BRANDEFENSE COUNTRY REPORT · SWEDEN 2026

Brandefense rapport om Sveriges cyberhotbild 2026

Identiteter, leverantörsexponering och kontinuitet i digitala och fysiska tjänster

Odin by Brandefense

Undersökningsperiod: 1 januari–22 november 2026

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

192 av 250

utvalda domäner publicerade DMARC med reject eller quarantine

7

påståendefall med autentiska maskerade utdrag

24

aktörsetiketter i Sveriges utpressningspubliceringar

23 av 25

utvalda finansdomäner publicerar DMARC med reject eller quarantine

INNEHÅLL

Innehåll

Translated with AI

Denna utgåva är översatt med AI från den engelska originaltexten. Vid skillnader gäller den engelska utgåvan.

01	Sammanfattning	05
	Rapportöversikt	09
02	Sveriges digitala och institutionella sammanhang	10
03	Nationell exponering: en utvald portfölj	14
04	Observationer i kriminella miljöer och påståendefall	22
05	Incidenter och besked per sektor	37
06	Hacktivism, tillgänglighet och operativa system	49
07	Hotaktörer, publiceringsetiketter och attribuerade kampanjer	53
08	Bedrägeri, informationshandel och följdskador	60
09	Bank, finansiella kontaktlistor och betalningskontinuitet	64
10	Regler och nationell hantering	68
11	Utsikter och villkorade scenarier	72
12	Åtgärdsplan och belägg för genomförande	76
A	Bilaga A. Omfattning och underlagets gränser	82
B	Bilaga B. Underlagsregister	85
C	Bilaga C. Källor	86
D	Bilaga D. Ordlista	90
	Om rapporten	91

Styrelse och ledning	01 05 10 11 12
Säkerhetschef och tjänsteägare	03 04 05 10 12
SOC och hotanalys	04 06 07 12 B
Bedrägeriförebyggande och kundverksamhet	05 08 09 12
Dataskydd, juridik och kommunikation	05 06 10 12

Om denna utgåva

Översatt med AI. Vid skillnader gäller den engelska utgåvan.

Sveriges dokumenterade incidenter kopplar samman identitetsmissbruk, leverantörslagrade uppgifter och tjänstekontinuitet. Verifiera varje exponering och behåll skillnaden mellan påståenden och bekräftade följder.

62

Sverige-märkta utpressningspubliceringar; kriminella påståenden, inte bekräftade intrång

775 020

observerade Sverige-anknutna inlägg under perioden; inget incidentantal

50/100

Nationellt Atlas-huvudvärde; 242 bedömda domäner i den utvalda portföljen

22

fallbeskrivningar: 7 påståendefall och 15 offentliga händelsefall

Innehåll och läsvägar

Kapitel	Fråga
1 Sammanfattning	Vilka beslut bör ledningen ta först?
2 Sammanhang	Vilka beroenden och myndighetsförändringar påverkar hanteringen?
3 Utvalda domäners exponering	Vilka konfigurationsobservationer behöver ägarens kontroll?
4 Observationer i kriminella miljöer	Vad visar annonser, förfrågningar och vidareförmedling?
5 Incidenter per sektor	Vad bekräftade eller rapporterade organisationer och myndigheter?
6 Tillgänglighet och operativa system	Hur skiljer sig påståenden från tjänsteeffekter och fysiska följder?
7 Aktörer och kampanjer	Vilka samband och attribueringar har källstöd?
8 Bedrägeri	Hur kan information stödja en vilseledande förfrågan?
9 Bank	Vilka observationer gäller bank, kund eller beroende?
10 Regler	Vilken juridisk person, grund, mottagare och tidsfrist gäller?
11 Utsikter	Vilka villkorade signaler ändrar bedömningen?
12 Åtgärdsplan	Vem agerar och hur visas genomförandet?
Bilagor A–D	Omfattning, underlag, källor och definitioner

KAPITEL 01

Sammanfattning

01

DETTA KAPITEL BESVARAR

Vilket underlag stödjer omedelbara beslut för svenska organisationer?

62

Sverige-märkta utpressningspubliceringar under perioden

Fyra beslut för ledningen 07

Året i siffror 07

KAPITEL 01

Sammanfattning

I KORTHET

Underlaget motiverar separata prioriteringar för identitetskontroll, leverantörers uppgiftsförlust och tjänstekontinuitet. Ransompedia registrerar 62 Sverige-märkta publiceringar, var och en ett kriminellt påstående. Offentliga besked visar e-poståtkomst, exponerade kunduppgifter och avsiktliga tjänsteavstängningar. 73 av 242 bedömda domäner hade inloggningsuppgifter till försäljning. Nationellt Atlas-huvudvärde är 50/100. Den senaste aktivitetsperioden innehåller flera kundbesked där omfattningen är avgörande. Kontrollera egna konton, öva kritiska beroenden och ge driftåterställning och risk för människor skilda ansvariga.

Perioden är 1 januari–22 november 2026 efter inläggets tid. Senaste aktivitet omfattar 8–22 november. Publiceringsantal och aktuellt material kontrollerades efter UTC-sluttiden den 23 november. Rapporten är en daterad ögonblicksbild, inte en fullständig incidentkartläggning. Publiceringsdatum fastställer inte intrångsdatum.

1. Publiceringsantal motiverar beredskap utan att fastställa nationellt angreppsantal. De 62 Sverige-märkta utpressningspubliceringarna har 24 aktörsetiketter. De tre vanligaste står för 30 publiceringar, eller 48,4 %. Landanknytningar och återkommande organisationer begränsar tolkningen av unika organisationer. Publicering bekräftar inte kryptering, stöld eller betalning. [S2]

2. Identitetshantering omfattar mer än att byta lösenord. Vårdmyndighetsfallet skiljer 99 berörda e-postkontons inloggningsuppgifter från 44 konton där meddelanden lästes. CERT-SE:s novembervarning beskriver flera nätfiskekampanjer mot svenska organisationer. Relevanta konton kräver kontroll av inloggningar, sessioner och rättigheter, medan e-postinnehållets exponering bedöms separat. [S18][S33]

3. Leverantörs- och kundgrupper behöver egna nämnare. Lykos formella besked skiljer 36 000 svenska kunder från 60 000 på samtliga marknader. Universeums nya besked gäller en leverantörshändelse i slutet av oktober. Cabonlines besked väcker frågor om reseuppgifter. Gruppernas överlapp är okänt och de summeras inte till en svensk total. [S28][S30][S29]

4. Aktuella annonser kräver kontokontroll. 73 av 242 bedömda domäner hade inloggningsuppgifter till försäljning. Den bedömda portföljens nationella Atlas-huvudvärde är 50/100. Exponeringen förblir okänd för 8 utvalda domäner. Separat publicerar 192 av 250 domäner DMARC med reject eller quarantine. Observationerna är inte bekräftade intrång eller nationell prevalens. [S4][S3]

5. Tjänsteeffekter och fysiska följder kräver olika belägg. Officiella kylvarningar gäller uppkopplad operativ utrustning. Ett tillverkningsbesked gäller skyddsavstängning och produktionsavbrott. Ett webbplatspåstående ensamt fastställer varken operativ kontroll eller datastöld. Ge teknik och verksamhet ansvar tillsammans med incidentteamet. [S25][S27]

Fyra beslut för ledningen

1. **Verifiera identitetsunderlaget.** Bekräfta egna konton, aktuell användning och tidigare rättning; begränsa verifierad åtkomst, relevanta sessioner och autentiseringsändringar (§3–4, §12).
2. **Öva ändrade leverantörsbesked.** Kräv uppgiftskategorier, berörd tjänst och uppdateringar; bedöm risk för människor separat från teknisk återställning (§5, §8–10).
3. **Visa säker kontinuitet.** Testa minsta tjänst och säker reservdrift med leverantörsunderhåll och identitetsberoenden (§6, §9, §12).
4. **Ge varje tidsfrist ansvar.** Ange juridisk person, grund och mottagare; dokumentera kännedom och klassificering separat och ordna reservåtkomst för anmälan (§10, §12).

Året i siffror

775 020

Observerade Sverige-anknutna inlägg [S1]

VAD DET INTE MÄTER

Verifierade svenska incidenter eller unika offer

727 150

Januari- och februariinlägg inom gruppen [S1]

VAD DET INTE MÄTER

Två månaders bekräftad angreppstillväxt

62

Sverige-märkta utpressningspubliceringar [S2]

VAD DET INTE MÄTER

Unika organisationer eller bekräftade intrång

47

Sverige-märkta publiceringar under hela 2025 [S2]

VAD DET INTE MÄTER

En matchad observationsperiod

24

Aktörsetiketter i 2026-gruppen [S2]

VAD DET INTE MÄTER

Verifierade skilda operatörer

250

Utvalda domäner med konfigurationsobservationer [S3]

VAD DET INTE MÄTER

Alla svenska organisationer eller oberoende juridiska personer

73 av 242

Bedömda domäner med inloggningsuppgifter till försäljning [S4]

VAD DET INTE MÄTER

Testade inloggningsuppgifter eller bekräftade intrång

50/100

Nationellt Atlas-huvudvärde för den bedömda portföljen [S4]

VAD DET INTE MÄTER

Intrångsandel eller nationell prevalensskattning

192 av 250

Domäner med DMARC reject eller quarantine [S3]

VAD DET INTE MÄTER

Verifierad meddelandeleverans eller förhindrade bedrägerier

22

Sju påståendefall och femton offentliga händelsefall

VAD DET INTE MÄTER

Ett nationellt incidentantal utan dubbelräkning

VIKTIGA SLUTSATSER

01

Verifiera påståenden före ingripande begränsning.

02

Behåll gränser mellan leverantör, kund och tjänstepåverkan.

03

Kräv genomförandebelägg för identitet, kontinuitet och rapporteringsbeslut.

Rapportöversikt

Läsvägar och rapportöversikt. Tolv kapitel, fem läsvägar. Följ beslutet som motsvarar ansvaret och behåll underlagets gränser tillsammans med slutsatsen.

Styrelse och ledning	Resurssätt kontinuitet och kräv genomförandebelägg	Gå till 1 5 10 11 12
Säkerhetschef och tjänsteägare	Prioritera egna exponeringar och beroenden	Gå till 3 4 5 10 12
SOC och hotanalys	Skilj observation, påstående och attribuering	Gå till 4 6 7 12 Bilaga B
Bedrägeriförebyggande och kundverksamhet	Förebygg trovärdig vilseledning och följdskador	Gå till 5 8 9 12
Dataskydd, juridik och kommunikation	Bestäm omfattning, tidsfrister och försiktigt språk	Gå till 5 6 10 12

Underlagstyperna är **observation**, **aktörspåstående**, **officiell redogörelse**, **källbunden rapportering** och **analytisk slutsats**. En annons kan observeras direkt medan innehållet är obekräftat. Även vid en bekräftad incident kan attribueringen och hela den berörda gruppens omfattning vara oklara.

KAPITEL 02

Sveriges digitala och institutionella sammanhang

02

DETTA KAPITEL BESVARAR

Vilka beroenden påverkar hanteringen av en incident i Sverige?

1 juli 2026

CERT-SE blev en del av NCSC vid FRA

2.1 Digitala tjänster skapar beroenden för kontinuiteten 11

2.2 Två myndighetsförändringar har olika datum 11

2.3 Leverantörer skapar olika slags exponering 12

2.4 Politiska teman återges som källornas uppgifter 12

2.5 Ge varje tidsfrist en ansvarig 12

KAPITEL 02

Sveriges digitala och institutionella sammanhang

I KORTHET

Sveriges digitala tjänster knyter samman identiteter, leverantörer, betalningar och fysisk verksamhet. Avgör vilket beroende som har fallerat och vilka belägg som finns för följderna. Ansvarsfördelningen ändrades också under året: CERT-SE blev en del av NCSC vid FRA den 1 juli. Använd aktuella rapporteringsvägar, behåll datumen för äldre händelser och testa verksamhetens tjänst tillsammans med den tekniska återställningen.

2.1 Digitala tjänster skapar beroenden för kontinuiteten

Riksbanken beskriver den svenska betalningsmarknaden som nästan helt digital. I rapporten för 2026 lyfter banken störningar i el och datakommunikation som sårbarheter, vid sidan av cyberangrepp. Det är Riksbankens bedömning av motståndskraften, inte ett konstaterande att betalningar generellt är osäkra. [S7]

För en säkerhetschef är tjänstekedjan den praktiska utgångspunkten. Ett köp kan bero på handlare, nätverk, betaltjänst, identifiering och kundens enhet. Ett fel i en del visar inte att någon har fått åtkomst till alla deltagare. Kartlägg vilken minsta tjänst som kan fungera när ett beroende saknas.

Behandla alternativa betalningssätt och kundstöd som operativa skydd. Bestäm vem som får godkänna dem, vilka uppgifter de kräver och hur transaktioner stäms av efter återställningen. Detta är planeringsråd, inte påståenden om att någon namngiven organisation saknade en reservlösning.

2.2 Två myndighetsförändringar har olika datum

MSB blev Myndigheten för civilt försvar den 1 januari 2026. Äldre logotyper och webbadresser kan därför finnas kvar på giltigt myndighetsmaterial. En kvarvarande MSB-beteckning innebär inte i sig att ett meddelande är inaktuellt. [S6]

NCSC är en del av FRA. Den 1 juli 2026 fördes informations- och cybersäkerhetsverksamhet från Myndigheten för civilt försvar över till NCSC, däribland CERT-SE. Centret beskriver samverkan med försvars-, polis-, telekom- och säkerhetsmyndigheter. Rapporten behandlar inte denna samverkan som en attribuering av en incident. [S5]

Anteckna utgivare, publiceringsdatum och aktuell kontaktväg i incidentjournalen. Råd från tiden före juli kan fortfarande vara relevanta även om rapporteringsvägen och organisationen har ändrats. Kontrollera rätt portal före en övning så att en gammal kontaktväg inte upptäcks först under ett avbrott.

2.3 Leverantörer skapar olika slags exponering

En leverantör kan förvara en kopia av kunduppgifter, ha privilegierad supportåtkomst eller driva själva tjänsten. Dessa relationer kräver olika åtgärder. Ett stulet marknadsföringsutdrag visar inte åtkomst till ett betalningssystem. En tjänst kan stängas av som försiktighetsåtgärd även när eventuell informationsåtkomst är oklar.

Be varje kritisk leverantör ange juridisk person, tjänst, uppgiftskategorier, behörigheter och vilka belägg kunderna kan få. Kräv en kontaktväg för uppdateringar om omfattningen. Tidiga antal kan ändras när utredningen skiljer mellan poster, konton, kontakter och personer.

Fallbeskrivningarna i kapitel 5 behåller dessa skillnader. Överlappande kundgrupper summeras inte till ett svenskt totalantal drabbade personer. En utländsk leverantör kan påverka svenska användare utan att det innebär ett separat intrång hos den svenska kunden.

2.4 Politiska teman återges som källornas uppgifter

Påståenden som hänvisar till Natoanslutningen, Ryssland, Israel och Gaza, koranbränningar eller val kräver särskild försiktighet. Ett tema som en aktör nämner visar inte orsak, nationalitet, statlig styrning eller ett verifierat tekniskt resultat. Rapporten tar inte ställning till regeringsbeslut, partier, religion eller utrikespolitik.

Officiella attribueringar förblir den ansvariga myndighetens bedömning. Formuleringen blir inte författarnas egen attribuering för att flera medier upprepar den. Språk, en flagga eller ett alias räcker inte för att knyta en operatör till ett land.

En politisk kalender kan stödja beredskapsplanering när en källa dokumenterar ett relevant hot. Den motiverar inte att skapa en kampanj som saknar belägg eller tillskriva cyberaktivitet ett valresultat. Säkerhetsteam bör skydda konton och kontinuitet likvärdigt oavsett tillhörighet.

2.5 Ge varje tidsfrist en ansvarig

Cybersäkerhetslagen trädde i kraft den 15 januari 2026. Kraven för betydande incidenter skiljer sig från GDPR:s rapportering av personuppgiftsincidenter och finanssektorns Dora-rapportering. Kapitel 10 beskriver de olika tidsfristerna och ansvariga funktionerna. [S8][S10][S11]

Använd en gemensam incidentjournal för fakta men dokumentera rapporteringsbesluten separat. Anteckna tid för kännedom, tjänstepåverkan, berörda uppgifter, leverantörsbesked, säkerhet i bedömningen och nästa uppdatering. Juridik och dataskydd bedömer relevanta krav medan tekniska team säkrar belägg och begränsar verifierad åtkomst.

VIKTIGA SLUTSATSER

01

Återställ verksamhetens tjänst tillsammans med applikationen.

02

Använd aktuell myndighetsväg och behåll meddelandets ursprungliga datum.

03

Knyt politiska och statsanknutna bedömningar till källan och basera åtgärder på belägg.

KAPITEL 03

Nationell exponering: en utvald portfölj

03

DETTA KAPITEL BESVARAR

Vilka uppmätta skyddsobservationer behöver tillgångsägarna kontrollera?

192 av 250

utvalda domäner publicerade DMARC med reject eller quarantine

3.1 Underlagets avgränsning 15

3.2 E-postdomänpolicy per sektor 16

3.3 Övriga konfigurationsobservationer behåller sina nämnare 17

3.4 Aktuella annonser vägleder exponeringsbeslutet 17

3.5 Gör observationer till ansvariga beslut 20

KAPITEL 03

Nationell exponering: en utvald portfölj

I KORTHET

73 av 242 bedömda domäner hade inloggningsuppgifter till försäljning vid kontrollen. Den bedömda portföljens nationella Atlas-huvudvärde är 50/100; 8 utvalda domäner har okänd exponering. Konfigurationsobservationer gäller 250 domäner, varav 192 publicerar DMARC med reject eller quarantine. Signalerna är separata, inte bekräftade intrång eller nationell prevalens. Kontrollera aktuella konton, utred relevanta personalenheter och granska e-postkonfiguration med ansvariga ägare.

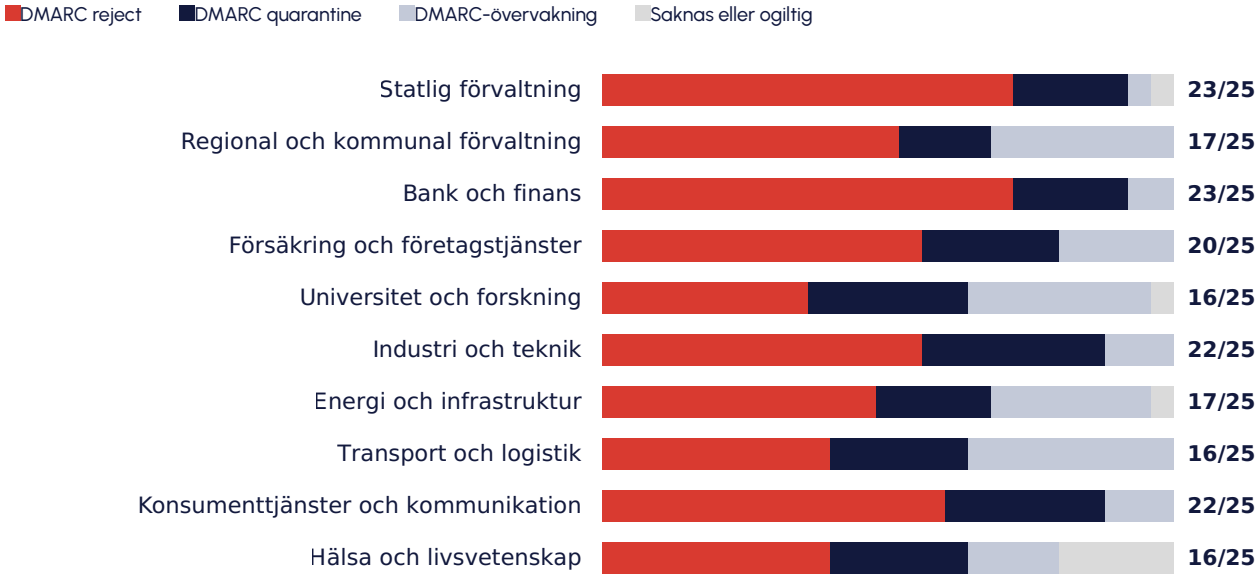
3.1 Underlagets avgränsning

Del	Omfattning
Urval	250 ändamålsenligt utvalda organisationer och kandidatdomäner; ingen omsättningsrankning eller nationell prevalensskattning
Sektorer	10 grupper med 25 utvalda poster vardera
Enhet	Domänobservation; juridiskt ägarskap och oberoende mellan organisationer är inte verifierade
Konfigurationsbild	22 november 2026; konfigurationsbild, inte ett års intrångsantal
Exponeringsdata	242 bedömda domäner; 8 utvalda domäner förblir okända; kumulativa enhets-, inloggnings- och dokumentkopplingar, aktuella annonser och liknande domännamn under 30 dagar [S4]
Tolkning	Saknad observation fastställer inte ett saknat skydd

Urvalet omfattar offentliga tjänster, finans, utbildning, industri, infrastruktur, transport och konsumenttjänster. Storleken gör det inte till ett slumpmässigt urval. Närliggande tjänster kan ha samma operatör; en domänkoppling fastställer inte en separat oberoende juridisk person. [S3]

3.2 E-postdomänpolicy per sektor

De flesta utvalda domäner publicerar tillämpande DMARC-policy, med skillnader mellan sektorer



Källa: konfigurationsobservationer för 250 utvalda domäner [S3]. Publicerade policyer fastställer inte lyckad meddelandeleverans eller förhindrade bedrägerier.

