

SAMSIK's meddelelse fra 13. januar vedrører grupper, som hævder adgang til danske kamerabilleder. Styrelsen beskriver grupperne som prorussiske og anbefaler stærkere legitimationsoplysninger, opdateret udstyr og deaktivering af ubrugte funktioner. Den politiske betegnelse er fortsat styrelsens vurdering. [S40]

Behandl ikke et offentliggjort billede som en fuldstændig adgangsbeskrivelse. Operatøren skal fastslå udstyr, konto, optagelsestidspunkt og eksponering for egen installation. Undgå at sprede billeder, som identificerer uvedkommende personer eller steder.

Kølemeddelelserne fra november kræver en anden indsats. Den 2. november oplyste SAMSIK, at styrelsen undersøgte, om danske virksomheder var berørt. Den anbefalede gennemgang af direkte internetadgang, sikkerhedsopdateringer og begrænsninger, som bevarer kritiske funktioner. [S25]

Den 5. november oplyste SAMSIK, at to grupper havde påtaget sig ansvaret. Styrelsen kunne hverken be- eller afkræfte deres medvirken og vurderede, at det var for tidligt at fastslå deres rolle. Gentagelse af påstandene fjerner ikke usikkerheden. [S26]

Et opslag dateret 3. november bærer signaturen NoName057(16) og hævder webstedsforstyrrelser, virkninger på kølesystemer og eksponerede legitimationsoplysninger knyttet til en udstyrsleverandør. Det bevarede opslag dokumenterer ikke procesafbrydelse, legitimationsoplysningernes oprindelse eller verificeret intern indtrængen. Sprogvarianter giver ikke uafhængig bekræftelse. [S3]

Påstanden er adskilt fra myndighedsudtalelserne. Hverken opslaget eller dets eksterne tilgængelighedslinks fastslår, hvilke danske installationer der eventuelt oplevede fysisk påvirkning. Rapporten udleder ikke, at den officielle undersøgelse bekræfter netop denne leverandørpåstand.

Panelet knytter hver beslutning til den nødvendige evidens.

Spørgsmål	Påstand eller omtale	Officiel afgrænsning	Sikkerhedsansvarliges beslutning
Webstedspåvirkning	Kampagneomtale beskriver mange navngivne websteder [S41]	Citerede svar skelner mellem afbrydelser og håndterede forsøg [S41]	Afprøv den faktiske brugeropgave og registrér varigheden
Kameraadgang	Grupper hævder adgang til billeder [S40]	SAMSIK anbefaler udstyrsgennemgang; ingen fuldstændig berørt population angives [S40]	Validér installationen og begræns usikker adgang
Dansk kølepåvirkning	Angreb omtales andre steder i Europa [S25]	SAMSIK undersøger, om danske virksomheder er berørt [S25]	Kontrollér lokale målinger og autoriserede vedligeholdelsesoplysninger
Køleangrebs tilskrivning	To grupper påtager sig ansvaret [S26]	SAMSIK kan hverken be- eller afkræfte deres rolle [S26]	Inddæm verificeret eksponering uden at tilskrive en ubekræftet aktør

En bygningsansvarlig og en IT-ansvarlig bør aftale, hvem der kan begrænse fjernvedligeholdelse. Udstyrsleverandøren bør forklare, hvordan lokal styring og akut service fortsætter. Kontrollér fysiske målinger, før fordærv, sikkerhedsfølger eller procesmanipulation beskrives.

6.6 Trusselsvurderinger vejleder forberedelse, ikke efterfølgende optælling

SAMSIK's juniadvarsel beskriver en øget destruktiv trussel, herunder datasletning og manipulation af operationel teknologi. Septembervurderingen hæver trusselsniveauet til høj og vurderer det sandsynligt, at Rusland vil forsøge at udføre destruktive cyberangreb mod Danmark. Det er styrelsens tilskrevne vurderinger. [S42][S43]

De begrunder gennemgang af genopretning og styringsafhængigheder. De dokumenterer ikke, at enhver dansk afbrydelse var destruktiv, at alle påstande kom fra statsstøttede aktører, eller at novembers kølepåstande har fælles operatør.

PET, FE og SAMSIK's valgvurdering fra februar beskriver også risiko for udenlandsk påvirkning og begrænsede cyberangreb. Den er fremadskuende. Rapporten udleder ingen konklusion om et valgresultat eller en politisk beslutning af den. [S9]

Brug samme disciplin ved enhver politisk indrammet påstand. Bekræft tjenestens faktiske forhold, undgå at gentage slogans, og angiv uafklarede spørgsmål. En organisation kan forklare en afbrydelse uden at tilslutte sig aktørens årsagsforklaring.

6.7 Dokumentation for beredskab

Afprøv en afbrydelse af en offentlig tjeneste og en særskilt hændelse med forbundet udstyr. Øvelserne bør have forskellige tekniske og forretningsmæssige ansvarlige. En fungerende webreserve dokumenterer ikke sikker lokal udstyrsstyring.

Kontrol	Ansvarlig	Dokumentation for afslutning
Tjenestetilgængelighed	Digitale tjeneste- og netværksteams	Fejlet brugeropgave genskabt og alternativ drift demonstreret
Fjernadgang til udstyr	Bygningsansvarlig og autoriseret leverandør	Adgangsejerskab bekræftet og sikker begrænsning afprøvet
Fysisk kontinuitet	Drift	Lokale målinger, eskalationskanal og genopretningskriterier registreret
Offentlig opdatering	Kommunikation og hændelsesleder	Godkendt faktuel meddelelse med tidspunkt for næste opdatering

HOVEDPOINTER

01

Verificér legitim tjenestepåvirkning, før en afbrydelsespåstand gentages.

02

Hold kameraadgang, weboverbelastning og fysiske procesændringer adskilt.

03

Afprøv sikker begrænsning af fjernadgang og et brugbart driftsalternativ.

KAPITEL 07

Aktører, kampagner og evidensforbindelser

07

DETTE KAPITEL BESVARER

Hvilke aktørforbindelser understøttes, og hvilke konklusioner ville gå ud over evidensen?

29

danske ransomwareopslag i undersøgelsesperioden

7.1 Et kort over evidensforbindelser 65
7.2 Ransomwareopslag og regional kontekst 67
7.3 De førende betegnelser beskriver ikke én kriminel kæde 68
7.4 WhiteArmor: en omtalt påstand og en snævrere virksomhedsudtalelse 70
7.5 Officielle vurderinger er ikke en hændelsesvis tilskrivningsmatrix 71
7.6 Operation Endgame og indsatsens grænser 72
7.7 Hvad et aktørnavn bør ændre 72

KAPITEL 07

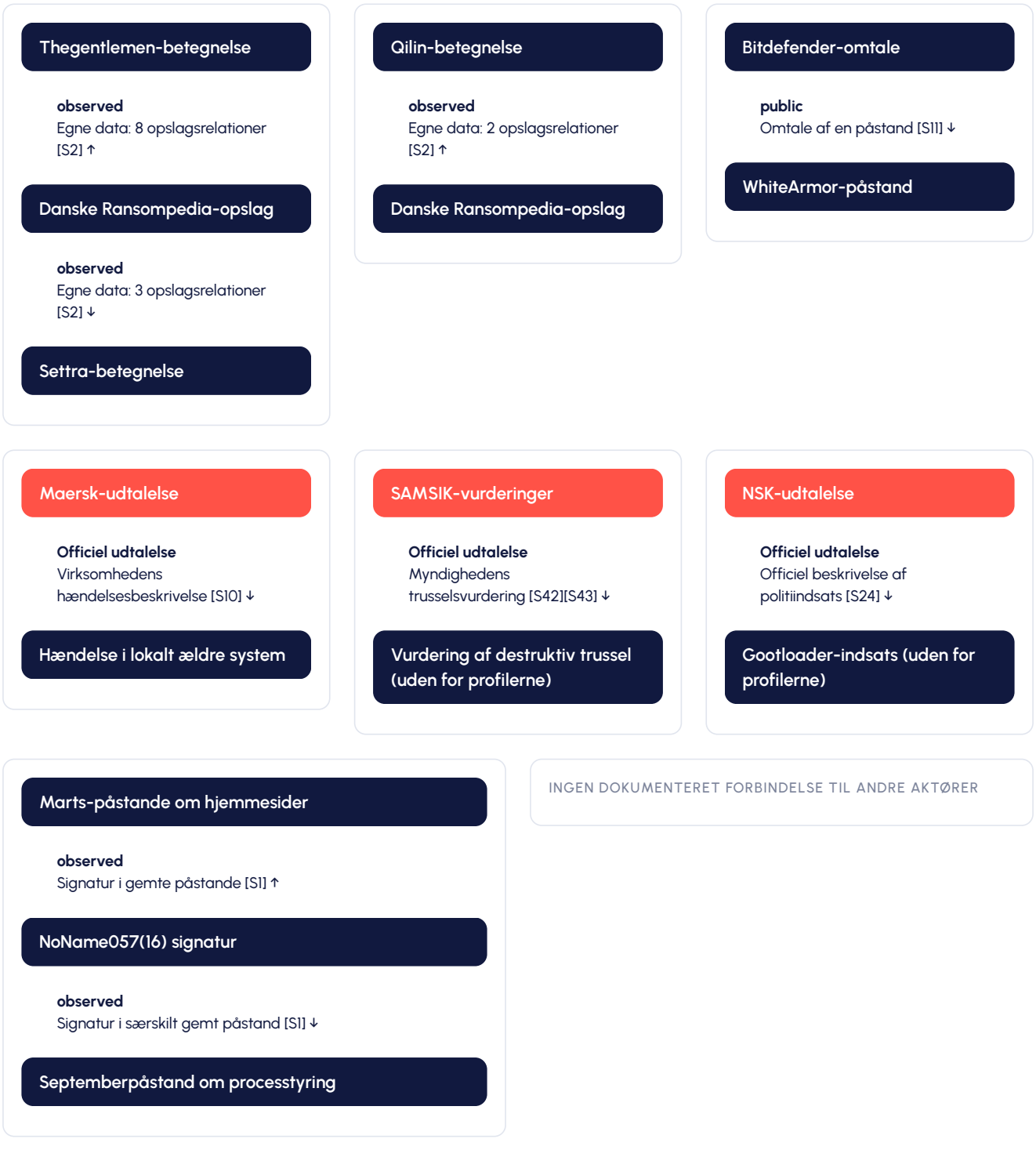
Aktører, kampagner og evidensforbindelser

KORT FORTALT

Ransompedia registrerer 29 danske opslag under 19 betegnelser. De er kriminelle påstande, adskilt fra bekræftede hændelser og statslige trusselsvurderinger. WhiteArmors omtalte påstand om Maersk går også ud over virksomhedens afgrænsede offentlige udtalelse. Officiel omtale af politiindsatser beskriver en anden del af det kriminelle miljø. Brug forbindelseskortet til at bevare kildegrænserne, og prioritér verificeret eksponering, driftsgenopretning og de konkrete konti.

7.1 Et kort over evidensforbindelser

Eget opslag Videreformidling Officiel udtalelse Offentlig omtale Vores observation



Kortet er en analytisk model af kildeforbindelser. Hver forbindelse angiver en observation i egne data, en tilskrevet vurdering eller offentlig omtale. Det dokumenterer ikke samarbejde, fælles infrastruktur eller fælles operatører blandt grupperne.

