ORTEC FINANCE

Major ICT-incidenten 2025

Wat pensioenfondsen moeten leren van het eerste ESA-overzicht onder DORA

Inhoudsopgave

Managementsamenvatting 3
1. Niet het incident zelf, maar de keten eromheen bepaalt de impact 4
2. Wat het ESA-rapport laat zien 4
3. Waarom dit voor pensioenfondsen extra relevant is 5
4. Drie incidenttypen die voor pensioenfondsen bijzonder relevant zijn 5
   4.1. De systeemfout bij een kritieke leverancier 6
   4.2. De verstoring die ontstaat dieper in de uitbestedingsketen 6
   4.3. Het cyberincident met datalek- of ransomwarecomponent 6
5. Generieke aandachtspunten 6
   5.1. Ken de kritieke afhankelijkheden in de keten 6
   5.2. Regel incidentafspraken expliciet in contracten en SLA's 6
   5.3. Maak communicatie onderdeel van incidentbeheersing 7
   5.4. Oefen realistische scenario's in de keten 7
   5.5. Verbind techniek aan bestuurlijke besluitvorming 7
6. Vijf bestuurlijke vragen voor de eerste uren van een incident 7
7. Conclusies 7
8. Auteurs 8

Managementsamenvatting

Digitale incidenten zijn geen uitzonderingen meer. Het eerste gezamenlijke jaaroverzicht van de Europese toezichthouders laat zien dat in 2025 in de Europese Unie 3.383 major ICT-related incidents zijn gemeld onder DORA. De toezichthouders benadrukken dat deze aantallen niet zonder meer wijzen op structurele zwaktes, maar vooral iets zeggen over de mate waarin de financiële sector digitaal, complex en onderling verbonden is geworden. Weerbaarheid blijkt vooral uit het vermogen om incidenten tijdig te signaleren, te beheersen en de schade voor klanten en processen te beperken.

Een belangrijke nuancering is dat de impact van veel incidenten beperkt bleek. Dat laat zien dat digitale weerbaarheid niet alleen gaat over het voorkomen van incidenten, maar ook over tijdige detectie, effectieve respons en het beperken van doorwerking naar deelnemers, processen en ketenpartners.

Voor pensioenfondsen is vooral de onderliggende boodschap relevant. Voor pensioenfondsen ligt een belangrijke kwetsbaarheid vaak niet alleen in de techniek zelf, maar juist ook in de bestuurlijke beheersing van uitbestedingsketens. Pensioenfondsen opereren in een omgeving waarin de uitvoering zoals pensioenadministratie, vermogensbeheer en communicatie voor een belangrijk deel buiten de eigen organisatie plaatsvinden. Daardoor ontstaan bij incidenten vaak vragen over regie, informatiepositie, verantwoordelijkheden, communicatie en escalatie.

Dat in het ESA-overzicht relatief weinig major ICT-incidenten in de pensioensector zijn gemeld, betekent niet dat pensioenfondsen ook weinig ICT-risico lopen. Incidenten kunnen zich juist voordoen bij uitvoerders, IT-leveranciers, vermogensbeheerders of andere ketenpartijen, en daardoor alsnog pensioenprocessen, deelnemersgegevens, communicatie of besluitvorming raken. Bovendien spelen veel van de onderliggende ICT-risico's ook in andere financiële subsectoren, zoals verzekeraars, waar grootschalige verwerking van gevoelige persoonsgegevens laat zien hoe groot de potentiële impact kan zijn. Voor pensioenfondsen ligt de kern daarom niet in het aantal meldingen, maar in het vermogen om ketenrisico's tijdig te herkennen, te beheersen en bestuurlijk te regisseren.

De belangrijkste lessen voor pensioenfondsen zijn daarom strategisch van aard. Ten eerste moet het fonds weten welke processen en ketenpartners werkelijk kritisch zijn. Ten tweede moeten verantwoordelijkheden en informatiebehoeften vooraf concreet zijn uitgewerkt. Ten derde moet communicatie net zo serieus worden voorbereid als herstelmaatregelen. En ten vierde is oefenen essentieel. Niet om technische kennis te toetsen, maar om besluitvorming, samenwerking en communicatie onder druk te doorleven.

Kernboodschap

Voor pensioenfondsen is een major ICT-incident zelden alleen een technisch incident. Het is vooral een test van governance, ketenregie en communicatie.