Sektor	Domäner	Reject eller quarantine	Övervakning	Saknad eller ogiltig
Statlig förvaltning	25	23	1	1
Regional och kommunal förvaltning	25	17	8	0
Bank och finans	25	23	2	0
Försäkring och företagstjänster	25	20	5	0
Universitet och forskning	25	16	8	1
Industri och teknik	25	22	3	0
Energi och infrastruktur	25	17	7	1
Transport och logistik	25	16	9	0
Konsumenttjänster och kommunikation	25	22	3	0
Hälsa och livsvetenskap	25	16	4	5
ALLA	250	192	50	8

Källa: Brandefense konfigurationsobservationer [S3]. Reject och quarantine omfattar tillsammans 192 av 250 domäner, eller 76,8 %. En publicerad policy visar inte att varje legitimt meddelande överensstämmer eller att varje mottagande tjänst tillämpar den. Inga exponeringsbetyg per sektor publiceras.

3.3 Övriga konfigurationsobservationer behåller sina nämnare

Observation	Antal	Begränsning
SPF-post finns	243 av 250	Förekomst visar inte korrekt avsändar-behörighet eller överensstämmelse
DKIM-relaterad post observerad	210 av 250	Utebliven observation visar inte att domänen saknar e-postsignering
DNSSEC-delegationspost finns	130 av 250	Fastställer inte fullständig kedjevalide-ring
TLS-certifikat kunde valideras	243 av 250	4 valideringsfel och 3 otillgängliga resul-tat behöver ägarens granskning
Domäner med tillgängliga HSTS-resultat	222 av 250	Resultat för övriga utvalda domäner är otillgängliga
HSTS observerat	178 av 222	Fastställer inte fullständig täckning eller skyddseffekt

Detta är konfigurationsobservationer, inte uppmätt skyddseffekt. Resultaten fastställer inte fullständig täckning av underdomäner, tjänster eller klientanslutningar. Utebliven observation fastställer inte en helårsexponering eller ett lyckat angrepp. [S3]

3.4 Aktuella annonser vägleder exponeringsbeslutet

73 av 242 bedömda domäner hade inloggningsuppgifter till försäljning vid kontrollen. Exponeringsobservationer finns för 242 av de 250 utvalda domänerna; övriga 8 förblir okända. Nationellt Atlas-huvudvärde för den bedömda portföljen är 50/100. Endast detta nationella värde publiceras. [S4]

Huvudvärdet stödjer prioritering inom den bedömda portföljen. Det är varken andelen drabbade eller sannolikhe-ten för framtida intrång. Sektortabeller visar uppmätta signalantal och bedömda nämnare, utan sektor- eller organisationsbetyg.

Sektor	Bedömda domäner	Domäner med inlogg-ningsuppgifter till försälj-ning	Domäner med personal-enhetskopplingar	Domäner med doku-mentkopplingar
Statlig förvaltning	24	5	9	16
Regional och kommu-nal förvaltning	25	2	24	23

Sektor	Bedömda domäner	Domäner med inloggningsuppgifter till försäljning	Domäner med personalenhetskopplingar	Domäner med dokumentkopplingar
Bank och finans	24	7	12	17
Försäkring och företagstjänster	22	4	10	13
Universitet och forskning	25	8	24	23
Industri och teknik	25	7	23	24
Energi och infrastruktur	24	4	11	9
Transport och logistik	24	12	11	9
Konsumenttjänster och kommunikation	25	19	22	20
Hälsa och livsvetenskap	24	5	20	12
Totalt	242	73	166	166

I `c03_exposure_signals.csv` räknar `orgs_listed_for_sale_now` bedömda domäner med inloggningsuppgifter till försäljning. Samma domänantal finns som `current_listing_domains` i `c04_sector_exposure.csv`. Inget av fälten fastställer oberoende organisationer eller organisationer som erbjuds till försäljning. [S4]

En aktuell annons registrerar ett erbjudande, inte genomförd försäljning, testad hemlighet eller bekräftat intrång. Kontrollera kontoägarskap, aktualitet, behörigheter, användning och tidigare åtgärder. Kund-, student- och personalkopplingar behöver olika ansvariga.

Enhets- och inloggningsantal nedan beskriver kumulativa kopplingar, inte incidenter under 2026. Personalvyn ingår i enhetsgruppen och får inte läggas till den. Poster kan överlappa mellan källor och domäner. [S4]

Enhets- och inloggningskopplingar kräver separat kontroll inom den bedömda portföljen



Enhetskopplingar, minst (anställdas delmängd inom parentes)



Kopplingar till inloggningsposter (separat skala)



Källa: Brandefense exponeringsobservationer för 242 bedömda domäner av 250 utvalda domäner [S4]. Kumulativa kopplingar kan överlappa; de är inte unika personer eller bekräftade intrång.

Sektor	Bedömda domäner	Enheter, minst	Personalenheter	Inloggningsposter
Statlig förvaltning	24	7 272	66	89 950
Regional och kommunal förvaltning	25	12 625	2 331	1 037 498
Bank och finans	24	10 673	108	145 637
Försäkring och företagstjänster	22	2 632	61	96 728
Universitet och forskning	25	10 359	2 484	915 857
Industri och teknik	25	33 120	3 697	1 523 898

Sektor	Bedömda domäner	Enheter, minst	Personalenheter	Inloggningsposter
Energi och infrastruktur	24	2 560	50	36 922
Transport och logistik	24	14 188	116	121 075
Konsumenttjänster och kommunikation	25	112 144	2 991	971 904
Hälsa och livsvetenskap	24	2 593	181	119 364
Totalt	242	208 166	12 085	5 058 833

Den bedömda portföljen innehåller minst 208 166 enhetskopplingar och 5 058 833 inloggningspostkopplingar. Detta är inte unika personer, bekräftat infekterade företagsägda enheter eller bevis för att organisationens egen infrastruktur lämnade materialet. Utred styrkta personalenheter och relevanta sessioner tillsammans.

Dokumentobservationerna är 2 885 över 166 bedömda domäner. En dokumentkoppling fastställer inte sekretess, olovligt förvärv eller angripåtkomst. Liknande domännamn omfattar 15 469 observationer över 183 domäner under föregående 30-dagarsvy. Likhet fastställer inte skadlig användning eller ägarskap. [S4]

Konfigurationsportföljen omfattar 250 domäner, medan exponeringen omfattar 242. Jämför endast observationer med deras angivna nämnare. Saknade exponeringsvärden är inte nollor och huvudvärdet är ingen nationell prevalensskattning.

En organisation som får ett relevant kontolarm bör kontrollera ägarskap, ålder, behörighet, aktuell användning och tidigare åtgärder. Vid giltig aktuell åtkomst, granska sessioner och autentiseringsändringar tillsammans med lösenord. Kund-, student- och personalkopplingar behöver rätt ansvarig; en domän ensam skiljer inte dessa personer åt.

Separat forskning som QiAnXin XLab publicerade den 17 juni beskrev minst 4 300 äldre routrar med AryStinger-infektion världen över. Forskarna placerade 6,40 % av de infekterade routrar som observerades i Sverige. Det är forskarens enhetsobservation, inte Brandefenses utvalda portfölj, ett antal svenska organisationer eller en nationell infektionsandel. Forskarna kunde inte kvantifiera NAS-varianten. Infrastrukturansvariga bör identifiera gatewayenheter utan stöd, granska relevanta tillverkarråd och utreda tecken på obehörig kontroll. Ingen namngiven svensk organisation eller operatörsattribuering fastställs här. [S78]

3.5 Gör observationer till ansvariga beslut

E-postansvariga bör kontrollera legitima avsändare innan policy ändras. Testa överensstämmelse för viktiga tjänster och behåll undantag med ägare och slutdatum. Infrastrukturteam bör utreda misslyckad certifikatvalidering och bekräfta avsedd anslutningspunkt före rättning.

Skilj konfigurationsgranskning från incidentbeslut. En saknad post motiverar kontroll av den egna tjänsten, inte slutsatsen att information har stulits. Dokumentera resultat, åtgärd och nästa kontroll för varje verifierat fynd.

VIKTIGA SLUTSATSER

01

Nämnaren för domänurvalet är 250, inte alla svenska organisationer.

02

Konfigurationsobservationer beskriver synlig konfiguration, inte angreppsutfall.

03

Aktuella annonser, enheter och dokument kräver separat kontroll; saknad exponering förblir okänd.

KAPITEL 04

Observationer i kriminella miljöer och påståendefall

04

DETTA KAPITEL BESVARAR

Vad visar bevarade annonser om uppgifter med svensk anknytning?

7

påståendefall med autentiska maskerade utdrag

4.1 Underlagets avgränsning 23

Observerad publiceringsvolym per månad 24

Publiceringskanaler och språk 25

4.2 Sju påståenden och besluten de stödjer 26

4.3 Äldre material och vidareförmedlade påståenden 34

4.4 Senaste aktivitet och analysens gränser 35

4.5 Ytterligare bevarade påståenden 35

KAPITEL 04

Observationer i kriminella miljöer och påståendefall

I KORTHET

Materialet innehåller erbjudanden om inloggningsuppgifter, efterfrågan på identitets- och fordonsdata, annonserade verksamhetsuppgifter och återpublicerade äldre påståenden. Sju fall visar olika åtgärdsfrågor. Nya exempel gäller publicering, inte bevis för nyss stulna uppgifter. En svensk etikett fastställer inte ursprung eller bosättning. Kontrollera relevanta påståenden mot egna konton och uppgifter innan en incident fastställs eller ingripande åtgärder rekommenderas.

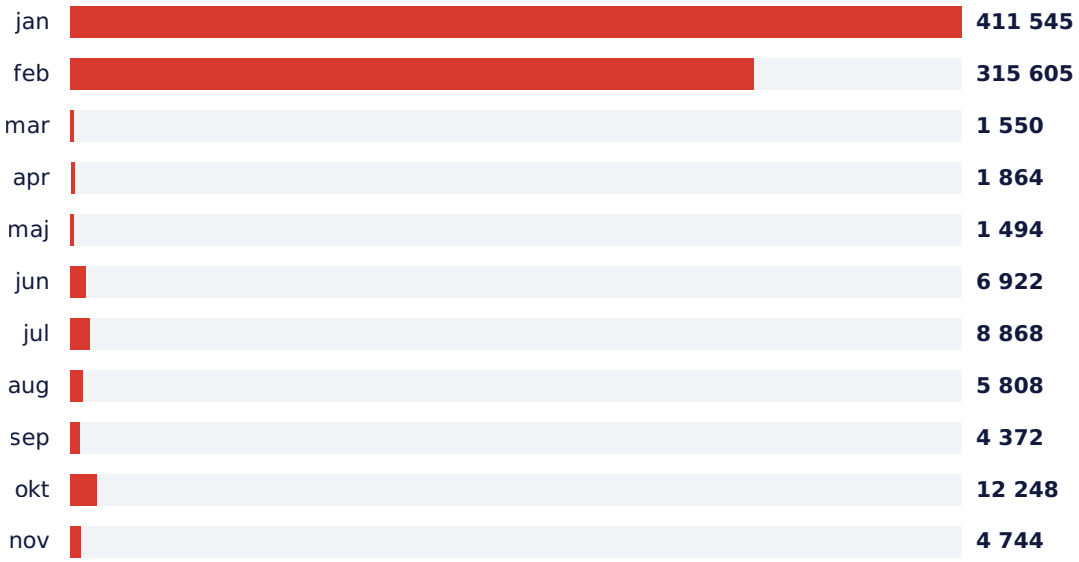
4.1 Underlagets avgränsning

Del	Omfattning
Period	1 januari–22 november 2026, efter inläggets tid
Bevarat material	49 045 olika inlägg i rapportens underlag
Sverige-märkt forummaterial	484 bevarade inlägg; inte alla är kriminella erbjudanden eller verifierade svenska incidenter
Nytt landanknutet material	3 018 bevarade inlägg daterade 8–22 november; överlappar materialet ovan
Nytt Sverige-märkt forummaterial	42 inlägg inom den senaste gruppen
Illustrationer	Autentiska citat med offeridentifierare och kontaktuppgifter borttagna
Begränsningar	Landanknytning, aktualitet, giltighet, innehav och genomförda affärer fastställs inte av annonser

Källa: Odin by Brandefense [S1]. Det bevarade materialet och den bredare observerade publiceringen är olika enheter. Saknat material fastställer inte frånvaro av aktivitet. Rapporten skattar ingen nationell förekomst av brottstyper från de illustrerade fallen.

Observerad publiceringsvolym per månad

Januari och februari står för de flesta observerade landanknutna inläggen



Källa: Brandefense Blackhole, observerade Sverige-anknutna inlägg, 1 januari–22 november 2026; november är ofullständig [S1]. Inlägg är inte bekräftade incidenter; språkkopplingar kan överlappa.

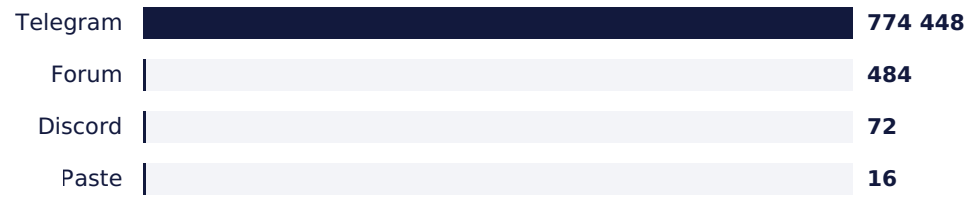
Månad	Inlägg	Månad	Inlägg
Januari	411 545	Juli	8 868
Februari	315 605	Augusti	5 808
Mars	1 550	September	4 372
April	1 864	Oktober	12 248
Maj	1 494	November till slutdatum	4 744
Juni	6 922	Totalt	775 020

Januari och februari står för 727 150 inlägg, eller 93,8 %. Marknadsföring och upprepad annonsering kan dominera landanknuten volym. Detta visar inte en motsvarande intrångstopp eller en jämförbar månadsvis hottrend. [S1]

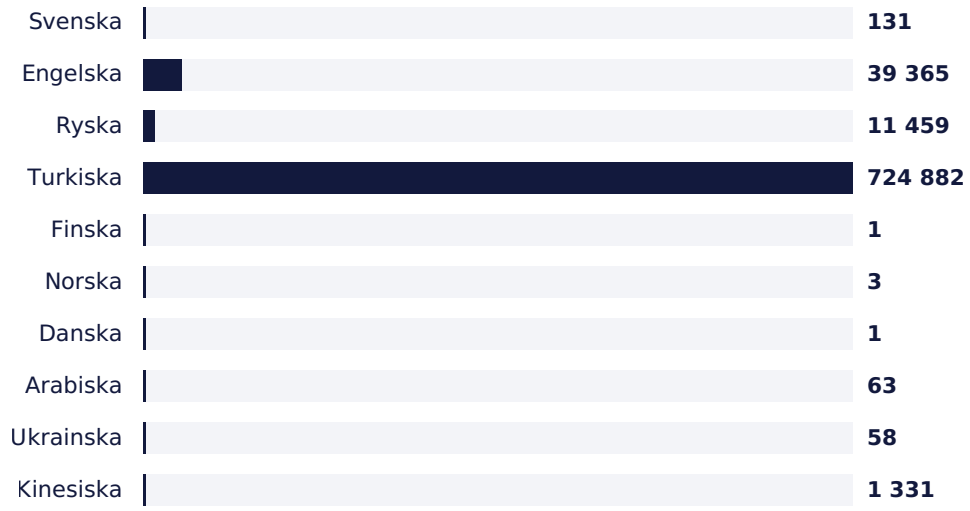
Publiceringskanaler och språk

Publiceringskanaler och språkkopplingar beskriver synlighet, inte angreppsprevalens

Plattform



Språk



Källa: Brandefense Blackhole, observerade Sverige-anknutna inlägg, 1 januari–22 november 2026; november är ofullständig [S1]. Inlägg är inte bekräftade incidenter; språkkopplingar kan överlappa.

Kanal	Anknytna inlägg
Telegram	774 448
Forum	484
Discord	72
Paste	16

Språkanknytning	Inlägg
Svenska	131
Engelska	39 365
Ryska	11 459

Språkanknytning	Inlägg
Turkiska	724 882
Finska	1
Norska	3
Danska	1
Arabiska	63
Ukrainska	58
Kinesiska	1 331

De flesta språkanknytningar är turkiska (724 882 inlägg); detta beskriver publiceringens synlighet och fastställer inte svenska måltavlor, ursprung eller aktörers nationalitet. [S1]

Språkanknytningar kan överlappa och kanalantal beskriver publiceringar, inte angrepp eller unika operatörer. Landanknytning fastställer inte målval, hemvist eller ursprung. Koncentrationen i januari–februari förblir en observation om publiceringsvolym. [S1]

4.2 Sju påståenden och besluten de stödjer

A

FALL A

Landmärkta inloggningsuppgifter, även ett novembererbjudande

Påstående obekräftat

Underlagskort B01 | 30 jan 2026 | Forumtråd | Information över sektorsgränser

PÅSTÅENDE	En annons den 30 januari beskriver en Sverige-märkt samling med e-post och lösenord på 17 K++ rader. Ett inlägg den 19 november erbjuder 30 K++ rader med liknande språk. Antal och aktualitet är säljarnas påståenden. [S1]
BEGRÄNSNING OCH ALTERNATIV	Inläggen visar annonsering, inte fungerande uppgifter, unika konton eller två skilda stulna datamängder. Liknande formuleringar verifierar inte samma fil, gemensam operatör eller senare insamlingsdatum.
ÅTGÄRD	Kontrollera ett eget konto mot aktuellt läge, inloggningar och tidigare åtgärder. Om aktuell användning bekräftas, hantera relevanta sessioner och autentiseringsmetoder tillsammans med lösenord. Dra ingen nationell återställningsslutsats från annonserade radantal.

Slutsats

Kontrollera ett eget konto mot aktuellt läge, inloggningar och tidigare åtgärder.

Underlagskort B01 30 jan 2026

Publicerare (alias utelämnat) Forumtråd Forum Engelska

ORIGINALTEXT

Database : Sweden Type : Email , Password Condition: Fresh,HQ Combo: 17 K++ Line

ÖVERSÄTTNING

Databas: Sverige. Typ: e-post, lösenord. Skick: aktuell, hög kvalitet. Kombination: 17 K++ rader.

Anmärkning. Ordet "fresh" är annonsörens beskrivning. Publiceringen visar inte när uppgifterna samlades in.

Fastställt
En Sverige-märkt samling med e-post och lösenord annonseras som 17 K++ rader.

Inte fastställt
Äkthet, unika konton, lösenordens giltighet, insamlingsdatum, ursprung eller genomförd överföring.

Underlagskort B07 19 nov 2026

Publicerare (alias utelämnat) Forumtråd Forum Engelska

ORIGINALTEXT

Database : Sweden Type : Email , Password Condition: Fresh,HQ Combo: 30 K++ Line

ÖVERSÄTTNING

Databas: Sverige. Typ: e-post, lösenord. Skick: aktuell, hög kvalitet. Kombination: 30 K++ rader.

Anmärkning. En ny annons kan innehålla äldre material. Inläggsdatum och påstått insamlingsdatum skiljer sig.

Fastställt
En annons den 19 november hävdar en Sverige-märkt e-post- och lösenordssamling på 30 K++ rader.

Inte fastställt
Ny insamling, fungerande lösenord, unika personer, ursprung, överlapp eller genomförd överföring.