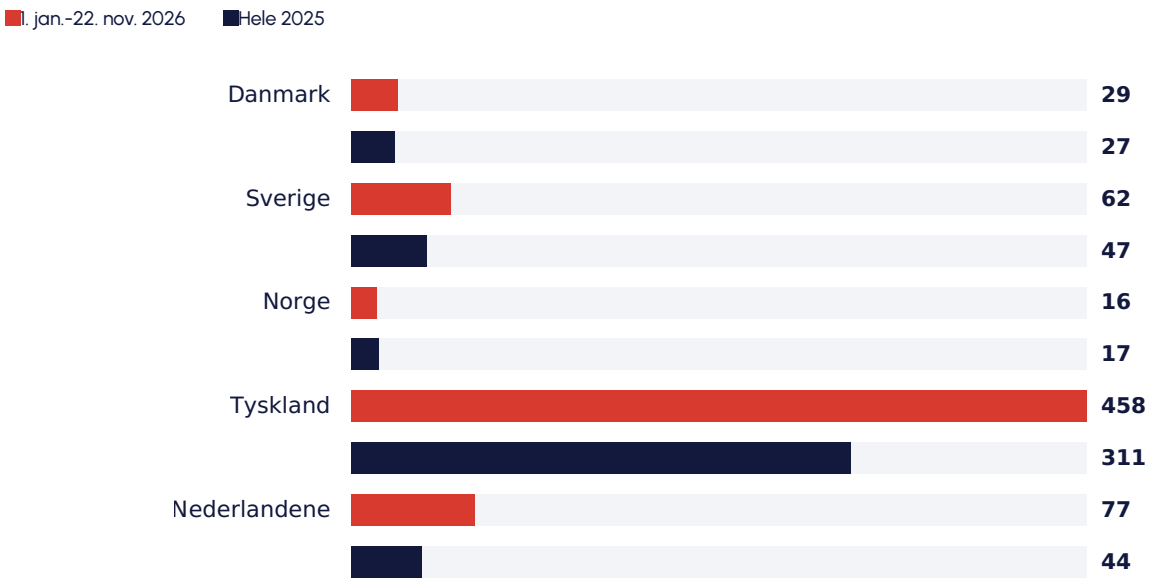
En Ransompedia-forbindelse registrerer en opslagsrelation i Brandefenses egne data. En leverandørartikel om en aktørs påstand er noget andet end virksomhedens hændelsesbekræftelse. Kortet holder forbindelserne adskilt. [S2][S10][S11]

Det samme gælder officielle advarsler. En myndigheds vurdering af en statslig trussel tilskriver ikke enhver rapporteret hændelse til den stat. Intet sprog, alias eller politisk udsagn dokumenterer her nationalitet eller statslig styring.

7.2 Ransomwareopslag og regional kontekst

Ransompedia registrerer 29 danske opslag fra 1. januar til 22. november 2026 mod 27 i hele 2025. Perioderne er forskellige. Det er en sammenligning af opslagspopulationer, ikke en vækstrate for samme periode. [S2]

Danske opslag indgår i en bredere regional afpresningspopulation



Kilde: Brandefense Ransompedia, 1. januar–22. november 2026 mod hele 2025 [S2]. Forskellige perioder, kildedækning og økonomier; ikke vækst for samme periode eller en national sikkerhedsrangliste.

Sammenligningslandene er udelukkende valgt som eksempler for at give kontekst; de indebærer ingen rangordning eller politisk vurdering.

Land	Opslag i undersøgelsesperioden	Hvad antallet beskriver
Danmark	29	Opslag med dansk landebetegnelse
Sverige	62	Opslag med svensk landebetegnelse
Norge	16	Opslag med norsk landebetegnelse
Tyskland	458	Opslag med tysk landebetegnelse
Nederlandene	77	Opslag med nederlandsk landebetegnelse

Alle tal vedrører samme undersøgelsesperiode. Økonomisk størrelse, rapportering og kildedækning er forskellige. Tallene rangerer ikke national risiko, kontrolkvalitet eller sandsynligheden for en hændelse hos den enkelte organisation. [S2]

Et opslag dokumenterer ikke kryptering, dataægthed, økonomisk tab, gennemført betaling eller et unikt offer. Relaterede brands og gentagne påstande kan også vanskeliggøre fortolkningen. Brug relevante opslag til validering gennem autoriserede organisationsoplysninger.

En bevaret besked fra 22. november videregiver en yderligere listepåstand under navnet LockBit5. Den tilhører opslagkorpusset, ikke Ransompedia-øjebliksbilledet med 29 opslag. Den lægges ikke til dette tal og behandles ikke som endnu en bekræftet indtrængning. [S1][S2]

7.3 De førende betegnelser beskriver ikke én kriminel kæde

Thegentlemen står for otte danske opslag, Settra for tre og Qilin for to. Samlet står de for 13 af 29, eller 44,8 %. Seksten yderligere betegnelser har ét opslag hver. [S2]

Selv den større andel efterlader over halvdelen af opslagene uden for disse tre betegnelser. Genopretningsplaner bør derfor omfatte afpresningsformer og afhængigheder frem for at antage, at én navngiven gruppe vil definere næste hændelse.

Thegentlemen

Betegnelse i afpresningsopslag | Ingen statslig eller politisk tilskrivning vurderet

I DANMARK, 2026

1. januar–22. november
8 danske opslag i Ransompedia-øjebliksbilledet

PÅSTÅEDE MÅL

Organisationer beskrevet i opslagene; identiteter tilbageholdt

I OFFENTLIG OMTALE

[S2] Egne data: Ransompedia registrerer 8 danske opslag under denne betegnelse.

VORES VURDERING

Opslagsrelationen understøtter validering, genopretning og underretningsberedskab. Den dokumenterer ikke kryptering, dataægthed, en fælles tilknyttet aktør, en adgangsvej eller gennemført betaling.

SIKKERHED I VURDERINGEN
Høj for det bevarede opslagsantal; underliggende hændelsesudsagn er fortsat påstande

Settra

Betegnelse i afpresningsopslag | Ingen statslig eller politisk tilskrivning vurderet

I DANMARK, 2026

1. januar–22. november

3 danske opslag i Ransompedia-øjebliksbilledet

PÅSTÅEDE MÅL

Organisationer beskrevet i opslagene; identiteter tilbageholdt

I OFFENTLIG OMTALE

[S2] Egne data: Ransompedia registrerer 3 danske opslag under denne betegnelse.

VORES VURDERING

Opslagsrelationen understøtter validering, genopretning og underretningsberedskab. Den dokumenterer ikke kryptering, dataægthed, en fælles tilknyttet aktør, en adgangsvej eller gennemført betaling.

SIKKERHED I VURDERINGEN

Høj for det bevarede opslagsantal; underliggende hændelsesudsagn er fortsat påstande

Qilin

Betegnelse i afpresningsopslag | Ingen statslig eller politisk tilskrivning vurderet

I DANMARK, 2026

1. januar–22. november

2 danske opslag i Ransompedia-øjebliksbilledet

PÅSTÅEDE MÅL

Organisationer beskrevet i opslagene; identiteter tilbageholdt

I OFFENTLIG OMTALE

[S2] Egne data: Ransompedia registrerer 2 danske opslag under denne betegnelse.

VORES VURDERING

Opslagsrelationen understøtter validering, genopretning og underretningsberedskab. Den dokumenterer ikke kryptering, dataægthed, en fælles tilknyttet aktør, en adgangsvej eller gennemført betaling.

SIKKERHED I VURDERINGEN

Høj for det bevarede opslagsantal; underliggende hændelsesudsagn er fortsat påstande

En opslagsbetegnelse kan være nyttig til at finde den relevante påstand. Den identificerer ikke en tilknyttet aktør, viser ikke en adgangsvej og dokumenterer ikke, at alle hændelser under betegnelsen brugte samme værktøjer.

Indsatsen begynder med organisationens egen evidens. Fastslå, om de påståede data eller konti tilhører organisationen, om adgang er aktuel, og om inddæmning kræves. Bevar forskellen mellem en gammel registrering og en aktiv session.

Genopretning og underretningsberedskab kan fortsætte, mens tilskrivningen er uafklaret. Tjenesteansvarlige kan afprøve genopretning, og databeskyttelsesteams kan vurdere datarisici uden at vente på identiteten bag et opslag.

7.4 WhiteArmor: en omtalt påstand og en snævrere virksomhedsudtalelse

Bitdefenders artikel fra 12. november omtaler, at WhiteArmor påtog sig ansvaret for en Maersk-hændelse og fremsatte et afpresningskrav. Det er tilskrevet omtale af gruppens påstand. Det er ikke virksomhedens bekræftelse af aktøransvar. [S11]

WhiteArmor-betegnelsen optræder også én gang blandt de 29 Ransompedia-opslag; opslaget er en påstand, ikke virksomhedens bekræftelse. [S2]

Maersks udtalelse fra 11. november bekræfter uautoriseret adgang og dataudtræk fra et lokalt ældre system arvet gennem et tidligere opkøb. De indledende resultater tydede på ingen videregivelse af følsomme oplysninger og ingen påvirkning af andre integrerede systemer. [S10]

Virksomheden oplyste også, at den ikke forventede afbrydelse af kundernes drift. Den daterede vurdering bør ikke blive til et udsagn om, at alle undersøgelsens dele var afsluttet. Den bekræfter hverken aktørens fulde beskrivelse eller indholdet af det annoncerede materiale. [S10][S11]

WhiteArmor

Afpresningsbetegnelse og påstand i leverandøromtale | Ingen statslig eller politisk tilskrivning fastslået

I DANMARK, 2026

11. november
Maersk offentliggør en afgrænset hændelsesudtalelse [S10]

12. november
Bitdefender omtaler WhiteArmors påtagelse af ansvar [S11]

PÅSTÅEDE MÅL

En omtalt påstand om Maersk; ingen bredere offerliste udledt

I OFFENTLIG OMTALE

[S2] Egne data: Ransompedia registrerer ét dansk opslag under denne betegnelse; opslaget er en påstand, ikke virksomhedens bekræftelse.

[S11] Bitdefender omtaler gruppens påstand og krav; Maersk bekræftede ikke aktørens fulde beskrivelse.

[S10] Maersk bekræfter adgang og dataudtræk fra et lokalt ældre system med de angivne begrænsninger.

VORES VURDERING

Hold den omtalte aktørpåstand adskilt fra den virksomhedsbekræftede systemhændelse. Validér opkøbte systemers ejerskab, relevante identiteter og kundekommunikation gennem autoriserede oplysninger.

SIKKERHED I VURDERINGEN
Høj for de offentliggjorte beskrivelser; aktøransvar er ikke uafhængigt fastslået

For en organisation med opkøbte systemer er det nyttige spørgsmål ejerskab. Identificér, hvem der vedligeholder systemet, hvilke identiteter der stadig har adgang, og hvilke oplysninger det indeholder. Betegnelsen ældre system dokumenterer ikke forsømmelse eller en bestemt teknisk fejl.

Svindelteams bør også forberede sig på henvendelser, som henviser til en ægte offentlig hændelse. Verificér væsentlige anmodninger via en kendt kontaktkanal. En omtale af hændelsen dokumenterer ikke, at afsenderen har stjålne data eller repræsenterer den berørte virksomhed.

7.5 Officielle vurderinger er ikke en hændelsesvis tilskrivningsmatrix

SAMSIK's vurderinger af den destruktive trussel fra juni og september beskriver styrelsens vurdering af statsrelateret risiko. Septemberpublikationen hæver vurderingen fra middel til høj. Deres betydning er forberedelse af kontinuitet og genopretning med kildespecifik tilskrivning. [S42][S43]

Januars kameraadvarsel og novembers kølemeddelelser er forskellige spor. Sidstnævnte efterlader udtrykkeligt gruppernes medvirken uafklaret. Lignende politisk sprog forbinder ikke en kamerapåstand, en DDoS-kampagne og en kølesystemhændelse. [S40][S26]

Ingen verificeret landespecifik tekniktilknytning understøtter en dansk MITRE ATT&CK-matrix for disse spor her. Produktsårbarheder og generelle aktørbeskrivelser kan ikke levere den manglende hændelsesevidens. Gennemgå de aktiver og handlinger, hver kilde faktisk beskriver.

For SOC er en aktivspecifik opgave mere nyttig end en udokumenteret aktørprofil. Kontrollér relevante logins, kontorettigheder, administrative ændringer og gendannelsesoplysninger mod organisationens faktiske arkitektur. Eskalér bekræftede afvigelser gennem hændelsesansvarlig.

7.6 Operation Endgame og indsatsens grænser

NSK's udtalelse fra 12. november beskriver en international indsats mod Gootloader. Myndighederne fjernede skadelig kode fra 681 WordPress-websteder i Danmark og udlandet. Indsatsen omfattede også 218 domæner og 14 servere i udlandet. [S24]

Tallene vedrører forskellige infrastrukturpopulationer. De er ikke 681 danske ofre, 681 gennemførte ransomware-hændelser eller en optælling af forebyggede tab. Myndigheden beskriver indsatsen som del af Operation Endgame. [S24]

NSK vurderede, at stjålne adgangskoder havde muliggjort adgang til webstederne. Anbefalingerne omfatter gennemgang af administratorkonti, ændring af adgangskoder, multifaktorautentificering og opdatering af webstedssoftware. Vurderingen af adgangsvejen er NSK's. [S24]

En berørt webstedsejer skal stadig fastslå kontrollen over konti og undersøge applikationens tilstand. Fjernelse af én skadelig komponent dokumenterer ikke, at alle tidligere adgangsveje eller eksponerede legitimationsoplysninger er håndteret.