1. Niet het incident zelf, maar de keten eromheen bepaalt de impact

Een ICT-incident begint zelden met volledige duidelijkheid. Vaak begint het met losse signalen: een melding van een uitvoerder, beperkte beschikbaarheid van systemen, vertraging in gegevensverwerking of een bericht dat nader onderzoek loopt. Juist in die eerste fase ontstaat voor pensioenfondsen de echte bestuurlijke uitdaging. Niet omdat het bestuur de techniek moet oplossen, maar omdat het snel moet bepalen wat er mogelijk speelt, welke belangen geraakt kunnen worden, wie de regie voert en welke communicatie noodzakelijk is. In een uitbestede omgeving wordt een operationele storing daardoor al snel een governancevraagstuk.

Die realiteit sluit nauw aan op het eerste gezamenlijke jaaroverzicht van de Europese toezichthouders onder DORA. In 2025 zijn in de Europese Unie 3.383 major ICT-related incidents[1] gemeld. Volgens de toezichthouders is dat geen bewijs van structurele onveiligheid, maar een weerspiegeling van de digitalisering, complexiteit en verwevenheid van de financiële sector. Het rapport benadrukt dat de weerbaarheid van organisaties blijkt uit hun vermogen om die incidenten tijdig te identificeren, te beheersen en de gevolgen te beperken.

Voor pensioenfondsen is dat een belangrijke boodschap. De sector kent immers een hoge mate van uitbesteding. Besturen blijven eindverantwoordelijk, terwijl de feitelijke uitvoering van kritieke processen veelal bij externe partijen ligt. Bij incidenten ontstaat daardoor gemakkelijk onduidelijkheid: wie beoordeelt de ernst, wie informeert het fonds, wie onderhoudt contact met toezichthouders, en wie bepaalt het moment van externe communicatie? De complexiteit zit dus niet alleen in de techniek, maar vooral in de keten van afhankelijkheden en communicatie met stakeholders.

2. Wat het ESA-rapport laat zien

Drie cijfers die ertoe doen

- *3.383 major ICT-related incidents gemeld in 2025 in de EU.*
- *Ongeveer één derde had een grensoverschrijdende impact.*
- *Bijna één derde kwam voort uit verstoringen of tekortkomingen bij derde partijen.*

Deze cijfers moeten worden gelezen als eerste, geaggregeerde indicatie onder het nieuwe DORA-rapportageraamwerk. Het ESA-rapport wijst erop dat rapportagepraktijken en datakwaliteit zich nog ontwikkelen. Ook is ongeveer 15% van de in 2025 gemelde major incidents niet meegenomen in de analyse, omdat op de peildatum nog geen finaal rapport beschikbaar was.

[1] Onder DORA betreft dit ICT-gerelateerde incidenten met een grote nadelige impact op de netwerk- en informatiesystemen die kritieke of belangrijke functies van een financiële entiteit ondersteunen.

Het ESA-rapport beschrijft de eerste jaarlijkse geaggregeerde analyse van major ICT-related incidents onder DORA. In totaal werden 3.383 major incidents gemeld in 2025. Ongeveer één derde van deze incidenten had een grensoverschrijdende impact. Daarnaast kwam bijna één derde voort uit verstoringen bij derde partijen, waaronder ICT-dienstverleners, andere financiële instellingen en infrastructuurproviders. Het rapport noemt systeemfouten en externe gebeurtenissen als de dominante oorzaken van incidenten.

Het rapport laat zien dat ICT-risico's zich vaak niet beperken tot één organisatie of één land. Dat komt doordat financiële instellingen steeds vaker gebruikmaken van gedeelde infrastructuren, gemeenschappelijke ICT-diensten en internationale ketens van dienstverlening. Voor pensioenfondsen is dit relevant, omdat een incident daardoor ook kan ontstaan of doorwerken buiten de directe uitvoerder of contractrelatie. Dit onderstreept dat incidentmanagement niet alleen om herstel draait, maar ook om tijdige en betrouwbare informatie uit de keten.

3. Waarom dit voor pensioenfondsen extra relevant is

Voor pensioenfondsen zit de extra relevantie van dit rapport vooral in de bestuurlijke gevolgen van incidenten in een uitbestede keten. Bij een verstoring is niet alleen van belang wat er technisch is gebeurd, maar vooral of snel duidelijk wordt welke processen zijn geraakt, wie verantwoordelijk is voor de opvolging en welke informatie beschikbaar is voor besluitvorming en communicatie.

