Artikel Privacy
Tekst Paul Bloemen
Ivo Kouters
Ad Meeuwesen
Beeld Thinkstock

PRIVACY:
mens en organisatie vragen voortdurend aandacht

De afgelopen jaren zijn we geconfronteerd met verschillende grote privacy-incidenten, zoals de Panama Papers, WikiLeaks en Diginotar. Hoe kunnen we adequaat onze privacygevoelige gegevens beschermen en financiële en reputatieschade voorkomen? In dit artikel aandacht voor de organisatorische en menselijke componenten hierbij.

Naast eerdergenoemde spectaculaire privacy-incidenten hebben zich herhaaldelijk kleinere vormen van datalekken voorgedaan, waarbij persoonsgegevens bewust of onbewust openbaar zijn gemaakt. Voor de getroffen organisaties, eigenaar van de gegevens, was de schade vaak beperkt. Dit leidde tot onvoldoende aandacht voor het voorkomen van privacy-incidenten. De schade voor de getroffen personen is echter vaak groot en maatschappelijk gezien zeer ongewenst.
Dit heeft per 1 januari 2016 geleid tot een aanpassing van de Wet bescherming persoonsgegevens (Wbp). Deze is namelijk aangevuld met de meldplicht datalekken, als onderdeel van het afhandelen van een incident. Deze aanvulling op de wet loopt vooruit op de Europese verordening gegevensbescherming die in 2018 van kracht wordt.
In Nederland is de Autoriteit Persoonsgegevens (AP) belast met de handhaving van de Wbp. Zij geeft richtlijnen over de aard van datalekken en hoe ermee om te gaan. De AP is tevens het meldpunt voor de datalekken. Zij is bevoegd boetes op te leggen als blijkt dat een datalek niet tijdig is gemeld en als blijkt dat de voorzieningen om datalekken te voorkomen onvoldoende waren. Ten slotte is de AP bevoegd om zelfstandig onderzoek bij een organisatie te doen en aanwijzingen ter verbetering te geven.

Inbedding noodzakelijke maatregelen
Veel maatregelen die nodig zijn voor de bescherming van privacygevoelige gegevens zijn ook noodzakelijk tegen andere typen bedreigingen van de informatievoorziening. Daarom kan de aanpak voor het omgaan met privacygevoelige gegevens het best onderdeel uitmaken van informatiebeveiliging. Basis voor de organisatie en de inhoud van informatiebeveiliging is onder andere te vinden in ISO 27001, privacy maakt hier deel van uit. Aanvullende aspecten komen met name voort uit de Wbp en de nog in te voeren Europese verordening gegevensbescherming.
Bij informatiebeveiliging vormt de risicoanalyse de belangrijkste inbreng voor de te nemen maatregelen. Deze maatregelen

worden opgenomen in het informatiebeveiligingsbeleid van de organisatie. Onderdelen van het beleid zijn controle en rapportage met betrekking tot het functioneren van de maatregelen. Op deze manier is het organisatorische bouwwerk van informatiebeveiliging ook van toepassing op privacy.

Twaalfvlak privacygevoelige gegevens

Om de beschreven maatregelen voor privacy te waarborgen, wordt invulling gegeven aan enerzijds de aspecten organisatie, mensen en techniek en anderzijds aan de aspecten preventief, detectief, repressief en correctief. Dit levert een twaalfvlakmodel op voor alle relevante privacy maatregelen (zie *figuur1*). Wat hierbij opvalt is de veelheid aan maatregelen voor de aspecten organisatie en mens. Voor privacy ligt hier het zwaartepunt. Met behulp van dit twaalfvlak kan een organisatie nagaan of en in hoeverre zij een evenwichtige set aan maatregelen getroffen heeft.

Organisatie

In kaart brengen – Om de noodzakelijke maatregelen te bepalen, moeten de privacygevoelige gegevens van een organisatie in kaart gebracht worden. Dit kunnen zowel formele als informele gegevensverzamelingen zijn: formele gegevens maken deel uit van toepassingen, veelal opgeslagen op centraal beheerde servers. Informele gegevens worden door gebruikers zelf beheerd, bijvoorbeeld in spreadsheets of lijsten op een laptop, tablet, smartphone of USB-stick. Formele en informele gegevens kunnen ook opgeslagen zijn in de cloud, deze verdienen daarom bijzondere aandacht.