En virksomhed, der modtager en meddelelse om en politiindsats, bør bevare den og udpege en ansvarlig. Fastslå, hvilket aktiv meddelelsen vedrører, hvilken handling der er afsluttet, og hvad organisationen stadig skal gøre. Registrér opfølgningens evidens frem for at antage, at indsatsen afslutter hændelsen.

7.7 Hvad et aktørnavn bør ændre

Brug et navn til at finde evidens og autoritativ vejledning. Brug validerede tekniske forhold til at vælge inddæmning og genopretning. Tilskrivning kan forblive uafklaret, mens en aktuel konto eller usikker fjernforbindelse håndteres akut.

Ledelsen bør efterspørge udsagn, kilde og beslutning samlet. "Et opslag findes", "virksomheden bekræftede adgang" og "en myndighed vurderer en trussel" understøtter forskellige konklusioner. Adskillelsen beskytter både driftsmæssig dømmekraft og offentlig kommunikation.

HOVEDPOINTER

01

Behandl opslagsbetegnelser som evidensrelationer, ikke verificerede hændelsesudfald.

02

Hold virksomhedsbekræftelse adskilt fra en omtalt aktørpåstand.

03

Følg politimeddelelser op med aktivspecifik validering og dokumenteret genopretning.

KAPITEL 08

Svindel efter dataeksponering

08

DETTE KAPITEL BESVARER

Hvordan kan en informationshændelse blive til en ny hændelse for kunder og ansatte?

3

beslutninger: kontrollér kontakten, den ønskede handling og modtagerdestinationen

8.1 Kendte oplysninger bekræfter ikke identitet 74

8.2 Hotel- og bookingoplysninger kan understøtte målrettede betalingsbeskeder 74

8.3 Opbevaring ændrer den mulige skade 75

8.4 Annoncer måler ikke svindeløkonomien 75

8.5 Betalingskortobservationer 76

8.6 Et brugbart forløb for kundebeskyttelse 76

KAPITEL 08

Svindel efter dataeksponering

KORT FORTALT

Dataeksponering kan gøre en svindelbesked mere overbevisende uden at give afsenderen legitim bemyndigelse. Danske meddelelser beskriver risikoen gennem personidentifikatorer, hotelbookinger og leverandørforhold. Beskyttelsen kræver kundeservice sammen med sikkerhed. Giv mennesker en uafhængig kontrolkanal, afbryd mistænkelige betalingsændringer, og bevar indberetninger, som viser, hvordan svindlen nåede dem.

8.1 Kendte oplysninger bekræfter ikke identitet

Datatilsynets råd efter CPR-sagen adskiller eksponering fra dokumenteret misbrug. Tilsynet advarer om, at en afsender kan kende en persons navn og adresse og stadig være svindler. Det er relevant for organisationer, hvor support ofte autentificerer personer med biografiske spørgsmål. [S16]

Konsekvensen for forsvaret er en planlægningsvurdering. Gennemgå, hvilke spørgsmål en opkalder kan besvare med oplysninger, som allerede er offentliggjort eller givet til en anden tjeneste. En nødprocedure bør ikke acceptere samme oplysning som både bekymringsgrund og bekræftelse af opkalderens identitet.

Adskil tre beslutninger. Fastslå først, hvem der kontakter organisationen. Fastslå dernæst, om personen har ret til at anmode om handlingen. Verificér til sidst den konto, destination eller enhed, som modtager resultatet. En ægte leverandørkontakt kan stadig have en forkert betalingsdestination i en besked.

En hændelsesadvarsel kræver også en uafhængig vej. Henvis kunder til en kanal, de selv kan finde via eksisterende tjenestemateriale. En advarsel med et ukendt link kan ligne den svindel, den skal forebygge. Kundeservice bør afprøve beskeden med personer uden for hændelsesteamet.

8.2 Hotel- og bookingoplysninger kan understøtte målrettede betalingsbeskeder

Meddelelserne om hotelsoftware i kapitel 5 forbinder en datahændelse med svigagtig kommunikation. Den vigtige forskel er mellem at lukke en læk og fjerne alle allerede erhvervede kopier. En leverandørs inddæmningsopdatering kan ikke dokumentere, at alle modtagere af kopierede oplysninger har slettet dem. [S18]

Et hotel bør spørge, hvilke reservationer, kundekontakter og betalingsinstrukser der er berørt. Det bør give gæster en tydelig kanal ved nye betalingskrav. En leverandør bør give kunder tilstrækkelige omfangsoplysninger til en nyttig advarsel uden at distribuere unødvendige personoplysninger.

Svindel- og kundeserviceteams bør dele en afgørelsesproces. Bevar beskeden og transaktionsreferencen via autoriserede kanaler, kontrollér betalingsforsøg, og forklar kunden, hvordan hjælp fås. Bed ikke kunden sende følsomme dokumenter til en improviseret postkasse.

8.3 Opbevaring ændrer den mulige skade

Datatilsynets novemberafgørelse vedrører tidligere ondsindet indtrængen hos en bilforhandler. Den siger, at over 48.000 personer var berørt, og at oplysninger om mellem 25.000 og 30.000 personer allerede burde have været slettet. Uautoriseret adgang fandt sted den 30. december 2024 og blev opdaget den 5. januar 2025; afgørelsen giver nyere tilsynslæring. [S22][S23]

Læren er ikke, at enhver opbevaret registrering vil blive misbrugt. Den er, at opbevaring og sletning påvirker den population, som potentielt kan skades ved en hændelse. Den dataansvarlige skal kontrollere behovet for hver kategori, og om den gennemførte sletteproces når ældre lagre.

En politik og en automatisk slettefunktion kan eksistere sammen med et ustyret arkiv. Afslutning kræver derfor evidens fra de faktiske lagersteder, herunder arvede systemer. Bed den ansvarlige demonstrere en repræsentativ sletning og forklare lovlige undtagelser. Gem begrundelse og valideringsresultat i kontrolregistreringen.

8.4 Annoncer måler ikke svindeløkonomien

Tilbud i kriminelle miljøer kan annoncere identiteter, konti eller adgang. En udbudspris dokumenterer ikke et salg, en brugbar konto eller størrelsen af et nationalt marked. Et landenavn i en salgsmenu dokumenterer ikke, at sælgeren har fungerende materiale for landet.

Kapitel 4 registrerer bevaret evidens og udsagnenes grænser. Dette kapitel omregner ikke annoncer til svindeltab eller kundetal. En relevant annonce skaber en valideringsopgave for organisationen; bekræftet misbrug kræver særskilt evidens.

Et svindelteam kan stadig bruge forskellen i praksis. Registrér det påståede materiale, den kontrollerede interne evidens, den fastslåede kundeskade og handlingen. Lad ukendte felter stå udtrykkeligt ukendte. Dermed kan sagen opdateres uden at gentagelse gør en oprindelig påstand til en bekræftet hændelse.

Dansksprogede tilbud kræver særskilt undersøgelse. En besked dateret 26. april henvender sig til danske læsere og annoncerer betaling på 8–15k. Kravene omfatter myndighedsalder, en bankkonto, en konto hos en betalingstjeneste og identifikation. Beskeden dokumenterer ikke valuta, udført arbejde, kontokontrol, en gennemført betaling eller et kriminelt formål. [S1]

Det er en rekrutteringsobservation, ikke en bekræftet sag om muldyrkonti eller et indtjeningstal. Det relevante forsvarsspørgsmål er, om nogen bliver bedt om at overføre penge, oplyse loginoplysninger eller overdrage kontokontrol. Fastslå den ønskede handling og dens autorisation, før I konkluderer, at der er tale om svindel.

Andre beskeder annoncerer masseudsendelse af SMS til Danmark, herunder valgfri afsenderidentifikation og mulighed for test. Ordlyden dokumenterer en markedsført tjeneste, ikke verificeret levering, en vellykket phishingkampagne eller ulovlig brug. Rapporten udelader tjenestenavne og kontakter. [S1]

Genkendelig afsendertekst bør ikke erstatte en uafhængig kontrolkanal. Vurder en konkret mistænkelig besked, destination eller kontohændelse gennem organisationens svindelproces. Gør ikke en udbyders reklamepåstand til en observeret evne eller et skøn over national svindelmængde.

8.5 Betalingskortobservationer

KORTTALLENES AFGRÆNSNING

Tallene beskriver betalingskortregistreringer i den bevarede opslagssamling. De måler ikke national korteksponering, korttyveri eller svindeltab.

Det bevarede korpus indeholder 43 betalingskortposter med tilknytning til Danmark. Observationerne fastslår ikke aktive kort, udstedernes tab eller det samlede antal eksponerede danske kort. [S4]

Kortobservationerne og deres afgrænsede nævner fremgår af dataoversigten. De understøtter ikke udstedermarkedsandele, antal aktive kort eller et dansk tabsestimat. En annonceret status er opslagsskriverens udsagn, ikke betalingsnetværkets verifikation. [S4]

Konto-, kort- og slutenhedsevidens er forskellige populationer. En kunde kan optræde i flere kilder, mens en observeret registrering kan være historisk. Udstedere og betalingstjenester bør anvende egen transaktions- og kontoevidens før beslutning om indgribende kundehandling.

8.6 Et brugbart forløb for kundebeskyttelse

Udløser	Første beslutning	Ansvarlig	Dokumentation for afslutning
Relevant datameddelelse	Identificér berørte kundegrupper og muligt misbrug	Databeskyttelse og kundeservice	Godkendt omfang og forståelig advarsel
Uventet betalingsanmodning	Verificér anmodningen gennem kendt kanal	Økonomi og kundesupport	Registreret kontrol før overførsel
Kontogendannelse efter eksponering	Kontrollér identitet og bemyndigelse uafhængigt	Identitet og svindelbekæmpelse	Gendannelsesbeslutning og sessionskontrol
Indberettet svindelforsøg	Bevar kontakten og vurder faktisk skade	Svindel- og hændelseshåndtering	Sagsafgørelse og kundevejledning
Fundet ældre lager	Fastslå behov, opbevaringsregel og sletningens rækkevidde	Dataansvarlig	Dokumenteret opbevaringsbeslutning og afprøvet sletning

Det er anbefalede kontroller, ikke påstande om, at hver berørt organisation manglede dem. Vælg handling efter de oplysninger og den skade, som er fastslået i den konkrete hændelse.

HOVEDPOINTER

01

Personkendskab kan gøre svindel troværdig uden at bekræfte afsenderens identitet.

02

Lukning af en læk sletter ikke kopierede oplysninger.

03

Knyt opbevaring, kundeadvarsler og betalingskontrol til navngivne ansvarlige.

KAPITEL 09

Bankers og betalingstjenesters afhængigheder

09

DETTE KAPITEL BESVARER

Hvilke finansielle beslutninger følger af eksponeringsobservationer og bekræftede tilsynsresultater?

3

særskilte forhold: institutionssystemer, kundesvindel og kontinuitet i fælles tjenester

9.1 Definér, hvilket forhold evidensen vedrører 79

9.2 Udstederdomæner bevarer populationsgrænsen 79

9.3 Kontinuitetsresultater kræver forretningsansvar 80

9.4 Leverandørudtræden skal være en driftsmæssig evne 80

9.5 DORA-indberetning følger ikke persondatafristen 80

9.6 Kundekommunikation er del af betalingssikkerheden 81

9.7 Spørgsmål til næste ledelsesmøde 81

KAPITEL 09

Bankers og betalingstjenesters afhængigheder

KORT FORTALT

Finansielle institutioner, kunder og betalingsleverandører kan påvirkes forskelligt. En driftsafbrydelse dokumenterer ikke stjålne kortdata, og kundesvindel dokumenterer ikke adgang til bankens interne systemer. Eksponeringsvisningen adskiller observationer vedrørende institutioner, udstedere og kunder. Brug officielle tilsynsresultater til at afprøve kontinuitet, leverandørudtræden og indberetningsansvar, og validér relevante konto- og svindelalarmer mod intern evidens.

9.1 Definér, hvilket forhold evidensen vedrører

Den udvalgte bank- og finansgruppe indeholder 25 kandidatdomæner. Den omfatter finansielle tjenester og infrastruktur. Den er ikke et fuldstændigt register over danske banker med tilladelse, en kortudstederpopulation eller grundlag for institutionssammenligning. Det daterede eksponeringsøjebliksbillede giver observationer af enheder, legitimationsposter og tilbud for denne udvalgte gruppe. [S3]

Hold institutionsadgang adskilt fra svindel mod kunder. En annonce med en bankreference kan vedrøre kundekonti, en betalingsformidler, en historisk liste eller en ubekræftet påstand. Ingen af mulighederne alene dokumenterer indtrængen i institutionens produktionsmiljø.

