Ik heb een datalek in mijn contactcenter, wat nu?

Preventie, respons en herstel voor contactcentermanagers

STEAM®
CONNECT
empowering conversations

Dataveiligheid in contactcenters in 2026
Geschreven door Thom Boland & Jesse Schabracq.
In samenwerking met de redactie van Ziptone.

Uitgegeven door:
STEAM® CONNECT | empowering conversations

Mediapartner:
ziptone

LinkedIn

+31 85 0 474747
sales@steam-connect.com
steam-connect.com

Inhoudsopgave

Inleiding

Weet jij wat je moet doen als er morgen een datalek is in jouw contactcenter?

Niet in grote lijnen, maar concreet: wie bel je als eerste? Wat zet je stil en wanneer moet je een melding maken? De meeste contactcentermanagers hebben daar geen helder antwoord op. Niet omdat ze het niet belangrijk vinden, maar omdat een datalek zelden begint met een alarm. Vaak begint het met één overtuigend verzoek en een medewerker die gewoon zijn of haar werk doet.

Medewerkers hebben dagelijks toegang tot CRM-systemen, klantprofielen en financiële gegevens. Daarmee kan één account in de praktijk meerdere systemen tegelijk ontsluiten. Wanneer het misgaat, blijft de impact niet beperkt tot data alleen. Een incident leidt tot onderzoek, meldplicht, aanpassingen in toegangsrechten en een langdurige nasleep voor de operatie.

Deze whitepaper helpt je begrijpen hoe een datalek begint, hoe het zich ontwikkelt en wat je vandaag al kunt doen om je organisatie beter te beschermen.

Dataveiligheid is geen onderwerp waar je met plezier je agenda voor vrijmaakt. Toch is het precies het soort onderwerp waar je als contactcentermanager niet omheen kunt. Deze whitepaper geeft je de inzichten die je nodig hebt.

Veel leesplezier!

Thom Boland & Jesse Schabracq

1.Waarom contactcenters een aantrekkelijk doelwit zijn

Contactcenters bevinden zich op een unieke plek binnen organisaties. Ze vormen de schakel tussen klant en organisatie en hebben daardoor toegang tot een breed scala aan systemen en gegevens. Agents moeten tijdens een gesprek of chat snel klantinformatie kunnen opzoeken, wijzigingen kunnen doorvoeren en problemen kunnen oplossen.

Die efficiëntie is nodig voor goede service, maar heeft ook een keerzijde: één gebruikersaccount kan in de praktijk meerdere systemen ontsluiten. CRM-platforms, ticketsystemen en klantdatabases zijn vaak geïntegreerd, waardoor een succesvolle login veel meer toegang kan geven dan op het eerste gezicht zichtbaar is.

Daarbij maakt schaal het probleem niet fundamenteel anders, maar wel anders van vorm. Grote organisaties hebben vaak complexe CRM-landschappen, veel integraties en duizenden gebruikersaccounts, waardoor de aanvalsoppervlakte groeit. Kleinere organisaties hebben doorgaans minder complexe omgevingen, maar ook minder middelen en specialistische capaciteit om security structureel in te richten.

Fictieve case:
Energiecontact Nederland

Energiecontact Nederland is een middelgrote energieleverancier met circa 120.000 klanten en een contactcenter van 85 medewerkers. Klanten kunnen bellen, mailen en chatten.

Agents werken vanuit twee locaties en hebben dagelijks toegang tot CRM-gegevens, contracthistorie en betaalgegevens.

In de komende pagina's nemen we je mee in drie perspectieven op één incident: dat van de agent die het doelwit werd, de aanvaller die er gebruik van maakte en de manager die ermee werd geconfronteerd.

Daardoor is het contactcenter, ongeacht omvang, een plek waar kwetsbaarheid en verantwoordelijkheid samenkomen. Onderzoek van IBM laat zien waarom juist klantdata zo aantrekkelijk is voor aanvallers. In het Cost of a Data Breach Report 2025 had 53% van de onderzochte breaches betrekking op klantgegevens zoals e-mailadressen, adressen of identificerende gegevens. [1]

In een contactcenter, waar precies dat type informatie dagelijks wordt gebruikt, is dat een direct relevant risico. Dat maakt klantdata niet alleen aantrekkelijk voor aanvallers. Het is ook het datatype met de grootste meldplicht-impact onder de AVG. Persoonsgegevens van klanten vallen namelijk vrijwel altijd onder de categorie die melding aan de Autoriteit Persoonsgegevens vereist bij een breach. [4]

Check met je team: Waar ligt binnen jouw organisatie de nadruk? Op het beschermen van systemen, of op het gedrag van gebruikers?

2. Hoe een datalek meestal begint

Zoals te lezen valt in de fictieve casus hiernaast, begint een hack in een contactcenter meestal niet met zichtbare chaos, maar met geloofwaardigheid. Een e-mail lijkt van IT te komen. Een telefoontje klinkt alsof het van een leverancier of interne afdeling afkomstig is.

