

Gir KI flere dataangrep?

Ja, men ingen kan ennå måle hvor mye. Angrepene mot virksomheter har økt kraftig i 2026, og i de dokumenterte sakene gjør KI dem billigere og raskere. Statistikken skiller likevel ikke ut hvor stor del av økningen KI står for. Denne rapporten viser tallene, metoden og vurderingene bak.

TALL OG KILDER PER 26. OKTOBER 2026
AMUND STRANDÅ KRISTIANSEN • SPADECONSULTING.NO



Hovedfunn

- | | | |
|-------|--|---|
| 01 | Antallet ofre har økt kraftig i 2026.
Løsepengegruppene hengte ut 36 prosent flere virksomheter enn i samme periode i fjor, delvis fordi sommeren 2025 var svak. I august var antallet mer enn doblet. | 8 637
<small>ofre på lekkasjesider 1.1.–25.10.
2025: 6 359</small> |
| <hr/> | | |
| 02 | Dobbelt så mange nye hull, og flere blir angrepet.
Antallet nye sårbarheter er doblet fra i fjor. Den amerikanske sikkerhetsmyndigheten CISA har allerede ført opp flere utnyttede sårbarheter i katalogen sin enn i hele 2025. | 272
<small>utnyttede hull hos CISA 1.1.–25.10.
2025: 210</small> |
| <hr/> | | |
| 03 | KI gjør angrepene billigere og raskere.
I oktober kom én aktør med KI-agenter inn på nettsidene til over 100 selskaper på under fire uker. Veiene inn er likevel stort sett de gamle. | 100+
<small>selskaper rammet av én aktør med
KI-agenter <i>*Reuters</i></small> |
| <hr/> | | |
| 04 | Omtrent like mange norske ofre, men nesten tre ganger så mange angrepsmeldinger.
18 norske virksomheter er hengt ut i år, mot 17 i fjor. Datatilsynet fikk likevel nesten tre ganger så mange meldinger om tilsiktede angrep, blant annet fordi ett angrep hos en leverandør rammer mange. | 282
<small>meldinger om tilsiktede angrep,
1. halvår
2025: 103 <i>*Datatilsynet</i></small> |

For en norsk SMB betyr det: Tett hull i VPN og brannmurer raskere, og bytt til innlogging som ikke kan phishes. Alle tiltakene står på side 15.

Sammendrag

Rapporten ser på hva tall målt i 2026 sier om KI og dataangrep mot virksomheter. Den bygger på egne opptellinger i rådata, rapporter fra sikkerhets- og forsikringsselskaper og norske kilder.

Løsepengegruppene hengte ut 8 637 virksomheter på lekkasjesidene fra 1. januar til 25. oktober 2026, 36 prosent flere enn i samme periode i fjor. CISA har lagt til 272 utnyttede sårbarheter i katalogen sin, flere enn i hele 2025, og antallet nye sårbarheter er doblet. Ofrene og de utnyttede hullene økte mest i tredje kvartal.

Veiene inn er de samme som før: stjålne eller lurte innlogginger og sårbarheter i systemer som står mot internett, men forsøkene er langt flere. Innbrudd som starter med en telefon til en ansatt, ble doblet fra andre halvår 2025 til første halvår 2026, og ondsinnede Teams-anrop, oftest med falsk IT-støtte, ligger på rundt ti ganger nivået fra sommeren 2025.

KI gjør deler av jobben for flere angripere. AWS, Google og Anthropic har i år dokumentert kriminelle som lot KI planlegge og gjennomføre store deler av angrep. I oktober beskrev NorForge og Reuters én aktør som med KI-agenter kom inn på nettsidene til over 100 selskaper, og Microsoft en statstilknyttet aktør som brukte KI-agenter mot over 2 250 virksomheter. Statistikken skiller likevel ikke ut hvor stor del av økningen KI står for. Nærmest kommer Rapid7, som fant KI nevnt som del av angrepet i 8 prosent av trusselrapportene i tredje kvartal.

Jeg tror KI virker på to måter. Den gjør det billigere å prøve mange dører samtidig, og den hjelper både angripere og forsvarere med å finne flere hull. Antallet nye sårbarheter er doblet, men Linux-kjernen sto alene for 14 prosent av dem i september, og hvor mye KI står for, vet ingen.

Pengene har ikke fulgt etter. Bare 19 prosent av ofrene i Covewares saker betalte løsepenger i andre kvartal, og GuidePoint melder om under 21 prosent i tredje. Prisene på cyberforsikring har falt 13 kvartaler på rad. Resilience skriver at KI gjør phishing og manipulering langt mer effektivt, og disse angrepene sto for 85 prosent av tapene selskapet dekket i første halvår.

I Norge er antallet kjente ofre omtrent som før, 18 virksomheter fra 1. januar til 25. oktober, mot 17 i fjor. Datatilsynet fikk likevel 282 meldinger om tilsiktede angrep i første halvår, mot 103 i fjor. Flere av de største norske sakene i år gikk via leverandører, som hos Telia, Alpha IT og Laerdal, og kundene synes ikke på lekkasjesidene.

Det mest sannsynlige det neste året er flere ofre internasjonalt, mens norske virksomheter rammes mest via leverandører og eksponerte systemer. Rapporten har åtte etterprøvbare prognoser og åtte tiltak, ordnet etter hva en norsk SMB bør gjøre først.

Innhold

Metode og datagrunnlag	3	Målene samlet	4
Lekkasjesidene	5	Utnyttede sårbarheter	6
Veiene inn og masseangrep	7	Løsepenger og forsikring	8
Svindel mot bedrifter	9	KI i angrepene	10
Hvor KI virker	11	Norge og Norden	12
Hovedscenarioet	13	Åtte prognoser	14
Tiltak	15	Faktasjekk og kilder	16

Metode og datagrunnlag

Rapporten bruker bare tall som er målt i 2026. Årsrapporter som beskriver 2025, som Verizon DBIR, Sophos og Mandiant M-Trends, er utelatt. Tall fra 2025 og 2024 er bare med som sammenligning for samme periode, eller som del av en tidsserie. Alle tall er sjekket mot kildene 26. oktober 2026, og faktasjekken står på side 16.

Slik har jeg talt og sammenlignet

Tallene for lekkasjesidene har jeg talt opp selv i hele datasettet til ransomware.live, 33 231 oppføringer hentet 26. oktober 2026, etter datoen ransomware.live registrerte oppføringen. Tallene for utnyttede sårbarheter er talt opp i CISAs katalog, versjon 2026.10.23, etter datoen sårbarheten ble lagt til. CVE-listen er talt etter publiseringsdato, uten avviste poster. Året så langt betyr 1. januar–25. oktober.

Siste måling står mot samme måned, kvartal eller halvår ett og to år før. Rapporten handler om angrep og svindel mot virksomheter, så svindel mot privatpersoner er utelatt. Internasjonale tall er med når de måler angrepsveier norske virksomheter deler med andre land: VPN, skytjenester, leverandører og e-post. Europa er her EU/EØS, Storbritannia og Sveits, og Norden er Norge, Sverige, Danmark og Finland.

