



Beyond The Breaches

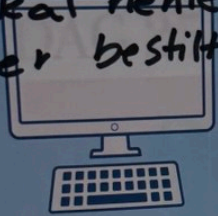
What I learned from the Datatilsynet reports

Michael Markevich

Who Am I

- Cybersecurity practitioner with over 25 years of experience
- 3 x CISO, startup advisor and founder
- Career mentor and academic lecturer
- Open-source software engineer and privacy enthusiast

Ta kontakt med
personalet dersom
du skal hente varer
som er bestilt.



Vårt datasystem
er nede

Vi kan dessverre ikke
ekspedere kunder nå.

Se hele programmet på foreside-siden

 **APOTEK 1**
Vår kunnskap - din trygghet

The Story

Why this talk?

Article 33 GDPR

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority [...]

Article 33 GDPR (continued)

3. The notification referred to in paragraph 1 shall at least:
 - (a) describe the nature of the personal data breach [...];
 - (b) [...];
 - (c) describe the likely consequences of the personal data breach;
 - (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach [...].

elnnsyn



Provides access to correspondence to and from governmental agencies in Norway.

A screenshot of the elnnsyn website's search interface. The browser window shows the URL www.elnnsyn.no. The website header includes the elnnsyn logo, navigation links for Search, Meeting calendar, and About us, and user options for Cart, English, and My elnnsyn. The main section has a large blue background with the text "Search for document" and a search bar with the placeholder "Search here...". To the right of the search bar are links for "Advanced search" and a "Search" button. Below the search bar is a "Filter" section with five expandable filter boxes: "Document type", "State", "Municipality", "County", and "Date", each with a plus sign. A "Hide filter" button is located to the right of the filter section.

The Request



I requested data breach reports from private companies (AS) submitted to Datatilsynet from January 2025.

The screenshot shows a web browser window with the URL www.einnsyn.no/minside/innsynskrav. The page title is 'Access request (468)' and there is a 'Download' button. The main content is a table with the following columns: Title, Organisation/committee, Published, Case no., Doc. type, and Status. Two rows are visible, both from the 'Data Protection Authority'.

Title	Organisation/ committee	Published	Case no.	Doc. type	Status
Melding om avvik - TIBE MOLDE AS	Data Protection Authority	30.06.2025	2025/1987	Incoming document	Sent to organisation 18.08.2025 Remove
Melding om avvik - HÅNDVERKSDATA AS	Data Protection Authority	04.07.2025	2025/2138	Incoming document	Sent to organisation 18.08.2025 Remove

The Response

Mottak av over 400 innsynskrav til Datatilsynet [eInnsyn/Datatilsynet x](#)



← **Postkasse** <postkasse@datatilsynet.no>

to me ▾

19 Aug 2025, 10:07



Hei

Vi viser til dine innsynskrav i et veldig høyt antall dokumenter hos Datatilsynet.

Vi ønsker å gjøre deg oppmerksom på at behandling av disse over 400 innsynskravene må behandles manuelt hos Datatilsynet, noe som krever at vi må bruke betydelig med ressurser på akkurat dette.

Er det noe spesielt du er ute etter, så kan vi bistå med å gi innsyn i aktuelle dokumenter i stedet for å bruke store deler av vår kapasitet på å behandle innsynskrav som kanskje ikke er interessant for deg.

Hvis du ønsker å opprettholde alle disse innsynskravene, gjør vi deg oppmerksom på at det vil ta mer tid enn 1-3 virkedager før samtlige anmodninger er behandlet (jf. offentleglova § 29).

Med vennlig hilsen



The Response (continued)

In the following three weeks I received ~**500 responses** from Datatilsynet, and **319 full reports** in total.

The remaining ~**180 reports** were not received due to sensitivity of the information.

Data Quality

Average :(so automated and manual verification was applied.

1 of 5 25_00905-1 1 Hoveddokument.pdf 50%

Melding om avvik

 Datatilsynet

Innsender

Organisasjonsnummer	984661185
Navn	POSTEN BRING AS
Adresse	Postboks 1500 Sentrum
Postnr og sted	0001 OSLO

Det er sendt inn en melding om avvik for denne avgiveren tidligere.