B

FALL B

Efterfrågan på svenska personnummer

Underlagskort B02 | 15 feb 2026 | Forumtråd | Information över sektorsgränser

Påstående obekräftat

PÅSTÅENDE	Ett foruminlägg den 15 februari efterfrågar en svensk databas med personnummer. Det är en begäran om att skaffa information, inte ett påstående om att beställaren redan har den. [S1]
BEGRÄNSNING OCH ALTERNATIV	Inget köp, ingen stöld, drabbad grupp eller källorganisation fastställs. En begäran om personnummer visar inte åtkomst till ett offentligt register eller förmåga att autentisera sig som någon annan.
ÅTGÄRD	Testa kundstöd och kontoåterställning mot personer som känner till verkliga identitetsuppgifter. Behandla dem som sammanhang, inte som tillräcklig behörighet för utlämning eller betydelsefulla ändringar.

Slutsats

Testa kundstöd och kontoåterställning mot personer som känner till verkliga identitetsuppgifter.

Underlagskort B02 15 feb 2026

Publicerare (alias utelämnat) Forumtråd Forum Engelska

ORIGINALTEXT

Looking for any type of database from Sweden that includes Swedish personnummer / personal ID number / Social security number.

ÖVERSÄTTNING

Söker valfri databas från Sverige med svenska personnummer eller motsvarande identitetsnummer.

Anmärkning. Detta är efterfrågan, inte ett genomfört köp eller ett besked om datastöld.

Fastställt

En köpare efterfrågar svenska personnummer och nämner tidigare annonserade datamängder.

Inte fastställt

Förvärv, databasåtkomst, antal berörda personer, ursprung eller nytt intrång.

FALL C

C

En infostealeretikett och ett geografiskt påstående

Underlagskort B04 | 23 apr 2026 | Forumtråd | Information över sektorsgränser

Påstående obekräftat

PÅSTÅENDE	En aprilannons märker en datamängd som Vidar Stealer-material och anger SE som källgeografi. Inloggnings- och autofyllnadsuppgifter erbjuds. Malware- och geografietiketterna är publicerarens påståenden. [S1]
BEGRÄNSNING OCH ALTERNATIV	Det bevarade inlägget verifierar inte malwarefamilj, enhetsägarskap, insamlingsdatum, fungerande sessioner eller ett intrång hos en svensk organisation. Påstådd enhetsplats avgör inte tjänstens nationalitet.
ÅTGÄRD	Om ett behörigt larm matchar en egen klient eller ett konto, utred enheten och dess inloggningsuppgifter tillsammans. Granska sessionsexponering och tidigare begränsning innan beslut om byte av hemligheter.

Slutsats

Om ett behörigt larm matchar en egen klient eller ett konto, utred enheten och dess inloggningsuppgifter tillsammans.

Underlagskort B04 — 23 apr 2026

Publicerare (alias utelämnat) | Forumtråd | Forum | Engelska

ORIGINALTEXT

Malware Family . Vidar Stealer [...] Source Geo ..... SE [...] Credentials .... Yes [...] Autofill Data .. Yes

ÖVERSÄTTNING

Malwarefamilj: Vidar Stealer [...] Källgeografi: SE [...] Inloggningsuppgifter: ja [...] Autofyllnadsuppgifter: ja.

Anmärkning. Detta är publicerarens etiketter. Enhetsgeografi och tjänstens nationalitet är olika slutsatser.

Fastställt

Ett foruminlägg märker annonserat infostealermaterial som Vidar och anger SE som geografi.

Inte fastställt

Malwarefamilj, enhetsägarskap, insamlingsdatum, fungerande uppgifter, sessionsåtkomst eller användning mot svensk organisation.

FALL D

D

Kund- och fakturauppgifter inom fordonsservice

Underlagskort B05 | 5 sep 2026 | Forumtråd | Information över sektorsgränser

Påstående obekräftat

PÅSTÅENDE	Ett septembererbjudande beskriver en svensk fordonsservicedatabas med kund-, order-, faktura- och förvaringsuppgifter. Kategorierna ger verksamhetssammanhang som kan göra en senare förfrågan trovärdig. Annonsen ensam visar inte sådan användning. [S1]
BEGRÄNSNING OCH ALTERNATIV	Ursprung, äkthet, åtkomst till källsystem och kundantal är obekräftade. En leverantörskopia, ett äldre utdrag eller vilseledande beskrivning kan ge liknande annonsering. Ingen genomförd försäljning fastställs.
ÅTGÄRD	Kontrollera relevanta larm med uppgiftsägaren. Verifiera ändrat fakturakonto och hämtnings- eller leveransbegäran genom en känd kanal. Låt inte kunskap om en riktig order ersätta identitetskontroll.

Slutsats

Kontrollera relevanta larm med uppgiftsägaren.

Underlagskort B05 5 sep 2026

Publicerare (alias utelämnat) Forumtråd Forum Engelska

ORIGINALTEXT

Swedish tire and rubber-repair shop database [...] Customer, order, invoice, and tire storage data

ÖVERSÄTTNING

Svensk databas för [fordonsservice] [...] Kund-, order-, faktura- och förvaringsuppgifter.

Anmärkning. Organisationsnamn, platser, exempelposter och systemidentifierare är utelämnade.

Fastställt
Ett inlägg erbjuder påstådda fordonsserviceuppgifter med länkade kund- och verksamhetsposter.

Inte fastställt
Ursprung, behörighet, äkthet, kundantal, åtkomst till källsystem eller genomförd affär.

E

FALL E

Ny efterfrågan på fordonsuppgifter

Underlagskort B06 | 18 nov 2026 | Forumtråd | Information över sektorsgränser

Påstående obekräftat

PÅSTÅENDE	En forumförfrågan den 18 november söker fordonsdatabasuppgifter via VIN. Originalet nämner en tillverkare och en annan datatjänst. Namnen utelämnas eftersom förfrågan inte fastställer en incident hos någon av dem. [S1]
BEGRÄNSNING OCH ALTERNATIV	Förfrågan visar intresse. Den visar inte tillgänglighet, innehav, åtkomst, säljarrespons eller köp. Fordonsuppgifter kan också komma från legitima offentliga, kommersiella eller äldre källor.
ÅTGÄRD	En tillgångsägare bör kontrollera faktiska kategorier och tjänstebehörigheter om ett relevant larm uppstår. Bedrägeriteam bör bedöma den konkreta transaktionen i riskzonen i stället för att förklara tillverkarintrång utifrån en köpförfrågan.

Slutsats

En tillgångsägare bör kontrollera faktiska kategorier och tjänstebehörigheter om ett relevant larm uppstår.

Underlagskort B06 18 nov 2026

Publicerare (alias utelämnat) Forumtråd Forum Engelska

ORIGINALTEXT

[…] WIll buy db for [vehicle manufacturer] and [vehicle database] vehicle data per VIN […]

ÖVERSÄTTNING

[…] Vill köpa databas för [fordonstillverkare] och [fordonsdatabas] med uppgifter per VIN […]

Anmärkning. En förfrågan visar informationsintresse, inte att informationen är tillgänglig.

Fastställt
En forumförfrågan söker fordonsrelaterat databasmaterial den 18 november.

Inte fastställt
Innehav, säljarrespons, databasåtkomst, genomfört köp eller ny tillverkarincident.

FALL F

F

Nya Sverige-märkta identitetsuppgifter

Underlagskort B13 | 17 nov 2026 | Forumtråd | Information över sektorsgränser

Påstående obekräftat

PÅSTÅENDE	En forumannons den 17 november erbjuder kontaktuppgifter som beskrivs som aktuella för Sverige och andra länder, med ett påstått totalantal på 200k. Fälten omfattar namn, personnummer, adresser och kontaktuppgifter. [S1]
BEGRÄNSNING OCH ALTERNATIV	Det annonserade totalantalet är inte ett verifierat antal svenska personer. Inlägget fastställer inte aktualitet, äkthet, källorganisation, lagligt ursprung, genomförd affär eller samband med något nytt företagsbesked.
ÅTGÄRD	Förbered kundstödet på förfrågningar med rimliga persondetaljer. Kontrollera relevanta datalarm mot behöriga register och tidigare besked. Anpassa åtgärden till kategorier och faktiskt belagd användning.

Slutsats

Förbered kundstödet på förfrågningar med rimliga persondetaljer.

Underlagskort B13 17 nov 2026

Publicerare (alias utelämnat) Forumtråd Forum Engelska

ORIGINALTEXT

Selling fresh leads for Sweden and other countries. Total count 200k. [...] Person Nr [...] Source: Financial company.

ÖVERSÄTTNING

Säljer aktuella kontakter för Sverige och andra länder. Totalt 200k. [...] Personnummer [...] Källa: finansföretag.

Anmärkning. Finansföretagsursprunget är säljarens påstående. Exempelposter och personidentifierare är utelämnade.

Fastställt

En säljare den 17 november annonserar 200k kontaktposter för Sverige och andra länder med personnummer och kontaktfält.

Inte fastställt

Unika personer, aktualitet, fungerande kontakter, ursprung, samtycke, finansföretagsrelation eller genomförd affär.

FALL U

U

Annonserad åtkomst till finansiella tjänster

Underlagskort B16 | 14 apr 2026 | Forumtråd | Finansiella tjänster

Påstående obekräftat

PÅSTÅENDE	Ett foruminlägg daterat den 14 april annonserar två åtkomster till svenska finansiella verksamheter: fjärrövervakning och fjärradministration (RMM) med påstådd behörighet som enterprise-administratör samt SSH-fjärrinloggning med påstådd behörighet som domänanvändare. Det är säljarens beskrivningar av förmågan. [S1]
BEGRÄNSNING OCH ALTERNATIV	Inlägget verifierar ingen åtkomstväg, behörighet, aktuell användbarhet eller målidentitet. Det fastställer inte banktillstånd, två skilda organisationer, genomförd affär, datastöld eller utplacerad utpressningsprogramvara. Erbjudandena kan överlappa eller felbeskriva den underliggande tillgången.
ÅTGÄRD	Om ett behörigt larm kan kopplas till egen infrastruktur bör fjärråtkomstens ansvariga och SOC granska kontobehörigheter, godkända administrationsverktyg och autentiseringshistorik. Bevara underlaget, återkalla obehöriga sessioner och inloggningsuppgifter samt kontrollera kvarvarande åtkomst innan larmet avslutas. En allmän sektorsetikett eller säljarens behörighetspåstående räcker inte för att fastställa intrång hos ett institut.

Slutsats

Kontrollera egna fjärråtkomstvägar, behörigheter och sessioner innan intrång fastställs.

Underlagskort B16 14 apr 2026

Forumskribent (alias utelämnat) Forumtråd Forum Engelska

ORIGINALTEXT

[RMM (vendor redacted)] Financial Services - Sweden ([revenue redacted]) […] Privilege ..... Enterprise Admin […] [SSH] Financial Services - Sweden ([revenue redacted]) […] Privilege ..... Domain User […]

ÖVERSÄTTNING

[RMM (leverantör utelämnad)] Finansiella tjänster – Sverige ([omsättning utelämnad]) […] Behörighet ..... Enterprise Admin […] [SSH] Finansiella tjänster – Sverige ([omsättning utelämnad]) […] Behörighet ..... Domain User […]

Anmärkning. Erbjudandena kan överlappa. Publiceringen fastställer inte utnyttjande, datastöld eller utplacerad utpressningsprogramvara; identifierande leverantörs- och omsättningsuppgifter utelämnas.

Fastställt
Ett inlägg annonserar två åtkomster till svenska finansiella verksamheter, via RMM med påstådd behörighet som enterprise-administratör och SSH med påstådd behörighet som domänanvändare.

Inte fastställt
Verifierad åtkomst, behörighet, användbarhet, målidentitet, banktillstånd, två skilda organisationer eller genomförd affär.

4.3 Äldre material och vidareförmedlade påståenden

Underlagskort B09 — 8 apr 2026

Publicerare (alias utelämnat) | Forumtråd | Forum | Engelska

ORIGINALTEXT

Source Code [software supplier] Data Breach [...] in November, 2025

ÖVERSÄTTNING

Källkod från [programvaruleverantör], påstått dataintrång [...] i november 2025.

Anmärkning. Publiceringen gäller 2026; den påstådda bakomliggande händelsen gäller 2025.

Fastställt
Ett aprilinlägg upprepar ett källkodspåstående som det daterar till november 2025.

Inte fastställt
Nytt intrång 2026, kodens äkthet, källsystemsåtkomst eller verifierad attribuering.

Underlagskort B11 — 8 mar 2026

Publicerare (alias utelämnat) | Forumtråd | Forum | Engelska

ORIGINALTEXT

[...] [the supplier] [...] was the victim of a ransomware attack.

ÖVERSÄTTNING

[...] [leverantören] [...] utsattes för ett ransomwareangrepp.

Anmärkning. Det citerade påståendet är publicerarens uppgift. Offentlig bekräftelse behöver fastställas separat.

Fastställt
Ett inlägg citerar en tråd om en tidigare leverantörsincident och annonserade uppgifter.

Inte fastställt
Nytt intrång 2026, påstått personantal, filidentitet, aktualitet eller aktuell åtkomst.

Underlagskort B10 — 30 apr 2026

Publicerare (alias utelämnat) | Vidareförmedlat foruminlägg | Forum | Engelska

ORIGINALTEXT

The attackers claim they have access to the company's source code, cloud infrastructure, and various keys.

ÖVERSÄTTNING

Angriparna påstår att de har åtkomst till företagets källkod, molninfrastruktur och olika nycklar.

Anmärkning. Vidareförmedling är inte oberoende bekräftelse av ursprungspåståendet.

Fastställt
Ett aprilinlägg vidareförmedlar påståenden om källkod, personaluppgifter och molnmaterial hos en läkemedelsorganisation.

Inte fastställt
Aktuell åtkomst, giltiga nycklar, ursprung, fullständighet, attribuering eller effekt på drift eller patientdata.

B09 daterar sin påstådda programvaruhändelse till november 2025. B11 citerar ett leverantörsförlopp från ett tidigare år. Båda inläggen hör till rapportens publiceringsperiod; inget fastställer ett nytt intrång 2026. Offentliga tillsynsbeslut om äldre incidenter förblir en separat källgrupp.

B10 är ett vidareförmedlat foruminlägg med påståenden om läkemedelsrelaterad källkod och molnmaterial. Upprepning är inte oberoende verifiering. Rapporten verifierar inte nycklar, aktuell åtkomst, personalantal eller patientdataeffekter från detta inlägg. [S1]

4.4 Senaste aktivitet och analysens gränser

Kontaktuppgiftsannonsen den 17 november, fordonsförfrågan den 18 november och inloggningserbjudandet den 19 november är nya publiceringar med olika betydelse. En begäran är efterfrågan; ett erbjudande hävdar tillgänglighet. Inget fastställer genomförd överföring eller insamlingsdatum.

En annons den 9 november om internationella mäklarkontakter omfattar också Sverige. Den fastställer inte intrång i ett svenskt finansinstitut eller verifierade saldon. Kapitel 9 skiljer kontaktlistor från åtkomst till banksystem och kundkonton. [S1]

Underlagskort B14 — 9 nov 2026

Publicerare (alias utelämnat) | Forumtråd | Forum | Engelska

ORIGINALTEXT

Quantity : (38K) Country: MIXED TIER-1/2/3 (Sweden, Norway, Netherlands etc.)

ÖVERSÄTTNING

Antal: (38K). Land: blandade marknader (Sverige, Norge, Nederländerna med flera).

Anmärkning. Totalantalet gäller en blandad internationell lista, inte 38K svenska personer.

Fastställt
Ett inlägg den 9 november erbjuder 38K mäklaranknutna kontakter i flera länder, däribland Sverige.

Inte fastställt
Svensk andel, källrelationer, unika personer, aktuella saldon, giltiga insättningar eller genomförd överföring.

Exemplen visar åtgärdsskillnader, inte ett mått på hur ofta påståenden lyckas. Liknande formuleringar fastställer inte filidentitet, gemensam operatör eller en kriminell affärskedja. Saknat eller oklart material förblir en täckningsbegränsning, inte ett konstaterande att ingen incident skett.

4.5 Ytterligare bevarade påståenden

Ett inlägg från årets början erbjuder en detaljhandels- och e-handelsdatabas; senare trådaktivitet upprepar erbjudandet. Publicering och senare diskussion fastställer inte nya stölder, fungerande kundkonton eller genomförd affär. Uppgiftsägarskap, aktualitet och eventuella tidigare besked behöver kontrolleras separat. [S1]

Andra bevarade erbjudanden beskriver Sverige-märkta inloggningslistor, förenings- eller verksamhetsdatabaser, kontakter till finansiella insättare och identitetshandlingar. Vissa hävdar stora lager eller upprepar äldre citat. De annonserade totalerna kan inte summeras till ett antal svenska personer. Inget av erbjudandena ger oberoende belägg för källorganisation, insamlingsdatum eller aktuell användbarhet. Svar som begär en ny länk eller berömmer en säljare bekräftar inte grundpåståendet. [S1]

En separat tråd pekar på en påstådd datamängd inom industriautomation. En annan annonserar uppgifter om företagsbeslutsfattare med ett påstått ursprung hos ett annat företag. En hänvisning, ett leverantörsnamn eller ett känt kundnamn verifierar inte innehav av uppgifter eller intrång hos en namngiven verksamhet. [S1]

VIKTIGA SLUTSATSER

01

En annons verifierar publicering, inte den annonserade tillgången.

02

Förfrågningar, erbjudanden, vidareförmedling och äldre inlägg kräver olika tolkning.

03

Nya inläggsdatum fastställer inte ny stöld eller samband med nya företagsbesked.

KAPITEL 05

Incidenter och besked per sektor

05

DETTA KAPITEL BESVARAR

Vad fastställde organisationer och myndigheter, och vad innebär det för tjänsteägaren?

15

fallbeskrivningar; grupperna överlappar och ska inte summeras

5.1 Läs tidslinjen före rubriken 38

5.2 Daterade fallbeskrivningar 39

5.3 Övriga händelser behåller sin underlagstyp 47

5.4 Senaste aktivitet: 8–22 november 2026 47

5.5 Sårbarhetsråd är inget incidentantal 48

KAPITEL 05

Incidenter och besked per sektor

I KORTHET

Fallen skiljer mellan e-poståtkomst, leverantörslagrade uppgifter, driftstörning och ändrad omfattning. Skillnaden mellan händelsedatum och offentligt besked behålls. Femton fall illustrerar beslut; de är inget nationellt incidentantal. Den senaste aktivitetsperioden, 8–22 november, omfattar kundbesked och leverantörshändelser. Använd varje falls fastställda fakta för att välja åtgärd och kontrollera sedan motsvarande beroende i den egna tjänsten.

5.1 Läs tidslinjen före rubriken

Ett novemberbesked kan beskriva en leverantörshändelse i oktober eller äldre bokningar. Flera personuppgiftsansvariga kan anmäla samma leverantörshändelse. Två e-posthändelser inom en sektor kan däremot vara separata tills tekniska belägg visar ett samband. Fallen nedan behåller dessa enheter.

Sektor	Observerad följd	Första ansvariga funktion
Vård	Åtkomst till personalens e-post och vidareförmedlat nätfiske	Identitet, dataskydd och vårdledning
Utbildning	Informationsstöld i gemensam plattform och försiktighetsbegränsningar	Plattformägare och dataskyddsombud
Kommunal verksamhet	Avbruten IT och senare fynd om personaluppgifter	Incidentledare och tjänsteägare
Detaljhandel och besöksverksamhet	Kontaktuppgifter och risk för trovärdiga bedrägerier	Kundverksamhet och dataskydd
Transport	Boknings-, rese- och kontouppgifter hos leverantörer	Leverantörsansvarig och resenärsstöd
Tillverkning och fastighetsdrift	Produktionsstopp eller problem med uppkopplad styrning	Teknik, säkerhet och kontinuitet

5.2 Daterade fallbeskrivningar

FALL G

G

Regionala vårdmyndighetens e-postkonton

Vård

Marsbesked: aktivitet över två år

FASTSTÄLLD REDOGÖRELSE	Den 5 mars meddelade Region Värmland att inloggningsuppgifter för 99 medarbetares e-postkonton berördes. E-post hade lästs i 44 konton minst en gång mellan oktober 2025 och februari 2026. Åtkomsten stängdes. [S18][S53]
BEGRÄNSNING	Antalen gäller medarbetares e-postkonton, inte patienter, meddelanden eller separata intrång. Perioden överlappar föregående år. Beskedet fastställde inte åtkomst till andra system.
ÅTGÄRD	Granska inloggningar, delegerade rättigheter, vidarebefordran och aktiva sessioner för verifierat berörda konton. Bedöm personuppgifter i varje e-postkonto separat. Ett lösenordsbyte visar inte ensamt att all åtkomst har upphört.