Een medewerker krijgt een verzoek dat logisch lijkt binnen de context van het werk: opnieuw inloggen, een account controleren, een wachtwoord resetten of een koppeling bevestigen. Juist omdat medewerkers in contactcenters gewend zijn om snel te helpen, kunnen zulke verzoeken overtuigend overkomen en een snelle reactie uitlokken.

De eerste stap is meestal het verkrijgen van toegang tot een account. Dat kan gebeuren via phishing, gestolen wachtwoorden of social engineering. IBM rapporteerde in 2025 dat phishing nog steeds de meest voorkomende initiële aanvalswijze was[1]. Het was goed voor 16% van de onderzochte breaches. Met deze aanvalsroute wordt niet per se eerst de techniek aanvallen, maar het vertrouwen en gedrag rondom toegang.

Voor contactcenters is dit voorbeeld extra relevant, omdat het werk van klantcontactmedewerkers juist draait om snelheid, klantgerichtheid en overtuigende communicatie. Dat betekent niet dat medewerkers onzorgvuldig zijn, maar wel dat aanvallers precies proberen in te spelen op de praktijk van een doorsnee werkdag.

Een lek begint daarom vaak niet bij een technisch defect, maar bij een menselijke interactie die op het verkeerde moment geloofwaardig genoeg lijkt.

De klantenservicemedewerker

Het is kwart over negen als Lisa haar headset opzet. Koffie staat klaar. CRM-scherm start op. Eerste klant al in de wacht.

Ze werkt al vier jaar bij Energiecontact Nederland en kent het systeem op haar duimpje. Namen, adressen, contractgegevens, IBAN-nummers. Alles netjes in één overzicht. Zo hoort het ook. Hoe zou ze anders klanten snel kunnen helpen?

Rond half elf krijgt ze een bericht via de interne chat. Of ze even haar inloggegevens kan bevestigen. Er is een storing op de server. IT heeft toegang tot haar account nodig om een reset door te voeren. **Urgent**, staat er. Haar collega twee stoelen verderop heeft hetzelfde bericht ontvangen.

Het ziet er precies uit zoals berichten van IT er altijd uitzien. Zelfde opmaak. Zelfde toon. Zelfs het profielplaatje klopt.

Lisa heeft het druk. Er staan acht klanten in de wacht. Ze vult in wat gevraagd wordt en gaat verder met haar dag. Helaas zit er aan de andere kant van dat bericht geen IT-collega.

Binnen het uur hebben de aanvallers toegang tot het klantcontactsysteem. Ze bewegen zich rustig door de omgeving. Bekijken welke data beschikbaar is. Exporteren klantprofielen. Namen. Adressen. Telefoonnummers. Contracthistorie. IBAN-nummers.

Geen alarm of melding, want het systeem ziet het als normaal gebruik. De login is namelijk legitiem.

3. Hoe een lek zich ontwikkelt in het contactcenter

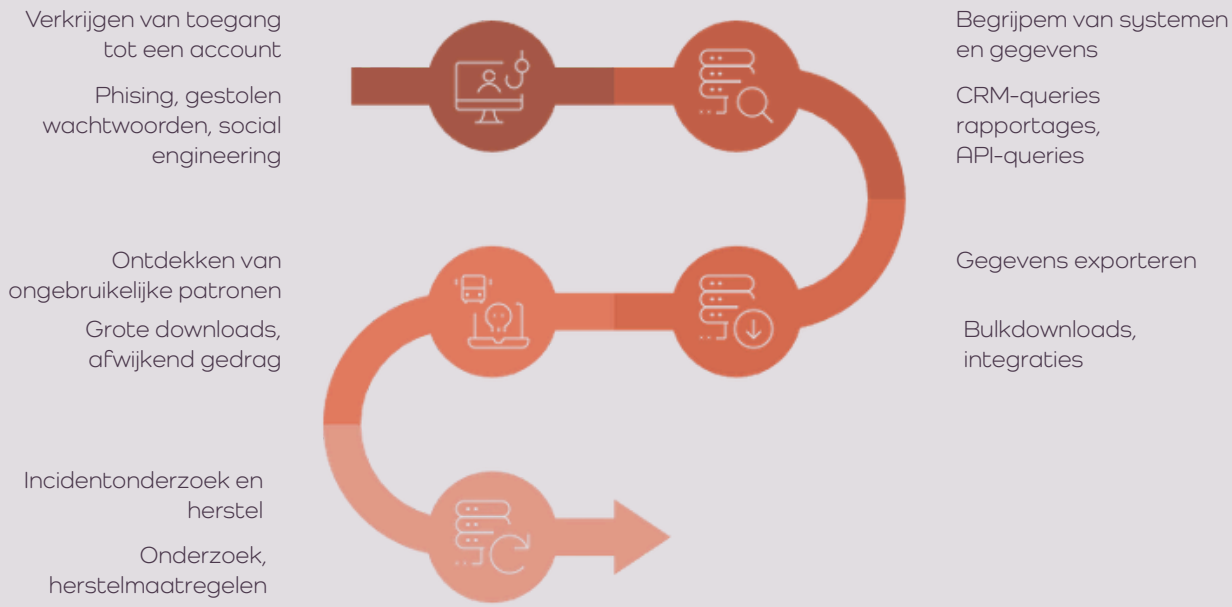
Zodra een aanvaller toegang heeft tot een account, begint meestal eerst een verkennende fase. Er wordt gekeken welke systemen bereikbaar zijn, welke data zichtbaar is en welke rechten een account precies heeft. In een contactcenter kan dat betekenen dat klantprofielen worden geopend, rapportages worden bekeken, exports worden getest of gekoppelde applicaties worden benaderd. Omdat veel van die handelingen lijken op normaal gebruik, valt dit niet altijd meteen op.