Datakildene

Kilde	Hva den måler	Siste måling
Ransomware.live	Ofre hengt ut på lekkasjesider	25.10.2026, egen opptelling
CISA KEV	Sårbarheter bekreftet utnyttet	25.10.2026, egen opptelling
CVE-listen, kontrollert mot NVD	Nye sårbarheter per måned	September 2026, egen opptelling
GuidePoint, ReliaQuest, Check Point, Cyble	Ofre og angrep per kvartal og måned	3. kvartal 2026
Google, VulnCheck, Rapid7	Utnyttede sårbarheter og KI i angrepene	3. kvartal 2026 (Rapid7)
CrowdStrike, Expel, Beazley Security	Hvordan angriperne kom inn	1. halvår og 2. kvartal 2026
Coveware	Betaling av løsepenger	2. kvartal 2026
Microsoft, APWG	E-postsvindel mot bedrifter	2. kvartal 2026
Resilience, Coalition, Beazley, Marsh	Forsikringstap og priser	3. kvartal 2026 (Marsh)
Datatilsynet, NSM, Kripos, norske medier	Norske hendelser og varsler	26.10.2026

Forbehold

- 01 Lekkasjesidene viser bare ofrene gruppene velger å henge ut, og datasettet vokser når nye grupper spores. Teller en etter datoen gruppene publiserte, blir økningen 32 prosent i stedet for 36.
- 02 Sikkerhets- og forsikringsselskapene måler sine egne kunder. Covewares betalingsandel gjelder bare selskapets saker, og Resilience forsikrer mellomstore og store selskaper.
- 03 De norske tallene er små. Én sak mer eller mindre gir store prosentutslag, så jeg oppgir antall, ikke prosent.
- 04 Mange av kildene selger sikkerhet eller KI. Derfor ser jeg etter flere kilder som peker samme vei.

Kilder: Ransomware.live; CISA KEV; kildene i tabellen over.

Angrepene øker, betalingene faller

Tabellen samler målene i rapporten. Alle oppdateres minst hvert halvår og gjelder angrep mot virksomheter. Den siste målingen står mot samme periode ett og to år før.

Mål	2024	2025	2026	Endring fra i fjor
Ofre				
Ofre hengt ut på lekkasjesider, august	488	530	1 209	×2,3
Ofre hengt ut på lekkasjesider, september	406	598	879	+47 %
Ofre hengt ut på lekkasjesider, 3. kvartal	1 326	1 675	3 040	+81 %
Ofre hengt ut på lekkasjesider, 1.–25. oktober	452	649	907	+40 %
Ofre hengt ut på lekkasjesider, 1.1.–25.10.	4 637	6 359	8 637	+36 %
Ofre i Europa, 1.1.–25.10.	1 035	1 341	2 064	+54 %
Ofre i Norden, 1.1.–25.10.	68	99	119	+20 %
Ofre i Norge, 1.1.–25.10.	18	17	18	+1
Ofre for løsepengevirus, 2. kvartal <i>*GuidePoint</i>	1 110	1 591	2 279	+43 %
Sårbarheter				
Nye sårbarheter i CVE-listen, januar–september <i>*CVE-listen</i>	28 871	35 364	72 802	×2,1
Nye utnyttede sårbarheter hos CISA, september	25	16	43	×2,7
Nye utnyttede sårbarheter hos CISA, 3. kvartal	58	51	100	×2,0
Nye utnyttede sårbarheter hos CISA, 1.1.–25.10.	148	210	272	+30 %
Utnyttede sårbarheter, 1. halvår <i>*VulnCheck</i>	390	432	495	+15 %
Penger				
Ofre som betalte løsepenger, 2. kvartal <i>*Coveware</i>	36 %	26 %	19 %	–7 poeng
Snittkrav ved e-postsvindel med bankoverføring, 2. kvartal <i>*APWG</i>	89 520 \$	83 099 \$	61 732 \$	–26 %

Lekkasjesider, Europa, Norden, Norge, CISA og CVE-listen: egen opptelling i rådata, uttrekk 26.10.2026.

Slik Leser jeg tabellen

Nesten alle målene for ofre og sårbarheter ligger klart over fjorårets nivå, og økningen er størst i tredje kvartal. Det gjelder både lekkasjesidene, CISAs katalog og CVE-listen, som telles helt uavhengig av hverandre.

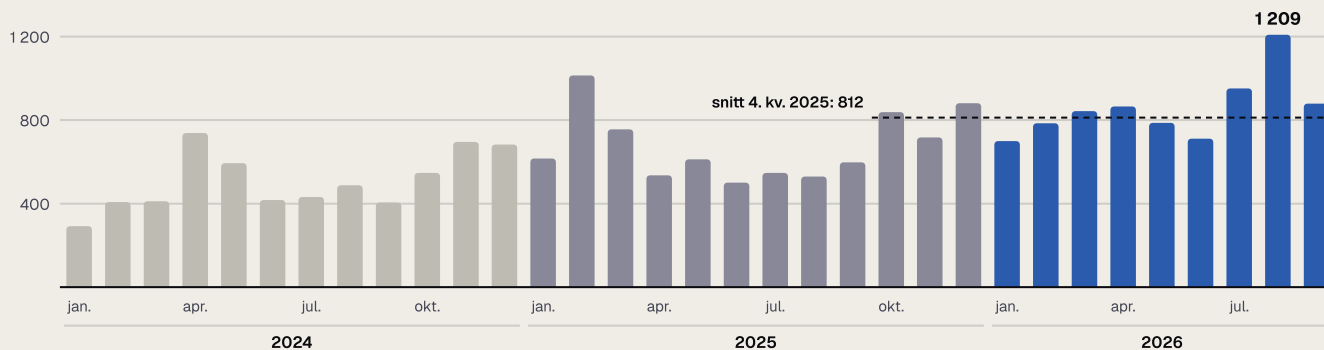
Unntakene er like tydelige. Norge ligger omtrent flatt, antallet utnyttede hull vokser langt saktere enn antallet nye, og både betalingsandelen og snittkravet i e-postsvindel går ned. Flere angrep betyr altså ikke automatisk mer penger til angriperne.

Kilder: Ransomware.live, rådata hentet 26.10.2026; CISA KEV, versjon 2026.10.23; CVE-listen via cve.Oxosprey.com, kontrollert mot NVD; GuidePoint GRIT Q2 2024–2026; VulnCheck 1H 2024–2026; Veeam/Coveware Q2 2026; APWG Q2 2024–2026.

36 prosent flere ofre på lekkasjesidene

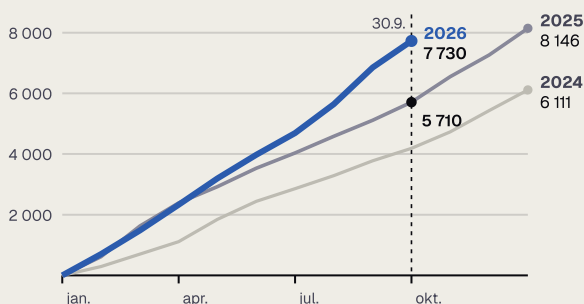
Lekkasjesidene er nettstedene der løsepengegruppene henger ut virksomheter som ikke har betalt. De er det mest brukte målet på hvor mange som rammes, fordi gruppene selv publiserer ofrene.

Nivået steg høsten 2025, og august 2026 er den høyeste måneden hittil



Ofre per måned, alle land. Egen opptelling i rådata fra ransomware.live, uttrekk 26.10.2026.

35 % flere enn i fjor per 30. september



Punktet på 2025-linjen er samme dato i fjor, endepunktene er hele året.

Delvis en baseeffekt

Sommeren 2025 var svak, og nivået steg allerede høsten 2025, til rundt 810 ofre i måneden. En del av økningen fra i fjor skyldes derfor at fjoråret var lavt.

Tredje kvartal i år lå likevel 25 prosent over fjerde kvartal 2025, på rundt 1 010 i måneden. Oktober har gitt 907 ofre på 25 dager, mot 649 i fjor.