Det samme gælder enhedsobservationer. Et finansielt tjenestedomæne kan optræde i materiale knyttet til både kunder og ansatte. Fastslå konto, slutenhed og forretningsforhold, før alarmen tildeles. Betegn ikke alle relationer uden medarbejderklassifikation som verificerede kundeenheder.

Forhold	Evidens, der besvarer spørgsmålet	Understøttet beslutning
Institutionens interne systemer	Autoriserede logs, hændelsesevidens og relevante leverandøroplysninger	Inddæmning og driftsgenopretning
Kundekonto eller betaling	Kontoejerskab, transaktion og verificeret kontakt	Svindelindgreb og kundesupport
Betalingstjenesteleverandør	Leverandøromfang, berørte funktioner og kontinuitetsevidens	Alternativ drift, gentilslutning og indberetning
Historisk kontoregistrering	Aktuel gyldighed og tidligere afhjælpning	Forholdsmæssig kontohandling

9.2 Udstederdomæner bevarer populationsgrænsen

Otte af de 25 udvalgte bank- og finansdomæner tilhører kortudstedere. Denne udstederpopulation er ikke en optælling af danske banker. Disse udstederdomæner har 539 relationer til andre enheder end medarbejderenheder og 47 relationer til medarbejderenheder. Aktuelle legitimationstilbud vedrører ét af disse udstederdomæner. [S3]

Samme visning indeholder 7 kort-til-udstederrelationer fra de bevarede opslag. Disse relationer adskiller sig fra det nationale bevarede antal på 43 kortposter. De dokumenterer ikke aktive kort, gennemført svindel eller adgang til en banks interne systemer. Øvrige kortposter henføres ikke til en udvalgt udsteder. [S3][S4]

Identitets-, endepunkts- og svindelteams bør validere deres egen evidens særskilt. En fælles domænerelation fastslår ikke, at enhedsmateriale og en betalingskortpost beskriver samme person eller hændelse. Ingen udstederidentitet eller udstedervurdering offentliggøres.

9.3 Kontinuitetsresultater kræver forretningsansvar

Finanstilsynets inspektionsredegørelse fra juli beskriver svagheder i en betalingstjenesteleverandørs IKT-risikostyring, beredskab og tredjepartskontroller. Tilsynet vurderer svaghederne som relevante for alvoren af to hændelser, én i 2025 og én i maj 2026. Udtalelsen dokumenterer ikke ransomware eller tyveri af betalingskort-data. [S21]

Den praktiske relevans rækker ud over sikkerhedsdrift. Et genopretningsmål skal knyttes til forretningsfunktionen, og kontinuitetsplanen skal vise, hvordan funktionen fortsætter under genopretning. En vellykket infrastrukturgen-start er ikke det samme som genoprettet betalingstjeneste for alle afhængige kunder.

Leverandøren og hver afhængig institution bør vide, hvem der erklærer tjenesten genoprettet, godkender gentilslutning og kontrollerer afstemning. Det er anbefalinger udledt af tilsynsresultaterne. De hævder ikke, at alle institutioner med fælles leverandør har samme svaghed.

9.4 Leverandørudtræden skal være en driftsmæssig evne

Samme inspektion beskriver uafprøvede exitplaner for kritiske eller vigtige leverandører. En kontraktlig opsigelsesret dokumenterer ikke alene, at en tjeneste kan flyttes under fortsat drift. Afhængighedsansvarlige bør identificere de nødvendige data, grænseflader, specialister og bemyndigelser. [S21]

Vælg en øvelse med en realistisk forretningsbegrænsning. Antag eksempelvis, at leverandøren teknisk kan kontaktes, men ikke kan give pålidelig evidens om et dataudtræk. Institutionen skal beslutte fortsatte funktioner, kompenserende kontroller og evidens for normal drift.

Registrér uafklarede afhængigheder frem for at erklære øvelsen vellykket, fordi et møde fandt sted. Dokumentation bør vise den alternative tjeneste, dens operatører og efterfølgende afstemning. En leverandørforsikring kan oplyse beslutningen uden at erstatte institutionens egen vurdering.

9.5 DORA-indberetning følger ikke persondatafristen

Finanstilsynets indberetningsside beskriver indledende, foreløbige og endelige rapporter for større IKT-hændelser. Den henviser omfattede enheder til den foreskrevne formular og forklarer, at estimater skal bruges, når præcise indledende eller foreløbige tal mangler. Det understøtter rettidig indberetning under fortsat undersøgelse. [S31]

En persondatahændelse kan også kræve en særskilt GDPR-vurdering. Den indberetningspligtige population, kendskabstidspunktet og den ansvarlige juridiske enhed kan være forskellige. Kapitel 10 angiver relevante frister og undtagelser. Kopiér ikke én 72-timersregel ind i alle procedurer.

Finanstilsynets septemberundersøgelse af forsikring og pension efterlyser stærkere ledelsestilsyn, dokumenterede risikorammer, kompetencer og afprøvet kontinuitet. Resultaterne vedrører udvalgte virksomheder undersøgt mellem oktober 2025 og marts 2026. De måler ikke alle finansielle organisationers sikkerhed ved denne skæringsdato. [S33]

9.6 Kundekommunikation er del af betalingssikkerheden

En datahændelse kan føre til anmodninger om en ny betalingsdestination, ekstra identitetsdokumenter eller akut kontonulstilling. Ansatte bør verificere både anmodning og destination gennem en eksisterende kanal. Mistænkelige beskeder bør indgå i svindelsagsforløbet, selv om IT-hændelsen er inddæmmet.

Forklar berørte kunder, hvad institutionen ved, hvad der er uafklaret, og hvilken handling der er relevant. Undgå at sige, at nulstilling af adgangskoden løser enhver eksponering af personoplysninger. Antyd heller ikke bekræftet økonomisk tab, blot fordi identitetsoplysninger blev tilgået.

9.7 Spørgsmål til næste ledelsesmøde

Spørgsmål	Ansvarlig funktion	Efterspurgt dokumentation
Kan en kritisk betalingsfunktion fortsætte under genopretning?	Drift og teknologi	Demonstreret alternativ drift og afstemning
Kan vi rettidigt få leverandørens omfangsoplysninger?	Tredjepartsrisiko	Aftalt kontakt og afprøvet meddelelse
Kan kunder uafhængigt kontrollere en ægte advarsel?	Svindelbekæmpelse og kundeservice	Afprøvet kommunikationskanal
Kan vi hurtigt klassificere og indberette en IKT-hændelse?	Compliance og hændelseshåndtering	Tidsmålt øvelse med trinvise rapporter
Kan vi forklare hver relevant kontoalarm?	Identitet og sikkerhed	Afgørelsesregister med ansvar efter alarmmodtagelse

HOVEDPOINTER

01

Skeln mellem banksystemadgang, kundesvindel og leverandørafbrydelse.

02

Afprøv forretningsfunktionen og leverandørudtræden, ikke kun den tekniske genstart.

03

Bevar DORA- og persondataafgørelser i samme faktuelle tidslinje med særskilte vurderinger.

KAPITEL 10

Regulering og den nationale indsats

DETTE KAPITEL BESVARER

Hvilke pligter gælder, hvem modtager indberetningen, og hvilken evidens bør hændelsesansvarlig bevare?

1. juli 2025

ikrafttrædelse af Danmarks NIS 2-lov

10.1 Begynd med enheden og tjenesten 83
10.2 Registrering og hændelsesindberetning kræver særskilt ansvar 84
10.3 NIS 2-forløbet følger kendskabstidspunktet 84
10.4 Persondataindberetning stiller et andet spørgsmål 85
10.5 Finansielle IKT-hændelser har egne frister 85
10.6 Tilsyn bør ændre den driftsmæssige dokumentation 86
10.7 Bøder og territorialt anvendelsesområde kræver præcis formulering 86
10.8 Afprøv en indberetningsbeslutning 86

KAPITEL 10

Regulering og den nationale indsats

KORT FORTALT

Danmarks NIS 2-lov er allerede i kraft. Persondatabrud og større finansielle IKT-hændelser har særskilte kriterier og indberetningsfrister. Registrering, teknisk håndtering og underretning er forskellige opgaver. En leverandørmeddelelse kan kræve flere beslutninger uden at dokumentere flere indtrængninger. Fastslå relevant enhed og sektor, bevar tidspunkter for kendskab og klassifikation, og afprøv indberetningskanalen med en ansvarlig og stedfortræder.

Kapitlet understøtter hændelsesplanlægning, ikke en enhedsspecifik juridisk afgørelse. Jura- og compliance-ansvarlige bør kontrollere gældende lov, sektorregler og faktiske forhold før beslutning om indberetning.

10.1 Begynd med enheden og tjenesten

NIS 2-loven trådte i kraft den 1. juli 2025. SAMSIK's vejledning beskriver særskilt gennemførelse for energi, telekommunikation og finans. En koncern kan derfor behøve flere vurderinger af anvendelsesområdet. [S27][S28]

Rapportens sektorbetegnelser afgør ikke juridisk omfang. Vurdér den relevante juridiske enhed, aktiviteter, størrelse og eventuelle særlige omfattelser eller undtagelser. Et udvalgt domæne i kapitel 3 dokumenterer ikke, at operatøren er en væsentlig eller vigtig enhed. [S28]

Opret en anvendelsesområderegistrering.

Spørgsmål	Ansvarlig	Dokumentation
Hvilken enhed leverer den berørte tjeneste?	Jura og tjenesteansvarlig	Enhed, aktivitet og kontraktligt ansvar
Hvilke oplysninger eller hvilken drift er berørt?	Hændelsesleder	Kendt påvirkning og uafklaret omfang
Hvilket sektorregelsæt gælder?	Compliance	Gældende tekst og kompetent myndighed
Hvem beslutter og indsender?	CISO og jura	Navngiven indberetter, stedfortræder og godkendelsesvej

Loven indeholder undtagelser for bestemte sektorordninger og tilsvarende EU-krav. Bestemmelser om national sikkerhed, forsvar, offentlig sikkerhed og retshåndhævelse er også relevante. Uddannelse eller offentligt ejerskab afgør ikke alene anvendelsesområdet. [S27]

En leverandør uden for loven kan møde kontraktlige sikkerhedskrav. SAMSIK knytter forskellen til sikkerheden i kundens forsyningskæde. Adskil leverandørens juridiske status fra kundens afhængighed. [S28]

10.2 Registrering og hændelsesindberetning kræver særskilt ansvar

SAMSIK's registreringsvejledning angiver 1. oktober 2025 som oprindelig frist. En enhed, der senere omfattes, skal registreres inden to uger. Ændringer i indsendte oplysninger kræver som udgangspunkt en opdateret indsendelse inden tre måneder. [S29]

Vejledningen bruger den nationale virksomhedsindberetningstjeneste. Den adskiller DORA-enheder fra denne registreringspligt. Den forklarer også, at de valgte sektorer afgør, hvilke kompetente myndigheder der modtager indsendelsen. [S29]

Afprøv adgang før en hændelse. Den udpegede indberetter bør vide, hvordan relevant formular findes, autentificering gennemføres og kvittering modtages. En stedfortræder bør kunne fortsætte.

SAMSIK's FAQ skelner mellem sektortilsyn og hændelseshåndtering. Sektormyndigheder fører tilsyn på egne områder; FE håndterer hændelsesindberetninger som national CSIRT. Funktionerne bør fremgå særskilt i beredskabsplanen. [S28]

10.3 NIS 2-forløbet følger kendskabstidspunktet

§ 12 vedrører væsentlige hændelser, herunder alvorlige driftsforstyrrelser, økonomiske tab eller betydelig skade på andre. § 13 angiver indberetningsforløbet. Maksimumsfristerne erstatter ikke pligten til at indberette uden unødigt ophold. [S27]

Trin	Generel maksimumsfrist	Nødvendig registrering
Tidlig varsling	24 timer efter kendskab	Kendskabstidspunkt og indledende vurdering
Hændelsesunderretning	72 timer efter kendskab	Alvor, påvirkning og tilgængelig evidens
Foreløbig opdatering	Efter CSIRT's anmodning	Aktuel status og ændrede forhold
Endelig rapport	En måned efter underretning	Årsag, påvirkning og håndteringsbeskrivelse

Tillidstjenesteudbydere har en maksimumsfrist på 24 timer for hændelsesunderretning. Ved fortsat hændelse kræver loven en statusrapport efterfulgt af en endelig rapport inden en måned efter håndtering. Én universel frist ville overse undtagelserne. [S27]

Bevar grundlaget for hvert tidspunkt. En sikkerhedsalarm, leverandørens opdagelse og organisationens kendskab kan være forskellige tidspunkter. Registrér, hvad der var kendt, hvem der vurderede det, og hvornår vurderingen ændredes.