Juist daar is de foutmarge klein. Pensioenuitkeringen moeten doorgaan, deelnemersgegevens moeten beschermd blijven en communicatie richting deelnemers, werkgevers en toezichthouders moet zorgvuldig blijven en tijdig plaatsvinden.

De kernvraag is daarom niet alleen wat er technisch is misgegaan, maar vooral wat het incident betekent voor het fonds en welke besluiten direct nodig zijn. Dat vraagt om voorbereiding, keteninzicht en een heldere rolverdeling.

Daarbij moet het fonds in de eerste uren kunnen bepalen of het incident raakt aan beschikbaarheid van kritieke processen, deelnemersgegevens, uitkeringen, wettelijke verplichtingen of reputatie. Juist deze impactvragen sluiten aan bij de manier waarop onder DORA wordt beoordeeld of een incident als major moet worden aangemerkt.

4. Drie incidenttypen die voor pensioenfondsen bijzonder relevant zijn

Meest relevante incidenttypen voor pensioenfondsen

- *Systeemfout bij een kritieke leverancier;*
- *Verstoring die ontstaat dieper in de uitbestedingsketen;*
- *Cyberincident met datalek- of ransomwarecomponent.*

4.1. De systeemfout bij een kritieke leverancier

Het ESA-rapport laat zien dat systeemfouten[2] tot de belangrijkste oorzaken van major incidents behoren. Voor pensioenfondsen is dat zeer relevant. Juist waar uitvoerende processen afhankelijk zijn van externe systemen en platformen. Een foutieve wijziging, mislukte update of technische storing kan dan leiden tot vertragingen in de verwerking, beperkte beschikbaarheid van gegevens of onzekerheid over de continuïteit van processen. De bestuurlijke uitdaging zit dan vaak in het feit dat in de eerste fase nog onduidelijk is wat precies geraakt is en hoe groot de impact is.

4.2. De verstoring die ontstaat dieper in de uitbestedingsketen

Bijna een derde van de major incidents was volgens het rapport terug te voeren op derde partijen. Voor pensioenfondsen is dit vooral relevant bij verstoringen die ontstaan bij pensioenuitvoeringsorganisatie, vermogensbeheerders , IT- of softwareleveranciers of andere partijen verderop in de uitbestedingsketen.

4.3. Het cyberincident met datalek- of ransomwarecomponent

Hoewel cyberincidenten volgens het ESA-rapport een kleiner deel van de gerapporteerde major incidents uitmaakten, blijven zij voor pensioenfondsen zeer relevant. Dat komt door de combinatie van gevoelige deelnemersgegevens, mogelijke verstoring van kritieke processen en de noodzaak tot beheerste communicatie. Zulke incidenten raken niet alleen de beschikbaarheid van systemen, maar ook vertrouwen, reputatie en de vraag hoe en wanneer stakeholders geïnformeerd moeten worden.

5. Generieke aandachtspunten

5.1. Ken de kritieke afhankelijkheden in de keten

Pensioenfondsen doen er goed aan om scherp te onderscheiden welke processen en ketenpartners werkelijk kritisch zijn. Voor partijen waarvan uitval direct kan doorwerken naar uitkeringen, datakwaliteit, deelnemersgegevens, of (verplichte) communicatie, moet het fonds precies weten welke afhankelijkheden er bestaan en welke informatie in een incident als eerste nodig is.

5.2. Regel incidentafspraken expliciet in contracten en SLA’s

Contracten en SLA’s moeten meer bevatten dan algemene bepalingen over dienstverlening en beschikbaarheid. Juist bij kritieke of belangrijke ICT-gerelateerde diensten moeten afspraken concreet zijn over melding van incidenten, informatie-uitwisseling, escalatie, herstel, auditrechten, medewerking aan onderzoek en communicatieafstemming.

[2] Met systeemfouten worden storingen of defecten in systemen of applicaties bedoeld, bijvoorbeeld als gevolg van softwareproblemen, foutieve configuraties, mislukte updates of andere technische mankementen.

5.3. Maak communicatie onderdeel van incidentbeheersing

Wanneer deelnemers, werkgevers, toezichthouders of media signalen oppakken terwijl het feitenbeeld nog onvolledig is, ontstaat al snel onrust. Daarom moet vooraf duidelijk zijn wie namens het fonds spreekt, hoe wordt afgestemd met uitvoerder of andere ketenpartners, welke kernboodschap in de eerste fase geldt en hoe vervolginformatie wordt gedeeld.