Andre som teller, finner det samme

GuidePoint talte 2 760 ofre i tredje kvartal, 75 prosent flere enn ett år før **GuidePoint*, og ReliaQuest kom til 2 252 i andre kvartal, rundt 51 prosent flere **ReliaQuest*. For august fant Cyble 1 034 ofre mot 467 ett år før **Cyble*, og Check Point talte 824 løsepengevirusangrep i september, 53 prosent flere enn i fjor **Check Point*.

Europa økte mer enn resten av verden, med 54 prosent fra 1. januar til 25. oktober. Norden økte med 20 prosent, og Norge med én virksomhet. Det kommer jeg tilbake til på side 12.

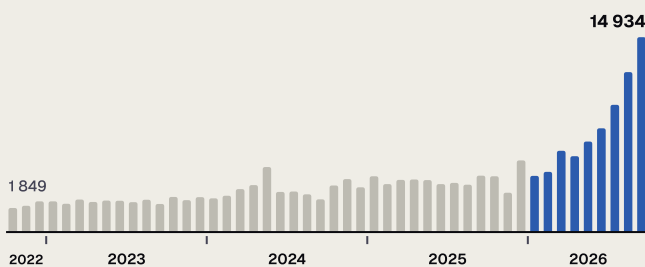
Gruppene henger ut dem som ikke betaler, så en lavere betalingsandel gir flere navn på lekkasjesidene selv om antallet angrep er det samme. I Covewares saker steg andelen som ikke betalte, fra 74 til 81 prosent på ett år. Med like mange angrep gir det rundt ti prosent flere ofre, ikke 36.

Kilder: Ransomware.live, rådata hentet 26.10.2026; GuidePoint GRIT Q3 2026 (8.10.2026); ReliaQuest Q2 2026; Cyble, august 2025 og 2026; Check Point, september 2026 (8.10.2026); Veeam/Coveware Q2 2026.

Dobbelt så mange nye hull, 30 prosent flere utnyttet

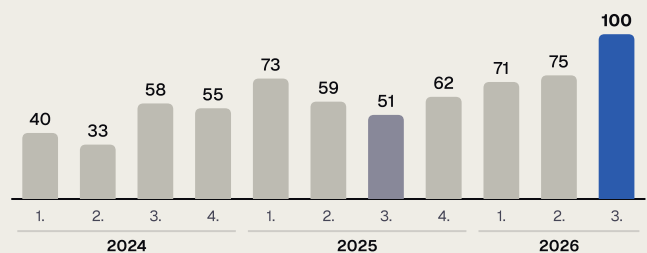
CISAs katalog lister sårbarhetene amerikanske etater må tette først, og en sårbarhet kommer bare på listen når CISA har bevis for at den angripes. Derfor er katalogen et godt mål på hvor mange hull angriperne bruker i reelle angrep.

Nye sårbarheter per måned, oktober 2022 til september 2026



Publiserte poster i CVE-listen, uten avviste. Egen opptelling, kontrollert mot NVD, uttrekk 26.10.2026. [*CVE-listen](#)

100 nye utnyttede hull hos CISA i tredje kvartal, mot 51 i fjor



Egen opptelling i CISAs katalog. Blått: siste kvartal. Mørk grå: samme kvartal i fjor. Per 25. oktober: 272 i år, mot 210 i fjor.

Dobbelt så mange nye sårbarheter

CVE-listen fikk 72 802 nye sårbarheter fra januar til september, mot 35 364 i samme periode i fjor. I september kom 14 934, 3,5 ganger så mange som ett år før. Linux-kjernen sto alene for 14 prosent av dem, fordi utviklerne registrerer nesten hver feilretting som en sårbarhet. [*NVD](#) Google registrerte 141 utnyttede sårbarheter fra januar til august, mot 127 i hele 2025. [*Google GTIG](#)

Antallet utnyttede hull vokser likevel langt saktere enn antallet nye. CISA la til 30 prosent flere enn i fjor, og VulnCheck finner at andelen som utnyttes, har falt fra 2,7 prosent i andre halvår 2023 til 1,4 prosent i første halvår 2026. Google har sett 1 av 431 sårbarheter fra 2026 utnyttet. Angriperne treffer en mindre andel, men det finnes så mange flere hull at antallet treff likevel øker.

Mediantiden fra en sårbarhet ble kjent til den ble bekreftet utnyttet, falt fra 120 til 80 dager, ifølge VulnCheck. Rapid7 fant at alvorlige sårbarheter i tredje kvartal ble utnyttet i snitt tre dager etter at de ble kjent.

[*VulnCheck](#) [*Rapid7](#)

Hvor mange av de nye hullene som er funnet med KI, vet ingen. VulnCheck har registrert 1 061 sårbarheter funnet med KI-hjelp i første halvår, og 14 av dem er bekreftet utnyttet. De to kritiske hullene i PHP som ble kjent 21. oktober, ble også funnet med KI-hjelp, ifølge forskerne bak. [*Tenable](#)

Hva det betyr for en SMB

Flere kjente hull betyr flere varsler og kortere tid. Avtal med driftsleverandøren hvem som leser NSMs varsler, og hvor raskt brannmurer, VPN og annet som står mot internett, blir oppdatert.

Kilder: CVE-listen og NVD, uttrekk 26.10.2026; CISA KEV, versjon 2026.10.23 (egen opptelling); Google GTIG (30.9.2026); VulnCheck 1H 2025 og 1H 2026; Rapid7 Q3 2026 (21.10.2026); Tenable (21.10.2026).

Samme veier inn, flere forsøk

Rapportene for første halvår peker på de samme to veiene inn som før: stjålne eller lurte innlogginger og sårbarheter i systemer som står mot internett. Mengden har økt klart.

2×

så mange innbrudd startet med en telefon i første halvår som i andre halvår 2025.

**CrowdStrike*

≈10×

så mange ondsinnede Teams-anrop i uka som sommeren 2025, oftest med falsk IT-

støtte. **Microsoft*

68 %

av hendelsene i andre kvartal gjaldt innlogging og brukerkontoer, opp fra 59 % i

første. **Expel*

67 %

av løsepengevirusinnbruddene i andre kvartal startet med stjålne innloggingsdata mot

VPN eller fjernskrivebord.

**Beazley Security*

Ifølge Coveware er phishing og annen manipulering, blant annet av brukerstøtten, igjen den vanligste veien inn for løsepengevirus **Coveware*, mens Beazley Security oftest ser stjålne VPN-innlogginger. Kildene ser ulike kunder og teller ulikt, men felles for dem er at innloggingen er det svakeste leddet. CrowdStrike fant at forsøkene på phishing med enhetskode, der den ansatte selv godkjenner angriperens innlogging, økte 15 ganger i løpet av første halvår. **CrowdStrike*

Når angrepskoden for en sårbarhet først er offentlig, går det fort. Av utnyttelsen CrowdStrike så i første halvår, skjedde 88 prosent innen 48 timer etter at koden ble kjent. **CrowdStrike*

Masseangrepene i 2026

Når	Hva skjedde	Vei inn
Mars	Angripere kom seg inn i EU-kommisjonens skymiljø via en kompromittert versjon av sikkerhetsverktøyet Trivy. Rundt 340 GB kom på avveie. <i>*Help Net Security</i>	Leverandørkjede
Juni	I lekkasjen kalt FortiBleed kom VPN-innloggingsdata og oppsett fra over 73 000 Fortinet-brannmurer på avveie. Rundt halvparten av dem som står mot internett, kan være berørt. <i>*Bitsight</i>	Stjålne VPN-innlogginger
Juni–juli	Clop utnyttet en nulldagssårbarhet i PTC Windchill og FlexPLM, programvare for produktdata i industrien, og hevdet 43 ofre. <i>*Tech Times *CyberScoop</i>	Nulldagssårbarhet
Sep.–okt.	To runder med aktivt utnyttede nulldagssårbarheter i Citrix NetScaler. NSM ba 3. oktober virksomhetene ta sårbare enheter av nett. <i>*NSM</i>	Nulldagssårbarhet
Oktober	To kritiske hull i PHP. Digdir, OsloMet og Feide stengte tjenester for sikkerhets skyld, og NSM kjente ikke til norske innbrudd. <i>*NSM *kode24</i>	Kritisk sårbarhet

Mønsteret går igjen: Ett hull i et mye brukt produkt, eller én kompromittert leverandør, gir mange ofre samtidig.