Er dette en ny avviksmelding eller et tillegg til en tidligere innsendt melding?

☒ Ny melding ☐ Tillegg til tidligere innsendt melding

Melder din virksomhet dette avviket som behandlingsansvarlig eller databehandler?

☒ Behandlingsansvarlig ☐ Databehandler

Beskrivelse av avviket

26.02.2025 15:13:12 AR667711417

Excluded Reports

Most common "boring" cases:

- Mass email sent to all recipients in To: or Cc: (instead of Bcc:)
- Wrong email recipient or data subject selected

Research Scope

Filter (from 319 total reports):

- Private sector (*AS*, *aksjeselskap*) only
- Submitted to Datatilsynet in 2025
- Only non-human (technical and other) issues

The final scope: 93 unique incidents reported by 85 companies.

The Statistics

Some numbers to consider

Incident Timings

Half of the incidents were resolved **within a day**.

The median for the remaining half was **32 days**.

NOTE: based on the context of incidents, the times are highly inaccurate in many cases.

Risk Assessment

Only 20% (18 of 93) of reports mention that risk assessment of the incidents was performed.

Supply Chain

Nearly 30% of incidents (29 of 93) are directly related to a third-party service provider (or cloud service).

Physical Security

Small but real! 5% of incidents (5 of 93) are related to equipment theft (*and 4 of 5 breaches use the same attack vector*).

The Analysis

Facts and conclusions

Root Causes

1. Phishing and credential theft
2. Misconfigurations and access control failures
3. Ransomware and direct hacking
4. Software bugs and API vulnerabilities

Root Causes (continued)

So human factor is still the most frequent problem. But what are the countermeasures?

Counter-measures

1. Account security tightening and access revocation
2. Updating and creating formal policies and routines
3. Employee training and awareness programs

What Could Be Done Better?

- More practical risk analysis
- Security automation (to eliminate human factor)
- More transparency in maintaining customer trust

Melder din virksomhet dette avviket som behandlingsansvarlig eller databehandler? ☒ Behan

Beskrivelse av avviket

Hovedårsak til avviket Teknisk svikt

Tidsrom for avviket 10/25/2024 til 10/26/2024

Når ble avviket oppdaget 10/27/2024 Kl. 14:00

Angi hvor mange personer som kan være berørt av avviket

Beskriv hva som har skjedd. Begrunn her om det er behov for å rapportere avviket, og hvilke hjemler som ligger til grunn. Datatilsynet vil gjøre en

Noen har kommet inn på våre servere og kryptert dem.

Hvordan oppstod avviket?

Foreløpig uklart - serverene driftes i et Azure-miljø av Abac data.

Beskriv hva slags type personopplysninger som ble berørt av avviket

Foreløpig uklart. Vi er en ortopediteknisk virksomhet (produksjon av proteser) som har en pasientdatabase som kan være berørt. Den er i utgangspunktet

Hvilken relasjon har virksomheten til de personene som er berørt av avviket

De er pasienter hos oss

Beskriv hvor personopplysningene befinner seg etter avviket, og hvilke mottakere som kan ha fått eller sett opplysningene.

Vi vet pr nå ikke om data er hentet ut, men det ser ikke slik ut. Vi har ikke mottatt noen krav på løsen eller tilsvarende.



Fun Time

(which was not actually fun at all)