Daarna volgt vaak verbreding. Een aanvaller probeert te begrijpen waar nog meer toegang mogelijk is, welke data waarde heeft en welke routes er bestaan naar andere omgevingen. Juist in organisaties waar data verspreid staat over omgevingen, kan dat de situatie aanzienlijk complexer maken. Het rapport uit 2025 laat zien dat breaches met data in cloud-omgevingen gemiddeld het langst duurden om te identificeren en te containen: 276 dagen in 2025, tegenover 217 dagen voor on-premise breaches. [1]

Real-world doorlooptijden (IBM 2025)

- Gemiddelde breach lifecycle: 241 dagen (identificatie + containment);
- Multi-environment breaches: 276 dagen vs 217 dagen voor on-premises;
- Ter vergelijking: in 2021 was het 287 dagen, waar het in 2024 gemiddeld nog 258 dagen was; [1, 2]

Responstijdlijn bij een cyberaanval



Check met je team: Worden bulkexports en grote downloads bij jullie automatisch gesignaleerd? Zo ja, door wie worden ze beoordeeld?

Volledige duidelijkheid over scope en schade komt in de praktijk altijd later dan organisaties vooraf verwachten[1]. Binnen 72 uur is het doorgaans mogelijk om het type incident te schetsen, een eerste inschatting te maken van de betrokken data en de containment-maatregelen te beschrijven. Maar de totale schade vraagt bijna altijd forensisch onderzoek en business impact-analyses die weken tot maanden in beslag nemen. Dat geldt in het bijzonder voor incidenten waarbij data verspreid staat over meerdere omgevingen.

De fase daarna is de fase waarin concrete schade ontstaat: ongebruikelijke exports, bulkdownloads, raadpleging van grote aantallen klantrecords of misbruik van meerdere sessies en accounts. Pas wanneer die patronen zichtbaar worden, wordt een incident sneller herkend. Dat onderstreept dat een hack zich vaak langer en onopgemerkter ontwikkelt dan managers vooraf verwachten.

De hacker

Hij begint zijn dag niet in een systeem, maar in een lijstje. Namen van medewerkers met functies en afdelingen. Kleine stukjes informatie die genoeg zijn om geloofwaardig te klinken. Hij kiest geen manager of specialist. Hij kiest iemand die toegang heeft en vooral bezig is met doorwerken.

Aan het einde van de ochtend verstuurt hij een bericht dat lijkt op iets wat in een contactcenter vaker langskomt. Een controle van een account met het verzoek om een sessie opnieuw te bevestigen. Niets groots. Niets dat meteen vragen oproept. Een paar minuten later ziet hij dat er beweging komt. Iemand heeft gedaan wat hij hoopte.

Daarmee begint het echte werk. Hij logt niet overal tegelijk in, maar opent eerst rustig de omgeving. Hij kijkt welke schermen direct beschikbaar zijn en opent een klantprofiel. Daarna nog een en daarna een scherm met historie.

Hij wil zien hoeveel informatie op één plek samenkomt en welke functies hij zonder extra controle kan gebruiken. Pas als dat duidelijk is, gaat hij verder. Hij probeert zoekfuncties, filters en kijkt of hij gegevens kan opslaan, verzamelen of in kleine stappen kan ophalen zonder op te vallen.

Hij werkt bewust langzaam. Een account dat zich gedraagt zoals een medewerker, krijgt minder aandacht. Dat weet hij. Zolang het account actief blijft, groeit zijn speelruimte.

Een naam wordt een adres. Een adres wordt een klantdossier. Een klantdossier wordt een bestand van grote waarde.