Hva det betyr for en SMB

Angrepene mot innlogging stopper dere langt på vei med to tiltak: innlogging som ikke kan phishes, også på VPN, og en brukerstøtte som sjekker hvem som ringer før den nullstiller noe. Hullene i tabellen krever i tillegg rask oppdatering, og masseangrepene viser at god egen drift ikke alltid er nok. Spør leverandørene hvordan de oppdager innbrudd hos seg selv, og hvor raskt dere blir varslet (side 15).

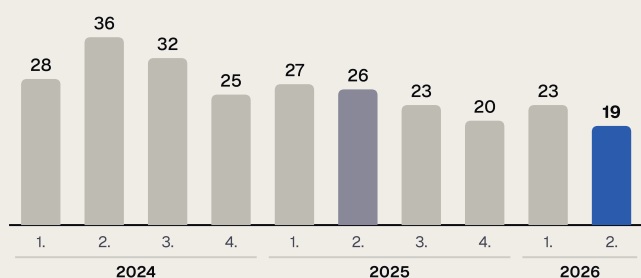
Kilder: CrowdStrike Threat Hunting Report 2026; Microsoft, Email threat landscape Q2 2026; Expel Q2 2026; Beazley Security Q2 2026; Coveware Q2 2026; Help Net Security (3.4.2026); Bitsight (18.6.2026); Tech Times (15.8.2026); CyberScoop (19.8.2026); NSM (3. og 21.10.2026); kode24 (23.10.2026).

Færre betaler, og manipulering står bak de fleste tapene

Covewares tall for andre kvartal viser at 19 prosent av ofrene betalte løsepenger, det laveste selskapet har målt. Ofre som bare fikk data stjålet, uten at noe ble kryptert, betalte i 15 prosent av sakene.

Medianbeløpet ble halvert fra første kvartal, til 150 000 dollar. GuidePoint melder om under 21 prosent i tredje kvartal. [*Coveware](#) [*GuidePoint](#)

Andelen som betaler, er den laveste Coveware har målt



Prosent av ofrene i Covewares egne saker, 1. kvartal 2024 til 2. kvartal 2026. Blått: siste kvartal. Mørk grå: samme kvartal i fjor. [*Veeam/Coveware](#)

Hva fallet betyr

Når færre betaler, får gruppene inntekter fra færre angrep, og de kan svare med å angripe flere. Det passer med at antallet ofre stiger mens betalingene faller, men tallene kan ikke vise at det er årsaken.

Betalingsandelen sier lite om hvor mye virksomhetene taper. Nedetid, gjenoppretting og stjålne data koster uansett, og for en SMB er det ofte de kostnadene som svir mest.

Forsikringsselskapene

85 %

av tapene i første halvår kom fra phishing, manipulering og svindel med overføringer, mot 18 % to år før. [*Resilience](#)

-4 %

i prisene på cyberforsikring i tredje kvartal, det trettende kvartalet på rad med nedgang. [*Marsh](#)

-15 %

i premievolum innen cyber i første halvår sammenlignet med i fjor, mens selskapet melder om flere store tap. [*Beazley](#)

Resilience forsikrer mellomstore og store selskaper, så tallene sier mindre om små bedrifter. Resilience skriver at KI gjør phishing og manipulering langt mer effektivt, og det er nettopp de angrepene som står for det meste av tapene. Angrep på virksomhetenes egne KI-systemer, som promptinjeksjon, ga ingen tap i første halvår.

Coalition, som forsikrer over 110 000 virksomheter, meldte 20. oktober om stabile krav og ingen økning i løsepengevirushendelser [*Coalition](#). Sammen med de fallende prisene tyder det på at forsikringsmarkedet ikke venter en kraftig økning i tapene ennå.

Planlegg som om dere ikke skal betale

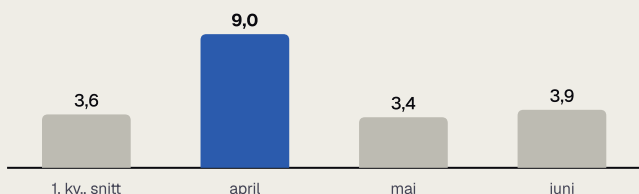
For en SMB betyr den lave betalingsandelen at gjenoppretting er det som avgjør hvor dyrt et angrep blir. Det krever sikkerhetskopier angriperen ikke kan nå, en øvd plan for å hente dem tilbake, og en avtale om hvem som hjelper dere de første døgnene, enten det er driftsleverandøren eller forsikringsselskapet.

Kilder: Coveware Q2 2026; Veeam/Coveware, Cyber Extortion Report Q2 2026; Resilience, H1 2026 Cyber Risk Report; Marsh, Global Insurance Market Index Q3 2026 (21.10.2026); Beazley, halvårsresultat 2026 via Reinsurance News (5.8.2026); GuidePoint GRIT Q3 2026; Coalition via Digital Insurance (20.10.2026).

Svindelen mot bedrifter svinger, og beløpene faller

E-postsvindel mot bedrifter, der svindleren utgir seg for å være sjefen eller en leverandør, er den formen for digital svindel som rammer virksomheter mest direkte. Tallene for 2026 svinger mye fra måned til måned.

Forsøkene toppet seg i april og falt i mai



Millioner forsøk per måned. Første kvartal: 10,7 millioner, i snitt 3,6 i måneden. [*Microsoft](#)

Microsoft registrerte rundt 9 millioner forsøk på e-postsvindel mot bedrifter i april, 2,5 ganger snittet i første kvartal, før tallet falt til 3,4 millioner i mai. Mengden hopper så mye at den sier lite om retningen.

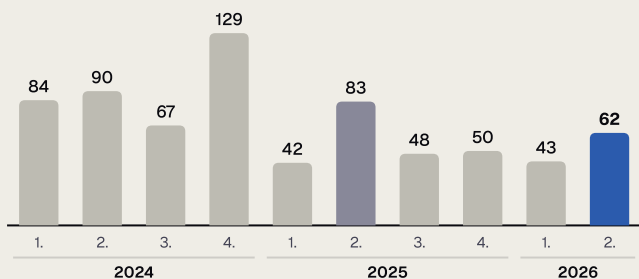
Snittkravet i svindel med bankoverføring har derimot falt to år på rad, til 61 732 dollar i andre kvartal, mot 83 099 dollar i 2025 og 89 520 dollar i 2024. Antallet slike forsøk økte likevel med 88 prosent fra første kvartal. [*APWG](#)

Falske stemmer

I januar ble en bedriftseier i kantonen Schwyz i Sveits lurt til å overføre flere millioner franc fra firmaet. Svindlerne ringte i to uker med en stemme manipulert med KI, slik at den lignet en kjent forretningspartner. [*Kantonspolizei Schwyz via Nau.ch](#)

Jeg har ikke funnet en dokumentert norsk sak fra 2026 der det ble brukt deepfake. Advarslene kommer likevel tett. Politiet i Nordland skrev i mai at flere norske foretak er svindlet for millionbeløp gjennom direktørsvindel over e-post eller telefon, og at KI vil bli en økende trussel [*Politiet Nordland](#). Finans Norge meldte i april at direktørsvindel og fakturasvindel fortsatt gir store tap i bedriftsmarkedet [*Finans Norge](#), og Tryg advarte i juni 43 000 norske bedriftskunder mot direktørsvindel med KI [*Tryg](#). Ingen har publisert norske tapstall for i år.