Slutsats

Granska inloggningar, delegerade rättigheter, vidarebefordran och aktiva sessioner för verifierat berörda konton.

FALL H

H

En IT-leverantör skiljer berörda miljöer åt

Teknikleverantörer

Företagets uppgifter återgivna av pressen

FASTSTÄLLD REDOGÖRELSE	Enligt rapporteringen beskrev en IT-leverantör åtkomst till system utanför produktion. Den angav att det saknades indikationer på påverkan på produktionsmiljöer eller kundtjänster. [S54]
BEGRÄNSNING	Företagets ursprungliga incidentbesked är inte tillgängligt för närvarande. Rapporten bygger därför på källbundet återgivna uppgifter och utelämnar leverantörens namn.
ÅTGÄRD	Fråga vilken miljö, uppgiftskopia och inloggningsuppgift som berördes. Granska separationen mellan utvecklingshemligheter och produktionsåtkomst. Dra inte slutsatsen att en kund har drabbats för att en applikation nämns i leverantörsmaterial.

Slutsats

Fråga vilken miljö, uppgiftskopia och inloggningsuppgift som berördes.

FALL I

I ■ Kommunal IT och kontinuitet

Kommunal verksamhet

Officiella störningsbesked

FASTSTÄLLD REDOGÖRELSE	Ett kommunalt besked beskrev ett IT-angrepp, begränsad IT-åtkomst och krisorganisation samt varnade för möjlig personuppgiftsläcka. [S20][S56]
BEGRÄNSNING	Beskeden fastställer inte hela omfattningen av berörda tjänster eller uppgifter.
ÅTGÄRD	Identifiera beroenden för identitet, anslutning och drift. Öva en minsta medborgarservice utan ordinarie IT och behåll varje personuppgiftsansvarigs riskbedömning.

Slutsats

Identifiera beroenden för identitet, anslutning och drift.

FALL J

J ■ Lärplattformens datastöld och flera anmälningar

Högre utbildning

Leverantörshändelse; kundernas hantering

FASTSTÄLLD REDOGÖRELSE	IMY uppgav att 51 personuppgiftsincidenter kopplade till Canvas hade anmälts den 8 maj. CERT-SE beskrev plattformsleverantörens bekräftelse av informationsstöld och tillfälliga åtkomstbegränsningar vid svenska lärosäten. [S21][S57][S69][S77]
BEGRÄNSNING	51 är antalet inkomna anmälningar vid den tidpunkten. Det är inte 51 separata leverantörsintrång, ett slutligt lärosätesantal eller antalet berörda studenter. Aktörens globala uppgift ersätter inte myndighetens måttenhet.
ÅTGÄRD	Kartlägg lärosätets faktiska uppgiftskategorier och kundmiljö. Öva undervisning, examination och studentinformation under en försiktighetsbegränsning. Återöppning bör bedöma både tjänstedrift och den fortsatta dataskyddsutredningen.

Slutsats

Kartlägg lärosätets faktiska uppgiftskategorier och kundmiljö.

FALL K

K ■ Ryde-konton i fyra länder

Transporttjänster

Bekräftad omfattning; landfördelning okänd

FASTSTÄLLD REDOGÖRELSE	Ryde uppgav att ett intrång upptäcktes den 2 augusti och stoppades kort därefter. Beskedet beskrev kontaktuppgifter, födelsedatum, delar av kortuppgifter och betalningshistorik. Enligt rapporteringen fördelades 4,5 miljoner konton över Sverige, Norge, Finland och Tyskland. [S22][S60]
BEGRÄNSNING	Totalen är inte antalet drabbade personer i Sverige. Företaget undantog fullständiga kortnummer och resornas platshistorik. Delvisa betalningsuppgifter visar inte användbara kortuppgifter eller bedrägliga transaktioner.
ÅTGÄRD	Varna kunder för meddelanden som använder verkliga konto- eller betalningsdetaljer. Kontrollera vilka uppgifter som faktiskt röjts innan kort- eller kontoåtgärder rekommenderas. Låt landfördelningen vara okänd tills den ansvarige anger den.

Slutsats

Varna kunder för meddelanden som använder verkliga konto- eller betalningsdetaljer.

FALL L

L ■ En IT-leverantörs interna system och kontrollerade återöppning

Teknikleveranskedja

Officiellt incident- och återställningsbesked

FASTSTÄLLD REDOGÖRELSE	Leverantörens incidentinformation beskriver obehörig åtkomst till interna IT-system, en tillfällig nedstängning och stegvis återöppning. [S23][S61]
BEGRÄNSNING	Återställda tjänster visar inte att varje kunddatabedömning eller leverantörsrelation är färdigutredd.
ÅTGÄRD	Fråga leverantören om den tjänst och det konto organisationen faktiskt använder. Bestäm belägg för återöppning och kontaktväg för senare omfattningsändringar. Håll teknisk återställning och granskning av kunduppgifter som separata steg.

Slutsats

Fråga leverantören om den tjänst och det konto organisationen faktiskt använder.

FALL M

M Kommunala personaluppgifter och ändrad omfattning

Kommunal verksamhet

Officiella besked: ändrad omfattning

FASTSTÄLLD REDOGÖRELSE	En kommuns besked beskrev att känsliga personaluppgifter kopierats till en extern plats efter ett IT-intrång. [S24][S62]
BEGRÄNSNING	Uppgifternas ålder visar inte upprepade intrång.
ÅTGÄRD	Bedöm känsliga anställningsuppgifter särskilt. Identifiera berörda personer och behörigt stöd utan att återge detaljerna. Bevara tidslinjen för ändrad omfattning och bedöm information till registrerade separat från tjänsteåterställningen.

Slutsats

Bedöm känsliga anställningsuppgifter särskilt.

FALL N

N Lyko preciserar kundomfattningen

Detaljhandel

Händelse 12 november; besked 18 november

FASTSTÄLLD REDOGÖRELSE	Lykos formella besked den 18 november beskrev upptäckt den 12 november och begränsning inom en timme. Det angav 36 000 kunder i Sverige inom 60 000 på samtliga marknader. Orderinformation berördes för 95 kunder. [S28] [S65]
BEGRÄNSNING	Företaget undantog betalningsuppgifter, lösenord och personnummer och uppgav att driften inte påverkats. Tidigare medieantal läggs inte till den senare formella omfattningen. De 95 är inte en extra verifierad grupp unika personer.
ÅTGÄRD	Använd det aktuella beskedet från den ansvarige när kunder får råd. Namn och kontaktuppgifter kan stödja trovärdig imitation även när lösenord undantas. Kontrollera ovanliga kontoåterställningar och orderändringar genom en känd oberoende kanal.

Slutsats

Använd det aktuella beskedet från den ansvarige när kunder får råd.

FALL O

O ■ Cabonlines bokningsuppgifter hos en leverantör

Transport och serviceresor

Leverantörsåtkomst bekräftad; vidare spridning oklar

FASTSTÄLLD REDOGÖRELSE	Cabonlines novemberbesked beskrev obehörig åtkomst hos en extern bokningsleverantör. Vissa kontakt-, boknings-, hämtnings- och destinationsuppgifter samt betalningsrelaterad information kunde beröras. Företaget uppgav att åtkomstvägen stängts. [S29][S66][S70]
BEGRÄNSNING	Företaget skilde betalningsrelaterad information från åtkomst till bankkonton eller möjlighet att göra obehöriga betalningar. Möjlig vidare spridning utreddes; beskedet fastställde ingen genomförd spridning. Anta inget antal skyddade identiteter.
ÅTGÄRD	Bedöm reseuppgifter utifrån personlig säkerhet och nätfiske. Kundservice och ansvariga för serviceresor bör samordna en säker stödväg. Behåll faktiska uppgiftskategorier och leverantörens uppdateringar i stället för ett generellt påstående om betalningsrisk.

Slutsats

Bedöm reseuppgifter utifrån personlig säkerhet och nätfiske.

FALL P

P ■ Universeums besökare och en bokningsleverantör

Besöksverksamhet

Besked 20 november; händelse i slutet av oktober

FASTSTÄLLD REDOGÖRELSE	Universeums besked den 20 november beskrev ett angrepp i slutet av oktober mot bokningssystemets leverantör. Organisationen uppgav att en obehörig part kommit åt uppgifter om omkring 280 000 besökare, bland annat namn, e-postadresser, telefonnummer och födelsedatum. Personnummer och betalkortsuppgifter undantogs. [S30][S67]
BEGRÄNSNING	Beskedet angav att bokningar och årskort fortsatt gällde och att ingen bedräglig användning var känd vid publiceringen. Detta är ett nytt besked om en tidigare händelse. Det kopplas inte till ett annat Göteborgsfall enbart genom plats eller tid.
ÅTGÄRD	Förbered information till besökare om vilka uppgifter som kan stödja vilseledande kontakt. Kontrollera meddelanden om bokningar eller årskort via den etablerade tjänsten. Leverantörens återställning och kundinformationen bör utgå från samma verifierade omfattning.

Slutsats

Förbered information till besökare om vilka uppgifter som kan stödja vilseledande kontakt.

FALL Q

Gothia Towers skiljer formulär från biljettuppgifter

Hotell och mässor

Upptäckt 18 november; utredning pågår

FASTSTÄLLD REDOGÖRELSE	Svenska Mässan Gothia Towers rapporterade upptäckt den 18 november i en avgränsad extern webbmiljö. Beskedet den 20 november beskrev omkring 14 000 kunder som möjligen berörts genom formuläruppgifter. Omkring 500 av dessa kunder hade också orderinformation och användaruppgifter som angetts vid köp av mässbiljetter som läckt. [S31][S68]
BEGRÄNSNING	Biljettkunderna är uttryckligen en delgrupp av de kunder som möjligen berörs. Kategorierna har olika säkerhet och läggs inte samman. Företaget undantog personnummer och betalningsinformation, uppgav att andra system inte berördes och markerade att utredningen fortsatte.
ÅTGÄRD	Behåll skillnaden mellan möjlig exponering och fastställd läcka i kundinformationen. Om biljettkontots uppgifter berördes, kräv lösenordsbyte och granska kontots inloggningar. Kontrollera webbmiljöns faktiska rättigheter och loggar. Behandla ändrad utredningsomfattning som ett uppdateringsbehov, inte som belägg för ett andra intrång.

Slutsats

Behåll skillnaden mellan möjlig exponering och fastställd läcka i kundinformationen. Om biljettkontots uppgifter berördes, kräv lösenordsbyte och granska kontots inloggningar.

FALL R

R

Flygbokningsuppgifter och äldre resor

Flygtransport

Återgivet företagsbesked; organisationsnamn utelämnat

FASTSTÄLLD REDOGÖRELSE	Rapporteringen beskrev ett flygbolagsbesked om bokningsreferenser och flygrelaterade uppgifter som kan ha röjts via en extern bokningsleverantör. [S63][S26]
BEGRÄNSNING	Beskedet gäller främst äldre bokningar och genomförda resor. Utredning och intrångsperiod var fortfarande oklara här. Det fastställer ingen grupp svenska invånare, aktiva passagerarkonton eller åtkomst till flygkontrollsystem.
ÅTGÄRD	Fråga vilka bokningsfält som röjts och om aktuella bokningar behöver skydd. Granska bokningstjänstens behörigheter och ovanliga sökningar. Slå inte samman beskedet med en incident på ett annat flygbolags betalningssida utan konkreta belägg.

Slutsats

Fråga vilka bokningsfält som röjts och om aktuella bokningar behöver skydd.

FALL S

S

Produktionsstopp efter ett intrång

Tillverkning

Företagets talesperson enligt rapporteringen

FASTSTÄLLD REDOGÖRELSE	En tillverkares talesperson uppgav i rapporteringen att system stängts för isolering efter ett intrång och att produktionen pausats. [S64][S27]
BEGRÄNSNING	Den citerade redogörelsen fastställer inte kryptering, aktör eller mängd stulna uppgifter. Upptäckt och besked är olika händelser. Skyddsavstängning betyder inte automatiskt angriparstyrda maskiner.
ÅTGÄRD	Öva ett säkert produktionsstopp och beläggen som krävs för omstart. Skilj återställning av verksamhets-IT från industrisäkerhet, planering och orderavstämning. Ange vem som får godkänna varje steg.

Slutsats

Öva ett säkert produktionsstopp och beläggen som krävs för omstart.

T

FALL T

Kylincidenter kräver fysisk verifiering

Detaljhandel och operativ teknik

Officiell kampanjvarning

FASTSTÄLLD REDOGÖRELSE	NCSC:s besked den 2 november bekräftade incidenter som berört livsmedelshandelns kylsystem och kontakt med drabbade verksamheter. Råden gällde internetexponering, underhållen utrustning och skydd i flera lager. Ett besked den 5 november satte händelserna i ett europeiskt sammanhang. [S25][S17]
BEGRÄNSNING	Den officiella redogörelsen anger inte ett svenskt totalantal drabbade eller en gemensam aktör för varje incident. En offentlig bild av ett styrsystem verifierar inte aktuell åtkomst eller fysisk skada. Anta inte påverkan på annan kritisk infrastruktur.
ÅTGÄRD	Låt drifttekniker kontrollera inställningar och säker lokal funktion. Ta bort onödig publik åtkomst, styr leverantörens underhållsvägar och bevara ändringshistorik. Bestäm isolering och reservdrift innan en styrenhet måste kopplas bort.

Slutsats

Låt drifttekniker kontrollera inställningar och säker lokal funktion.

V

FALL V

Trezors leveransuppgifter och en reviderad internationell grupp

Konsumenttjänster och leveranser

Officiellt besked

FASTSTÄLLD REDOGÖRELSE	Trezors besked den 13 augusti gällde leveranspartnern ShipMonk och kunder på flera marknader, uttryckligen även Sverige. De första 13 689 kunderna bestod av 11 742 vars kontakt- och leveransuppgifter exponerats och 1 947 med begränsade namn-, orts- och e-postuppgifter. Den senare gruppen omfattade också äldre beställningar. [S79][S80]
UPPDATERAD OMFATTNING	Uppdateringen den 4 september lade till omkring 67 000 amerikanska kunder med orderuppgifter från november 2019–augusti 2021. Den uppdaterade frågesidan anger totalt 80 689 kunder. Det är internationella grupper utan verifierat svenskt antal. Trezor uppgav att dess system och enheter inte påverkades. [S79]

ÅTGÄRD

Hantera exponerade leveransuppgifter som risk för nätfiske och personlig säkerhet. Lämna aldrig ut plånbokens säkerhetskopia efter en begäran i ett meddelande eller på en webbplats. Leverantörsansvariga bör begära belägg för att äldre kopior raderats; en policy eller tidigare försäkran bevisar inte radering.

Slutsats

Skilj svensk omfattning, enheternas säkerhet och kvarstående risk från leveransuppgifter.

5.3 Övriga händelser behåller sin underlagstyp

En organisation rapporterade ett intrång som berörde interna dokument, inklusive vissa personuppgifter, utan rapporterad påverkan på kundsystemet. [S19][S55]

En annan organisations e-postkonto användes för att skicka nätfiske; inga indikationer på bredare systempåverkan rapporterades. [S58]

Ett tjänsteföretag rapporterade en händelse under sommaren och senare läckta personaluppgifter. Källan beskriver administrativ information och avstängning; utpressningssidans etikett förblir ett separat påstående. Beskeden fastställer inte samma aktör, intrångsväg eller uppgiftsgrupp. [S59]

Ett separat vårdmyndighetsbesked i november beskrev att en anställds e-postkonto skickat fakturalockbeten. Myndigheten uppgav att IT isolerat händelsen och inte sett indikationer på påverkan på annan personal eller andra system vid publiceringen. [S32]

5.4 Senaste aktivitet: 8–22 november 2026

Tabellen skiljer mellan när uppgifter blev offentliga och den underliggande händelsens tid och säkerhet. November jämförs inte med en hel tidigare månad som ett tillväxtmått.

Beskedsdatum	Aktivitet eller uppdatering	Vad som hålls isär
november	Vårdpersonalens e-postkonto används för fakturalockbeten	Separat incident; ingen indikation på bredare systemeffekt vid publiceringen [S32]
17 november	CERT-SE varnar för flera nätfiskekampanjer	Kampanjvarning, inte nationellt antal drabbade [S33]
18 november	Lyko ger formellt omfattningsbesked	Upptäckt 12 november; Sverige och samtliga marknader hålls isär [S28]
19 november	Cabonlines leverantörsrelaterade bokningsbesked	Risk med reseuppgifter och osäkerhet om vidare spridning [S29]
20 november	Missbruk av tågbokningar under polisutredning	Inga belägg för åtkomst till tågstyrning; syfte och gärningsperson oklara [S41]

Beskedsdatum	Aktivitet eller uppdatering	Vad som hålls isär
20 november	Universeums leverantörsbesked	Händelse i slutet av oktober; inget samband antas utifrån geografi [S30]
20 november	Gothia Towers besked om extern webbmiljö	Möjlig formulärexponering respektive uppgiven biljettinformationsläcka [S31]

Den senaste perioden innehåller också tre Sverige-märkta utpressningspubliceringar. Publiceringsdatumen fastställer inte när ett intrång började och bekräftar inte självständigt något av fallen ovan. [S2]

5.5 Sårbarhetsråd är inget incidentantal

CERT-SE:s PHP-varning i oktober och leverantörens råd stödjer omedelbar tillämplighetskontroll. Båda identifierarna nedan kontrollerades mot NVD. Deras existens fastställer inte utnyttjande hos en svensk organisation. [S13] [S14][S15][S16]

Identifierare	Berört område	Minsta rättning för bristen	Åtgärd
CVE-2026-109618	Äldre utgåvor i angivna PHP-grenar; äldre grenar utan stöd kräver leverantörsstödd rättning eller migrering	PHP 8.2.35 / 8.3.36 / 8.4.27 / 8.5.12	Identifiera relevanta installationer, uppdatera och utred tecken på åtkomst
CVE-2026-109619	Äldre utgåvor i angivna PHP-grenar; faktisk exponering beror på driftsättning och förfrågningshantering	PHP 8.2.35 / 8.3.36 / 8.4.27 / 8.5.12	Följ underhållen leverantörsvägledning; tillfälliga åtgärder motsvarar inte fullständig rättning

Detta är oktobers minsta rättningar för två identifierade brister, inte en rekommendation om en gammal utgåva. Leverantören publicerade senare säkerhetsutgåvor den 19 november. Installera aktuell säkerhetsutgåva med stöd för miljön. Om direkt uppdatering inte går, bedöm isolering med tjänsteägaren. [S14]

VIKTIGA SLUTSATSER

01

Behåll händelse-, upptäckts- och beskedsdatum som olika fakta.

02

Håll leverantörshändelser, kundanmälningar och personer som olika enheter.

03

Hantera kunders och personers säkerhet tillsammans med teknisk återställning.

KAPITEL 06

Hacktivism, tillgänglighet och operativa system

06

DETTA KAPITEL BESVARAR

Hur skiljer sig påståenden från verifierad tjänsteeffekt eller fysisk följd?

3

skilda frågor: påstående, tjänsteeffekt och operativ effekt

6.1 En tidslinje över besked, inte en angreppsräknare 50

6.2 Ställ påståenden bredvid officiella uppgifter 51

6.3 Verifiera uppgiften användaren behöver utföra 52

6.4 Politisk neutralitet i incidentkommunikation 52

KAPITEL 06

Hacktivism, tillgänglighet och operativa system

I KORTHET

Ett offentligt påstående, en svarande webbplats och en fungerande fysisk process är olika underlag. Officiella kylvarningar motiverar driftkontroller utan att ange en gemensam aktör eller nationellt antal drabbade. Ett värmeverksförsök från föregående år som offentliggörs 2026 måste behålla sitt tidigare händelsedatum. Håll tjänstens tidslinje separat från aktörers budskap och ge tekniker ansvar för säker styrning och lokala inställningar.