4. Wat er gebeurt zodra je ontdekt dat er iets mis is

De AVG stelt een strikte meldplicht: de verwerkingsverantwoordelijke moet een datalek zonder onredelijke vertraging en waar mogelijk binnen 72 uur aan de toezichthouder melden [4]. Dat is een deadline voor het starten van de meldstroom. De European Data Protection Board (EDPB) erkent dat informatie gefaseerd kan worden aangeleverd wanneer niet alles tegelijk beschikbaar is [4]. De EDPB is een onafhankelijk Europees orgaan dat toeziet op toepassing van de AVG. Organisaties moeten een datalek bovendien intern registreren. Daaronder vallen feiten, effecten en genomen maatregelen. Hiermee kan de toezichthouder compliance verifiëren. De meldplicht en de registratieplicht zijn daarbij twee aparte verplichtingen.

Vanaf het moment dat er een serieus vermoeden is van een incident, verandert de situatie direct. In de praktijk bestaat een calamiteitenplan voor een datalek meestal niet uit één document, maar uit een combinatie van een Incident Response Plan, een crisis- of communicatieplan en een bedrijfscontinuïteitsplan (BCP) of een Disaster Recovery Plan (DRP) voor continuïteit en herstel. De doelen van die plannen worden toegelicht in hoofdstuk 6.

De eerste vraag is meestal niet of je rustig doorwerkt of alles stilzet, maar welke delen van de operatie je gericht moet beperken om verdere schade te voorkomen. Best practice is containment zo snel als nodig, maar zo beperkt als mogelijk. Dat kan betekenen dat specifieke accounts worden geblokkeerd, tokens worden ingetrokken, exports worden stilgezet of bepaalde services tijdelijk worden gedeactiveerd. Tegelijk moet bewijs behouden blijven en moeten beslissingen goed worden vastgelegd. NIST en het responsrapport noemen daarbij expliciet het belang van incidentlogboeken, evidence en duidelijke besluitvorming over wie wat mag stilzetten. [5]

Fictieve case: de contactcentermanager

Het begint met iets kleins: een supervisor vraagt of een export klopt. Een agent meldt dat een scherm vreemd reageert. Dan stuurt IT een vraag of bepaalde activiteit bekend voorkomt. Sandra denkt nog niet aan een hack. Ze denkt dat er iets misgaat in het systeem.

Binnen een paar minuten verandert dat gevoel. Meer signalen. Een tweede supervisor meldt iets vergelijkbaars. Een medewerker vraagt of accounts vaststaan. Mensen kijken haar kant op, maar de onrust loopt sneller op dan zij antwoorden heeft.

Haar eerste reactie is praktisch. Ze loopt naar de supervisor, vraagt wat er precies gezien is en belt IT. Ze laat screenshots maken en vraagt welke exports zijn gedraaid. Ondertussen blijft het contactcenter open. Klanten bellen door, agents werken door. Ze voelt dat er iets niet klopt, maar wil de operatie niet stilleggen zonder zekerheid.

Na een half uur voelt de situatie heel anders dan een normale storing. IT stelt meer vragen dan ze kan beantwoorden. Security wil weten welke teams toegang hebben tot welke schermen. Een supervisor wil weten wat hij tegen agents moet zeggen.

Bepaalde functies worden uitgezet. Rechten worden aangepast. Exports geblokkeerd. Agents merken direct dat ze minder inzage hebben. Wachttijden lopen op. Escalaties nemen toe. Ze stuurt de operatie niet meer gewoon aan, maar probeert vooral te voorkomen dat de onrust groter wordt.

Op dat moment voelt ze vooral één ding: dit is geen klein incident meer en ze hadden hier al veel eerder een duidelijk plan voor moeten hebben.

In de eerste 30 minuten draait het dus om signaleren, escaleren en een eerste commandostructuur neerzetten. In de eerste vier uur verschuift de focus naar containment, eerste scope en regie. In de eerste 24 uur wil je weten welke systemen mogelijk geraakt zijn, welke klantdata mogelijk in beeld is geweest, welke functies tijdelijk beperkt moeten blijven en hoe klantcontact onder die omstandigheden door kan gaan.

In veel organisaties betekent dat werken in een tijdelijke, beperkte modus. Hoewel de operationele continuïteit niet volledig is onderbroken, zijn de reguliere bedrijfsprocessen als gevolg van het incident significant verstoord. Voor die eerste 24 uur heeft de Autoriteit Persoonsgegevens (AP) een stappenplan opgesteld [4]. Hierin staan het beperken van schade en tegelijk bewijs/effecten beheersen centraal. De praktische volgorde die toezichthouders steeds terug laten komen is als volgt:

1. **Overzicht krijgen**
2. **Schade beperken**
3. **Beoordelen/ Melden**
4. **Communiceren**
5. **Herstel/ Lessons learned**

DE CONTACTCENTERMANAGER / DAG 0 TOT DAG 30

Dag 0
Eerste uur

Eerste signalen, eerste beslissingen
Ze belt IT terwijl ze nog op de vloer staat. Exports worden geblokkeerd, niemand wordt uitgelogd. Ze informeert de teamleads in twee zinnen en logt tijdstip, signalen en beslissingen op verzoek van IT.