Snittkravet i andre kvartal har falt to år på rad



Tusen dollar per kvartal. Blått: siste kvartal. Mørk grå: samme kvartal i fjor. [*APWG](#)

Hva som stopper det

Svindelen lykkes når én person kan endre et kontonummer eller godkjenne en hasteoverføring alene. Rutinen som stopper den, er gammel: Ring tilbake på et nummer dere allerede har, og la to personer godkjenne nye betalingsinstrukser.

Den virker like godt mot en KI-manipulert stemme som mot en falsk e-post, og den koster ingenting å innføre.

KI i angrepene i 2026

I år har det kommet flere godt dokumenterte saker der angripere lar KI gjøre store deler av jobben, og i oktober kom to saker der KI-agenter gikk mot hundrevis av virksomheter samtidig. Ofrene er sjelden navngitt.

Dokumenterte saker

- Januar–februar **AWS***
En russisktalende, økonomisk motivert aktør kom seg inn i over 600 Fortinet-brannmurer i over 55 land med svake passord og flere kommersielle KI-tjenester, og gikk etter sikkerhetskopiene.
- Mai **Google***
Den første utnyttelsen av en nulldagssårbarhet som Google mener ble utviklet med KI. En kriminell gruppe planla masseutnyttelse, og Google mener motaksjonen kan ha hindret bruken.
- September **Anthropic***
En gruppe som trolig er tilknyttet ShinyHunters, brukte Claude etter et innbrudd hos en SaaS-leverandør og hentet ut data fra rundt 200 av kundene. KI-agenter gjorde nesten alt arbeidet.
- September **Microsoft***
Storm-3168 lot en KI-agent slette ressurser i én virksomhets Azure-miljø på rundt sju minutter og prøve å fjerne låsene på sikkerhetskopiene. Motivet er ukjent.
- Oktober **NorForge *Reuters***
Én aktør lot KI-agenter angripe over 1 200 nettstedet på under fire uker og kom inn på nettsidene til over 100 selskaper. Anslått KI-kostnad: rundt 50 dollar per vellykket innbrudd.
- Oktober **Microsoft***
Storm-0940, en statstilknyttet aktør, brukte KI-agenter og stjalne leverandørnøkler mot over 2 250 virksomheter. I flere saker tok det under tre timer å få administratortilgang, men de fleste forsøkene mislyktes.

Det som taler imot

April **Nordic Financial CERT*

KI har gjort angrepene mer effektive, men CERT-en har ikke sett flere vellykkede, alvorlige innbrudd.

Juli **VulnCheck*

Bare 14 av 1 061 sårbarheter funnet med KI-hjelp er bekreftet utnyttet, 1,3 prosent, omtrent som for sårbarheter generelt.

Juli **Resilience*

Ingen forsikringstap i første halvår fra angrep på virksomhetenes egne KI-systemer, som promptinjeksjon.

Oktober **Coalition*

Forsikringskravene er stabile, og selskapet har ikke sett flere løsepengevirus hendelser.

Kildene har en skjevhet

Selskapene som melder om KI-misbruk, selger selv KI eller sikkerhet og ser bare det som skjer på egne plattformer. Tallene i Cairn-saken kommer fra angriperens egne kontrollpaneler, gjennomgått av NorForge og Reuters. Det gjør ikke sakene feil, men vi vet ikke hvor vanlige de er.

Det jeg ser etter fremover

Rapid7 er først ute med et tall: KI ble nevnt som del av angrepet i 8 prosent av trusselrapportene selskapet fulgte i tredje kvartal **Rapid7*. Det er rapporter, ikke angrep. Jeg ser etter at flere som etterforsker innbrudd, oppgir hvor stor andel av sakene som hadde KI i selve angrepet, og at forsikringsselskapene finner tap de kan knytte direkte til KI.

Kilder: AWS (20.2.2026); Google GTIG (11.5.2026); Anthropic (10.9.2026); Microsoft (25.9. og 21.10.2026); NorForge og Reuters (19.10.2026); Nordic Financial CERT (7.4.2026); VulnCheck 1H 2026; Resilience H1 2026; Coalition (20.10.2026); Rapid7 (21.10.2026).

KI synes tydeligst der hullene blir funnet

Når jeg sorterer det som er dokumentert i 2026 etter ledd i et angrep, blir mønsteret tydelig. Bare i ett ledd er KI-bruken talt opp: når sårbarheter blir funnet. Selv der er bare en liten del av de nye hullene registrert som funnet med KI. I resten av angrepet, også der det fører til tap, finnes enkeltsaker, men statistikken skiller ikke ut KI.

Enkeltsaker i alle ledd, tall bare i ett

Ledd i angrepet	Målt i tall	Enkeltsaker	Hva som er dokumentert i 2026
Finne sårbarheter	●	○	VulnCheck har registrert 1 061 sårbarheter funnet med KI-hjelp. Mozilla har rettet 271 feil funnet med KI. *VulnCheck *Mozilla
Lage angrepskode	○	●	Google fant den første utnyttelsen av en nulldagssårbarhet som trolig ble utviklet med KI. *Google
Komme inn	○	●	KI-tjenester hjalp én aktør inn i over 600 brannmurer. I oktober kom en annen med KI-agenter inn på nettsidene til over 100 selskaper. *AWS *Reuters
Utforske og hente ut data	○	●	KI-agenter gjorde nesten alt arbeidet da data fra rundt 200 kunder av en SaaS-leverandør ble hentet ut. *Anthropic
Ødelegge	○	●	En KI-agent slettet ressurser i et Azure-miljø på rundt sju minutter. *Microsoft
Svindle med falsk stemme	○	●	Én dokumentert sak i Sveits. Ingen kjent norsk sak i 2026. *Nau.ch
Føre til tap	○	●	Den falske stemmen i Sveits kostet flere millioner franc. Resilience skriver at KI gjør phishing og manipulering, som står for 85 prosent av tapene, langt mer effektivt. *Resilience

Min sortering av kildene på side 6, 8 og 10. Blått: målt i tall. Rødt: dokumentert i enkeltsaker.

Det nye er hvor mye én aktør rekker

Veiene inn er stort sett de samme som før. Forskjellen er at én aktør med KI-agenter kan lete gjennom et ukjent miljø, lage verktøy underveis og hente ut data fra mange kunder samtidig. AWS skrev om aktøren bak Fortinet-innbruddene at den nådde et omfang som tidligere ville krevd et betydelig større og dyktigere team. [*AWS](#) Aktøren NorForge fant i oktober, brukte rundt 23 timer og anslagsvis 50 dollar i KI-kostnad per vellykket innbrudd. [*NorForge](#)

KI-verktøyene er også blitt et mål. Google fant skadevare som gjemmer seg i mappene til kodeassistenter som Claude og Cursor [*Google](#), så utviklermaskiner og KI-verktøy må sikres som annen administratortilgang.