6.1 En tidslinje över besked, inte en angreppsräknare

15 apr 2026	**Regeringens uppgifter enligt AP** Ett misslyckat försök mot en värmeoperatör 2025 offentliggjordes; attribueringen förblir ministerns [S38]
14 sep 2026	**NCSC och samverkande bedömning** Inga större informations- eller cyberangrepp mot valets genomförande rapporterades i bedömningen [S39]
2 okt 2026	**NCSC** Varning för nätfiske som utger sig för att komma från NCSC och FRA; myndighetsnamn verifierar inte ett meddelande [S42]
2 nov 2026	**NCSC** Kylincidenter bekräftas; organisationer uppmanas granska uppkopplad utrustning [S25]
5 nov 2026	**NCSC** Bredare europeisk kylvarning; inget nationellt incidentantal anges [S17]
17 nov 2026	**CERT-SE** Flera nätfiskekampanjer mot svenska organisationer observerade [S33]

Posterna använder publiceringsdatum. Värmeoperatörens post gäller ett försök 2025, inte ett angrepp 2026. Valposten är en officiell bedömning av ett avgränsat ämne, inte ett bevis för att inga konton var måltavlor.

En spanskspråkig vidareförmedling den 22 april säger att en video laddats upp igen. Sammanhanget gäller en värmehändelse 2025. Utdraget visar cirkulation av ett påstående, inte videoäkthet, nytt angrepp 2026, aktörsidentitet eller självständig statlig attribuering. [S1]

Underlagskort B15 22 apr 2026

Publicerare (alias utelämnat) Forumtråd Forum Spanska

ORIGINALTEXT

[…] volvimos a subir el video del ataque […]

ÖVERSÄTTNING

[…] vi laddade upp videon av angreppet igen […]

Anmärkning. Inlägget 2026 visar cirkulation av ett påstående. Det ändrar inte den påstådda händelsens år, 2025, och bekräftar inte självständigt en aktörsattribuering.

Fastställt
En spanskspråkig vidareförmedling kopplar påstådd återuppladdning till en svensk ministers uppgifter om en värmeverkshändelse 2025 och nämner NoName057(16).

Inte fastställt
Videons äkthet, oberoende granskning av materialet, åtkomst till målsystem, aktörsidentitet, statlig attribuering eller en ny incident 2026.

6.2 Ställ påståenden bredvid officiella uppgifter

Fråga	Aktörens eller annat offentligt påstående	Officiell eller återgiven redogörelse	Underbyggd slutsats
Fastställdes fysisk skada?	Bilder eller påståenden kan hävda kontroll	NCSC bekräftade kylincidenter utan fullständigt nationellt konsekvensantal [S25]	Verifiera lokala inställningar, processhistorik och säkerhetsföljder
Vem var ansvarig?	Ett alias kan ta på sig ansvaret	Värmeattribueringen är ministerns uppgift om föregående års försök [S38]	För inte över attribueringen till en annan händelse
Röjdes uppgifter vid ett avbrott?	En aktör kan hävda flera utfall	Tillverkningsrapporteringen beskriver avstängning och produktionseffekt [S27]	Tillgänglighet och informationsåtkomst kräver skilda belägg
Utsattes valgenomförandet för ett större angrepp?	Politiska budskap kan hävda påverkan	NCSC:s eftervalsbesked angav inga större angrepp mot genomförandet i bedömningen [S39]	Behåll den avgränsade bedömningen utan att hävda allmän frånvaro

Inget numeriskt förhållande mellan angripar- och myndighetsuppgifter beräknas. Beskeden gäller olika enheter och verifieringsnivåer. Rapporten gör inte politiskt färgat språk till en verifierad orsak till tjänsteavbrott.

6.3 Verifiera uppgiften användaren behöver utföra

För en offentlig tjänst, kontrollera om människor kan slutföra den kritiska uppgiften, inte bara om startsidan svarar. Identitet, betalning eller dokumentleverans kan vara otillgänglig fast en informationssida fungerar. Bevara tjänsteövervakning, leverantörens skyddsåtgärder och kundstödsrapporter tillsammans.

För operativ utrustning, verifiera den fysiska processen med behörig driftpersonal. Ändrad fjärråtkomst kan kräva annan hantering än ett nätavbrott. Bekräfta säker lokal styrning, återställningsmandat och leverantörsåtkomst innan utrustningen ansluts igen.

Ett incidentbesked avgör inte om alla skydd har lyckats eller misslyckats. Skyddsisolering kan i sig avbryta en tjänst. Skilj angriparens effekter från avsiktlig begränsning i kommunikationen när underlaget stödjer skillnaden.

6.4 Politisk neutralitet i incidentkommunikation

Återge bara det minsta aktörspåstående som behövs för försvarsfrågan. Ta bort förolämpningar, skadeuppmaningar, religionskränkningar och slagord. Behåll officiell statlig attribuering som källans bedömning. Beskriv inte Natoanslutning, religiösa händelser eller regeringsbeslut som bevisad angreppsorsak utan särskilda källbelägg.

Ett bevarat foruminlägg söker teknisk hjälp mot ett webbhotell och hävdar att det har en svensk politisk webbplats som kund. Kopplingen till Sverige är indirekt; bolagets och infrastrukturens geografiska hemvist är oklar. Inlägget visar en uppmaning, inte ett försök till eller lyckat intrång. Personuppgifter och uppviglande anklagelser utelämnas. Det räknas inte som en bekräftad svensk incident. [S1]

En aktörs mållista fastställer inte fientlighet hos en befolkning, ett parti eller ett land. Beredskap bör följa relevant hot och tjänstens beroenden. Ge allmänheten faktabaserade, tidsavgränsade och användbara uppdateringar.

VIKTIGA SLUTSATSER

01
Verifiera tjänsteeffekter och fysiska effekter separat från påståenden.

02
Behåll tidigare händelsedatum i senare besked.

03
Ge faktabaserade lägesbesked utan att ta över aktörsretorik eller politiska förklaringar.

KAPITEL 07

Hotaktörer, publiceringsetiketter och attribuerade kampanjer

07

DETTA KAPITEL BESVARAR

Vilka samband stöds av vilket underlag?

24

aktörsetiketter i Sveriges utpressningspubliceringar

7.1 Sambandskartan visar underlagskopplingar 54

7.2 Utpressningspubliceringar och regionalt sammanhang 55

7.3 Internationella attribueringar förblir källornas 57

7.4 Bedömningssäkerhet gäller ett bestämt påstående 59

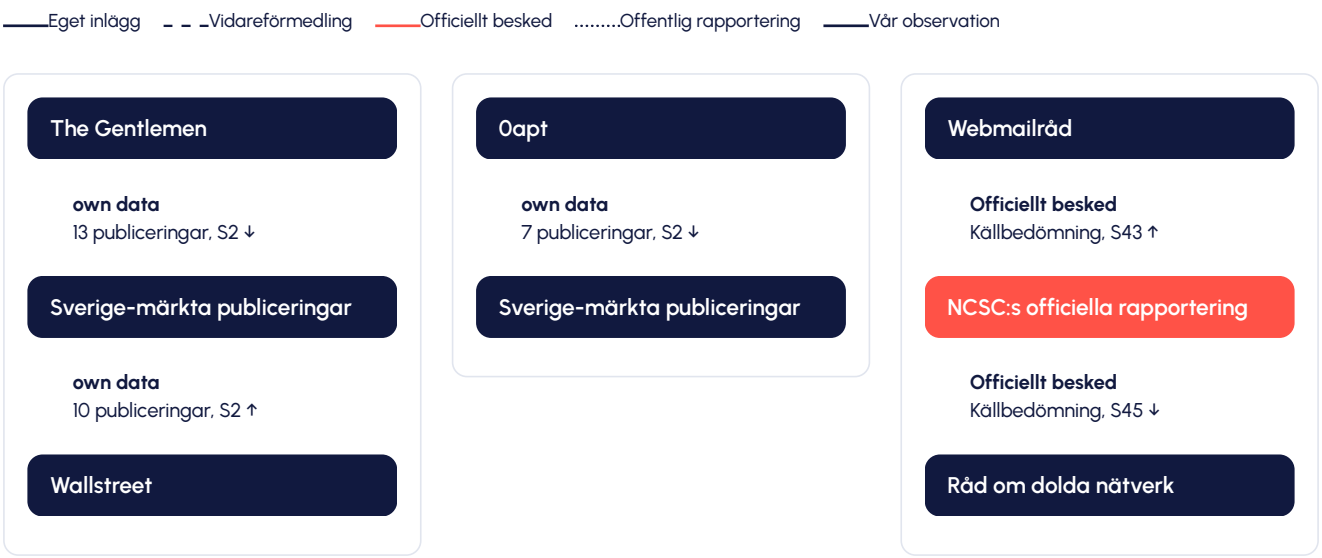
KAPITEL 07

Hotaktörer, publiceringsetiketter och attribuerade kampanjer

I KORTHET

Ransompedia registrerar 24 aktörsetiketter i 62 Sverige-märkta publiceringar. De tre vanligaste står för 30 publiceringar. Detta är registrerade påståenden, inte verifierade operatörer, kodfamiljer eller genomförda intrång. Internationella myndighetsråd beskriver andra kampanjer med egen attribuering och avgränsning. Knyt varje samband till sin källa och prioritera åtkomst- eller tjänstebeteenden som försvarare kan verifiera.

7.1 Sambandskartan visar underlagskopplingar



INGEN BELAGD KOPPLING TILL ANDRA AKTÖRER

Kartan kopplar publiceringsetiketter till det bevarade materialet som **egna data**. Den kopplar officiella kampanjbedömningar till utgivaren. Den ritar inte ett gemensamt operatörssamband mellan en kriminell annons, en kylhändelse och ett internationellt råd bara för att de gäller Sverige.

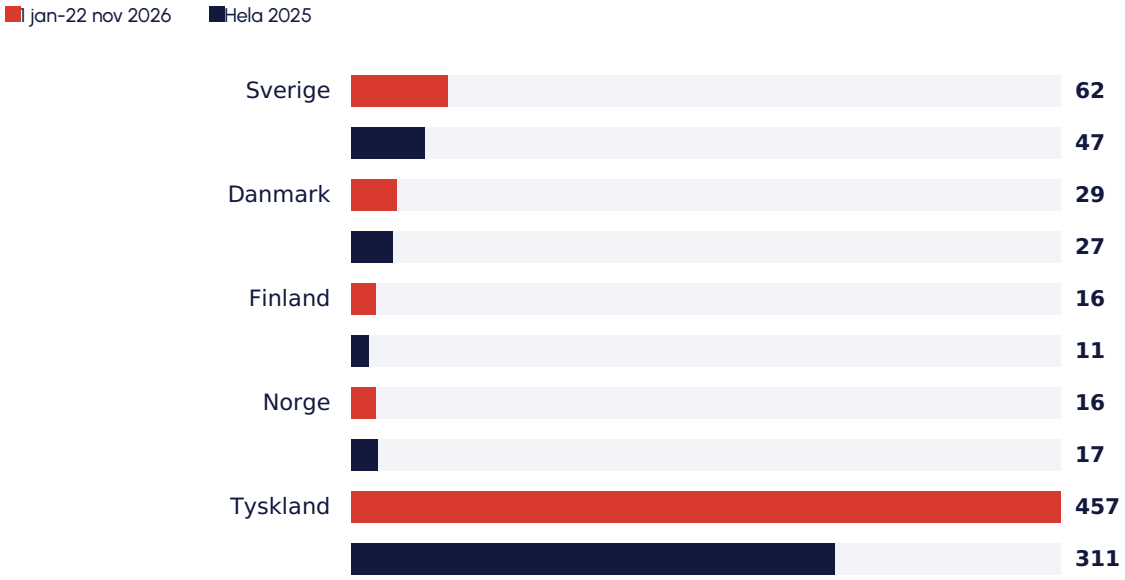
Ingen gemensam operatör har fastställts mellan dessa grupper. En bredare kedja av kriminella tjänster skulle vara en **analysmodell**, inte en observerad affär eller anknytning. Liknande inlägg skulle inte ensamma visa överföring av uppgifter eller åtkomst.

7.2 Utpressningspubliceringar och regionalt sammanhang

Danmark, Finland och Norge ger nordiskt tjänstesammanhang. Tyskland ger en större industriell jämförelse kring Östersjön.

Jämförelseländerna har valts som exempel enbart för att ge sammanhang; de innebär ingen rangordning eller politisk bedömning.

Sverige-märkta publiceringar motiverar återställningsberedskap i flera sektorer



Källa: Brandefense Ransompedia, 1 januari-22 november 2026 jämfört med hela 2025 [S2]. Olika perioder; landmärkta påståenden, inte unika offer, bekräftade intrång eller en rangordning av nationell säkerhet.

Land	Publiceringar under 2026-perioden	Hela 2025	Tolkning
Sverige	62	47	Publiceringar under del av året
Danmark	29	27	Separat landmärkt grupp
Finland	16	11	Separat landmärkt grupp
Norge	16	17	Separat landmärkt grupp
Tyskland	457	311	Större separat publiceringsgrupp

Källa: Ransompedia [S2]. Perioderna är inte jämförbara helår. Skillnader är inte befolkningsjusterade angreppstal, försvarseffektivitet eller en rangordning av nationell säkerhet. Landsetiketter kan avse en koncern, ett dotterbolag eller gränsöverskridande verksamhet.

Den svenska gruppen innehåller återkommande organisationer och en gränsöverskridande namnfråga. Antalet förblir 62 publiceringar, inte ett ändrat påstående om unika svenska organisationer. Tillverkning har 11 publiceringar, konsultverksamhet 8 och hälsa 7; källans sektorer fastställer inte nationella incidentfrekvenser. [S2]

The Gentlemen, Wallstreet och 0apt står för 13, 10 respektive 7 publiceringar. Tillsammans är det 30 av 62, eller 48,4 %. Övriga 32 publiceringar har andra etiketter. En etikett fastställer inte en unik partner, teknisk metod, lyckad kryptering eller genomförd betalning. [S2]

The Gentlemen

Etikett i bevarade publiceringar

Etikett för utpressningspublicering | Ingen statlig attribuering fastställd

I SVERIGE, 2026

2026-perioden

13 Sverige-märkta publiceringar, S2

PÅSTÅDDA MÅL

Listade organisationer; namn utelämnas och landanknytningen är avgränsad

I OFFENTLIG RAPPORTERING

[S2] 13 publiceringar registrerade i Ransompedia

VÅR BEDÖMNING

Publicering verifierar ett utpressningspåstående. Den fastställer inte unik operatör, kodursprung, kryptering, uppgiftsäkthet eller betalning. Kontrollera egna larm och förbered återställning oberoende av namn.

BEDÖMNINGSSÄKERHET

Hög säkerhet för registrerat antal; enskilda påståenden obekräftade

Wallstreet

Etikett i bevarade publiceringar

Etikett för utpressningspublicering | Ingen statlig attribuering fastställd

I SVERIGE, 2026

2026-perioden

10 Sverige-märkta publiceringar, S2

PÅSTÅDDA MÅL

Listade organisationer; namn utelämnas och landanknytningen är avgränsad

I OFFENTLIG RAPPORTERING

[S2] 10 publiceringar registrerade i Ransompedia

VÅR BEDÖMNING

Publicering verifierar ett utpressningspåstående. Den fastställer inte unik operatör, kodursprung, kryptering, uppgiftsäkthet eller betalning. Kontrollera egna larm och förbered återställning oberoende av namn.

BEDÖMNINGSSÄKERHET
Hög säkerhet för registrerat antal; enskilda påståenden obekräftade

0apt

Etikett i bevarade publiceringar

Etikett för utpressningspublicering | Ingen statlig attribuering fastställd

I SVERIGE, 2026

2026-perioden
7 Sverige-märkta publiceringar, S2

PÅSTÅDDA MÅL

Listade organisationer; namn utelämnas och landanknytningen är avgränsad

I OFFENTLIG RAPPORTERING

[S2] 7 publiceringar registrerade i Ransompedia

VÅR BEDÖMNING

Publicering verifierar ett utpressningspåstående. Den fastställer inte unik operatör, kodursprung, kryptering, uppgiftsäkthet eller betalning. Kontrollera egna larm och förbered återställning oberoende av namn.

BEDÖMNINGSSÄKERHET
Hög säkerhet för registrerat antal; enskilda påståenden obekräftade

7.3 Internationella attribueringar förblir källornas

NCSC:s webmailråd i juli återger en gemensam bedömning ledd av NSA med samverkande myndigheter. Den beskriver troligen Rysslandsanknutna aktörer och sårbar Zimbra-webbmail. Källan anger inget svenskt antal drabbade och fastställer inte att varje exponerad installation nåddes. [S43]

Ett separat routerråd i juli gäller skydd av nätverksutrustning och aktivitet som källorna attribuerar till ryska statliga aktörer. Ett aprilråd beskriver vad utgivarna kallar dolda nätverk med Kinaanknytning. Inget av råden skapar ett namngivet svenskt offer eller attribuerar de separata fallen i kapitel 5. [S44][S45]

Gemensamt webmailråd

Officiellt internationellt kampanjråd | Attribueringen förblir källmyndigheternas bedömning

I SVERIGE, 2026

2026

Officiellt råd, S43

PÅSTÅDDA MÅL

Källans internationella grupp; inget svenskt offer antas

I OFFENTLIG RAPPORTERING

[S43] NCSC:s officiella stödjande råd

VÅR BEDÖMNING

NCSC återger utgivarnas bedömning av trolig Rysslandsanknytning. Inget svenskt antal drabbade eller samband med övriga fall fastställs.

BEDÖMNINGSSÄKERHET

Hög säkerhet om myndighetsbeskedet; ingen egen operatörsattribuering

Råd om dolda nätverk

Officiellt internationellt kampanjråd | Attribueringen förblir källmyndigheternas bedömning

I SVERIGE, 2026

2026

Officiellt råd, S45

PÅSTÅDDA MÅL

Källans internationella grupp; inget svenskt offer antas

I OFFENTLIG RAPPORTERING

[S45] NCSC:s officiella stödjande råd

VÅR BEDÖMNING

Utgivarna använder attribuering med Kinaanknytning. Detta är källans attribuering och internationellt kampanjsammanhang, inte belägg för en namngiven svensk infektion.

BEDÖMNINGSSÄKERHET

Hög säkerhet om myndighetsbeskedet; ingen egen operatörsattribuering

Rapporten lägger inte till teknikidentifierare när det citerade avsnittet saknar uttrycklig mappning. De operativa prioriteringarna är underhållen programvara, styrd administrationsåtkomst, användbara enhetsloggar och stark fjärrautentisering. Ett råd motiverar bedömning av en relevant tillgång men visar inte att den är infekterad.

7.4 Bedömningssäkerhet gäller ett bestämt påstående

Det kan vara säkert att ett inlägg eller en publicering finns samtidigt som den erbjudna tillgången är obekräftad. Ett företag kan på samma sätt bekräfta informationsåtkomst medan gärningspersonen är okänd. Håll slutsatserna isär i aktörskort, fallrubriker och ledningsunderlag.

Ett alias kan ändras och en publiceringstjänst kan visa flera etiketter. Dra inte slutsatser om en persons identitet, plats, ideologi eller statskoppling bara från namnet. Källattribuering och tekniska samband behöver egna belägg.

VIKTIGA SLUTSATSER

01

Publiceringsetiketter räknar påståenden, inte verifierade operatörer.

02

Internationella råd behåller källans attribuering och geografiska gränser.

03

Koppla underlagsgrupper först när ett konkret samband stödjer länken.

KAPITEL 08

Bedrägeri, informationshandel och följdskador

DETTA KAPITEL BESVARAR

Hur kan information stödja en trovärdig förfrågan utan att bevisa intrång?

132

olika Sverige-märkta kortnummerposter; endast snäv omfattning av bevarade inlägg

8.1 Sammanhang är inte autentisering 61

8.2 Rekrytering och annonserade informationstjänster 61

8.3 Betalkortsmaterial: en snäv observation 62

8.4 Polisvarningar visar olika vägar till vilseledning 63

8.5 Förbered stöd till människor och system 63

KAPITEL 08

Bedrägeri, informationshandel och följdskador

I KORTHET

Identitets- och kontaktuppgifter kan göra en falsk förfrågan trovärdig utan att ge uppringaren behörighet. Inläggen visar kontaktlistor, efterfrågan och rekryteringspåståenden. Polisens rapportering ger separata belägg för imitationsmetoder. Ingen av grupperna fastställer en gemensam operatör eller nationell bedrägeriförlust. Verifiera betydelsefulla förfrågningar oberoende och samordna kundstöd, bedrägeriförebyggande och dataskydd när uppgifter röjs.