Dag 0
Eerste 4 uur

Crisisteam gevormd, operatie in beperkte modus
Security bevestigt ongeautoriseerde toegang. Crisisteam: IT, Legal, Communicatie en zij als operationeel verantwoordelijke. Contactcenter blijft open maar in beperkte modus. Legal levert standaardformulering.

Dag 0
Binnen 24 uur

Melding AP gestart, klanten bellen meer
Legal bevestigt meldplicht. Eerste scope onvolledig maar voldoende voor initiële melding aan de AP. Logboek wordt onderdeel van interne registratie. Klanten bellen vaker, over wachttijden, niet het incident.

Dag 1 t/m 3

Forensisch onderzoek loopt, scope nog onduidelijk
Dagelijkse updates maar zelden definitieve antwoorden. Welke records zijn ingezien? Zijn gegevens geëxporteerd? Operatie draait op 70% capaciteit. Twee systemen offline. Leverancier schort gedeelde koppeling op.

Dag 4 t/m 14

Klanten geïnformeerd, escalaties verdubbelen
Eerste volledige scope: gegevens van duizenden accounts mogelijk ingezien. Klanten ontvangen brief. Telefonie piekt. FAQ dekt vragen onvoldoende. Escalaties verdubbelen. Drie CRM projecten worden stilgelegd.

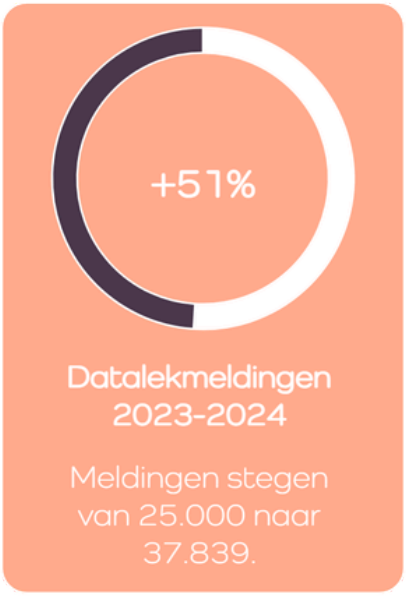
Dag 15 t/m 30

Onderzoek loopt nog, team niet op volledig vermogen
Incident gecontainerd maar niet afgesloten. Wekelijkse directie updates. Toegangsrechten worden per rol herbeoordeeld. Ze schrijft een draaiboek voor een volgend incident, niet uit energie, maar uit noodzaak.

*Disclaimer: Dit scenario is fictief. De volgorde van beslissingen, escalaties en verstoringen is gebaseerd op incidentpatronen beschreven door IBM Security (2025), ENISA (2024) en het NCSC (2023).

De AP benadrukt het krijgen van overzicht en het incident intern registreren als eerste stap [4]. NIST zegt dat vroege containment belangrijk is, omdat een incident anders resources kan overrulen of schade kan vergroten [5]. Deze containment vraagt expliciete beslissingen zoals systemen uitzetten, loskoppelen van netwerken en functies uitschakelen. Een andere vraag die vaak wordt gesteld is: "Wordt alles “bevroren”?". In de praktijk zelden alles, maar wat wel vaak gebeurt is het gericht stilleggen van bepaalde onderdelen in de bedrijfsvoering.

- **Technische freeze:** isoleren van getroffen accounts, blokkeren van kanalen, intrekken tokens, segmenteren en blokkeren IOC’s. NIST noemt service availability en evidence preservation als criteria om een containment-strategie te kiezen;
- **Change freeze:** tijdelijk beperken van changes op kritieke systemen om de situatie niet te verergeren en om forensische sporen niet te overschrijven. Dit sluit aan bij NIST’s nadruk op evidence preservation en besluitvorming;
- **Business freeze:** alleen waar noodzakelijk bij bijvoorbeeld actieve datadiefstal, ransomware of wanneer wet eist dat verwerking stopt. NIST waarschuwt tevens dat “delayed containment” gevaarlijk kan zijn omdat een aanvaller toegang kan uitbreiden of meer systemen kan aanvallen. Als je bewust later indamt om de aanvaller te observeren, moet dat worden afgestemd met legal. [5]



Zoals eerder beschreven loopt in de eerste 72 uur ook de juridische lijn mee:

- Melden aan toezichthouder (AVG art. 33): melding zonder onredelijke vertraging, waar mogelijk binnen 72 uur na kennisname. Bij meer dan 72 uur hoort een motivering. Informatie mag gefaseerd worden aangeleverd wanneer niet alles tegelijk beschikbaar is;
- Communicatie aan betrokkenen (AVG art. 34): bij waarschijnlijk hoog risico moeten medewerkers, klanten en overige betrokkenen zonder onredelijke vertraging worden geïnformeerd via specifieke berichten en niet vermengd met reguliere communicatie;
- Interne registratieplicht: los van de meldplicht moeten organisaties het datalek intern registreren, inclusief feiten, effecten en genomen maatregelen;
- Meerdere lekken tegelijk: als meerdere inbreuken worden ontdekt terwijl onderzoek loopt, kan in sommige situaties één melding meerdere inbreuken representeren. [4]

De juridische en technische respons vormt één lijn. Parallel daaraan loopt een tweede: wat er gebeurt met de mensen, de processen en het klantcontact terwijl het onderzoek nog loopt? Die operationele realiteit is voor contactcentermanagers vaak de zwaarste fase en de minst voorbereide.