Forsvarerne bruker de samme verktøyene

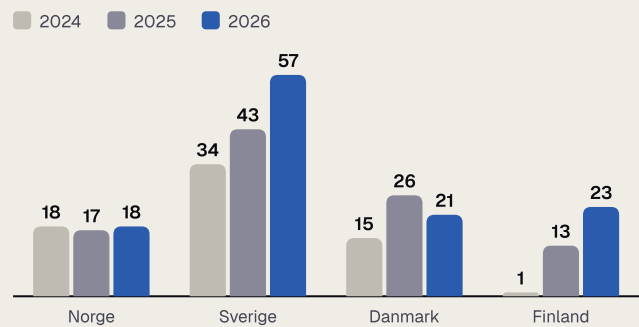
Mozilla har rettet 271 sikkerhetsfeil i Firefox som ble funnet med Anthropic Claude Mythos Preview, 180 av dem med høy alvorlighetsgrad [*Mozilla](#). NSM skrev i mai at bruk av språkmodeller til å finne og utnytte nulldagssårbarheter er, eller er i ferd med å bli, en del av det daglige risikobildet [*NSM](#). Flere funn gir flere rettelser, men også flere kjente hull som kan angripes før rettelser er installert. Det er her jeg tror KI betyr mest for en vanlig norsk virksomhet i år.

Kilder: VulnCheck 1H 2026; Mozilla (mai 2026); Google GTIG (11.5. og 8.9.2026); AWS (20.2.2026); Anthropic (10.9.2026); Microsoft (25.9.2026); Nau.ch (20.1.2026); Resilience H1 2026; NSM (12.5.2026); NorForge og Reuters (19.10.2026).

18 norske ofre mot 17 i fjor, men nesten tre ganger så mange angrepsmeldinger

Fra 1. januar til 25. oktober ble 18 norske virksomheter hengt ut på lekkasjesidene, mot 17 og 18 i samme periode de to foregående årene. Det er 0,2 prosent av ofrene globalt, og Norge har ikke fulgt Europa, der antallet økte med 54 prosent. Datatilsynet fikk derimot 282 meldinger om tilsiktede angrep i første halvår, mot 103 i fjor, det høyeste siden kategorien ble innført i 2023. Tilsynet forklarer det blant annet med at ett angrep hos en leverandør kan ramme mange virksomheter. [*Datatilsynet via kode24](#)

Sverige og Finland øker, Norge står stille, Danmark faller



Ofre på lekkasjesider, 1. januar–25. oktober. Egen opptelling i rådata fra ransomware.live. [*ransomware.live](#)

Norden øker mindre enn Europa

Norden samlet har 20 prosent flere ofre enn i fjor (119 mot 99), mens Europa har 54 prosent flere. Økningen kommer i Sverige og Finland. Lekkasjesidene viser bare virksomheten som ble angrepet. Når en leverandør rammes, teller kundene som regel ikke med. Derfor sier de internasjonale tallene om veiene inn mer om norsk risiko enn de norske lekkasjetallene gjør.

Store norske saker i 2026

Hvem	Når	Hva skjedde
Telia Norge	Februar	Innbruddet ble oppdaget i november 2025. Opplysninger om rundt 500 000 privatkunder og over 3 000 bedrifter ble lagt ut, og Nkom varslet tilsyn. *ITavisen
Lørenskog kommune	Mai	1,8 TB ble stjålet og publisert, blant annet barnevernssaker og pasientjournaler. *Lørenskog kommune
Alpha IT, Trondheim	Juni	IT-leverandør. Opptil 15 kundebedrifter kan være rammet. Hackerne oppgir 28,5 millioner filer, og saken er overført til Kripos. *digi.no *MN24
Offentlige fellestjenester	Aug.–okt.	Tjenestenektangrep slo ut ID-porten, MinID, Altinn og Helsenorge i flere runder. Skatteetatens tjenester, blant annet a-meldingen, ble hardt rammet. *digi.no *Regnskap Norge
Laerdal	Oktober	Et angrep på en programvareleverandør ga tilgang til personopplysninger om ansatte i Laerdal-selskapene siden 2018. Selskapet ser ingen tegn til at kundedata er rammet. *Laerdal

Hva norske myndigheter og bransjen sier

Nkom skrev i risikovurderingen for 2026, publisert 21. oktober, at KI senker terskelen for angrep [*Nkom](#). NSM varslet om aktivt utnyttede sårbarheter i Citrix NetScaler 27. september og 3. oktober og om de kritiske hullene i PHP 21. oktober [*NSM](#). I NorSIS' undersøkelse fra juni var nær 30 prosent av de ansatte i bedrifter med 11–50 ansatte usikre på om de klarte å håndtere digitale trusler [*NorSIS og Opinion](#).

Kilder: Ransomware.live, rådata hentet 26.10.2026; Datatilsynet via kode24 (20.10.2026); Laerdal (23.10.2026); Nkom (21.10.2026); ITavisen (4.3.2026); digi.no (26.6. og 26.8.2026); Lørenskog kommune (mai 2026); MN24 (21.8.2026); Regnskap Norge (5.10.2026); NSM; NorSIS og Opinion (1.6.2026).

Flere angrep, ujevnt fordelt

Slik jeg ser det

Mye av KI-debatten handler om feil ting. Angriperne kommer seg fortsatt inn på samme måte som før: med stjalne passord, en telefon til brukerstøtten eller et hull i en VPN ingen har rukket å oppdatere. Det nye er tempoet. KI gjør det billigere å finne hull, og angriperne har aldri hatt flere dører å prøve.

En norsk SMB blir neppe slått ut av en KI-agent i år. Den blir rammet fordi brannmuren sto uoppdatert en uke for lenge, eller fordi noen godkjente en innlogging de ikke burde. Det er egentlig gode nyheter, for det som stopper de fleste angrepene, er kjent og billig. Vi i sikkerhetsbransjen som selger KI-verktøy som svaret på KI-angrep, bør være ærlige om at det sjelden er der det brenner.

Norge har så langt sluppet billig unna på lekkasjesidene, men jeg ville ikke lest det som at vi er tryggere. Datatilsynet fikk nesten tre ganger så mange meldinger om tilsiktede angrep i første halvår, mens lekkasjesidene står stille. Vi bruker de samme VPN-ene og leverandørene som resten av Europa, og Telia, Alpha IT og Laerdal viser at det er leverandøren som blir angrepet, mens kundene og de ansatte tar regningen uten å dukke opp i statistikken.

Det neste året

Jeg tror det neste året gir flere ofre internasjonalt, mens norske virksomheter rammes mest via leverandører og eksponerte systemer. Farten taler for det: Tredje kvartal lå 25 prosent over fjerde kvartal i fjor, og CISA la til flere utnyttede hull i september enn i noen annen måned i år. Oktober ligger høyere enn i fjor på lekkasjesidene.

Samtidig blir det funnet flere hull. Antallet nye sårbarheter er doblet fra i fjor, og jeg tror KI bidrar, selv om Linux-kjernen står for en god del av økningen. Angriperne treffer en mindre andel enn før, men så mange flere hull gir likevel flere angrep. KI-agentene gjør det i tillegg billigere å prøve mange dører samtidig.

Tapene stiger trolig mindre enn antallet angrep. Færre betaler, og forsikringsprisene tyder på at heller ikke markedet venter en kraftig økning.