8.1 Sammanhang är inte autentisering

En uppringare som känner till bokning, faktura, namn eller personnummer kan låta trovärdig. Uppgifterna visar inte kontroll över kontot eller behörighet att ändra en betalning. Fall D, O och P gäller olika informationskategorier som kräver proportionerlig bedömning.

Kopplingen mellan information och senare imitation är en **analysmodell**. Rapporten fastställer inte att en viss bevarad säljare försörjde en viss bedrägerikampanj. De offentliga varningarna nedan vilar på egna belägg.

8.2 Rekrytering och annonserade informationstjänster

Underlagskort B08 — 24 maj 2026

Publicerare (alias utelämnat) | Forumtråd | Forum | Ryska

ORIGINALTEXT

ГЕО: Польша Чехия Румыния Норвегия Швеция

ÖVERSÄTTNING

Geografi: Polen, Tjeckien, Rumänien, Norge, Sverige.

Anmärkning. Kontaktuppgifter och nedsättande formuleringar återges inte.

Fastställt
Ett ryskspråkigt rekryteringsinlägg tar med Sverige bland flera geografiska marknader.

Inte fastställt
Svenskt offer, lyckat bedrägeri, aktiva lokala medarbetare, nationalitet eller gemensam operatör.

Underlagskort B12 — 7 nov 2026

Publicerare (alias utelämnat) | Forumtråd | Forum | Engelska

ORIGINALTEXT

This High quality phone database you can use for Spam [...] Sweden-100k

ÖVERSÄTTNING

Telefonlista med påstådd hög kvalitet för spam [...] Sverige-100k

Anmärkning. Inlägget ligger före den senaste perioden. Liknande titlar och antal visar inte samma fil eller operatör.

Fastställt
Ett inlägg den 7 november annonserar landmärkta telefonlistor och påstår 100k poster för Sverige.

Inte fastställt
Äkthet, unika abonnenter, insamlingsdatum, ursprung, lagligt förvärv, leverans eller faktiska spamutskick.

Det ryskspråkiga rekryteringsutdraget tar med Sverige bland flera marknader. Det fastställer en annons, inte aktiva lokala medarbetare, lyckat bedrägeri eller ett svenskt offer. Språkval fastställer inte nationalitet eller statlig styrning. [S1]

En telefonlisteannons den 7 november hävdar en svensk mängd på 100k inom ett internationellt erbjudande. Den ligger före den senaste perioden. Antal, äkthet, abonnenter, ursprung och leverans är obekräftade; det är inget incidentantal för en teleoperatör. [S1]

En identitetsförfrågan visar inte heller kringgående av kundkännedomskontroller. Kontrollera påstådd förmåga separat från berört konto eller transaktion. Rapporten skattar inte tillgången på otillåtna konton från annonser.

Ytterligare annonser och förfrågningar gäller nordiska sociala konton, brevlådeåtkomst, identitetsverifierings-tjänster, manipulation av visad uppringaridentitet och rekrytering av penningmålvakter. En annons för en nät-fiskepanel efterliknar en musiktjänst och hävdar flera steg för inloggningsuppgifter eller godkännanden. Den fastställer inte intrång i tjänsten. Ett internationellt erbjudande om spelkundsuppgifter omfattar Sverige utan verifierad svensk andel. Detta är olika påstådda förutsättningar för vilseledande, inte belägg för gemensam operatör eller genomförd bedrägerikedja. Granska misstänkt kontoåterställning, godkännanden som en uppringare begär och ovanliga betalningsändringar mot eget underlag. [S1]

En annons för en kontaktuppslagningsbot hävdar separat ett stort internationellt lager och omfattar Sverige. Den fastställer inte intrång i den nummerupplysningstjänst som nämns, uppgifternas ursprung eller ett verifierat antal svenska personer. En deltagare ifrågasätter också rimligheten i fälten i ett speldataexempel. Kritiken är en obekräftad forumbedömning, inte ett oberoende bevis för att den annonserade datamängden är äkta eller fabricerad. [S1]

En ytterligare annons den 19 augusti erbjöd landmärkt identitetsdata, inklusive påstådda svenska ID-kopplade poster. Den visar annonsering, inte innehav, äkthet, giltiga identifierare eller ett nytt organisationsintrång. [S1]

8.3 Betalkortsmaterial: en snäv observation

KORTUPPGIFTERNAS OMFATTNING

Antalen beskriver en begränsad grupp observerade publiceringar. De skattar inte svensk kortstöld, bedrägeriförluster eller betalningsgiltighet.

De bevarade inläggen innehöll 132 olika kortnummerposter märkta Sverige, med 141 förekomster i 135 inlägg. Ingen namngiven utgivare fastställs. Landetikett, faktisk utgivning, stöldstatus och betalningsgiltighet är obekräftade. Det är observerade poster i en snäv inläggsgrupp, inte bekräftat stulna svenska kort. [S1]

Antalet ensamt motiverar inte kortspärr. En utgivare eller kund som får ett relevant verifierat larm bör följa sin etablerade bedrägerihantering och de specifika uppgifterna som röjts. Inga personliga eller användbara betalningsdetaljer publiceras här.

8.4 Polisvarningar visar olika vägar till vilseledning

Publicering	Dokumenterat mönster	Försvarsföljd
28 januari	Ett falskt hyrbils-sms leder till en uppringare som imiterar en bank [S35]	Avsluta kontakten och nå den riktiga institutionen självständigt
24 april	Sms utger sig för att gälla trafikböter och kräver länkad betalning [S34]	Kontrollera det påstådda myndighetskravet utanför meddelandet
September	Kriminella imiterar verkliga kreditvärdiga företag genom nya webbidentiteter och obetalda order [S52]	Bekräfta företag, kontakt och leverans genom oberoende register
2 oktober	NCSC varnar för falska myndighetsmeddelanden med dess och FRA:s namn [S42]	Namn och hotad tidsfrist autentiserar inte en begäran
12 november	Polisen beskriver leveranslockbeten som kopplas vidare till falsk bankpersonal [S71]	Överföring mellan uppringare är inte oberoende verifiering
12 november	En betalkortsutredning beskriver vilseledande meddelanden och återuppringning [S72]	Bedöm begärd kortregistrering i stället för att lita på det påstådda larmet

Poliskällorna beskriver varningar eller utredningar vid angivna datum. Misstankar förblir misstankar; ett gripande eller åtal är inte en fällande dom. Rapporten summerar inte ärendebelopp till en nationell förlustskattning.

8.5 Förbered stöd till människor och system

En varning bör ange vilka uppgifter som faktiskt berörs, vad mottagaren kan göra och hur hjälp kan sökas säkert. Be inte människor lämna känsliga uppgifter genom en obekräftad kanal. När rese- eller hälsosammanhang berörs, bedöm personlig säkerhet med rätt ansvarig.

Teknisk återställning och bedrägeriskydd har olika avslutskriterier. En återställd bokningstjänst tar inte bort en uppringares kunskap om äldre resor. Granska ovanliga betalnings-, kontakt- och kontoåterställningsändringar och bevara normal åtkomst för legitima användare.

VIKTIGA SLUTSATSER

01

Äkta personuppgifter ger inte behörighet för en betydelsefull begäran.

02

Skilj kortobservationen från påståenden om stulna kort och bedrägeriförlust.

03

Förbered säkert kundstöd och oberoende kontroll av senare förfrågningar.

KAPITEL 09

Bank, finansiella kontaktlistor och betalningskontinuitet

09

DETTA KAPITEL BESVARAR

Vilka finansobservationer gäller institution, kund eller betalningsberoende?

23 av 25

utvalda finansdomäner publicerar DMARC med reject eller quarantine

9.1 Utvalda finansdomäner är inte alla tillståndspliktiga banker 65

9.2 En bankanknuten kontaktlista är inget banksystemfynd 66

9.3 Kundhandling och leverantörsåtkomst kräver olika belägg 66

9.4 Exponering på extern betalningssida är en annan enhet 67

9.5 Kontinuitet omfattar handlare och kund 67

KAPITEL 09

Bank, finansiella kontaktlistor och betalningskontinuitet

I KORTHET

Annonser om finansiella kontakter visar inte åtkomst till en banks system eller kunders pengar. Den utvalda finansgruppen ger exponeringskopplingar tillsammans med avgränsade konfigurationsobservationer. Polisvarningar gäller vilseledning och betydelsefulla kundhandlingar. Skilj institutionsåtkomst, kundimitation och betaltjänstkontinuitet åt och ge varje område en ansvarig för kontroll och åtgärd.

9.1 Utvalda finansdomäner är inte alla tillståndspliktiga banker

Finansgruppen innehåller 25 utvalda domäner, inte varje bank, finansiell entitet eller oberoende svensk juridisk person. 23 publicerar DMARC med reject eller quarantine och 2 övervakningspolicy. Detta är offentliga konfigurationsobservationer, inte ett exponeringsbetyg för sektorn. [S3]

SPF-poster finns för 24 domäner, DKIM-relaterade poster observeras för 22 och DNSSEC-delegationsposter för 16. TLS-validering lyckades för 24; ett resultat är otillgängligt. HSTS observerades för samtliga 22 finansdomäner med tillgängliga HSTS-resultat; resultat för övriga 3 utvalda domäner är otillgängliga. Ingen allmän finanssektorsslutsats följer. [S3]

Fråga	Tillgänglig observation	Ansvarig
Publicerar domänen tillämpande DMARC?	23 av 25	E-post- och domänägare
Erbjuds institutionens aktuella inloggningsuppgifter?	7 av 24 bedömda finansdomäner hade aktuell annons [S4]	Identitetsägare efter behörigt larm
Är enhetskopplingar knutna till aktuell åtkomst?	Minst 10 673 enhetskopplingar; aktuell åtkomst obekräftad [S4]	Ändpunkts- och identitetsteam
Fastställer en kontaktlista åtkomst till kundkonto?	Inget verifierat samband fastställt	Bedrägeriförebyggande och kundskydd
Kan betalningar fortsätta vid beroendeavbrott?	Ingen institutionsspecifik försäkran från rapporten	Betalnings- och kontinuitetsansvariga

9.2 En bankanknuten kontaktlista är inget banksystemfynd

Underlagskort B03 — 31 mar 2026

Publicerare (alias utelämnat) | Forumtråd | Forum | Engelska

ORIGINALTEXT

We are selling specific bank leads for all popular destinations in EU + America (+ some Asia)

ÖVERSÄTTNING

Vi säljer bankspecifika kontakter för vanliga destinationer i EU och Amerika samt delar av Asien.

Anmärkning. Inlägget begär 170 EUR per 1k bankspecifika kontakter. Det visar inte att en bank tillhandahöll informationen.

Fastställt
En säljare annonserar finansiella kontakter och har ett svenskt bankanknutet exempel bland flera länder.

Inte fastställt
Ursprung, samtycke, giltighet, aktuell bankrelation, kontoåtkomst, saldo eller genomförd affär.

Annonsen erbjuder bankanknutna kontakter i flera länder och har ett svenskt exempel. Begärt pris är 170 EUR per 1k kontakter. Det är ett annonserat pris och enhet, inte genomförd affär, kontovärde eller verifierad bankrelation. [S1]

En kontaktpost kan vara äldre marknadsföringsmaterial, en vilseledande beskrivning eller information från annan källa. Rapporten fastställer inte att en bank levererat uppgifterna, att personen har ett konto eller att ett saldo kan nås.

B14:s nya internationella mäklarannons har samma begränsningar. Koppla inte en finansiell lista till en separat flygbetalningsincident eller det privata domänurvalet utan särskilda belägg. [S1]

Fall U i kapitel 4 gäller annonserad fjärråtkomst till en verksamhet, medan B03 gäller finansiella kontaktuppgifter. Det första påstår en teknisk förmåga och det andra erbjuder register. Inget är oberoende verifierat och inget fastställer intrång i en bank med tillstånd. Skicka relevanta åtkomstlarm till infrastrukturansvarig och SOC; låt bedrägeri- och dataskyddsteam hantera missbruk av kontaktlistor. [S1]

9.3 Kundhandling och leverantörsåtkomst kräver olika belägg

Polisvarningar visar meddelanden som leder till en påstådd bank, ibland genom återuppringning eller vidarekoppling. Den relevanta frågan är vad kunden ombeds godkänna. Äkta personuppgifter, fakturabelopp eller tjänstenamn autentiserar inte begäran. [S35][S71][S72]

Institutioner bör ge en oberoende kontaktväg och ett säkert sätt att kontrollera kortregistrering eller betalningsändring. Granska kundrapporterade händelser mot faktisk transaktions- och autentiseringsinformation. Anta inte åtkomst till bankinfrastruktur för att en kund har vilseletts.

9.4 Exponering på extern betalningssida är en annan enhet

Rapporteringen beskrev ett flygbolags varning om att skadlig kod på webbsidor hos en leverantör kan ha exponerat kortuppgifter för vissa kunder, även i Sverige. [S40]

Detta är källbundet återgivna företagsuppgifter med internationell omfattning, inte ett antal svenska stulna kort från rapportens inläggsmaterial. Leverantören namngavs inte i den citerade redogörelsen. Inget samband med bokningsfallet eller en viss webbteknikleverantör fastställs här.

9.5 Kontinuitet omfattar handlare och kund

Riksbankens bedömning kopplar betalningar till el och kommunikation. Testa förlusten av ett beroende utan att anta ett angrepp. Ta med handlare, kundstöd, avstämning och återgångsbeslut i övningen. [S7]

Exponeringsobservationer gäller 24 av de 25 utvalda finansdomänerna; en förblir okänd. Bankdomänernas delgrupp omfattar 11 bedömda domäner. Där finns 6 med aktuell annons och 71 personalenhetskopplingar. Observationerna fastställer inte intrång hos institutionen. [S4]

Den smalare bankvyn innehåller minst 5 032 enhetskopplingar som inte identifierats som personalenheter. Ägarskap och aktuell åtkomst förblir obekräftade. Betalkortsmaterialet fastställer ingen verifierad utgivaranknytning och ger därmed inget validerat samband mellan kort och bank eller någon utgivarrankning. Behåll separata kontrollköer för identitet, ändpunkter och kundbedrägerier. [S1][S4]

VIKTIGA SLUTSATSER

01
Finansteman och kontaktpriser visar inte banksystemåtkomst.

02
Behåll finansdomänobservationerna inom urvalets nämnare.

03
Kontrollera kundhandlingar och betalningsberoenden separat från institutionens exponering.

KAPITEL 10

Regler och nationell hantering

10

DETTA KAPITEL BESVARAR

Vilket krav, vilken mottagare och vilken tidsfrist gäller för incidenten?

15 januari 2026

Cybersäkerhetslagen trädde i kraft

10.1 Börja med rätt juridisk person 69
10.2 Håll isär tidsfristerna 69
10.3 Dataskyddsansvaret följer uppgifterna och risken 70
10.4 Dora kräver uttryckliga beslut om undantag 71
10.5 Sanktionsbelopp är inte en prognos om böter 71

KAPITEL 10

Regler och nationell hantering

I KORTHET

Cybersäkerhetslagen, GDPR och Dora ställer olika frågor om samma händelse. En betydande tjänsteincident, en personuppgiftsincident och en allvarlig IKT-relaterad incident i finanssektorn kan överlappa utan att ha en gemensam tidsfrist. Aktuell vägledning hänvisar rapporter enligt cybersäkerhetslagen till NCSC. Fastställ tillämpning, mottagare och reservåtkomst till varje rapporteringsväg före en incident. Dokumentera tid för kännedom och klassificering separat.

10.1 Börja med rätt juridisk person

Cybersäkerhetslag (2025:1506) trädde i kraft den 15 januari 2026. Tillämpningen beror på lagens definitioner, verksamheter och undantag. Rapportens sektorsindelning avgör inte om alla utvalda organisationer omfattas av lagen. [S8]

Juridik och regelefterlevnad bör dokumentera juridisk person, verksamhet, storlek eller annan grund för tillämpning, tillsyn och relevanta undantag. I 1 kap. 10 § behandlas likvärdiga säkerhets- eller rapporteringskrav i annan författning. Utgå varken från allmän dubbelrapportering eller ett generellt undantag för finanssektorn. [S8]

Ledningen behöver också förstå sitt ansvar. I 2 kap. ställs krav på lämpliga och proportionella säkerhetsåtgärder samt utbildning för ledningen. En rapporteringslista visar inte att kraven är genomförda. Dokumentera vem i ledningen som accepterar kvarstående risk och vilken tjänsteägare som visar att åtgärderna fungerar. [S8]

10.2 Håll isär tidsfristerna

Tabellen visar huvudsakliga krav och steg. Den är ett stöd för operativ läsning, inte ett rättsligt utlåtande om en enskild incident.

Regelverk	Grund	Huvudsaklig tid	Mottagare
Cybersäkerhetslagen	Betydande incident hos verksamhetsutövare som omfattas	Upplysning inom 24 timmar från kännedom; incidentanmälan inom 72 timmar, eller 24 timmar för betrodda tjänster	NCSC via aktuell rapporteringsväg [S8][S9]
Cybersäkerhetslagens uppföljning	Samma rapporterade incident	Slutrapport inom en månad efter incidentanmälan; lägesrapport om incidenten pågår, sedan slutrapport inom en månad efter avslutad hantering	Samma utsedda myndighet [S8]

Regelverk	Grund	Huvudsaklig tid	Mottagare
GDPR	Personuppgiftsincident, om risk för rättigheter och friheter inte är osannolik	Anmäl till behörig tillsynsmyndighet inom 72 timmar från kännedom om möjligt; motivera försening	IMY eller annan behörig dataskyddsmyndighet [S10]
Dora	Allvarlig IKT-relaterad incident hos en finansiell entitet som omfattas	Inledande anmälan snarast, inom 4 timmar efter klassificering som allvarlig och normalt senast 24 timmar efter kännedom	Behörig finansiell tillsynsmyndighet; svensk vägledning från Finansinspektionen [S11] [S12]
Doras uppföljning	Samma allvarliga IKT-incident	Delrapport inom 72 timmar efter inledande anmälan, även om incidentens status eller hantering är oförändrad. Uppdaterad delrapport utan onödigt dröjsmål och i varje fall när ordinarie verksamhet har återställts. Slutrapport inom en månad efter delrapporten eller den senaste uppdaterade delrapporten	Finansiell tillsynsmyndighet [S11]

Cybersäkerhetslagen föreskriver också delrapport på myndighetens begäran. En betydande incident omfattar allvarlig faktisk eller möjlig driftsstörning eller ekonomisk skada, eller betydande skada för andra personer eller organisationer. Bedöm tillämpliga kriterier utan att invänta säker kunskap om en angripare. [S8]

PTS anger att rapporter enligt cybersäkerhetslagen går till NCSC och vidare till berörd tillsynsmyndighet. Vägledningen skiljer denna väg från eIDAS-rapportering för betrodda tjänster, som går till PTS. Antagandet att allt går till samma portal kan därför ge rätt rapport fel mottagare. [S9]

10.3 Dataskyddsansvaret följer uppgifterna och risken

IMY:s vägledning kräver en bedömning av följderna för människor. När anmälan krävs kan ofullständiga uppgifter kompletteras. Den personuppgiftsansvarige bör dokumentera incidenten och skälen även när bedömningen är att anmälan inte krävs. [S10]

Information till registrerade har en annan grund: sannolik hög risk för deras rättigheter och friheter. Utgångspunkten är information utan onödigt dröjsmål. En kriminell publicering fastställer inte automatiskt denna risk. Bekräftad uppgiftsförlust hos en leverantör kan kräva skyndsam bedömning innan hela omfattningen är känd. [S10]

Skilj mellan personuppgiftsansvarig och personuppgiftsbiträde. Fastställ vem som bestämmer ändamålet, vem som har den relevanta kopian och när respektive part fick kännedom. Avtalade meddelandekrav stödjer hanteringen men ersätter inte lagkraven.