5.4. Oefen realistische scenario's in de keten

Oefenen maakt zichtbaar waar verantwoordelijkheden onduidelijk zijn, waar informatievoorziening stokt en waar besluitvorming te lang duurt. Voor pensioenfondsen is het daarom verstandig om niet alleen interne tabletop-oefeningen te organiseren, maar ook scenario's te oefenen waarin uitvoerder en andere ketenpartners een rol spelen.

5.5. 5.5 Verbind techniek aan bestuurlijke besluitvorming

Pensioenfondsbesturen hoeven geen technische specialisten te zijn, maar moeten wel begrijpen welke technische thema's bestuurlijk relevant zijn. Denk aan herstelvermogen, back-up en recovery, change management, logging, toegangsbeheer en afhankelijkheid van specifieke ICT-leveranciers. Het doel is om de juiste vragen te kunnen stellen aan uitvoerders en leveranciers.

6. Vijf bestuurlijke vragen voor de eerste uren van een incident

1. Wat weten we zeker — en wat nog niet?
2. Welke kritieke processen, deelnemersgegevens, uitkeringen, wettelijke verplichtingen, of stakeholders kunnen geraakt worden?
3. Welke partij heeft nu de operationele leiding en welke rol heeft het fonds?
4. Welke informatie verwachten wij binnen welk tijdsvenster uit de keten?
5. Wat communiceren wij nu intern en extern?

7. Conclusies

De belangrijkste les uit het eerste ESA-overzicht is niet dat digitale incidenten uitzonderlijk zijn, maar dat zij waarschijnlijker worden in een sector die steeds digitaler, complexer en meer verweven raakt. 'Major incidents' in 2025 hingen vaak samen met systeemfouten, externe gebeurtenissen en verstoringen bij derde partijen.

Voor pensioenfondsen is digitale weerbaarheid meer dan technische beheersing alleen. Doorslaggevend is of het fonds zijn kritieke afhankelijkheden kent, verantwoordelijkheden helder heeft belegd en in een incident snel over betrouwbare informatie beschikt. Juist in een uitbestede keten bepaalt dat of een incident bestuurbaar blijft.

Digitale weerbaarheid is daarmee voor pensioenfondsen niet alleen een kwestie van beveiliging, maar vooral van goed bestuur.

8. Auteurs

Simon Heerings

Senior Risk Consultant

Simon.heerings@ortec-finance.com

Simon Heerings - Ortec Finance | LinkedIn

Aswin Bouwmeester

Senior Risk Consultant

Aswin.bouwmeester@ortec-finance.com

https://www.linkedin.com/in/aswin-bouwmeester-0163a217/

Disclaimer

Ortec Finance would like to emphasize that Ortec Finance is a software provider of technology and IT solutions for risk and return management for institutions and private investors. Please note that this information has been prepared with care using the best available data. This information may contain information provided by third parties or derived from third party data and/or data that may have been categorized or otherwise reported based upon client direction. For this information of third-party providers, the following additional terms and conditions regarding the use of their data apply: https://www.ortecfinance.com/en/legal/disclaimer.

Ortec Finance and any of its third-party providers assume no responsibility for the accuracy, timeliness, or completeness of any such information. Ortec Finance and any of its third-party providers accept no liability for the consequences of investment decisions made in relation on this information. All our services and activities are governed by our general terms and conditions which may be consulted on https://www.ortecfinance.com/ and shall be forwarded free of charge upon request.

Any analysis provided herein is derived from your use of Ortec Finance's software and does not constitute advice as to the value of securities or the advisability of investing in, purchasing, or selling securities. All results and analyses in connection with Ortec Finance's software are based on the inputs provided by you, the client. Ortec Finance is not registered as an investment adviser under the US Investment Advisers Act of 1940, an equivalent act in another country and every successive act or regulation. For the avoidance of doubt, in case terms like "client(s)" and "advisor(s)" are used in communications of Ortec Finance, then these terms are always referred to client(s) of Ortec Finance's contract client and its advisor(s).

contact@ortecfinance.com | www.ortecfinance.com

Rotterdam | Amsterdam | London | Zurich
Toronto | Melbourne | New York | Singapore