Flere kjente hull gir flere ofre

KI bidrar trolig her ↓



Her bryter du kjeden: tett kritiske hull på dager, ikke uker

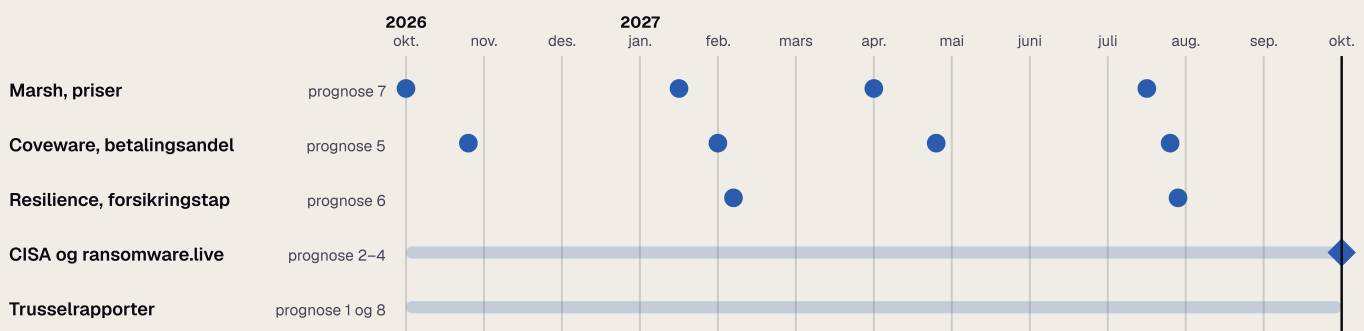
Min tolkning. Nye sårbarheter: januar–september 2026 mot samme periode i 2025. Treffrate: andelen av sårbarhetene fra 2026 som Google har sett utnyttet. CISA og lekkasjesider: 1. januar–25. oktober mot samme periode i 2025. Et svakt fjorår, lavere betalingsandel og stjalne innlogginger forklarer også en del av økningen i ofre (side 5 og 7).

Åtte prognoser frem mot oktober 2027

Hovedscenariot er en vurdering. De åtte hendelsene under har jeg tallfestet, slik at det går an å sjekke om jeg tok feil. Lekkasjesidene telles på samme måte som i denne rapporten, i et uttrekk 5. oktober 2027. Slår prognose 3 til og prognose 4 ikke, har hovedscenariot på side 13 slått til.

#	Prognose	Sannsynlighet	Avgjøres av
01	Minst ett nytt dokumentert, økonomisk motivert angrep der rapporten sier at KI-agenter utførte de fleste trinnene.	<div><div></div></div> 90 %	Trusselrapporter fra Google, Microsoft og KI-selskapene
02	CISA legger til flere sårbarheter fra oktober 2026 til september 2027 enn de 308 fra oktober 2025 til september 2026.	<div><div></div></div> 70 %	CISA KEV, oktober 2027
03	Flere ofre på lekkasjesidene fra januar til september 2027 enn de 7 730 i samme periode i 2026.	<div><div></div></div> 70 %	Ransomware.live, uttrekk 5.10.2027
04	Minst 20 norske virksomheter hengt ut fra januar til september 2027, mot 15 i 2026.	<div><div></div></div> 30 %	Ransomware.live, uttrekk 5.10.2027
05	Coveware oppgir en betalingsandel på 25 % eller lavere for hvert kvartal fra 3. kvartal 2026 til 2. kvartal 2027.	<div><div></div></div> 75 %	Coveware og Veeam
06	Resilience finner tap fra angrep på virksomhetenes egne KI-systemer i rapporten for andre halvår 2026 eller første halvår 2027.	<div><div></div></div> 40 %	Resilience
07	Marshs globale indeks viser prisøkning for cyberforsikring i minst ett kvartal fra 3. kvartal 2026 til 2. kvartal 2027.	<div><div></div></div> 25 %	Marsh, Global Insurance Market Index
08	En nordisk hendelse der angriperen brukte en virksomhets egen KI-assistent eller -agent for å få tilgang eller hente ut data.	<div><div></div></div> 35 %	Bekreftet av virksomheten eller en nasjonal myndighet

Flere prognoser kan avgjøres allerede i vinter, alle innen oktober 2027



Når kildene trolig publiserer, ut fra når de publiserte i 2026. Bånd: løpende kilder. Rombe: siste sjekk 5. oktober 2027.

Slik følger du med

De to målene jeg følger tettest, er CISAs katalog over utnyttede sårbarheter og de norske tallene på lekkasjesidene. Begge kan sjekkes når som helst, og stiger begge, blir jeg mer pessimistisk. Covewares betalingsandel og forsikringsselskapenes tall for KI-tap viser om økningen i angrep begynner å bli til tap.

Kilder: Egne anslag. Avgjøres mot CISA KEV, ransomware.live, Coveware, Resilience, Marsh og offentlige kilder.

Tett hullene og sikre innloggingen først

Tallene fra 2026 peker på de samme svakhetene som før, bare med flere angrep. Dette er tiltakene jeg ville prioritert i en norsk SMB nå, ordnet etter hva som bør gjøres først.

Denne uken

01 Tett kritiske hull i systemer som står mot internett.

Be driftsleverandøren bekrefte skriftlig at VPN, brannmurer og fjerntilgang er oppdatert. Av utnyttelsen CrowdStrike så, skjedde 88 prosent innen 48 timer etter at angrepskoden ble offentlig **CrowdStrike*. Finnes det ingen rettelse, tar dere enheten av nett, slik NSM ba om for Citrix.

02 Stram inn brukerstøtten, også hos driftsleverandøren.

Ingen får nullstilt passord eller flerfaktorautentisering (MFA) før dere har bekreftet hvem de er, via en kanal innringeren ikke styrer. Innbrudd som startet med en telefon, ble doblet fra andre halvår 2025 til første halvår 2026.

03 Ring tilbake før dere endrer et kontonummer, på et telefonnummer dere allerede har.

La to personer godkjenne nye betalingsinstrukser og hasteoverføringer. Det stopper både fakturasvindel og direktørsvindel, også med en falsk stemme.

Denne måneden

04 Bytt til innlogging som ikke kan phishes.

Passnøkler eller FIDO2 for e-post, sky og administratorkontoer. Slå av innlogging med enhetskode der dere ikke trenger den. Forsøkene økte 15 ganger i første halvår.

05 Avtal hvem som ser varslene, og hvor fort de reagerer.

I én sak gikk det under fem minutter fra overtatt konto til stjålne data **CrowdStrike*. Hvem følger med om natten, og hvem kan stenge en konto?

06 Beskytt sikkerhetskopiene.

I to av sakene fra i år gikk angriperne målrettet etter sikkerhetskopiene og låsene på dem. Ha minst én kopi angriperen ikke kan nå, og øv på å gjenopprette.

Dette kvartalet

07 Rydd i leverandørtilgangene.

Hvem har tilgang til hva, og hvilken logging finnes? Telia, Alpha IT og Laerdal viser hvordan ett angrep på en leverandør kan ramme mange. Står varsling ved hendelser i kontrakten?

08 Lag en enkel regel for KI-verktøy.

Hvilke data kan legges inn hvor? En agent som leser e-post fra fremmede, skal ikke kunne overføre penger eller dele filer uten at et menneske godkjenner det. Kodeassistenter og API-nøkler skal behandles som administratortilgang.