10.4 Dora kräver uttryckliga beslut om undantag

Om klassificering som allvarlig görs efter de första 24 timmarna från kännedom ska den inledande anmälan lämnas inom 4 timmar efter klassificeringen. Dokumentera varför bedömningen ändrades och behåll tidsuppgifterna. Byt inte tyst ut kännedomstidpunkten mot datumet för ett senare offentligt besked. [S11]

Förordningen medger viss lättnad vid helger och bankhelgdagar, med undantag för inledande anmälan och delrapport från kreditinstitut och andra angivna entiteter. Tillsynsmyndigheter kan också undanta vissa betydande entiteter. Utgå inte från att en bank kan vänta till nästa arbetsdag. Kontrollera artikel 5 och entitetens tillsynssituation. [S11]

Finansinspektionens oktobervägledning beskriver delegerade portalbehörigheter och rapporteringens tre steg. Kontrollera att behörig personal kan lämna rapport när ordinarie identitets- eller kommunikationstjänster inte fungerar. Spara kvittot och sambandet mellan rapporterna. [S12]

10.5 Sanktionsbelopp är inte en prognos om böter

I 4 kap. cybersäkerhetslagen anges en lägsta sanktionsavgift på SEK 5 000. För väsentliga enskilda verksamhetsutövare är högsta beloppet det större av 2% av föregående globala årsomsättning eller motsvarande EUR 10 000 000 i kronor. [S8]

För viktiga enskilda verksamhetsutövare är motsvarande högsta belopp det större av 1,4 % eller EUR 7 000 000. För offentliga verksamhetsutövare är högsta beloppet SEK 10 000 000. Lagbeloppen förutsäger inte en avgift för något fall i rapporten. [S8]

Styrelsens användbara fråga är om tillämpning, åtgärder, utbildning, rapporteringsåtkomst och beslutsunderlag kan visas. Dra inte slutsatsen att lagen har överträtts utifrån en saknad konfigurationsobservation, en annons i en kriminell miljö eller en försiktighetsavstängning.

VIKTIGA SLUTSATSER

01

Dokumentera kännedom, bedömning av betydande incident och allvarlighetsklassificering separat.

02

Kontrollera aktuell mottagare och en behörig reservväg för rapportering.

03

Lagens tillämpning och risken för människor kräver ett ansvarigt beslut, inte en slutsats från en publicering.

KAPITEL 11

Utsikter och villkorade scenarier

11

DETTA KAPITEL BESVARAR

Vilka signaler skulle ändra prioriteringarna efter slutdatumet?

4

villkorade planeringsscenarier, inte sannolikhetsberäkningar

11.1 Huvudbedömningar och begränsningar 73

11.2 Fyra planeringsantaganden 74

11.3 Vad som skulle ändra bedömningen 74

KAPITEL 11

Utsikter och villkorade scenarier

I KORTHET

Underlaget motiverar beredskap för identitetsmissbruk, följder av leverantörers uppgiftsförlust, utpressning och störningar i uppkopplad verksamhet. Det fastställer ingen nationell angreppssannolikhet eller gemensam operatör bakom de redovisade händelserna. Scenarierna beskriver beslut om vissa signaler uppträder. Ge varje signal en ansvarig, behåll alternativa förklaringar och ändra bedömningen när organisationens belägg förändras.

11.1 Huvudbedömningar och begränsningar

Bedömningarna gäller enskilda slutsatser, inte en allmän säkerhetsnivå för Sverige eller en aktör.

Bedömning	Säkerhet och grund	Begränsning	Beslut
Leverantörsåtkomst och leverantörslagrade uppgifter kan kräva insatser hos flera kunder	Hög för dokumenterade fall i kapitel 5	Olika leverantörer och omfattning; ingen gemensam kampanj fastställd	Öva uppdatering och anmälan med kritiska leverantörer
Identitetsmissbruk kan göra en känd avsändare till en nätfiskeväg	Hög för redovisade e-postfall och CERT-SE:s varning	Rapporten mäter inte allt lyckat nätfiske eller varje drabbat konto	Kontrollera inloggningar, sessioner och meddelandespår tillsammans
Utpressningsberedskap är motiverad i flera sektorer	Hög säkerhet att 62 Sverigemärkta publiceringar observerades [S2]	Publiceringar är påståenden; etiketter och återkommande organisationer begränsar geografi och unikhet	Visa återställning och en beslutsprocess för påstådd datastöld
Uppkopplad utrustning behöver en operativt ansvarig	Hög för officiella kylvarningar	Varken nationell påverkan eller gemensam operatör fastställd	Kontrollera exponering och säker lokal styrning med drift och leverantörer
Publiceringsvolym kan inte förutsäga framtida lyckade angrepp	Hög säkerhet i denna underlagsbegränsning	Synlighet och upprepad annonsering påverkar materialet	Välj begränsning utifrån verifierade belägg om egna tillgångar

Ett säkert bekräftat händelseförlopp kan ändå lämna intrångsväg, aktör och omfattning oklara. För över dessa oklarheter till incidentjournalen. Gör inte en försiktig fallbeskrivning till en starkare rubrik eller ledningsslutsats.

11.2 Fyra planeringsantaganden

Scenario A: relevanta inloggningsuppgifter upptäcks

Om ett aktuellt eget konto verifieras, granska inloggningar och behörigheter, återkalla relevanta sessioner och byt berörda hemligheter. Om posten är äldre och redan åtgärdad, dokumentera det. Inget av utfallen ska utläsas ur säljarens formulering.

Scenario B: en leverantör ändrar omfattningen

Om nya bekräftade kategorier gäller resor, hälsa, barn eller skyddade kontaktuppgifter, bedöm på nytt risk och informationsbehov. Om bara ett äldre offentligt utdrag matchar, begränsa bedömningen. Behåll leverantörens successiva besked i stället för att skriva över det första.

Scenario C: en operativ styrenhet beter sig oväntat

Om lokala loggar bekräftar ändrade inställningar eller förlorad säker styrning, aktivera teknisk isolering och beslutad reservdrift. Om problemet är ett kommunikationsavbrott utan belägg för manipulation, behåll den skillnaden. En skärmbild eller ett politiskt påstående fastställer inte det fysiska utfallet.

Scenario D: en offentlig tjänst utsätts för ett tillgänglighetspåstående

Om övervakningen bekräftar störning, aktivera skydd hos nätleverantören och bevara drifttidslinjen. Om ingen tjänstepåverkan syns, behåll påståendet som obekräftat. Kommunikationen bör ange uppmätt tjänstepåverkan och nästa uppdatering, utan att återge fientlig retorik.

11.3 Vad som skulle ändra bedömningen

Verifierad obehörig användning av ett eget konto skulle belägga en identitetsincident. En verifierad leverantörsrapport med berörda system och uppgifter skulle precisera kundpåverkan. En teknisk utredning med konkreta infrastruktur- eller åtkomstsamband skulle kunna stödja ett kampanjsamband.

Verifierade äldre uppgifter, en rättad landsetikett eller en avfärdad systemkoppling skulle i stället begränsa slutsatsen. Sådana ändringar är en normal del av analysen. De kräver inte att det ursprungliga obekräftade påståendet förklaras sant eller påhittat.

Avsnittet om den senaste aktiviteten lyfter publicering och besked under 8–22 november. Det skapar ingen jämförbar tillväxtmätning mellan perioder. Besked efter slutdatumet hör till en senare uppdatering även om de gäller äldre aktivitet.

VIKTIGA SLUTSATSER

01

Knyt bedömningssäkerheten till en slutsats och behåll dess oklarheter.

02

Begränsa åtkomst när egna belägg har verifierats.

03

Uppdatera scenarier när omfattning eller attribuering ändras och behåll tidigare besked.

KAPITEL 12

Åtgärdsplan och belägg för genomförande

12

DETTA KAPITEL BESVARAR

Vem agerar, under vilka villkor och hur visas genomförandet?

30 / 60 / 90

kontrollpunkter; brådskande begränsning börjar direkt

12.1 Omedelbara åtgärder och kontrollpunkter 77

12.2 Frågor för varje roll 79

12.3 Så kan Brandefense hjälpa 80

KAPITEL 12

Åtgärdsplan och belägg för genomförande

I KORTHET

Börja direkt med brådskande verifiering, begränsning och tillämpliga säkerhetsuppdateringar. Kontrollpunkterna nedan är inte ett skäl att lämna en känd kritisk exponering öppen. Ge varje prioriterad tjänst en teknisk ansvarig och en verksamhetsansvarig. Genomförande kräver belägg för att kontot, beroendet eller återställningsvägen fungerar som avsett. Kvarstående risker ska uttryckligen accepteras och dateras.

12.1 Omedelbara åtgärder och kontrollpunkter

Åtgärderna kopplar underlag till en ansvarig. Använd villkoren för att undvika ingripande åtgärder som bara bygger på en annons.

1Direkt		
Bekräfta behöriga larmkällor, bevakade tillgångar, mottagare och eskalering; testa ett syntetiskt larm innan överlämningen används	ANSVARIG Säkerhetschef, SOC och identitetsansvarig	BELÄGG FÖR GENOMFÖRANDE Larm mottaget, kvitterat och vidarebefordrat; saknad täckning har ägare
Prioritera nätfiskeresistent autentisering för privilegierad åtkomst och högriskåtkomst; testa säker återställning och sessionsåterkallelse	ANSVARIG Identitets- och tjänsteägare	BELÄGG FÖR GENOMFÖRANDE Godkänd inloggnings- och återställningsövning; obehöriga sessioner förlorar åtkomst
Verifiera ett relevant aktuellt kontolarm; begränsa bekräftad åtkomst och återkalla tillhörande sessioner	ANSVARIG Identitetsansvarig och incidentledare	BELÄGG FÖR GENOMFÖRANDE Kontobeslut, inloggningsgranskning och dokumenterad återkallelse
Identifiera tillämpliga kritiska eller aktivt utnyttjade brister; uppdatera tjänster eller följ godkänd isoleringsplan	ANSVARIG Applikations- och infrastrukturägare	BELÄGG FÖR GENOMFÖRANDE Belägg för installerad version och separat tjänstekontroll

Kontrollera styrenheters internetexponering och säker isolering

ANSVARIG

Teknik och fastighetsdrift

BELÄGG FÖR GENOMFÖRANDE

Godkänd anslutningsinventering, åtkomstgranskning och testad lokal styrning

2Senast dag 30

Stäm av privilegierade konton, tjänstekonton och leverantörskonton mot ansvariga ägare

ANSVARIG

Identitet och inköp

BELÄGG FÖR GENOMFÖRANDE

Granskade ägare, rättigheter och giltighetstider; ägarlös åtkomst borttagen

Bekräfta tillämpning, mottagare, kännedomstidpunkt och reservåtkomst till rapporteringsportaler

ANSVARIG

Juridik, dataskydd och regelefterlevnad

BELÄGG FÖR GENOMFÖRANDE

Beslutsunderlag per juridisk person och genomförd rapporteringsövning

Granska avsändardomäner, legitima e-postflöden och autentiseringspolicyer

ANSVARIG

E-postansvariga

BELÄGG FÖR GENOMFÖRANDE

Verifierad inventering, observationer om överensstämmelse och godkänd rättning

3Senast dag 60

Återställ en prioriterad tjänst isolerat, med identitets- och leverantörsberoenden

ANSVARIG

Tjänsteägare och återställningsansvarig

BELÄGG FÖR GENOMFÖRANDE

Godkänd återställningstid och accepterad dataförlust jämförd med uppmätt återställning och avstämning; reservdrift testad

Öva ett ändrat leverantörsbesked som gäller kund- eller personaluppgifter

ANSVARIG

Inköp, dataskydd och kundverksamhet

BELÄGG FÖR GENOMFÖRANDE

Tidsatt leverantörskontakt, kategorispecifik riskbedömning och godkänt informationsutkast

Öva tillgänglighetsincident utan att anta datastöld

ANSVARIG

Nätverk och kommunikation

BELÄGG FÖR GENOMFÖRANDE

Aktiverat skydd, uppmätt tjänstetidslinje och tydliga lägesbesked

4Senast dag 90

Testa kvarstående skydd igen och avsluta eller acceptera varje risk uttryckligen

ANSVARIG

Säkerhetschef och verksamhetsledning

BELÄGG FÖR GENOMFÖRANDE

Daterat beslut med kvarstående risk, ägare och nästa kontroll

Öva incident i uppkopplad utrustning med teknik och leverantörer

ANSVARIG

Fastighetsdrift, teknik och säkerhet

BELÄGG FÖR GENOMFÖRANDE

Visat säkert läge, bevarade inställningar och testat återställningsmandat

Kontrollera kundstödets motstånd mot förfrågningar med äkta stulna detaljer

ANSVARIG

Bedrägeriförebyggande och kundverksamhet

BELÄGG FÖR GENOMFÖRANDE

Godkända övningsresultat och oberoende kontroll av betydelsefulla ändringar

En misslyckad övning ger användbara belägg om den leder till en ansvarig rättning. Markera inte ett skydd som färdigt för att en policy finns eller en leverantör har svarat. Visa det beteende som behövs under incidenten.

Om behörig larmväg saknas bör säkerhetschefen ordna en intern väg eller lämplig leverantörsväg och markera beroende kontroll som otillgänglig tills överlämningen fungerar. Fortsätt direkt med trovärdiga belägg som redan kommit in. Testa återställning med ett godkänt imitationsscenario och en riktig användare som förlorat en faktor.

12.2 Frågor för varje roll

Styrelse och ledning. Vilken tjänst måste fortsätta, vilken minsta drift är godtagbar och vem får godkänna tillfälliga begränsningar? Begär senaste uppmätta återställningsresultat och den äldsta olösta beroenderisken. Ett enda portföljvärde besvarar inte frågorna.

SOC och identitetsteam. Kan ett larm knytas till ett eget konto, giltig åtkomst, aktuella sessioner eller observerade obehöriga ändringar? Behåll skillnaden mellan äldre inloggningsuppgifter och aktuell åtkomst. Ha en tydlig väg till ansvariga för klienter, molntjänster och e-post.

Teknik och fastighetsdrift. Vem kan ändra styrenheten, vem märker oväntade inställningar och vem kan återställa säker lokal drift? Testa frågorna med underhållsleverantören. Säkerhetsbeslut ska ligga hos behörig driftpersonal.

Dataskydd och juridik. Vilka människor och uppgiftskategorier kan beröras, när uppstod kännedom och vilka fakta saknas? Spara varje rapporteringsbeslut och senare ändring. Ett tekniskt återställningsbesked avslutar inte personuppgiftsbedömningen.

Inköp och leverantörsstyrning. Kan leverantören ange berörd kundmiljö, uppgiftskopia och supportkonto? Kräv skyndsamma omfattningsbesked, bevarande av belägg och en kontaktväg för kunder. Skilj allmänna leverantörsbesked från en bedömning av den egna tjänsten.

Bedrägeriförebyggande och kundverksamhet. Vilka förfrågningar blir trovärdigare om någon känner till riktiga bokningar, fakturor eller anställningsuppgifter? Kontrollera betydelsefulla ändringar genom en etablerad oberoende väg. Kända uppgifter ger sammanhang men ska inte ge behörighet.

12.3 Så kan Brandefense hjälpa

Brandefense kan stödja granskning av relevant hotinformation, extern exponering och observationer om identitets- och varumärkesmissbruk. Kom överens om bevakade varumärken, tillgångar, larmmottagare och verifieringsprocess innan ett fynd behandlas som en incident.

Använd rapportens skillnader mellan underlagstyper när en tjänst diskuteras: inlägg visar publicering, utpressningspubliceringar visar påståenden och exponeringsobservationer kräver tillgångsägarens kontroll. Ett tjänsteavtal ersätter inte intern utredning, operativ bedömning eller rättslig prövning.

Boka en Brandefense-demo för att diskutera tillgångar, beslut och åtgärdsbelägg som är relevanta för organisationen.

VIKTIGA SLUTSATSER

01

Börja brådskande begränsning och säkerhetsuppdatering nu och verifiera vid kontrollpunkterna.

02

Kräv uppmätta belägg från både tekniska ansvariga och verksamhetsägare.

03

Avsluta tjänste-, identitets- och personrelaterade följder separat.

BILAGOR

Bilagor

A–D

DETTA KAPITEL BESVARAR

Bilaga A. Omfattning och underlagets gränser · Bilaga B. Underlagsregister · Bilaga C. Källor · Bilaga D. Ordlista

80

källor

Bilaga A. Omfattning och underlagets gränser 82

Bilaga B. Underlagsregister 85

Bilaga C. Källor 86

Bilaga D. Ordlista 90

Bilaga A. Omfattning och underlagets gränser

Jämförelseländerna har valts som exempel enbart för att ge sammanhang; de innebär ingen rangordning eller politisk bedömning.

A.1 Period och källtyper

Publiceringsperioden är 1 januari–22 november 2026 efter inläggets tid, med 8–22 november särskilt belyst. Offentliga källor kontrollerades den 22–23 november 2026. Publiceringsantal och aktuellt material kontrollerades den 23 november, efter UTC-sluttiden. Besked kan gälla äldre händelser och dessa datum behålls uttryckligen.

Källorna omfattar inlägg från kriminella miljöer insamlade av Odin by Brandefense, utpressningspubliceringar, Atlas-exponeringsobservationer för utvalda domäner, en konfigurationsbild, organisationsbesked, myndighetsråd, tillsynsbeslut och medierapportering. Varje källa fastställer bara sin egen slutsats. [S1][S2][S3][S4]

A.2 Inlägg och observerad volym

Den observerade landanknutna gruppen är 775 020 inlägg. Januari och februari innehåller tillsammans 727 150, eller 93,8 %. Publiceringskoncentration mäter inte lyckade angrepp. Upprepad marknadsföring och internationellt material kan förekomma i landanknutna observationer. November är ofullständig. [S1]

Det bevarade underlaget är smalare än publiceringsgruppen. Det stödjer citerade utdrag och påståendebedömningar, inte en fullständig kartläggning av allt publicerat material. Visst källinnehåll saknas. Inga nationella brottsandelar, unika personantal eller uppskattningar av genomförda affärer härleds.

A.3 Utvalda organisationer och konfigurationsobservationer

Portföljen består av 250 kandidatdomäner i tio sektorsgrupper om 25. Urvalet är ändamålsenligt och ägarskap och oberoende är inte verifierade. Resultaten skattar inte förekomst i hela Sverige. E-postpolicy, certifikat och HSTS-observationer behåller sina bedömda nämnare. [S3]

En publicerad SPF- eller DKIM-relaterad post bevisar inte korrekt leverans. DNSSEC-delegation innebär inte fullständig validering. TLS- och HSTS-observationer fastställer inte fullständig täckning eller skyddseffekt. Okända resultat är inte fel och misslyckad validering kräver ägarens utredning innan orsak anges.

A.4 Exponering och betyg

Nationellt Atlas-huvudvärde är 50/100 för 242 bedömda domäner i den utvalda portföljen på 250 domäner. Övriga 8 domäner har okänd exponering. Sektor- och gruppbetyg för exponering publiceras inte. Kumulativa enhets-, inloggnings- och dokumentkopplingar samt aktuella annonser kräver tillgångsägarens kontroll. [S4]

A.5 Utpressningspubliceringar

De 62 Sverige-märkta publiceringarna är offentliga kriminella påståenden i Ransompedia, inte bekräftade intrång eller unika organisationer. Återkommande organisationer och gränsöverskridande etiketter begränsar tolkningen. Föregående års antal gäller helår; perioden 2026 är ofullständig. [S2]

A.6 Kortmaterialets omfattning

KORTUPPGIFTERNAS OMFATTNING

Antalen beskriver en begränsad grupp observerade publiceringar. De skattar inte svensk kortstöld, bedrägeriförluster eller betalningsgiltighet.

De 132 olika Sverige-märkta posterna, med 141 förekomster i 135 inlägg, fastställer inte faktisk utgivning, stöldstatus eller en namngiven bank. De är skilda från flygbolagets externt rapporterade betalningssidegrupp och kan inte läggas till den. [S1][S40]

A.7 Offentliga incidenter, äldre händelser och undantag

Femton offentliga fall och sju påståendefall illustrerar underbyggda beslut. En leverantörsincident kan ge flera personuppgiftsanmälningar. En uppdatering kan ändra tidigare omfattning. Rapporten presenterar därför inget nationellt incidentantal utan dubbelräkning.

Det offentliga registret innehåller också kampanjråd och uttryckliga undantag. Ett utländskt dotterbolagsbesked om en händelse 2025 fastställer inget svenskt intrång 2026. Ett tekniskt avbrott inom offentlig transportverksamhet, ett vårdsystemavbrott och en kommunal omsorgsstörning saknar fastställd skadlig orsak i källorna. [S48][S49][S50][S51]

IMY fattade under 2026 tillsynsbeslut om tidigare angrepp. Det är tillsynsutfall, inte nya intrång 2026. [S37][S36]

Ytterligare ett besöksbiljettbesked behålls som kvalificerat sammanhang; originalsidan var otillgänglig och den officiella sökpassagen verifierar inte självständigt en ny leverantörsincident. En regional bussoperatörs styrelseprotokoll beskriver manuell reservdrift och anger att passagerartrafiken inte påverkades. [S46][S47]

A.8 Bedömningssäkerhet och namn

Säkerheten gäller en slutsats. Ett erbjudande kan vara säkert observerat medan innehavet är obekräftat. Ett offer namnges bara när officiell bekräftelse och bred rapportering uppfyller namnregeln. Övriga fall använder roller som passar flera organisationer.