Enumerate All Parking Receipts For A Year

1 of 2

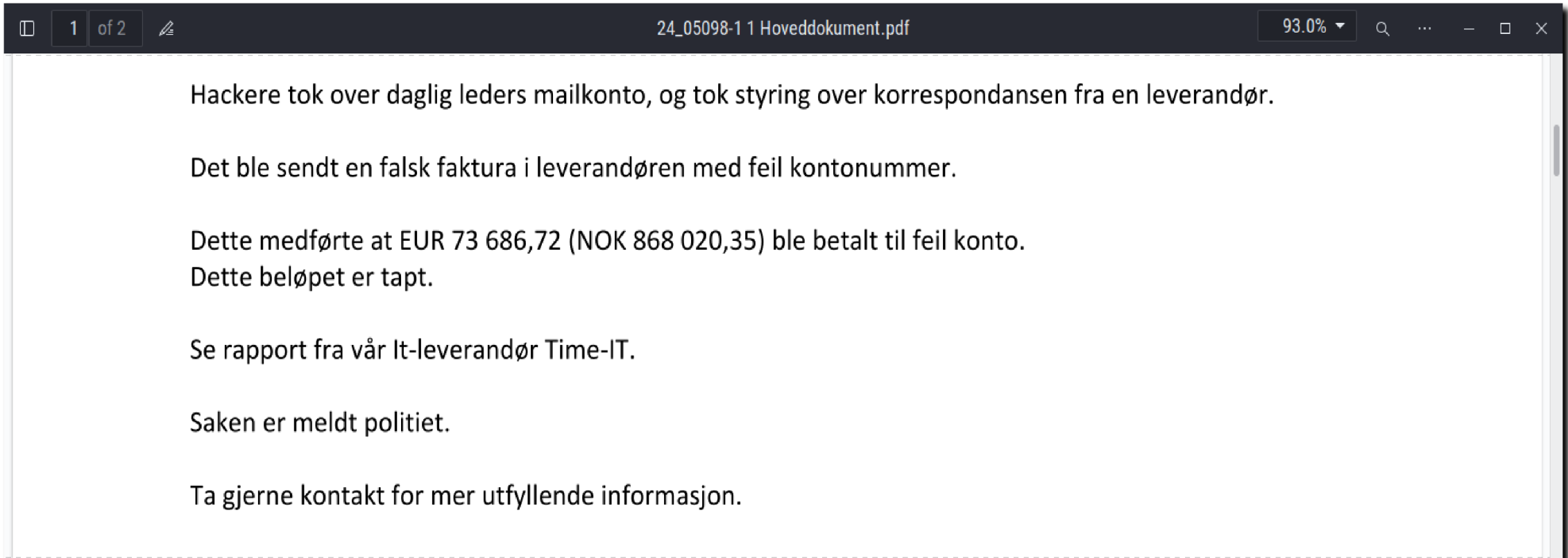
24_05035-1 1 Hoveddokument.pdf

92.9%

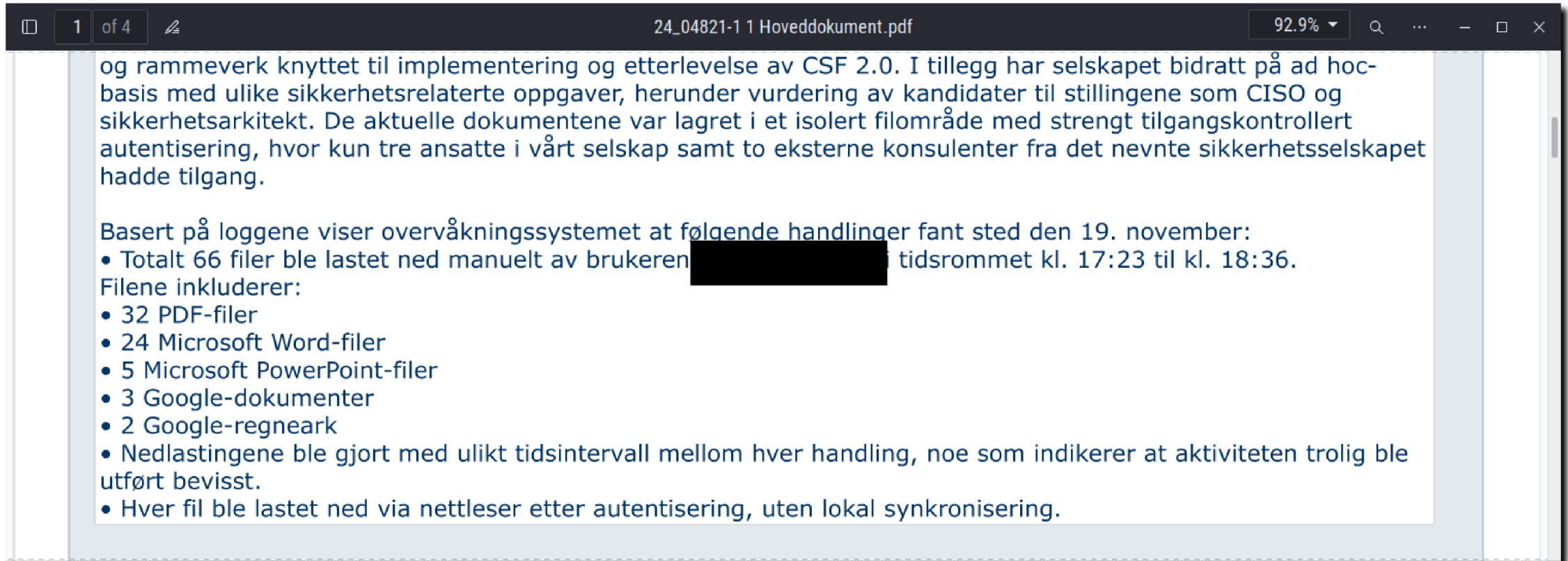
Q ... - □ X

Tidsrom for avviket	29.03.2023	til	06.12.2024
Når ble avviket oppdaget	06.12.2024	Kl.	10:00:00
Angi hvor mange personer som kan være berørt av avviket	1		
Beskriv hva som har skjedd. Begrunn her om det er behov for å unnta fra offentlighet hele/deler av meldingen, og hvilke hjemler som ligger til grunn. Datatilsynet vil gjøre en selvstendig vurdering av dette.			
Svakhet i et API som gjør at man har kunnet hente ut kvitteringsdata for andre personer/virksomheter enn seg selv. Det omhandler avgiftsparkerings-kvitteringer. Ved å endre en URL i nettleser vil man kunne få opp andre kvitteringer. Det er ikke mulig å spesifikt finne kvitteringer basert på person eller kjøretøy, de er nummerert med tall som ikke har sammenheng mot person eller kjøretøy. Da det er et stort antall kvitteringer vil det være tilnærmet umulig å hente ut spesifikk informasjon via denne svakheten.			
Hvordan oppstod avviket?			
Avviket oppstod i forbindelse med implementering av en ny funksjon i systemet.			

Pay 70K EUR To A Stranger