Bevar én tidslinje med særskilte indberetningsbeslutninger. Senere opdateringer kan rette omfanget, mens den første meddelelse bevares.

10.4 Persondataindberetning stiller et andet spørgsmål

Datatilsynets vejledning skelner mellem anmeldelse til tilsynet og underretning af berørte personer. Den dataansvarlige anmelder uden unødig forsinkelse og om muligt inden 72 timer efter kendskab, medmindre risiko for personers rettigheder og frihedsrettigheder er usandsynlig. [S30]

En databehandler underretter den dataansvarlige uden unødig forsinkelse. Den dataansvarlige beholder beslutningsansvaret. Tilgængelige oplysninger kan anmeldes først og suppleres hurtigt; en forsinket anmeldelse kræver begrundelse. De 72 timer løber også i weekender og på helligdage. [S30]

Berørte personer skal underrettes, når høj risiko er sandsynlig, med forbehold for gældende undtagelser. Underretningen skal være hurtig og forståelig; den har ingen særskilt universel 72-timersfrist. Dokumentér alle brud og begrundelser for anmeldelse eller undladt underretning. [S30]

Ved en leverandørhændelse skal det afklares, hvilke registreringer organisationen overlod til tjenesten. Fastslå, hvis oplysninger der er involveret, hvilken beskyttelse der gjaldt, og hvad personerne kan gøre nu. Leverandørens genopretningsmeddelelse besvarer ikke spørgsmålene.

Kundeservice bør modtage en godkendt beskrivelse af de fastslåede forhold og en kanal for mistænkelige henvendelser. Databeskyttelsesvurdering og praktisk hjælp bør fortsætte sammen, mens ubekræftede datamængder forbliver forbeholdne.

10.5 Finansielle IKT-hændelser har egne frister

Finanstilsynets DORA-vejledning kræver, at omfattede finansielle enheder indberetter større IKT-hændelser gennem den udpegede finansielle kanal. Forløbet omfatter indledende, foreløbig og endelig rapportering med mulighed for omklassifikation. [S31]

De detaljerede frister følger artikel 5 i delegeret forordning 2025/301. Bevar både kendskabstidspunkt og tidspunkt for klassifikation som større hændelse. De starter forskellige dele af forløbet. [S32]

Trin	Krav
Indledende underretning	Hurtigst muligt; inden fire timer efter klassifikation som større hændelse og senest 24 timer efter kendskab
Sen klassifikation som større hændelse	Ved klassifikation efter 24 timer: underret inden fire timer efter klassifikation
Foreløbig rapport	Inden 72 timer efter indledende underretning; opdatér hurtigt og ved genoptagelse af normal drift
Endelig rapport	Inden en måned efter foreløbig rapport eller dens seneste opdatering

Kan en frist ikke overholdes, skal myndigheden orienteres uden unødig forsinkelse og senest ved fristen med en begrundelse. Kalenderundtagelsen kan flytte en weekend- eller helligdagsfrist til middag næste arbejdsdag. [S32]

Undtagelsen gælder ikke indledende og foreløbige rapporter fra kreditinstitutter, centrale modparter, markedspladsoperatører og andre finansielle enheder, der er væsentlige eller vigtige efter NIS 2. Deres endelige rapporter er ikke udelukket af bestemmelsen. [S32]

Tilsyn kan også undtage indledende og foreløbige rapporter fra andre betydelige eller systemiske enheder fra kalenderordningen efter underretning af dem. Bevar en sådan afgørelse sammen med enhedens indberetningsinstruks. [S32]

Finanstilsynet angiver en alternativ kontaktvej, når tekniske problemer forhindrer den indledende indsendelse. Etablér kanalen, før normal indberetning bliver utilgængelig. Bevar indsendelse og bekræftelse særskilt. [S31]

10.6 Tilsyn bør ændre den driftsmæssige dokumentation

Finanstilsynets publikation fra 23. september beskriver en undersøgelse af udvalgte forsikrings- og pensionsselskaber mellem oktober 2025 og marts 2026. Den peger på forbedringsbehov i ledelsestilsyn, dokumenterede risikorammer, kompetencer og afprøvet driftsberedskab. [S33]

Tilsynet anmodede om handleplaner, hvor væsentlige mangler blev fundet. Resultaterne vedrører den undersøgte population. De dokumenterer ikke, at alle danske finansielle institutioner har samme mangel eller har været udsat for indtrængen. [S33]

Det praktiske svar er at forbinde ledelsesdokumentation med en tjenesteafprøvning. Bestyrelsen bør kunne se, hvilken kritisk tjeneste der blev afprøvet, hvad der svigtede, og hvem der ejer rettelsen. En politikgodkendelse er en anden slags dokumentation.

For en væsentlig leverandør bør forretningsansvarlig demonstrere et brugbart driftsalternativ. Registrér, hvordan identitet, kommunikation og kundesupport fortsætter, hvis leverandøren ikke kan give rettidige opdateringer.

10.7 Bøder og territorialt anvendelsesområde kræver præcis formulering

§ 32 fastsætter bødestraf for bestemte overtrædelser og giver mulighed for strafansvar for juridiske personer. Paragraffen angiver ikke numeriske bødeintervaller. Bøderisiko kræver vurdering efter relevant dansk regelsæt og den konkrete sag. [S27]

§ 34 siger, at loven ikke gælder for Færøerne og Grønland, men kan sættes særskilt i kraft ved kongelig anordning. Organisationer med drift dér bør fastslå den gældende lokale retstilstand. [S27]

10.8 Afprøv en indberetningsbeslutning

Brug en leverandørmeddelelse om mulig adgang til kundeoplysninger, mens en vigtig tjeneste er afbrudt. Giv øvelsesteamet ufuldstændige oplysninger og en senere rettelse. Det afprøver beslutninger under usikkerhed uden at antage, at leverandørens første estimat er endeligt.

Øvelsesbeslutning	Ansvarlig	Dokumentation for afslutning
Identificér enhed og sektorpligter	Jura og compliance	Skriftlig anvendelsesområdevurdering
Bevar kendskab og klassifikation	Hændelsesleder	Dateret tidslinje med begrundelser
Forbered relevante underretninger	Indberetter og stedfortræder	Udfyldte øvelsesformularer og kvitteringskanal
Forklar praktiske kunderisici	Databeskyttelse og kundeservice	Godkendt meddelelse og supportinstruks
Fortsæt den væsentlige tjeneste	Forretnings- og leverandøransvarlige	Demonstreret alternativ drift og genoprettelseskriterier

Afslut øvelsen med uafklarede spørgsmål, ansvarlige og frister. Afprøv stedfortræderen og den uafhængige kommunikationskanal. Ledelsen bør modtage dokumentation for afsluttede handlinger sammen med accepterede undtagelser.

HOVEDPOINTER

01

Fastslå enhed og sektoromfang, før indberetningskanalen vælges.

02

Bevar kendskab, klassifikation, underretninger og begrundelser i én tidslinje.

03

Afprøv indberetning og fortsat drift med en ansvarlig og stedfortræder.

KAPITEL 11

Udsigter: betingede beslutninger i næste kvartal

11

DETTE KAPITEL BESVARER

Hvilke forberedelser følger af evidensen uden at forudsige et nationalt angrebsantal?

4

planlægningsscenarier med tydelige udløsere og afslutningsdokumentation

11.1 Centrale vurderinger og deres grænser 89

11.2 Scenarie A: leverandørmeddelelse før fuldstændigt omfang 90

11.3 Scenarie B: en kontoannonce matcher en aktiv identitet 90

11.4 Scenarie C: en webstedspåstand falder sammen med en udstyrsalarm 90

11.5 Scenarie D: kopierede oplysninger understøtter overbevisende svindel 91

11.6 Hvad rapporten ikke forudsiger 91

KAPITEL 11

Udsigter: betingede beslutninger i næste kvartal

KORT FORTALT

Evidensen understøtter forberedelse på identitetsmisbrug, leverandørafbrydelse, efterfølgende svindel og hændelser i forbundne systemer. Den fastslår ikke deres fremtidige hyppighed eller en fælles operatør. Hvert scenarie har en udløser, som ændrer indsatsen. Udpeg beslutningsansvarlig nu, og afprøv den relevante afhængighed med evidens fra eget miljø.

11.1 Centrale vurderinger og deres grænser

Tillid knytter sig til et udsagn. En bekræftet offentliggørelse kan efterlade aktør eller adgangsvej uafklaret. En opslagsoptælling med høj tillid kan indeholde ubekræftede underliggende påstande. Tabellen adskiller betydningerne frem for at give en hel aktør én troværdighedsbetegnelse.

Vurdering	Tillid og grundlag	Begrænsning	Evidens, der ændrer vurderingen
Identitet og historiske registreringer kræver særskilte kontrolgennemgange	Høj for relevansen af dokumenterede universitets- og registermeddelelser	Ingen national hændelsesrate eller fælles adgangsvej fastslået	Bekræftet omfang, intern adgangshistorik og opbevaringsvalidering
Leverandøroplysninger kan samtidig påvirke kontinuitet og kundebeskyttelse	Høj for relevansen af hotel- og andre leverandørmeddelelser	Kunder kan opleve forskellige følger	Kundemiljøspecifikt omfang og demonstreret sikker genopretning
Afpresningsberedskab bør ikke afhænge af én aktørbetegnelse	Høj for de 19 betegnelser i den bevarede population på 29 opslag	Betegnelser identificerer ikke unikke operatører	Bekræftet indtrængningsmekanisme eller forbundet hændelsesevidens
Offentlige tilgængelighedspåstande afgør ikke fysisk påvirkning	Høj for forskellen i officiel vejledning og køleudtalelser	En senere undersøgelse kan fastslå andet omfang	Driftslogs og dateret officiel konklusion
Porteføljesignaler kræver validering hos den relevante ansvarlige	Høj for de daterede domæneobservationer	Atlas-vurderingen beskriver en udvalgt portefølje; passive kontroller mangler fortsat	Evidens om aktive konti, aktivernes ejerskab og tjenestekontekst

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

Det nyttigste ledelsesspørgsmål er, om en ny oplysning ændrer en handling. Et nyt gruppealias kan ændre et efterretningsnotat uden at ændre genopretningsprioriteter. Bekræftet brug af en privilegeret konto ændrer inddæmningen. En svigagtig betalingsbesked ændrer kundebeskyttelsen, selv om det oprindelige system er genoprettet.

11.2 Scenarie A: leverandørmeddelelse før fuldstændigt omfang

Planlægningsantagelse. En kritisk leverandør oplyser om uautoriseret adgang og kan endnu ikke identificere alle berørte kunder. Jeres tjeneste afhænger af en grænseflade, leverandøren driver.

Udløser. En meddelelse identificerer jeres kundemiljø, konto, integration eller datakategori, eller intern evidens forbinder hændelsen med jeres miljø. En generel landereference opfylder ikke alene kriteriet.

Beslutning. Tjenesteansvarlig og hændelsesleder vurderer fortsat drift, midlertidige begrænsninger og evidens for gentilslutning. Databeskyttelse og compliance vurderer egne indberetningspligter ud fra tilgængelige forhold. Kundeservice forbereder en advarsel, hvis kendte data kan understøtte svindel.

Afslutningsdokumentation. Registrér berørte grænseflader, leverandørens omfangsbeskrivelse, relevante interne observationer, alternativ drift og godkendelsen af normal drift. Genopretning afslutter et tilgængelighedsspørgsmål; den dokumenterer ikke, at kopierede oplysninger forsvandt.

Alternativ forklaring. En leverandør kan suspendere en tjeneste som forholdsregel uden at bekræfte adgang til kundedata. Hold forholdsreglen og det bekræftede eksponeringsomfang adskilt i kommunikationen.

11.3 Scenarie B: en kontoannonce matcher en aktiv identitet

Planlægningsantagelse. Organisationen modtager et tilbud om legitimationsoplysninger til en konto, den ejer. Opslaget er nyt, men det underliggende materiale kan være gammelt.

Udløser. Identitetsteamet bekræfter konto, adgangsomfang og evidens, som kræver handling. Opslagets dato dokumenterer ikke alene legitimationsoplysningernes aktualitet eller vellykket brug.