Check met je team: Is er een draaiboek voor de eerste 24 uur na een incident? En is dat draaiboek ooit geoefend?

5. Wat betekent een datalek voor je klantcontactoperatie

Na de eerste respons begint voor contactcentermanagers vaak de lastigste fase: de nasleep in de operatie. De impact zit dan niet alleen in techniek, maar in de optelsom van verstoringen. Agents hebben mogelijk minder toegang, wachttijden lopen op en supervisors krijgen meer escalaties. Ook rapportages zijn tijdelijk minder betrouwbaar en werkgroepen of projecten komen onder druk te staan of vallen stil.

Herstel duurt langer dan je denkt

IBM rapporteerde in 2025 dat 86% van de organisaties operationele verstoring ervoer als gevolg van een lek [1]. Daarnaast gaf 65% van de respondenten aan na een jaar nog niet volledig hersteld te zijn [1]. Van de organisaties die wél volledig herstelden, had 76% daar meer dan 100 dagen voor nodig, en 26% zelfs meer dan 150 dagen [1]. Dat betekent dat de impact voor veel organisaties niet stopt na containment, maar weken of maanden blijft doorwerken in klantcontact, planning en besluitvorming.

Ook de schadecomponenten uit het IBM-rapport uit 2025, sluiten aan op wat een contactcentermanager in de praktijk merkt [1]. "Lost business" omvat expliciet systeemdowntime, verlies van klanten en reputatieschade [1]. Dat betekent dat een incident niet alleen kosten veroorzaakt in juridische afhandeling, maar ook in minder bereikbaarheid, klantverlies en extra druk op commerciële en operationele teams.
Dit vertaalt zich vaak naar pieken in klantvragen, meer onzekerheid aan de lijn, vragen waar nog geen definitief antwoord op is en extra druk op supervisors en management. Juist daardoor wordt zichtbaar dat een datalek niet alleen een security-incident is, maar een gebeurtenis die direct ingrijpt op de bestuurbaarheid van de operatie.

Klantbediening en de dagelijkse operatie: wat verandert er concreet? Een datalek is ook een operatie-incident: Daarom wordt een war room / crisisteam samengesteld met Security/IT, Legal/Privacy, Communicatie, Customer Support en Business Owners (en eventueel verwerkers/leveranciers). De AP adviseert in de voorbereiding onder andere afspraken over wie wat doet en bereikbaarheid (achtervang, buiten kantooruren) [4]. Customer support krijgt vaak tijdelijke scripts of FAQ's om voorbereid te zijn op vragen over het lek. Het rapport benoemt business disruption expliciet als een drijver van kostenstijging [1].

Morgen beginnen: vier stappen die je nu al kunt zetten

Draait de operatie door? Meestal: ja, maar in een beperkte modus. Denk aan alternatieve processen, fallback-systemen (DRP), strengere toegangsrechten, extra monitoring, en soms tijdelijke beperkingen in datadeling naar partners/leveranciers totdat de scope helder is. Deze beperkte modus sluit aan bij de nadruk op herstelvermogen en het kunnen terugvallen op gemaakte plannen of afspraken.

Nu je weet wat een datalek doet met jouw operatie, je team en je klantcontact, is de vraag: wat kun jij vandaag al organiseren? Niet na het volgende incident of als er budget voor vrijkomt, maar vanaf dit moment. Hoofdstuk 6 geeft je vier concrete stappen waarmee je morgen kunt beginnen.

6. Wat jij vandaag al kunt organiseren

De eerste stap is om een datalek te zien als een operationele calamiteit. Je wilt vooraf duidelijk hebben wanneer er wordt opgeschaald, wie een incident uitroept en wie bevoegd is om delen van de operatie tijdelijk te beperken. Het IRP noemt dit expliciet als governancevraag: incidentdrempels, incidentverklaring en stekkermandaat moeten vooraf zijn uitgewerkt. [5]

De tweede stap is voorbereiden op de eerste uren. De benoemde set van plannen werk je hier uit voor een zo breed mogelijke dekking. Dat zijn een Incident Response Plan (IRP), een Disaster Recovery Plan (DRP) en een Business Continuity Plan (BCP). Hiermee dek je het draaien van de operatie, herstel, detectie, besluitvorming, externe communicatie en klantbediening af. Specifiek heeft het IRP betrekking op wat je doet bij detectie en tijdens de crisis. Het crisismanagementplan omvat alles met betrekking tot de besluitvorming, externe communicatie, klantbediening en het bestuur. Tot slot gaan het DRP en het BCP over hoe de operatie blijft draaien en hoe systemen en de dienstverlening worden hersteld.