När en källadress identifierar en utelämnad organisation kan pressens eller en officiell utgivares rotadress visas med markering om utelämnad artikeladress. Den utelämnade organisationens egen domän skrivs inte ut; den offentliga adressen lämnas tom. Tillgänglighetsgränser behålls utan falska verifieringspåståenden.

Bilaga B. Underlagsregister

Autentiska utdrag visas i texten. Inläggsdatum beskriver publicering; inget kort fastställer ensamt en genomförd affär eller ett bekräftat intrång.

Kort	Datum	Plats	Alias	Språk	Avsnitt
B01	2026-01-30	Forumtråd	Alias utelämnat	Engelska	4
B02	2026-02-15	Forumtråd	Alias utelämnat	Engelska	4
B03	2026-03-31	Forumtråd	Alias utelämnat	Engelska	9
B04	2026-04-23	Forumtråd	Alias utelämnat	Engelska	4
B05	2026-09-05	Forumtråd	Alias utelämnat	Engelska	4
B06	2026-11-18	Forumtråd	Alias utelämnat	Engelska	4
B07	2026-11-19	Forumtråd	Alias utelämnat	Engelska	4
B08	2026-05-24	Forumtråd	Alias utelämnat	Ryska	8
B09	2026-04-08	Forumtråd	Alias utelämnat	Engelska	4
B10	2026-04-30	Vidareförmedlat foruminlägg	Alias utelämnat	Engelska	4
B11	2026-03-08	Forumtråd	Alias utelämnat	Engelska	4
B12	2026-11-07	Forumtråd	Alias utelämnat	Engelska	8
B13	2026-11-17	Forumtråd	Alias utelämnat	Engelska	4
B14	2026-11-09	Forumtråd	Alias utelämnat	Engelska	4
B15	2026-04-22	Forumtråd	Alias utelämnat	Spanska	6
B16	2026-04-14	Forumtråd	Alias utelämnat	Engelska	4

Bilaga C. Källor

S1: Odin by Brandefense. Bevarade observationer från kriminella miljöer och publiceringsantal. Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-23.

S2: Ransompedia. Landmärkta utpressningspubliceringar för rapportperioden. Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S3: Odin by Brandefense. Konfigurationsbild för 250 utvalda domäner. Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S4: Brandefense Atlas exponeringsobservationer, 22 november 2026; nationellt värde för 242 bedömda utvalda domäner, slutfört 22 november 2026. Egna data; domännamn utelämnas.

S5: NCSC. Uppdrag och verksamhetsöverföring i juli 2026. https://www.ncsc.se/sv/om-centret/ Kontrollerad den 2026-11-22.

S6: Myndigheten för civilt försvar. MSB blev Myndigheten för civilt försvar. https://www.mcf.se/sv/om-oss/vart-uppdrag/msb-ar-myndigheten-for-civilt-forsvar/ Kontrollerad den 2026-11-22.

S7: Sveriges Riksbank. Betalningsrapport 2026: sammanfattning och rekommendationer. https://www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-report-2026/summary-and-recommendations/ Kontrollerad den 2026-11-22.

S8: Sveriges riksdag. Cybersäkerhetslag (2025:1506). https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/cybersakerhetslag-20251506_sfs-2025-1506/ Kontrollerad den 2026-11-22.

S9: PTS. Incidentrapportering enligt cybersäkerhetslagen. https://www.pts.se/sakerhet-och-integritet/cybersakerhetslagen/incidentrapportera-enligt-cybersakerhetslagen/ Kontrollerad den 2026-11-22.

S10: IMY. Hantering av personuppgiftsincidenter. https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/personuppgiftsincidenter/hantering-av-personuppgiftsincidenter/ Kontrollerad den 2026-11-22.

S11: EUR-Lex. Delegerad förordning (EU) 2025/301, artikel 5. https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng Kontrollerad den 2026-11-23.

S12: Finansinspektionen. Vägledning för incidentrapportering enligt DORA, 14 oktober 2026. https://www.fi.se/globalassets/media/dokument/lathundar//lathund_dora_incidentrapportering_2026-10-14.pdf Kontrollerad den 2026-11-22.

S13: CERT-SE. Kritiska PHP-sårbarheter, uppdaterad 27 oktober 2026. https://cert.se/2026/10/kritiska-s%C3%A5rbarheter-i-php.html Kontrollerad den 2026-11-22.

S14: PHP-projektet. Säkerhetsversioner och tillverkarråd, arkiv för 2026. https://www.php.net/archive/2026.php Kontrollerad den 2026-11-22.

S15: NVD. CVE-2026-109618. https://nvd.nist.gov/vuln/detail/CVE-2026-109618 Kontrollerad den 2026-11-22.

S16: NVD. CVE-2026-109619. https://nvd.nist.gov/vuln/detail/CVE-2026-109619 Kontrollerad den 2026-11-22.

S17: NCSC. Europeisk varning om kylsystem, 5 november 2026. https://www.ncsc.se/sv/aktuellt/eu-varnar-for-cyberincidenter/ Kontrollerad den 2026-11-22.

S18: Officiellt organisationsbesked. Nätfiske mot e-postkonton (en regional vårdmyndighet). https://www.regionvarmland.se/regionvarmland/nyhetsarkiv/press/2026-03-05-region-varmland-drabbat-av-personuppgiftsincident Kontrollerad den 2026-11-22.

S19: Organisationsbesked; identitet utelämnad. Intrång som berört interna dokument (en organisation). Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S20: Organisationsbesked; identitet utelämnad. IT-angrepp och tjänstestörning (kommunal verksamhet). Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S21: www.imy.se. Datastöld hos leverantör (högskolekunder på en gemensam lärplattform). https://www.imy.se/nyheter/dataintrang-mot-laroplattformen-canvas/ Kontrollerad den 2026-11-22.

S22: Officiellt organisationsbesked. Stöld av kunduppgifter (en mikromobilitetsleverantör verksam i Sverige). https://www.ryde-technology.com/security-incident-2026-08-02 Kontrollerad den 2026-11-22.

S23: Organisationsbesked; identitet utelämnad. Åtkomst till interna system och skyddsavstängning (en IT-tjänsteleverantör). Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S24: Organisationsbesked; identitet utelämnad. IT-intrång och stöld av känsliga personaluppgifter (en kommun). Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S25: www.ncsc.se. Manipulation av kylsystem (livsmedelsbutiker och livsmedelsdistribution). https://www.ncsc.se/sv/aktuellt/cyberangrepp-mot-kylsystem/ Kontrollerad den 2026-11-22.

S26: www.svt.se. Åtkomst till bokningsuppgifter (ett flygbolag med extern bokningsplattform). https://www.svt.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-22.

S27: www.svt.se. Intrång och produktionsstopp (en tillverkare). https://www.svt.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-22.

S28: Officiellt organisationsbesked. Åtkomst till kunduppgifter i avgränsade system (en skönhetsåterförsäljare). https://lyko.com/no/om-lyko/media/pressemeldinger/lyko-har-atgardat-dataintrang-i-en-avgransad-del-av-sitt-system Kontrollerad den 2026-11-22.

S29: Officiellt organisationsbesked. Åtkomst till bokningsuppgifter hos leverantör (en taxitjänst med extern bokningsleverantör). https://www.cabonline.se/it-incident Kontrollerad den 2026-11-22.

S30: Officiellt organisationsbesked. Stöld av besökaruppgifter hos leverantör (ett besöksmål med extern bokningsleverantör). https://newsroom.notified.com/news/457193/personuppgiftsincident Kontrollerad den 2026-11-22.

S31: Officiellt organisationsbesked. Intrång i extern webbmiljö (en hotell- och mässaktör). https://svenskamassan.se/2026/11/information-om-dataintrang-hos-svenska-massan-gothia-towers/ Kontrollerad den 2026-11-24.

S32: Organisationsbesked; identitet utelämnad. Nätfiske från personalens e-postkonto (en regional vårdmyndighet). Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S33: www.cert.se. Varning för nätfiskekampanj (svenska organisationer i flera sektorer). https://www.cert.se/2026/11/uppmanar-till-okad-vaksamhet-natfiske.html Kontrollerad den 2026-11-22.

S34: polisen.se. Sms-nätfiske med falska trafikböter (allmänheten). https://polisen.se/aktuellt/nyheter/nationell/2026/april/pagaende-vag-av-bedrageriforsok-via-sms/ Kontrollerad den 2026-11-22.

S35: polisen.se. Social manipulation från sms till telefonsamtal (allmänheten). https://polisen.se/aktuellt/nyheter/mitt/2026/januari/polisen-i-region-mitt-varnar-for-ett-nytt-bedragerimodus/ Kontrollerad den 2026-11-22.

S36: www.imy.se. Tillsynsbeslut efter ett angrepp tidigare år. https://www.imy.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-22.

S37: www.imy.se. Tillsynsbeslut efter ett angrepp tidigare år. https://www.imy.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-22.

S38: apnews.com. Attribuering av föregående års misslyckade förstöringsförsök (en värmeoperatör). https://apnews.com/ (artikeladressen utelämnad) Kontrollerad den 2026-11-22.

S39: www.ncsc.se. Officiell bedömning efter valet (valadministration). https://www.ncsc.se/sv/aktuellt/inga-storre-informations--eller-cyberangrepp-mot-svenska-valet/ Kontrollerad den 2026-11-22.

S40: www.svt.se. Exponering av betalningsuppgifter på leverantörswebbplats (svenska kunder hos ett flygbolag). https://www.svt.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-22.

S41: www.aftonbladet.se. Missbruk av bokningar under polisutredning (en järnvägsoperatör). https://www.aftonbladet.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-22.

S42: www.ncsc.se. Nätfiske med myndighetsimitation (mottagare av falska myndighetsvarningar). https://www.ncsc.se/sv/aktuellt/nationellt-cybersakerhetscenters-namn-anvands-i-natfiskekampanj/ Kontrollerad den 2026-11-22.

S43: www.ncsc.se. Internationellt kampanjråd (användare av sårbar webbmejl). https://www.ncsc.se/sv/aktuellt/co-seal-med-nsa-om-zimbra/ Kontrollerad den 2026-11-22.

S44: www.ncsc.se. Internationellt kampanjråd (nätverksoperatörer inom kritisk infrastruktur). https://www.ncsc.se/sv/aktuellt/nya-internationella-rad-mot-cyberangrepp-pa-sarbar-natverksutrustning/ Kontrollerad den 2026-11-24.

S45: www.ncsc.se. Internationellt kampanjråd (organisationer med anslutna kantnätverksenheter). https://www.ncsc.se/sv/aktuellt/nya-internationella-rad-for-att-forsvara-sig-mot-dolda-natverk-med-kopplingar-till-kina2/ Kontrollerad den 2026-11-22.

S46: Organisationsbesked; identitet utelämnad. Åtkomst till bokningsuppgifter hos leverantör (besöksmål med gemensam biljettleverantör). Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S47: Organisationsbesked; identitet utelämnad. IT-nedstängning med manuell fortsatt drift (en regional bussoperatör). Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S48: www.maine.gov. Anmälan om föregående års leverantörsintrång (ett utländskt dotterbolag till ett företag med huvudkontor i Sverige). https://www.maine.gov/ (artikeladressen utelämnad) Kontrollerad den 2026-11-22.

S49: www.cert.se. Tekniskt avbrott (ett offentligt organ inom transportsektorn). https://www.cert.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-24.

S50: www.cert.se. Tekniskt avbrott hos leverantör (regionala vårdorganisationer). https://www.cert.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-24.

S51: www.cert.se. IT-störning (en kommun med hemtjänst). https://www.cert.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-24.

S52: polisen.se. Falsk leverantörs- eller kundidentitet (svenska företag). https://polisen.se/aktuellt/nyheter/syd/2026/september/fler-bedragerier-mot-foretag--polisen-varnar-for-metoden/ Kontrollerad den 2026-11-22.

S53: www.svt.se. Nätfiske mot e-postkonton (en regional vårdmyndighet). https://www.svt.se/nyheter/lokalt/varmland/natfiskeattack-mot-region-varmland-personuppgifter-har-lackt Kontrollerad den 2026-11-22.

S54: www.svt.se. Intrång (en IT-tjänsteleverantör). https://www.svt.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-22.

S55: Organisationsbesked; identitet utelämnad. Intrång som berört interna dokument (en organisation). Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S56: www.cert.se. IT-angrepp och tjänstestörning (kommunal verksamhet). https://www.cert.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-24.

S57: www.cert.se. Datastöld hos leverantör (högskolekunder på en gemensam lärplattform). https://www.cert.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-24.

S58: www.cert.se. Vidareförmedlat nätfiske från e-postkonto (en offentlig organisation). https://www.cert.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-24.

S59: www.cert.se. Ransomware och stulna personaluppgifter (ett tjänsteföretag). https://www.cert.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-24.

S60: www.svt.se. Stöld av kunduppgifter (en mikromobilitetsleverantör verksam i Sverige). https://www.svt.se/nyheter/lokalt/norrbotten/ryde-utsatt-for-dataintrang-alla-kunder-drabbade Kontrollerad den 2026-11-22.

S61: techtidningen.se. Åtkomst till interna system och skyddsavstängning (en IT-tjänsteleverantör). https://techtidningen.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-22.

S62: Organisationsbesked; identitet utelämnad. IT-intrång och stöld av känsliga personaluppgifter (en kommun). Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S63: www.cert.se. Åtkomst till bokningsuppgifter (ett flygbolag med extern bokningsplattform). https://www.cert.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-24.

S64: www.cert.se. Intrång och produktionsstopp (en tillverkare). https://www.cert.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-24.

S65: www.aftonbladet.se. Åtkomst till kunduppgifter i avgränsade system (en skönhetsåterförsäljare). https://www.aftonbladet.se/minekonomi/a/kMJBkk/lyko-hackat-kunduppgifter-lackta Kontrollerad den 2026-11-24.

S66: www.svt.se. Åtkomst till bokningsuppgifter hos leverantör (en taxitjänst med extern bokningsleverantör). https://www.svt.se/nyheter/inrikes/taxikunder-drabbade-av-dataintrang-bokningsuppgifter-kan-ha-lackt Kontrollerad den 2026-11-22.

S67: www.svt.se. Stöld av besökaruppgifter hos leverantör (ett besöksmål med extern bokningsleverantör). https://www.svt.se/nyheter/lokalt/vast/dataintrang-hos-universeum-varnar-for-bedrageriforsok Kontrollerad den 2026-11-22.

S68: www.svt.se. Intrång i extern webbmiljö (en hotell- och mässaktör). https://www.svt.se/nyheter/lokalt/vast/dataintrang-mot-gothia-towers Kontrollerad den 2026-11-22.

S69: www.cert.se. Datastöld hos leverantör (högskolekunder på en gemensam lärplattform). https://www.cert.se/ (artikeladressen utelämnad) Kontrollerad den 2026-11-24.

S70: Besked från kund inom offentlig service; identitet utelämnad. Åtkomst till bokningsuppgifter hos leverantör (en taxitjänst med extern bokningsleverantör). Adress utelämnad; källmappning bevarad. Kontrollerad den 2026-11-22.

S71: Polismyndigheten. Varning för leveransförevändningar och bankimitation. https://polisen.se/aktuellt/nyheter/nord/2026/november/bedragare-kontaktar-aldre-om-falska-mobelleveranser/ Kontrollerad den 2026-11-22.

S72: Polismyndigheten. Utredning av imitation med betalkort som förevändning. https://polisen.se/aktuellt/nyheter/stockholm/2026/november/man-haktad-misstankt-for-tio-fall-av-grova-bedragerier-pa-gotland/ Kontrollerad den 2026-11-22.

S73: RFC Editor. Protokollreferens för DMARC. https://www.rfc-editor.org/rfc/rfc7489.html Kontrollerad den 2026-11-22.

S74: RFC Editor. Protokollreferens för SPF. https://www.rfc-editor.org/rfc/rfc7208.html Kontrollerad den 2026-11-22.

S75: RFC Editor. DKIM-signaturer. https://www.rfc-editor.org/rfc/rfc6376.html Kontrollerad den 2026-11-22.

S76: RFC Editor. HTTP Strict Transport Security. https://www.rfc-editor.org/rfc/rfc6797.html Kontrollerad den 2026-11-22.

S77: SVT. Svenska högskoleanvändare berörda av Canvas-incidenten. https://www.svt.se/nyheter/inrikes/flera-svenska-universitet-drabbade-i-hackerattack Kontrollerad den 2026-11-22.

S78: QiAnXin XLab. AryStinger-forskning, 17 juni 2026. https://blog.xlab.qianxin.com/arystinger-botnet-hijacks-legacy-routers-for-global-attacks-en/ Kontrollerad den 2026-11-24.

S79: Trezor. Nya kunduppgifter röjda i incident hos fraktleverantör; uppdaterad 4 september 2026. https://trezor.io/blog/news/recent-customer-data-exposed-in-shipping-provider-incident Kontrollerad den 2026-11-22.

S80: Protos. Trezor uppger att 13 689 kunder drabbats av dataintrång hos fraktpartner, 13 augusti 2026. https://protos.com/trezor-says-13689-customers-hit-by-data-breach-at-shipping-partner/ Kontrollerad den 2026-11-22.

Bilaga D. Ordlista

- **CSIRT.** Ett incidenthanteringsteam som stödjer förebyggande arbete och hantering av IT-incidenter. [S5]
- **DMARC.** En domänpolicy för hantering och rapportering av e-post som inte klarar samordnade autentiseringskontroller. [S73]
- **SPF.** En mekanism där en domän anger godkända avsändarservrar. [S74]
- **DKIM.** En kryptografisk e-postsignatur som knyter en signerande domän till ett meddelande. [S75]
- **HSTS.** En webbläsarpolicy som kräver säkra anslutningar till den angivna webbplatsen. [S76]
- **DORA.** EU:s ram för digital operativ motståndskraft hos finansiella entiteter som omfattas. [S11]
- **GDPR.** EU:s dataskyddsförordning; incidentkraven beror på fakta och risk. [S10]
- **NCSC / CERT-SE.** Sveriges nationella cybersäkerhetscenter och nationella incidentfunktion; organisatoriska datum skiljs åt i kapitel 2.
- **Personnummer / VIN.** Svenskt personnummer respektive fordonsidentifieringsnummer; kännedom om något av dem autentiserar inte en förfrågan.
- **Personuppgiftsansvarig / personuppgiftsbiträde.** Den som bestämmer behandlingens ändamål och medel respektive den som behandlar uppgifter för dennes räkning; ansvar kräver bedömning av fallet.
- **DNSSEC / DS.** Signerad DNS-information och en delegationspost; förekomst fastställer inte fullständig validering.
- **TLS.** Teknik som skyddar en anslutning.
- **Nätfiskeresistent MFA.** Autentisering som motverkar vidareförmedling via en falsk tjänst; vanlig kod- eller nummerbekräftelse är inte automatiskt motståndskraftig.
- **KYC.** Kundkännedomskontroller; annonserat kringgående förblir ett förmågepåstående tills det verifieras.
- **Session.** Fortsatt autentiserad åtkomst som kan behöva återkallas separat från lösenordsbyte.
- **Inlägg / publicering / anmälan.** Ett meddelande, ett offentligt utpressningspåstående och en myndighetsanmälan; de är olika räkneenheter.
- **Nationellt Atlas-huvudvärde.** Ett exponeringsvärde för den bedömda portföljen; varken andel intrång eller incidentsannolikhet.
- **Analysmodell.** En föreslagen förklaring eller planeringsrelation som inte är en observerad affärskedja.
- **TLP:CLEAR.** Delbart utan TLP-begränsning; dataskydd och andra skyldigheter gäller fortfarande.

Om rapporten

Framtagen av Odin by Brandefense. Version 1.0 gäller perioden till 22 november 2026 och lyfter 8–22 november separat. Uppföljningen av egna data slutfördes den 23 november. Underlagstyper, källdatum och kvarstående oklarheter följer slutsatserna. Detta är ingen nationell kartläggning eller försäkran om en organisations fullständiga säkerhetsläge.

Den svenska utgåvan översätter den engelska huvudtexten; vid skillnader gäller den engelska utgåvan. Råden behöver kontrolleras mot läsarens egna tillgångar, tjänstekrav och rättsliga skyldigheter.

© 2026 Brandefense. Alla rättigheter förbehållna.

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