Beslutning. Identitets- og hændelsesteams vælger forholdsmæssig inddæmning med sessions- og gendannelsesgennemgang efter behov. Slutenhedsteamet undersøger tilknyttede enheder, når evidensen identificerer dem. Kundeservice modtager særskilt validerede kundekontoproblemer.

Afslutningsdokumentation. Bevar alarm, ejerskabskontrol, gyldighedsvurdering, adgangsundersøgelse og begrundet afhjælpning. Mangler en brugbar alarmkilde, registreres afhængigheden, og input skaffes før måling af afgørelsesdækning.

Alternativ forklaring. Annoncen kan gentage tidligere afhjulpne data eller fejlbetegne en fælles tjeneste. En dokumenteret falsk eller historisk relation er et gyldigt udfald, når evidensen understøtter det.

11.4 Scenarie C: en webstedspåstand falder sammen med en udstyrsalarm

Planlægningsantagelse. En aktør hævder afbrydelse, mens et driftsteam modtager en alarm fra forbundet udstyr. Tidspunkterne overlapper, men en fælles årsag er ukendt.

Udløser. Driftsansvarlig observerer en uautoriseret tilstandsændring, fjernsession eller konfigurationsændring eller modtager en relevant officiel advarsel. Et skærmbillede af et utilgængeligt websted dokumenterer ikke udløseren.

Beslutning. Driftsansvarlig kontrollerer sikker drift og kan isolere fjernadministration gennem en autoriseret procedure. Sikkerhed bevarer relevante logs. Kommunikation skelner mellem offentlig tjenestetilgængelighed, dataadgang og fysiske proceseffekter.

Afslutningsdokumentation. Bevar udstyrstilstand, godkendt konfiguration, fjernadgangsgennemgang, sikkerhedsbeslutning og afprøvet genopretning. Angiv årsagen som uafklaret, indtil undersøgelsen understøtter én. Tilskriv ikke en statslig aktør ud fra sprog eller politisk slogan.

Alternativ forklaring. En almindelig udstyrsfejl og en særskilt tilgængelighedspåstand kan forekomme samtidig. Muligheden skal holdes åben, indtil evidensen forbinder dem.

11.5 Scenarie D: kopierede oplysninger understøtter overbevisende svindel

Planlægningsantagelse. Efter en leverandør- eller registermeddelelse indberetter en kunde en besked med kendte person- eller bookingoplysninger og et betalingskrav.

Udløser. Kundeservice modtager en faktisk besked, et transaktionsforsøg eller en uafhængigt verificerbar indberetning. Generel bekymring efter en nyhedsartikel begrunder forklaring af kontrolkanalen, ikke dokumentation for svindeltab.

Beslutning. Svindelteamet verificerer destinationen, bevarer kontakten og fastslår risiko for penge eller kontoadgang. Databeskyttelsesteamet forbinder kun hændelsen med tidligere omfang, hvor evidensen understøtter relationen.

Afslutningsdokumentation. Registrér kundens sikre kanal, transaktionsafgørelse, udsendt kommunikation og eventuelle ændringer af tjenestekontroller. Brug ikke en teknisk genopretningsmeddelelse som grund til at lukke indberetninger om senere misbrug.

Alternativ forklaring. Svindel kan bruge oplysninger fra en anden kilde. Matchende biografiske oplysninger fastslår ikke alene, hvilken hændelse der leverede dem.

11.6 Hvad rapporten ikke forudsiger

Opslags- og afpresningspopulationerne understøtter ikke et fremtidigt dansk hændelsesantal, en angrebssandsynlighed, et økonomisk tab eller en markedsstørrelse. Den udvalgte portefølje fastslår ikke national udbredelse. Politiske begivenheder behandles ikke som angrebsårsager uden evidens for udsagnet.

En ny officiel konklusion, verificeret kontobrug eller leverandørspecifikt omfang kan ændre vurderingerne. Opdatér hændelsesregistrering og handlingsansvarlig, når det sker. Bevar den tidligere usikkerhed frem for at omskrive den oprindelige påstand, som om den altid var bekræftet.

HOVEDPOINTER

01

Brug betingede scenarier til at vælge handlinger, ikke antyde forudsagte hændelsesantal.

02

Definér evidensen, der ændrer inddæmning, indberetning eller kundebeskyttelse.

03

Hold alternativer åbne, indtil relevant tjeneste- og kontoevidens afklarer dem.

KAPITEL 12

Handlingsplan: ansvar og afslutningsdokumentation

12

DETTE KAPITEL BESVARER

Hvad bør ledelsen kræve inden for de næste 30, 60 og 90 dage?

4

arbejdsspor: identitet, leverandører, kontinuitet og indberetning

12.1 Planen for 30/60/90 dage 94
12.2 Identitets- og SOC-teams 96
12.3 Tjeneste- og driftsansvarlige 96
12.4 Databeskyttelse, jura og kommunikation 97
12.5 Svindelbekæmpelse, kundeservice og økonomi 97
12.6 Et ledelsesoverblik med dokumenterbare resultater 98
12.7 Sådan kan Brandefense hjælpe 98

KAPITEL 12

Handlingsplan: ansvar og afslutningsdokumentation

KORT FORTALT

Begynd med brugbare alarmer, tjenesteejerskab og hændelseskontakter. Afprøv derefter kontogendannelse, leverandøromfang og forretningskontinuitet gennem realistiske øvelser. Afslutningsdokumentation bør vise en fungerende beslutning, ikke kun en politik eller et møde. Aktive trusler og akutte eksponerede sårbarheder kræver øjeblikkelig handling; forbedringsplanen er ikke tilladelse til at vente. Giv hvert arbejdsspor en ansvarlig, og kræv dokumentationen nedenfor.

12.1 Planen for 30/60/90 dage

Sporene fastlægger rækkefølgen for forbedringsarbejdet. Bekræftet aktivt misbrug, sikkerhedsrisiko eller en akut relevant sårbarhed tilsidesætter tidsplanen. Hændelsesleder bør registrere den øjeblikkelige handling og begrundelsen.

1Dag 1–30

Etablér relevante eksterne alarmer og afgørelseskanal

ANSVARLIG
CISO og efterretningsansvarlig

DOKUMENTATION FOR AFSLUTNING
Første alarm modtaget, ansvar tildelt og indsats afprøvet

Kortlæg kritiske tjenesters identitets-, data- og leverandørafhængigheder

ANSVARLIG
Tjenesteansvarlige og teknologi

DOKUMENTATION FOR AFSLUTNING
Godkendt tjenestekort med alternativ drift og kontakter

Afstem privilegeret, inaktiv og nødadgang

ANSVARLIG
Identitets- og systemansvarlige

DOKUMENTATION FOR AFSLUTNING
Adgangsafgørelser og afprøvet nødgendannelse

Verificér indberetningskanaler og stedfortrædende beslutningstagere

ANSVARLIG
Jura, databeskyttelse og compliance

DOKUMENTATION FOR AFSLUTNING
Enhedsspecifikt kanalkort og tilgængelige kontakter

Gennemgå arvede systemer og historiske persondatalagre

ANSVARLIG

Data- og teknologiansvarlige

DOKUMENTATION FOR AFSLUTNING

Opbevaringsformål, ansvarlig og sletteundtagelser registreret

2Dag 31–60

Afprøv en leverandørmeddelelse med ufuldstændigt omfang

ANSVARLIG

Hændelseshåndtering og tredjepartsrisiko

DOKUMENTATION FOR AFSLUTNING

Tidsmålt omfangsanmodning, driftsbeslutning og underretningsvurdering

Genopret en kritisk tjeneste uden dens normale afhængighed

ANSVARLIG

Drift og genopretning

DOKUMENTATION FOR AFSLUTNING

Demonstreret alternativ drift, sikker genopretning og afstemning

Afprøv kontogendannelse mod overbevisende identitetsbedrag

ANSVARLIG

Identitet og svindelbekæmpelse

DOKUMENTATION FOR AFSLUTNING

Bedrag afvist og legitim bruger gendannet via godkendt kanal

Afprøv kundeadvarsler og kontrol af betalingsændringer

ANSVARLIG

Kundeservice og økonomi

DOKUMENTATION FOR AFSLUTNING

Advarsel forstået og destination uafhængigt kontrolleret

3Dag 61–90

Afprøv isolation af forbundet udstyr med driftsansvarlig

ANSVARLIG

Drift og sikkerhed

DOKUMENTATION FOR AFSLUTNING

Sikker isolation, bevaret evidens og godkendt genstart

Demonstrér leverandørudtræden for kritisk afhængighed

ANSVARLIG

Indkøb, drift og teknologi

DOKUMENTATION FOR AFSLUTNING

Alternativ tjeneste, dataadgang og afstemning demonstreret

Gennemgå alarmafgørelser efter brugbare observationer	
ANSVARLIG	DOKUMENTATION FOR AFSLUTNING
Sikkerhed og identitet	Evidensbaserede afgørelser og ansvar for uafklarede input
Rapportér resterende risiko og forsinkede afhængigheder til ledelsen	
ANSVARLIG	DOKUMENTATION FOR AFSLUTNING
CISO og ansvarlig direktion	Accepteret risiko, finansieret handling og navngiven afslutningsfrist

12.2 Identitets- og SOC-teams

Etablér input. Aftal, hvilke aktiver og konti eksterne alarmer dækker, hvor de modtages, og hvem der accepterer dem. Bekræft, at eskalation virker uden for normal arbejdstid. Kommer ingen observation, behandles dækning som uafprøvet frem for perfekt valideret.

Kontrollér udsagnet. Adskil annoncerede legitimationsoplysninger, en gyldig konto, et vellykket login og bekræftet dataadgang. Hvert forhold kræver forskellig evidens. Bevar alarmen og interne resultater, så senere opdateringer ikke overskriver den oprindelige usikkerhed.

Gennemgå gendannelse og sessioner. Hvor evidensen begrunder inddæmning, undersøges kontogendannelse, privilegerede ændringer og aktive sessioner sammen med adgangskodehandling. Fastslå slutenhedens ejer før isolation. Historisk materiale bør kontrolleres mod tidligere afhjælpning.

Prioritér relevante akutte svagheder. Identificér installeret produkt og relevant konfiguration, brug leverandørvejledning, og registrér rettet version eller afhjælpning. Undersøg tidligere adgang, hvor vejledning eller intern evidens begrunder det. En vellykket opdatering og en indtrængningsundersøgelse besvarer forskellige spørgsmål.

12.3 Tjeneste- og driftsansvarlige

Definér minimumsdrift. Identificér, hvad der skal fortsætte, mens det normale identitets-, booking-, betalings- eller administrationssystem er utilgængeligt. Et teknisk genopretningsmål bør knyttes til forretningskravet. Afprøv alternativ drift med de personer, der skal udføre den.

Styr gentilslutning. Angiv, hvem der kan gendanne en leverandørgrænseflade, og hvilken evidens der kræves. En leverandørs melding om tilgængelighed fastslår ikke automatisk jeres dataomfang. Registrér midlertidige begrænsninger og deres forretningsfølger.

Beskyt forbundet udstyr. Bevar ejerskabs- og fjernadgangsoplysninger for styringer, der påvirker fysiske processer. Afprøv sikker isolation med driftsspecialisten. Udled ikke fysisk påvirkning af et utilgængeligt offentligt websted eller en aktørpåstand.

12.4 Databeskyttelse, jura og kommunikation

Bevar tidslinjen. Registrér tidspunkter for opdagelse, kendskab, klassifikation, inddæmning, offentliggørelse og opdatering særskilt. Forklar, hvilket tidspunkt der starter hver gældende indberetningspligt. Forsink ikke en påkrævet indledende meddelelse, blot fordi alle berørte registreringer endnu ikke er optalt.

Skriv ud fra fastslåede forhold. Skeln mellem uautoriseret adgang, kopierede data, afbrudte tjenester og ubekræftede afpresningspåstande. Tilskriv en aktørbetegnelse til dens kilde. Angiv uafklarede forhold og næste opdateringstidspunkt.

Brug forholdsmæssige offentlige detaljer. Forklar nødvendige handlinger uden unødvendige identifikatorer eller gentagelse af aktørretorik. En nyttig advarsel giver en kendt kontaktkanal, relevant beskyttelseshandling og klare begrænsninger.

12.5 Svindelbekæmpelse, kundeservice og økonomi

Verificér anmodninger og destinationer. Kræv en kendt kanal for ændrede betalingsinstrukser, kontogendannelse og anmodninger om identitetsdokumenter. En opkalders kendskab til navne, bookinger eller adresser dokumenterer ikke bemyndigelse.