Vervolgens kun je de schade structureel beperken als het misgaat. Met het oog op de voorbereiding betekent dat in de praktijk: minder data bewaren dan nu, minder tonen dan nu, bewaartermijnen verkorten waar mogelijk, exports beperken, encryptie toepassen waar passend en gevoelige gegevens standaard afschermen of pseudonimiseren. Dataminimalisatie, opslagbeperking en privacy by design/default verkleinen de blast radius van een incident [4]. Encryptie kan bovendien in bepaalde omstandigheden helpen om de impact richting betrokkenen te beperken.

Een vierde stap is investeren in zichtbaarheid en snellere detectie. NIST (National Institute of Standards and Technology) noemt logmonitoring en automatische rapportage als basis voor effectieve incidentrespons [5]. Dat wordt aangevuld met tools voor detectie op apparaatniveau, bredere netwerkmonitoring en software die voorkomt dat gevoelige data ongeautoriseerd de organisatie verlaat. Samen zorgen die ervoor dat je een incident sneller opmerkt en sneller kunt handelen.

Tot slot helpt het om maatregelen concreet en meetbaar te maken. Bijvoorbeeld:

- 100% van nieuwe medewerkers volgt in de eerste maand security-onboarding;
- elk kwartaal een korte update over phishing, vishing en verdachte verzoeken;
- elk halfjaar een tabletop-oefening voor supervisors;
- bulkdownloads en exports worden gelogd en wekelijks beoordeeld.

Een eenvoudig draaiboek, een duidelijke escalatielijn en een halfjaarlijkse oefening zijn al een significant betere uitgangspositie dan geen plan. De checklist in het volgende hoofdstuk biedt een strategisch kader per domein voor managers die verder willen gaan.

Check met je team: Welke van de vier stappen in dit hoofdstuk is bij jullie nog niet geregeld? Wat houdt dat tegen?

7. Checklist voor contactcentermanagers

1. Toegang en monitoring: wat kun jij vandaag al organiseren?

- ◯ MFA is verplicht en actief voor 100% van de agents, supervisors en tijdelijke krachten met toegang tot klantdata, zonder uitzonderingen.
- ◯ Het systeem genereert automatisch een melding bij een loginpoging vanaf een onbekende locatie, een onbekend apparaat of buiten reguliere werktijden.
- ◯ Elke melding van een verdachte loginpoging wordt binnen één werkdag beoordeeld door een aangewezen verantwoordelijke.
- ◯ Per functierol is schriftelijk vastgelegd welke systemen, schermen en exportfuncties toegankelijk zijn, op basis van het principe van minimale toegang.
- ◯ Toegangsrechten per medewerker worden minimaal één keer per zes maanden gecontroleerd en waar nodig bijgesteld.
- ◯ Er is een duidelijke en bekende escalatieroute voor verdachte verzoeken

Wil je de hele checklist ontvangen?
Klik op de link of Scan de QR-code hieronder

Woordenlijst

AP: Autoriteit Persoonsgegevens. De Nederlandse toezichthouder die toeziet op de naleving van de AVG en waarbij datalekken gemeld moeten worden.

AVG: Algemene Verordening Gegevensbescherming. De Europese privacywet die organisaties verplicht tot zorgvuldige verwerking van persoonsgegevens en die de meldplicht bij datalekken regelt.

BCP: Business Continuity Plan. Een plan dat beschrijft hoe een organisatie haar dienstverlening voortzet tijdens en na een incident, ook als systemen tijdelijk niet beschikbaar zijn.

CRM: Customer Relationship Management. Een systeem waarmee organisaties klantgegevens, contacthistorie en interacties beheren. In contactcenters de primaire werkomgeving van agents.

DRP: Disaster Recovery Plan. Een plan voor het herstel van systemen, data en processen na een calamiteit of incident.

EDPB: European Data Protection Board. Het onafhankelijke Europese orgaan dat toeziet op de consistente toepassing van de AVG in alle EU-lidstaten en richtlijnen uitvaardigt voor organisaties.

EDR: Endpoint Detection and Response. Beveiligingssoftware die verdacht gedrag op apparaten zoals laptops en werkstations detecteert en er automatisch op reageert.

IOC: Indicator of Compromise. Een technisch signaal dat wijst op een mogelijk beveiligingsincident, zoals een verdacht IP-adres, een ongebruikelijk bestand of afwijkend netwerkverkeer.

IRP: Incident Response Plan. Een gedocumenteerd draaiboek dat beschrijft hoe een organisatie reageert bij een beveiligingsincident: wie doet wat, in welke volgorde en binnen welke termijn.

MFA: Multi-Factor Authenticatie. Een inlogmethode waarbij naast een wachtwoord een tweede verificatiestap vereist is, zoals een code via een app of sms. Ook aangeduid als tweefactorauthenticatie (2FA).