Ingen av tiltakene er nye, og ingen av dem krever KI. Det er et dårlig salgsargument for en konsulent: Det meste kan dere begynne med selv. Trenger dere hjelp med resten, finner dere meg på spadeconsulting.no.

Faktasjekk og kilder

Alle tall i rapporten er sjekket mot kildene 26. oktober 2026. Tabellen viser hvordan hovedtallene er kontrollert, og hvilke forbehold som gjelder.

Påstand	Status	Merknad
Lekkasjesider, CISA, Europa, Norden og Norge	Egen optelling	Totalen for 2025 stemmer med ransomware.live (8 146) og CISAs publiserte tall (245).
Nye sårbarheter i CVE-listen	Egen optelling	September: 14 934 i CVE-listen, 15 074 i NVD med avviste poster. Linux-kjernen: 2 117 i NVD.
GuidePoint, ReliaQuest, Cyble, Check Point	Bekreftet	Hver kilde teller på sin egen måte, så tallene kan ikke legges sammen.
Google GTIG, VulnCheck og Rapid7	Bekreftet	Googles tall løper til og med august. Rapid7s 8 prosent gjelder trusselrapporter, ikke angrep.
Coveware, APWG, Resilience, Beazley, Marsh	Bekreftet	19 prosent står i Veeams PDF. Marshs tall for cyber gjelder tredje kvartal.
GuidePoint og Coalition om betaling og krav	Forbehold	GuidePoint oppgir ikke perioden for sammenligningen. Coalition er gjengitt via Digital Insurance.
NorForge og Reuters: Cairn-saken	Forbehold	Tallene kommer fra angriperens kontrollpaneler. 50 dollar er NorForges anslag. NorForge er norskledet, med morselskap i USA.
Microsoft: Storm-0940	Bekreftet	Microsofts egne data. De fleste forsøkene mislyktes.
Microsoft: ≈10× via Teams	Forbehold	Gjelder alle ondsinnede Teams-anrop. Falsk IT-støtte er det vanligste lokkemiddelet.
KI-sakene fra AWS, Google, Anthropic, Microsoft, Mozilla, Nordic Financial CERT og Kantonspolizei Schwyz	Bekreftet	Tallet på rundt 200 kunder hører til saken med gruppen tilknyttet ShinyHunters.
CrowdStrike: telefon, enhetskode, 88 prosent	Forbehold	Doblingen er mot andre halvår 2025. 88 prosent gjelder sårbarheter med offentlig angrepskode.
Beazley Security: 67 prosent	Forbehold	Gjelder innloggingsdata mot VPN og fjernskrivebord i innbrudd Beazley undersøkte.
Google, mai: KI-utviklet angrep	Forbehold	Google skriver at motaksjonen kan ha hindret bruken, ikke at den gjorde det.
Alpha IT	Forbehold	Filtallet er hackernes eget, og saken er overført til Kripos.
Clop, FortiBleed, Storm-3168	Forbehold	43 Clop-ofre er gruppens påstand. FortiBleed: «kan være berørt». Storm-3168: motivet er ukjent.
NSM om Citrix og om språkmodeller	Bekreftet	Hovedrådet 3. oktober er å ta enhetene av nett. Uttalelsen fra mai er gjengitt som referat.
Telia, Lørenskog, Laerdal, Datatilsynet, Nkom, NSM, politiet, Finans Norge, Tryg, NorSIS	Bekreftet	Laerdal bekrefter angrepet på leverandøren. Datatilsynets tall er gjengitt via kode24 og NTB.

Kilder

[Ransomware.live. Rådata og statistikk 2026.](#)
[CISA. Known Exploited Vulnerabilities Catalog.](#)
[GuidePoint. GRIT Q2 2026 \(9.7.2026\).](#)
[GuidePoint. GRIT Q3 2026 \(8.10.2026\).](#)
[ReliaQuest. Ransomware Q2 2026.](#)
[Check Point. September 2026 \(8.10.2026\).](#)
[Cyble. Ransomware brief, august 2026.](#)
[VulnCheck. State of Exploitation 1H 2026.](#)
[Google GTIG. Exploitation trends in the AI era \(30.9.2026\).](#)
[CrowdStrike. Threat Hunting Report 2026.](#)
[Expel. Q2 2026 Threat Report.](#)
[Beazley Security. Q2 2026.](#)
[Coveware. Q2 2026.](#)
[Veeam/Coveware. Cyber Extortion Report Q2 2026.](#)
[Microsoft. Email threat landscape Q2 2026.](#)
[APWG. Phishing Activity Trends Q2 2026.](#)
[Resilience. H1 2026 Cyber Risk Report.](#)
[Beazley, halvår 2026, via Reinsurance News.](#)

[Help Net Security. EU-kommisjonen \(3.4.2026\).](#)
[Bitsight. FortiBleed \(18.6.2026\).](#)
[Tech Times. Clop og PTC Windchill \(15.8.2026\).](#)
[CyberScoop. Clop og PTC Windchill \(19.8.2026\).](#)
[NSM. Citrix NetScaler \(3.10.2026\).](#)
[AWS. AI-augmented threat actor \(20.2.2026\).](#)
[Nau.ch. Schwyz \(20.1.2026\).](#)
[Google GTIG. AI and initial access \(11.5.2026\).](#)
[Google GTIG. From Prompting to Autonomy \(8.9.2026\).](#)
[Anthropic. Threat report, september 2026.](#)
[Microsoft. Storm-3168 \(25.9.2026\).](#)
[Microsoft. Storm-0940 \(21.10.2026\).](#)
[Mozilla. Hardening Firefox \(mai 2026\).](#)
[NorForge. Inside Cairn \(19.10.2026\).](#)
[Reuters via CP24. KI-agenter \(19.10.2026\).](#)
[Rapid7. Q3 2026 \(21.10.2026\).](#)
[CVE-listen via cve.Oxosprey.com.](#)
[Coalition via Digital Insurance \(20.10.2026\).](#)
[Marsh. Index Q3 2026 \(21.10.2026\).](#)

[Datatilsynet via kode24 \(20.10.2026\).](#)
[Laerdal. Pressemelding \(23.10.2026\).](#)
[NSM. To kritiske sårbarheter i PHP \(21.10.2026\).](#)
[kode24. Ingen tegn til hacking i Norge \(23.10.2026\).](#)
[Tenable. PHP2Shell FAQ \(21.10.2026\).](#)
[Nkom. ROS 2026 \(21.10.2026\).](#)
[Nordic Financial CERT, intervju \(7.4.2026\).](#)
[NSM. Om Mythos og Anthropic \(12.5.2026\).](#)
[ITavisen. Telia \(4.3.2026\).](#)
[Lørenskog kommune. IT-hendelsen.](#)
[digi.no. Alpha IT \(26.6.2026\).](#)
[MN24. Trondheimsbedrift hacket \(21.8.2026\).](#)
[digi.no. Angrep mot Digdir \(26.8.2026\).](#)
[Regnskap Norge. Altinn og Skatteetaten \(5.10.2026\).](#)
[Politiet Nordland. Nyhetsbrev, mai 2026.](#)
[Finans Norge. Svindel 2026 \(8.4.2026\).](#)
[Tryg. Direktørsvindel med KI \(17.6.2026\).](#)
[NorSIS og Opinion. Digital dømmekraft \(1.6.2026\).](#)

Lekkasjesider, CISA og CVE-listen: egen optelling i rådata per 26. oktober 2026. Sannsynlighetene er mine egne anslag. Spørsmål og innspill: [spadeconsulting.no](#).