Hire A Security Firm To Leak CISO Candidate CVs

A screenshot of a PDF document viewer showing a document titled "24_04821-1 1 Hoveddokument.pdf". The document content is in Norwegian and discusses the implementation of CSF 2.0 and a security audit. It mentions that a security firm was hired to leak CISO candidate CVs. The document is displayed on page 1 of 4, with a zoom level of 92.9%.

og rammeverk knyttet til implementering og etterlevelse av CSF 2.0. I tillegg har selskapet bidratt på ad hoc-basis med ulike sikkerhetsrelaterte oppgaver, herunder vurdering av kandidater til stillingene som CISO og sikkerhetsarkitekt. De aktuelle dokumentene var lagret i et isolert filområde med strengt tilgangskontrollert autentisering, hvor kun tre ansatte i vårt selskap samt to eksterne konsulenter fra det nevnte sikkerhetsselskapet hadde tilgang.

Basert på loggene viser overvåkningssystemet at følgende handlinger fant sted den 19. november:

- Totalt 66 filer ble lastet ned manuelt av brukeren [REDACTED] tidsrommet kl. 17:23 til kl. 18:36.

Filene inkluderer:

- 32 PDF-filer
- 24 Microsoft Word-filer
- 5 Microsoft PowerPoint-filer
- 3 Google-dokumenter
- 2 Google-regneark