NIST: National Institute of Standards and Technology. Een Amerikaanse overheidsinstantie die wereldwijd erkende standaarden en richtlijnen publiceert voor informatiebeveiliging.

Over Steam-connect

Alles wat je in deze whitepaper hebt gelezen over toegangsbeheer, detectie en schadebeperking begint bij de omgeving waarin jouw medewerkers dagelijks werken. Steam-connect is het platform waarmee contactcenters al hun klantcontact beheren. Dataveiligheid is daarin een standaard onderdeel van hoe het platform werkt.

We begrijpen dat een contactcentermanager geen security-expert hoeft te zijn. Daarom zorgen wij dat de basis staat. Met tweefactorauthenticatie, een IP-whitelist en Passgrid regel je dat alleen de juiste mensen op de juiste plekken toegang krijgen tot jouw omgeving.

Automatische notificaties bij downloads en exports zorgen dat je het ziet op het moment dat het gebeurt en niet pas achteraf. Anonimisatie van gevoelige klantgegevens beperkt wat zichtbaar is voor wie het niet hoeft te zien. En een sterk wachtwoordbeleid wordt organisatiebreed afgedwongen, zonder dat jij daar elke keer achteraan hoeft.

Zo houd jij de regie over je operatie, ook op het gebied van dataveiligheid. Benieuwd wat Steam-connect voor jouw contactcenter kan betekenen? Vraag een demo aan en ontdek hoe wij dataveiligheid en efficiënt klantcontact samenbrengen.

Steeds meer organisaties onderzoeken hoe zij dataveiligheid nog beter kunnen integreren in hun klantcontactomgeving. Benieuwd hoe jouw organisatie klantdata veilig kan verwerken binnen het contactcenter?

Op onze website vind je meer inzichten, praktijkvoorbeelden en een demo van de mogelijkheden van het Steam-connect platform.

Klaar voor de volgende generatie klantcontact?

Vraag een demo aan

+31 85 0 474747

sales@steam-connect.com

www.steam-connect.com

Noten

1. IBM Security. (2025). Cost of a data breach report 2025. https://ibm.com/reports/data-breach
2. IBM Security. (2024). Cost of a data breach report 2024. https://ibm.com/reports/data-breach
3. Verizon Business. (2024). 2024 data breach investigations report. https://verizon.com/business/resources/reports/dbir
4. European Data Protection Board. (2022). Guidelines 9/2022 on personal data breach notification under GDPR. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en
5. National Institute of Standards and Technology. (2024). Computer security incident handling guide (NIST Special Publication 800-61 Rev. 3). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-61r3
6. Nationaal Cyber Security Centrum. (2023). Handreiking incidentrespons. Ministerie van Justitie en Veiligheid. https://ncsc.nl/documenten/handreikingen/2023/incidentrespons
7. European Union Agency for Cybersecurity (ENISA). (2024). ENISA threat landscape 2024. https://enisa.europa.eu/publications/enisa-threat-landscape-2024
8. Mandiant. (2025). M-Trends 2025. Google Cloud. https://cloud.google.com/security/resources/m-trends
9. Microsoft. (2024). Microsoft digital defense report 2024. https://microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2024
10. Federal Bureau of Investigation. (2024). Internet crime report 2024. U.S. Department of Justice. https://ic3.gov/AnnualReport
11. Cloudflare. (2024). DDoS threat report Q4 2024. https://blog.cloudflare.com/ddos-threat-report-for-2024-q4
12. Cyber Readiness Institute. (2024). Cyber readiness report 2024. https://cyberreadinessinstitute.org/resource/2024-cyber-readiness-report

Contactcenters spelen een cruciale rol in moderne organisaties. Ze vormen het directe contactpunt met klanten en verwerken dagelijks grote hoeveelheden informatie. Juist daardoor bevinden zij zich ook op een kwetsbare positie binnen de digitale infrastructuur van een organisatie.

Cyberaanvallen richten zich steeds vaker op identiteiten en medewerkers in plaats van uitsluitend op technische systemen. Dat betekent dat beveiliging niet alleen een IT-onderwerp is, maar ook een operationele verantwoordelijkheid.

Door aandacht te besteden aan toegangsbeheer, dataminimalisatie, monitoring en awareness kunnen organisaties hun risico's aanzienlijk verkleinen.

Wanneer security wordt geïntegreerd in de dagelijkse processen van het contactcenter, hoeft dit niet ten koste te gaan van efficiënt klantcontact. Sterker nog: een goed beveiligde omgeving kan juist bijdragen aan betrouwbaarder en stabieler klantcontact.

Uitgegeven door:
STEAM® CONNECT
empowering conversations

Mediapartner:
ziptone

LinkedIn

+31 85 0 474747
sales@steam-connect.com
steam-connect.com

STEAM® CONNECT
empowering conversations