Hold indberetninger åbne efter genopretning. Kopierede oplysninger kan fortsat bruges til svindel. Giv kunder en kanal for mistænkelige henvendelser, og vurder faktisk forsøgt eller gennemført skade. Knyt kun indberetningen til en tidligere hændelse, når evidensen understøtter forbindelsen.

Afprøv forståelige advarsler. Bed en person uden for hændelsesteamet følge advarslen og finde kontrolkanalen. Fjern unødvendigt fagsprog. En advarsel bør reducere risikable beslutninger uden at kræve tillid til en ukendt kontakt.

12.6 Et ledelsesoverblik med dokumenterbare resultater

Ledelsesspørgsmål	Mål inden dag 90	Dokumentation til kontrol
Når relevante alarmer en ansvarlig?	Fungerende kanal med første afprøvede modtagelse	Alarm- og eskalationsregistrering
Kan vi forklare handlinger på relevante identitetssignaler?	Hver modtaget væsentlig alarm har afgørelse eller afhængighed med ansvar	Sagsregister og valideringsevidens
Kan kritiske tjenester fortsætte under leverandørafbrydelse?	Afprøvet alternativ drift for prioriteret tjeneste	Forretningsdemonstration og afstemning
Kan vi opfylde gældende indberetningspligter?	Enhedsspecifik øvelse afsluttet med lukkede rettelser	Tidsmålt forløb og indsendelsesudkast
Kan kunder verificere en ægte anmodning?	Kendt kanal afprøvet med kundeservice	Kommunikationstest og svindelforløb
Har ældre registreringer en ansvarlig?	Prioriterede lagre gennemgået og undtagelser godkendt	Opbevaringsafgørelse og slettevalidering

Det er foreslåede ledelsesmål, ikke målte resultater for danske organisationer. Ledelsen bør vælge den prioriterede tjeneste og udtrykkeligt acceptere resterende afhængigheder. Målet er en beslutning, som kan demonstreres under en hændelse.

12.7 Sådan kan Brandefense hjælpe

Brandefense tilbyder trusselsefterretninger, overvågning af kriminelle onlinemiljøer og indsigt i den eksterne angrebsflade. En nyttig demonstration bør følge et aktiv med kendt ejer fra ekstern observation gennem validering, tildeling og afslutning. Spørg, hvordan alarmen når teamet, og hvilken evidens der understøtter beslutningen. [S39]

Rapporten lover ikke, at et værktøj forebygger enhver hændelse, eller at en annonce dokumenterer adgang. Driftsværdien afhænger af relevant dækning, ansvarlige ejere og en proces, som adskiller påstande fra bekræftede resultater.

Bestil en Brandefense-demonstration.

HOVEDPOINTER

01

Etablér brugbare input og ansvarlige ejere, før indsatsen måles.

02

Afprøv tjeneste, gendannelsesvej og leverandørbeslutning med forretningsdeltagere.

03

Kræv afslutningsdokumentation, mens aktive trusler og akutte svagheder håndteres straks.

BILAG

Bilag

A–D

DETTE KAPITEL BESVARER

Bilag A. Omfang og evidensgrænser · Bilag B. Evidenskortregister · Bilag C. Kilder · Bilag D. Ordliste

76
kilder

Bilag A. Omfang og evidensgrænser 101
Bilag B. Evidenskortregister 104
Bilag C. Kilder 106
Bilag D. Ordliste 110

Bilag A. Omfang og evidensgrænser

Sammenligningslandene er udelukkende valgt som eksempler for at give kontekst; de indebærer ingen rangordning eller politisk vurdering.

A.1 Periode og datobetydninger

Rapportens ønskede periode er 1. januar–22. november 2026 efter opslagstidspunkt. Seneste aktivitet omfatter 8.–22. november 2026. Offentlige hændelsesdatoer følger kilden: hændelse, opdagelse, offentliggørelse og senere opdateringer adskilles. En publikation i den seneste periode dokumenterer ikke ny indtrængen i samme periode.

Undersøgelsen bruger bevarede opslag fra kriminelle miljøer, offentlige afpresningsopslag, en udvalgt domæneportefølje, myndighedsmeddelelser, organisationsudtalelser og understøttende presse- eller teknisk omtale. Hver population har sin egen enhed. Totalerne kan ikke lægges sammen til et nationalt hændelsesantal. [S1][S2] [S3]

Det offentlige kildemateriale omfatter dansk, engelsk, russisk og tyrkisk. Kildetilgængelighed og arkivdækning er forskellige. Rapporten attesterer ikke fravær af hændelser i en måned, hos en udvalgt organisation eller på en tjeneste uden bekræftet offentliggørelse.

A.2 Opslag, annoncer og sagsdossierer

Et opslag er en bevaret meddelelse. Det kan indeholde en annonce, et svar, viderebragte nyheder, en aktørpåstand, en landereference eller irrelevant materiale. En landerelation dokumenterer ikke målretning, systemets placering eller opslagsskriverens nationalitet. [S1]

De seks dossierer fra kriminelle miljøer er udvalgte eksempler, som understøtter forskellige valideringsbeslutninger. De er ikke en repræsentativ stikprøve af danske hændelser eller kriminel aktivitet. Flere beskeder kan vedrøre én påstand. Lignende ordlyd understøtter en annonceringsrelation uden at dokumentere identiske filer, gennemført handel eller fælles kontrol.

Autentiske uddrag bevarer redaktioner i kantede parenteser. De beskriver opslagsskriverens udsagn med dato og forumtype ved kortet. Rapporten offentliggør ikke fungerende legitimationsoplysninger, persondatarækker, kriminelle kontaktoplysninger eller identifikatorer for ubekræftede mål. Et citat gør ikke den underliggende påstand til en bekræftet hændelse.

En offentliggørelse og et opslag om den kan beskrive samme hændelse. Viderebragte nyheder bekræfter ikke uafhængigt den rapport, de gentager. Et kort svar dokumenterer heller ikke køb eller vellykket download. Påstande forbliver afgrænsede i sammenfatninger, kort, tabeller og anbefalinger.

A.3 Afpresningsopslag og sammenligningslande

Ransompedias daterede øjebliksbillede indeholder Danmarkstilknyttede opslag og de fire sammenligningspopulationer for Sverige, Norge, Tyskland og Nederlandene. Opslagsdatoerne ligger i den ønskede periode. Foregående års tal dækker hele 2025 og er derfor ikke sammenligningsgrundlag for samme periode. [S2]

Et opslag registrerer en kriminel påstand. Det dokumenterer ikke kryptering, dataudtræk, betaling, økonomisk tab eller den præcise begyndelse på indtrængen. Lande- og branchebetegnelser beskriver opslagspopulationen. De er ikke juridiske ejerskabsafgørelser eller nationalt repræsentative sektorstikprøver.

Gruppebetegnelser identificerer ikke unikke operatører. Flere betegnelser kan involvere overlappende personer eller tjenester, men relationen udledes ikke uden konkret evidens. Sammenligningstallene giver ingen landerangering, befolkningsjusteret angrebssandsynlighed eller måling af kontrolvirkning.

A.4 Udvalgt domæneportefølje og eksponeringsobservationer

Den udvalgte portefølje indeholder 250 kandidatdomæner i ti grupper med 25 i hver. Udvælgelsen afspejler tjeneste- og sektorrelevans. Den er ikke en officiel virksomhedsrangliste eller sandsynlighedsstikprøve. Brands, datterselskaber og fælles tjenester kan overlappe; et domæne repræsenterer ikke nødvendigvis en selvstændig juridisk enhed. [S3]

Atlas leverer den nationale vurdering på 45/100 (B) for den udvalgte portefølje. Legitimationsoplysninger blev annonceret til salg for 37 af 250 domæner ved kontrollen. Sektortabeller offentliggør kun signaltællinger. Ingen organisations- eller sektorvurdering offentliggøres. Enheds- og legitimationsrelationer kan overlappe og dokumenterer ikke aktuel kontogyldighed. [S3]

Observationer af enheder, legitimationsposter, dokumenter og aktuelle tilbud blev læst 22. november 2026. Årlig omtale blev læst 23. november 2026 og slutter 18. november 2026. Lignende navne dækker 19. oktober–18. november 2026. Passive kontrolobservationer mangler fortsat, så intet hygiejneindeks eller mailpolitikresultat offentliggøres. Domæneopslag alene validerer ikke ejerskab eller en sikkerhedstilstand.

Valideringsvejledningen forbinder observationer med ansvarlige interne kontroller. Den angiver første kontrol, ansvarlig og afslutningsdokumentation for en modtaget observation. Læseren bør modtage relevante alarmer og bekræfte tjenesteforholdet før beslutning om afhjælpning eller underretning.

Den organisationsrelaterede opslagkontekst er en særskilt evidenspopulation fra læsekorpusset i kapitel 4 og betalingskortobservationerne. Den leverer daterede påstande, ikke yderligere bekræftede hændelser. Posterne lægges ikke til læsekorpussets tal eller totalerne for ransomwareopslag. [S3]

I c03 tæller `orgs_listed_for_sale_now` udvalgte domæner med aktuelle legitimationstilbud. Feltet tæller ikke uafhængige organisationer, annoncer eller organisationer udbudt til salg.

A.5 Officiel bekræftelse og tilskrivning

Officiel bekræftelse knytter sig til det udsagn, organisationen eller myndigheden faktisk fremsætter. Den kan fastslå adgang, mens aktør, adgangsvej, kopieret mængde eller driftspåvirkning forbliver uafklaret. En leverandørbekræftelse dokumenterer ikke identiske følger hos alle kunder.

En organisation navngives kun, hvor officiel bekræftelse og bred offentlig omtale understøtter hændelsesbeskrivelsen. Andre sager bruger generelle tjeneste- eller sektorbetegnelser. Identificerer en kilde et tilbageholdt mål, beskytter den offentlige reference identiteten sammen med teksten. Kildeadresser ejet af ofret udelades.

Statstilskrivning forbliver den citerede myndigheds vurdering. Sprog, politisk indramning, geografi eller alias dokumenterer ikke nationalitet, støtte eller fælles kontrol. Forbindelseskortet registrerer kilderelationer; det antyder ikke samarbejde mellem ellers uforbundne aktører.

A.6 Betalingskortenes afgrænsning

KORTTALLENES AFGRÆNSNING

Tallene beskriver betalingskortregistreringer i den bevarede opslagssamling. De måler ikke national korteksponering, korttyveri eller svindeltab.

Observerede registreringer, annoncerede statusser og udbudspriser dokumenterer ikke aktive kort, gennemførte køb eller udstedertab. Kort-, konto- og enhedsobservationer er særskilte populationer. Intet nationalt svindelmarkedsestimat udledes af dem. [S4]

A.7 Tillid og beslutninger

Evidensbetegnelse	Hvad den understøtter	Vigtigste begrænsning
Observation	Den bevarede kilde indeholder den angivne meddelelse eller registrering	Underliggende indhold og følger kan være ubekræftede
Aktørpåstand	En opslagsskriver eller et afpresningsopslag hævder den beskrevne aktivitet	Vellykket adgang, oprindelse og tab kræver særskilt evidens
Officiel bekræftelse	Den udstedende organisation eller myndighed bekræfter angivet omfang	Beskrivelsen kan være foreløbig eller efterlade tilskrivning uafklaret
Analytikerslutning	En begrundet fortolkning eller planlægningskonsekvens	Alternativer og ændrende evidens forbliver tydelige

Tillid knytter sig til et udsagn, ikke en person eller gruppe. Den anbefalede handling bør passe til fastslået evidens. En valideret historisk eller unøjagtig relation kan begrunde afslutning, mens uafklaret evidens kræver en ansvarlig og næste valideringstrin.