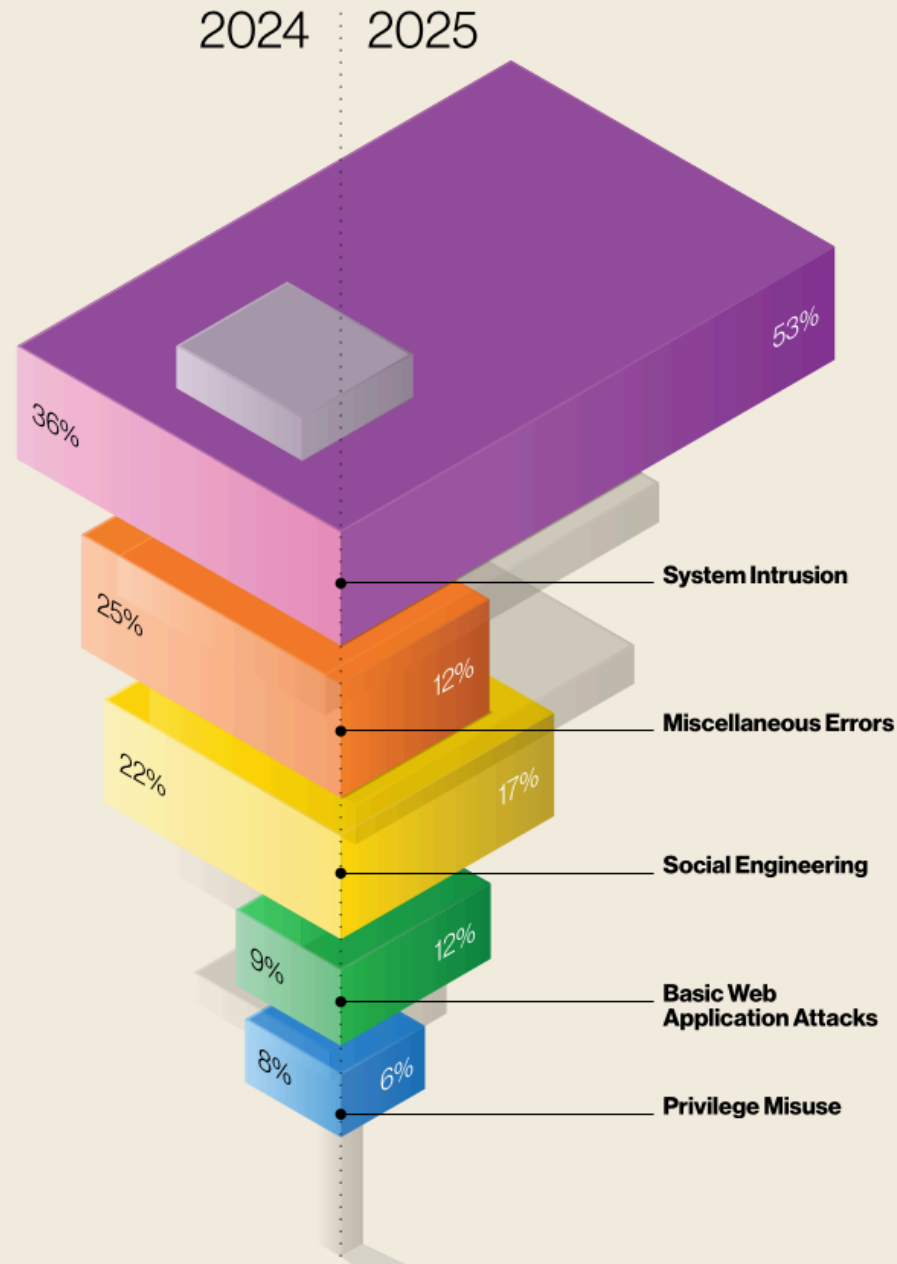
Nedlastingene ble gjort med ulikt tidsintervall mellom hver handling, noe som indikerer at aktiviteten trolig ble utført bevisst.

- Hver fil ble lastet ned via nettleser etter autentisering, uten lokal synkronisering.

The Summary

Conclusions and remarks





Verizon Data Breach Investigations Report 2025

Conclusions

Protecting against human-factor vulnerabilities with human-factor counter-measures doesn't work anymore.

Conclusions (continued)

Many companies still trust their providers more than they should, and critical scenarios are still viewed as unrealistic, ignoring global industry trends.

Conclusions (still continued)

Many companies are not able to maintain and demonstrate trust to their clients and users.

Acknowledgements

The Datatilsynet team and personally Kristine Stenbro for useful insights and feedback.



Thank You

