Bij de term datalek wordt vaak in eerste instantie gedacht aan een externe aanvaller die erin slaagt de beveiliging van een gemeente te doorbreken. In de praktijk blijkt echter dat datalekken regelmatig van binnenuit ontstaan. Het gaat daarbij meestal om medewerkers die — al dan niet bewust — persoonsgegevens vernietigen, verliezen, wijzigen of onrechtmatig verstrekken. Dit kan per ongeluk gebeuren of opzettelijk. In beide gevallen is sprake van een datalek in de zin van de Algemene verordening gegevensbescherming (AVG). Bovendien komen datalekken in de praktijk vaker voor dan wordt gemeld of erkend.

Preventie bij onopzettelijke datalekken

Preventieve maatregelen ter voorkoming van per ongeluk veroorzaakte datalekken door eigen medewerkers zijn onder meer:

- Het verbeteren van technische beveiliging (zoals encryptie en tweefactorauthenticatie);
- Het opstellen en aanscherpen van duidelijke werkprocessen en protocollen;
- Het trainen van medewerkers in privacybewust en zorgvuldig werken;
- Het controleren en actualiseren van verwerkersovereenkomsten;
- Het evalueren van incidenten en het vastleggen van verbetermaatregelen.

Preventie bij opzettelijke datalekken

Wanneer sprake is van een opzettelijk veroorzaakt datalek door een medewerker, zijn naast preventieve ook repressieve maatregelen noodzakelijk. Te denken valt aan:

- Het onmiddellijk blokkeren van de toegang van de betrokken medewerker of het gecompromitteerde account;
- Het isoleren van systemen bij sabotage of hacking;
- Het veiligstellen van bewijsmateriaal (logbestanden, e-mails, toegangsgegevens);
- Interne escalatie naar directie, de Functionaris Gegevensbescherming (FG) en eventueel de CISO;
- Het zorgvuldig vastleggen van de aard en omvang van het incident, inclusief de betrokken persoonsgegevens en personen.

Daarnaast kunnen arbeidsrechtelijke en strafrechtelijke stappen aan de orde zijn.

Laakbaar bestuur

Indien een gemeentebestuur nalaat passende preventieve maatregelen te treffen, is dat ernstig. Nog ernstiger is het wanneer signalen van een mogelijk datalek — ook als deze niet expliciet als zodanig worden benoemd — worden genegeerd of gebagatelliseerd. In dat geval bestaat het risico dat persoonsgegevens langdurig blootstaan aan onrechtmatige verwerking of misbruik.

Gemeentebesturen die geen adequaat privacybeleid hebben vastgesteld en geïmplementeerd, lopen een aanzienlijk risico tekort te schieten bij het voorkomen, signaleren en adequaat afhandelen van datalekken.