Bilag B. Evidenskortregister

Kortene registrerer udvalgte bevarede annoncer. Datoerne er beskeddatoer, og aliaser identificerer opslagssignaturer frem for verificerede personer. Kort B01–B06 vises ved sagerne i kapitel 4; de øvrige kort vises ved påstandene i kapitel 6. [S1]

Kort	Dato	Forumtype	Alias	Sprog	Dossier
B01	2026-07-02	Forum	thejackal101	Engelsk	A: gentaget beskrivelse af legitimationsoplysninger
B02	2026-09-12	Forum	K0d3x	Engelsk	B: påstand om finansielle kunder
B03	2026-10-14	Forum	MrData	Engelsk	C: påstand om fællesskabsdata
B04	2026-08-24	Forum	Bitcoins	Engelsk	D: påstand om udviklingssystem
B05	2026-11-05	Forum	marlowfinch42	Engelsk	E: regionalt tilbud om adgang til softwarebygning
B06	2026-01-04	Forum	selluk	Engelsk	F: katalogtematisk tilbud
B07	2026-01-28	Telegram	inteid	RU	Påstand i kapitel 6
B08	2026-02-02	Telegram	inteid	RU	Påstand i kapitel 6
B09	2026-03-26	Telegram	NoName057(16) (signatur i opslaget)	RU	Påstand i kapitel 6
B10	2026-09-28	Telegram	NoName057(16) (signatur i opslaget)	EN	Påstand i kapitel 6

Navngivne offentlige sager og understøttende omtale

Følgende kildepar understøtter offentlig navngivning for den konkrete hændelsesbeskrivelse. De godkender ikke uvedkommende påstande og identificerer ikke ubekræftede efterfølgende ofre.

Offentlig sag	Officiel beskrivelse	Understøttende omtale
DTU	[S13][S53]	[S55]
Københavns Universitet	[S12]	[S56]

Offentlig sag	Officiel beskrivelse	Understøttende omtale
AU	[S14]	[S57]
CPR-hændelsen	[S15]	[S58]
Mobiloperatøren 3	[S47]	[S65]
Lejre Kommune	[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]

Bilag C. Kilder

S1: Odin by Brandefense. Retained Denmark-associated underground posts, 1 January–22 November 2026. Egne belæg; ingen offentlig adresse. Kontrolleret den 23. november 2026.

S2: Ransompedia. Denmark and four regional peer listing snapshot, 1 January–22 November 2026. Egne belæg; ingen offentlig adresse. Kontrolleret den 23. november 2026.

S3: Odin by Brandefense. Selected Danish domain portfolio, Atlas exposure observations and organisation-associated post context. Egne belæg; ingen offentlig adresse. Kontrolleret den 23. november 2026.

S4: Odin by Brandefense. Payment-card observations in the retained post corpus. Egne belæg; ingen offentlig adresse. Kontrolleret den 23. november 2026.

S5: SAMSIK. Digital sikkerhed i virksomheder 2026. https://samsik.dk/publikation/digital-sikkerhed-i-virksomheder-2026/ Kontrolleret den 24. november 2026.

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

S7: FE. FE current cyber role. https://www.fe-ddis.dk/da/arbejdsomrade-a/Cybertruslen/ Kontrolleret den 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/ Kontrolleret den 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/ Kontrolleret den 23. november 2026.

S10: Maersk. Maersk official incident. https://www.maersk.com/news/articles/2026/11/11/it-security-incident Kontrolleret den 23. november 2026.

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

S12: University of Copenhagen. KU incident and FAQ. https://www.ku.dk/orientering-om-bruddet-paa-persondatasikkerheden Kontrolleret den 23. november 2026.

S13: Technical University of Denmark. DTU incident latest update. https://dtu.dk/english/about/contact/it-information Kontrolleret den 23. november 2026.

S14: AU. AU official incident notice. https://medarbejdere.au.dk/nyheder/nyhed/artikel/au-har-vaeret-udsat-for-hackerangreb Kontrolleret den 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/ Kontrolleret den 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 Kontrolleret den 23. november 2026.

S17: Public-sector body. Supplier-related personal-data notice, 30 October; update 4 November 2026. Artikeladresse udeladt; kildens meddelelse læst. Kontrolleret den 23. november 2026.

S18: Techotel. Techotel operational log. https://techotel.dk/operation/?page=target Kontrolleret den 23. november 2026.

S19: BrickLink. BrickLink latest official recovery. https://maintenance.bricklink.com/recovery.html Kontrolleret den 23. november 2026.

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

S21: Finanstilsynet. Payment-service provider IT inspection, 10 July 2026. https://www.finanstilsynet.dk/ (artikeladresse udeladt) Kontrolleret den 23. november 2026.

S22: Datatilsynet. Autoforhandler får alvorlig kritik for manglende sletning: announcement. https://www.datatilsynet.dk/ (artikeladresse udeladt) Kontrolleret den 23. november 2026.

S23: Datatilsynet. Datatilsynet vehicle-retailer decision. https://www.datatilsynet.dk/ (artikeladresse udeladt) Kontrolleret den 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 Kontrolleret den 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/ Kontrolleret den 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/ Kontrolleret den 23. november 2026.

S27: Retsinformation. NIS2 statutory text. https://www.retsinformation.dk/eli/lta/2025/434/pdf Kontrolleret den 23. november 2026.

S28: SAMSIK. Spørgsmål og svar om NIS 2. https://samsik.dk/nis2/faq/ Kontrolleret den 23. november 2026.

S29: SAMSIK. Registrering af enheder efter NIS 2-loven. https://samsik.dk/nis2/registrering-nis2/ Kontrolleret den 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 Kontrolleret den 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 Kontrolleret den 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 Kontrolleret den 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 Kontrolleret den 23. november 2026.

S34: Apache Software Foundation. Apache HTTP Server 2.4 security advisories. https://httpd.apache.org/security/vulnerabilities_24.html Kontrolleret den 23. november 2026.

S35: NVD. CVE-2026-119618 record. https://nvd.nist.gov/vuln/detail/CVE-2026-119618 Kontrolleret den 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 Kontrolleret den 23. november 2026.

S37: NVD. CVE-2026-123890 record. https://nvd.nist.gov/vuln/detail/CVE-2026-123890 Kontrolleret den 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 Kontrolleret den 24. november 2026.

S39: Brandefense. Platform demonstration. https://brandefense.io/request-a-demo/ Kontrolleret den 23. november 2026.

S40: SAMSIK. SAMSIK camera warning. https://samsik.dk/artikler/2026/01/opfordring-husk-sikkerheden-paa-overvaagningskameraer/ Kontrolleret den 23. november 2026.

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

S42: SAMSIK. SAMSIK June destructive warning. https://samsik.dk/publikation/skaerpet-trussel-fra-destruktive-cyberangreb/ Kontrolleret den 23. november 2026.

S43: SAMSIK. SAMSIK September high threat. https://samsik.dk/publikation/destruktive-cyberangreb-september-2026/ Kontrolleret den 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 Kontrolleret den 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 Kontrolleret den 23. november 2026.

S46: Regional health authority. Hospital building-network incident notice. Artikeladresse udeladt; kildens meddelelse læst. Kontrolleret den 23. november 2026.

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

S48: Press publisher. Education-provider incident report quoting institutional leadership. https://presse-fotos.dk/ (artikeladresse udeladt) Kontrolleret den 23. november 2026.

S49: Publishing customer. Print-distribution supplier incident: customer notice, 12 November. Artikeladresse udeladt; kildens meddelelse læst. Kontrolleret den 23. november 2026.

S50: Subscriber organisation. Print-distribution supplier incident: customer notice, 13 November. Artikeladresse udeladt; kildens meddelelse læst. Kontrolleret den 23. november 2026.

S51: Membership-service organisation. Web-platform provider incident and customer-impact boundary. Artikeladresse udeladt; kildens meddelelse læst. Kontrolleret den 23. november 2026.

S52: Specialist public information service. User-administration incident notice, 4 November. Artikeladresse udeladt; kildens meddelelse læst. Kontrolleret den 23. november 2026.

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

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

S57: Ritzau. AU Ritzau coverage. https://ni.dk/ni-news/id/01f6c003-4349-46fe-a1f8-ba2ba8342961/ Kontrolleret den 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 Kontrolleret den 23. november 2026.

S59: Tunnelling Journal. FLC industry press. https://tunnellingjournal.com/cyber-incident-hits-fehmarnbelt-tunnel-contractor/ Kontrolleret den 23. november 2026.

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

S61: Brickset. BrickLink back online, 12. november 2026. https://brickset.com/article/136115/bricklink-back-online Kontrolleret den 23. november 2026.

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

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

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

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

S68: Company statement via Ritzau. Department-store internal IT incident and continuing customer operations, 21 October 2026. https://via.ritzau.dk/ (artikeladresse udeladt) Kontrolleret den 23. november 2026.

S69: Travelmarket. Information om säkerhetsincident hos Travelmarket. https://www.travelmarket.se/blog/sakerhetsincident-travelmarket/ Kontrolleret den 23. november 2026.

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

S71: Nyhed24. Restaurant customer notice concerning a reservation supplier, 3 November 2026. https://nyhed24.dk/ (artikeladresse udeladt) Kontrolleret den 23. november 2026.

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

Bilag D. Ordliste

Begreb	Enkel forklaring
Kontogendannelse	Den autoriserede proces til at genskabe legitim adgang efter et problem
Autentificering	Kontrol af en identitet før adgang gives
Omgåelse af autentificering	En fejl, som gør det muligt for uvedkommende at undgå en tilsigtet identitetskontrol [S37]
Kendskabstidspunkt	Når den relevante enhed ved nok om en hændelse til at begynde den gældende vurdering
System til softwarebygning (build-system)	En tjeneste, som klargør software til test eller udgivelse
CFCS	Center for Cybersikkerhed, hvis tidligere ansvar blev fordelt mellem nuværende funktioner [S6][S7]
Aktørbetegnelse	Navnet knyttet til en kriminel påstand; det identificerer ikke en verificeret person
Combolist	En samlet liste over kontonavne og adgangskoder fra forskellige kilder
CPR	Danmarks personregistreringssystem; en identifikator bekræfter ikke en opkalders bemyndigelse [S16]
CSIRT	Et team til håndtering af computersikkerhedshændelser; FE varetager Danmarks nationale NIS2-funktion [S7]
Dataansvarlig	Den part, som beslutter, hvorfor og hvordan personoplysninger behandles
Databehandler	En part, som behandler personoplysninger på den dataansvarliges vegne
Dataopbevaring	Bevaring af oplysninger til et begrundet formål og tidsrum efterfulgt af passende sletning
DDoS	Distribueret trafik, som har til formål at overbelaste en online-tjeneste [S8]
DMARC	Mailpolitik og rapportering, som forbinder afsenderdomæne-overensstemmelse med autentificeringsresultater [S62]
DORA	EU-regler om digital operationel modstandsdygtighed for omfattede finansielle enheder [S31][S32]
Slutenhed	En enhed eller et system i kanten af et administreret miljø
Afpresningsopslag	En kriminel offentliggørelse med en påstand om en organisation

Begreb	Enkel forklaring
FE	Forsvarets Efterretningstjeneste med cyberfunktionerne beskrevet i den aktuelle vejledning [S7]
GDPR	EU's databeskyttelsesramme med særskilte pligter til anmeldelse og underretning ved brud [S30]
IAM	Identitets- og adgangsstyring: administration af konti og deres tildelte rettigheder
IKT	Informations- og kommunikationsteknologi
MFA	Autentificering, der kræver mere end én type faktor
NIS2	EU-cybersikkerhedsdirektiv gennemført som nationale pligter for omfattede enheder [S27]
OT	Teknologi, der overvåger eller styrer fysiske processer
Phishing	Bedragerisk kontakt, som søger oplysninger eller en usikker handling
Ransompedia	Brandefenses kilde til ransomwareopslag; opslag registrerer påstande
SAMSIK	Styrelsen for Samfundssikkerhed [S6]
Session	En periode med autentificeret adgang, som kan kræve særskilt gennemgang ved kontoproblemer
Signeringsnøgle	Kryptografisk materiale brugt til at skabe digitale signaturer, som understøtter kontrol af indholds oprindelse og integritet
Smishing	Phishing via tekstbeskeder
Leverandørudtræden	Flytning fra en leverandør med bevarelse af den nødvendige tjeneste
TLP:CLEAR	Oplysninger kan deles uden begrænsning med forbehold for andre gældende pligter
VPN	En kontrolleret netværksforbindelse til fjernadgang til tjenester

Om rapporten

Udarbejdet af Odin by Brandefense til sikkerhedsledelse, tjenesteansvarlige, hændelsesteams, svindelteams, databeskyttelsesansvarlige og kommunikationsteams. Version 1.0 dækker den ønskede periode 1. januar–22. november 2026 med seneste aktivitet vist for 8.–22. november.

Resultaterne skelner mellem bevarede observationer, aktørpåstande, officiel bekræftelse og analytikerslutninger. Den udvalgte portefølje estimerer ikke national udbredelse. Manglende observationer forbliver utilgængelige frem for at antyde nul eksponering.

Den danske udgave er oversat fra den engelske hovedudgave. Den engelske udgave har forrang ved betydningsforskelle.

© 2026 Brandefense. Alle rettigheder forbeholdes.

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