

Oplossingen voor (interne) onderzoekers

Er zijn vele soorten onderzoek, uitgevoerd door uiteenlopende partijen, maar grote onderzoeken hebben een ding gemeen: bij deze onderzoeken wordt veel informatie verzameld die moet worden doorzocht en op een transparante manier moeten worden gestructureerd zodat de resultaten door alle betrokken partijen gedeeld kunnen worden. Onderzoeksteams moeten in staat zijn om in complexe kluwen uiteenlopende informatie verbanden te leggen en specifieke kennis te vinden die van belang is voor de zaak.

Opsporing van omkoping en corruptie

Bij strafrechtelijke onderzoeken zoals moord, georganiseerde misdaad, drugs-, wittenboordencriminaliteit en cybercriminaliteit richt het informatieonderzoek zich vooral op in beslag genomen documenten, computers, internet en e-mail. Daarnaast wordt er gezocht in gegevens van hoorzittingen, ondervragingen, getuigenverslagen en informatie van derden.

In fraude- en financiële onderzoeken ligt de nadruk vooral op financiële administraties. Hierbij speuren de onderzoekers naar complexe (verborgen) transacties en codewoorden (synoniemen) die zijn gebruikt om acties te verbergen.

Met de oplossingen van ZyLAB vindt u meer relevante informatie dan met elk ander product op de markt.

Databeveiliging en IP diefstal

Toezichthouders gebruiken steeds vaker forensische technieken om verschillende vormen van de diefstal van gegevens en het lekken van informatie te onderzoeken. Wanneer zij gegevens onderzoeken op hard- en thumb drives, smartphones, laptops en overige opslagmedia, is het belangrijk dat de content en oorspronkelijke gegevens over bijvoorbeeld wijziging, verwijdering en kopiëring bij het uitpakken van de informatie in hun originele staat wordt bewaard.

De beveiliging van informatie en data is cruciaal voor de gezondheid van een organisatie. De gevolgen van een informatielek of databreuk kunnen zware consequenties hebben die verder gaan dan de kosten van de breuk, het verliezen van informatie; het bedrijf wordt bloot gesteld aan een scala van mogelijke rechtszaken.

ZyLAB helpt organisaties om hun informatiebeveiliging te optimaliseren door bijvoorbeeld het periodiek uitvoeren van risico audits en door actief te zoeken naar risicovolle data combinaties, potentiële stomiteiten en het opsporen van verdachte e-mails en documenten voordat ze de deur uitgaan.



Oplossingen voor (interne) onderzoekers

De software van ZyLAB helpt u een praktisch beleid uit te voeren voor dagelijks records management, helpt u bij de naleving van dit beleid en biedt u snel toegang tot informatie wanneer u die nodig hebt. In het geval van een geschil kunt u ZyLAB gebruiken om eventuele informatie asymmetrie met onderzoekers te voorkomen.

Mededingingsonderzoeken

Mededingingsonderzoeken richten zich op de vraag of bedrijven hun leidende positie misbruiken door bijvoorbeeld klanten te dwingen meer diensten of producten af te nemen. Ook klachten over oneerlijke concurrentie kunnen resulteren in een mededingingsonderzoek.

In Nederland worden deze onderzoeken uitgevoerd door Autoriteit Consument & Markt (ACM), een fusie tussen Nederlandse Mededingingsautoriteit (NMa), de Consumentenautoriteit en de OPTA. Op Europees niveau is dat de Europese Commissie en in Amerika is de Federal Trade Commission (FTC) de belangrijkste toezichthouder.

ZyLAB ondersteunt zowel toezichthouders als bedrijven bij de uitvoering van onderzoeken in het kader van mededinging.

Privacy en databescherming

Het toenemende aantal en de complexiteit van de regels voor de bescherming van persoonsgegevens en privacy, verhogen de druk op de verantwoordelijke professionals om hun activiteiten te automatiseren. Alle bedrijven die grote hoeveelheden informatie (ook wel Big Data genoemd) beheren, dienen zich ervan bewust te zijn dat zij, met opzet of per ongeluk, een grote hoeveelheid informatie beheren, die onderworpen is aan de steeds strenger wordende regels voor de bescherming van persoonsgegevens en privacy.

Bijna ieder bedrijf slaat gegevens over klanten en werknemers op. Vaak wordt ook informatie met betrekking tot de gezondheid van werknemers of credit card gegevens van klanten opgeslagen. Om deze gegevens te beschermen, hebben bedrijven een hoger niveau van IT-beveiliging en in sommige gevallen is het nodig gegevens te anonimiseren.

Het beschermen van persoonsgegevens van klant of werknemer, moet proactief worden verankerd in de dagelijkse bedrijfsvoering. Dit proces begint met de identificatie en lokalisatie van de persoonlijk identificeerbare informatie (PII) die moet worden beveiligd.

ZyLAB biedt organisaties de technologie om PII te identificeren en lokaliseren en spoort incidenten op die kunnen leiden tot ongewenste of ongeautoriseerde openbaarmaking van persoonsgegevens.