Eigenaar – Alle privacygevoelige gegevens moeten een formele eigenaar hebben die aangesproken kan worden op de inhoud, het gebruik en het beheer van de gegevens. Er zijn verschillende eigenaren voor de verschillende gegevensverzamelingen in verschillende businessprocessen. Aangezien een eigenaar deel uitmaakt van een businessproces heeft hij vaak onvoldoende voeling met de specifieke privacyproblematiek en de technische aspecten van het beheer van de gegevens. Daarom is het verstandig de benodigde werkzaamheden aan te laten sturen door een security- of privacyspecialist, waarbij de besluiten door de data-eigenaren genomen worden. Een voorbeeld hiervan is de privacy risicoanalyse en de daaruit voortvloeiende besluitvorming over de maatregelen.

Beperkte toegang – Duidelijk moet zijn wie toegang heeft tot privacygevoelige gegevens. Deze toegang moet beperkt worden op basis van de noodzaak voor de bedrijfsprocessen. Hieronder vallen ook regels voor het gegevenstransport. Dit kan zowel binnen de organisatie, tussen verschillende organisaties als tussen de organisatie en privépersonen plaatsvinden. Voor het transport van privacygevoelige gegevens dienen strenge voorwaarden te gelden, met name voor privégebruik en voor communicatie met externe organisaties.

IT – Wat betreft IT-voorzieningen en -processen, kun je stellen dat die adequaat moeten worden beheerd. Indien de beheerswerkzaamheden door een externe (cloud)organisatie worden uitgevoerd, verdient het extra aandacht. Het is dan zelfs wettelijk verplicht om met deze organisatie een zogenaamde bewerkersovereenkomst af te sluiten. Onderdelen hiervan zijn aansprakelijkheid, eisen voor het authenticatie- en autorisatiebeheer en het functioneren van de technische voorzieningen.

Organisatie

Preventief
- Inventarisatie van privacygevoelige gegevensverzamelingen plus eigenaarschap
- Risicoanalyse privacy
- Inventarisatie opslagplaatsen van de gegevens
- Toegangsbeheer gebruikers van de gegevens
- Toegangsbeheer beheerders van de gegevens
- Beheer hoge rechten voor beheer infrastructuur
- Inventarisatie transport van de gegevens
- Bepaling toegestaan transport van de gegevens
- Bewerkersovereenkomsten met externen
- Beheer van IT-middelen

Detectief
- Controle en rapportage over rechten en technische voorzieningen
- Incident management en afhandeling
- Criteria voor melden datalekken aan AP en aan de getroffen personen
- Periodieke ethical hack

Repressief
- Incidentafhandeling - schadebeperking

Correctief
- Incidentafhandeling - herstel

Mens

Preventief
- Privacy binnen alle voorlichtingsvormen van informatiebeveiliging
- Gedragscode van de organisatie
- Periodieke basistraining voor alle medewerkers
- Formele toets met meetbare resultaten voor de trainingen van gebruikers
- Speciale voorlichting voor managers en eigenaren van privacygevoelige gegevens
- Opleiding technische hulpmiddelen beheerders
- Speciale thema-acties privacy

Detectief
- Opleiding incidentafhandeling voor beheerders
- Opleiding melding van datalekken voor beheerders
- Opleiding gebruik en beheer van Intrusion Detection System (IDS) en Security Incident and Event Management (SIEM)

Repressief
- Opleiding beheerders over procedurele en technische schadebeperking
- Voorlichting betrokkenen over incident, gewenste handelwijze

Correctief
- Opleiding beheerders aangaande de technische voorzieningen
- Evaluatie incident met betrokkenen, lessons learned

Techniek

Preventief
- Geëncrypte communicatie netwerkverkeer, VPN en HTTPS
- Firewalls
- Geëncrypte opslag gegevens op laptops, tablets, smartphones, USB-sticks
- Authenticatie- en autorisatievoorzieningen
- Voorzieningen voor beheer van hoge rechten

Detectief
- Intrusion Detection System (IDS)
- Security Incident and Event Management (SIEM)

Repressief
- Aanpassing technische voorzieningen, bijvoorbeeld aanpassing rechten

Correctief
- Herstel of aanpassing technische voorzieningen
- Opvolging resultaten ethical hack, periodieke rapportage over voortgang

Twee aspecten van het beheer van IT-middelen vragen bij privacygevoelige gegevens bijzondere aandacht: het vervangen van apparatuur en het uit dienst treden van medewerkers. Hierbij moet voorkomen worden dat de gevoelige informatie in verkeerde handen valt. Van alle betrokken apparatuur dienen de gegevens op een niet te herstellen manier verwijderd te worden voordat de apparatuur wordt verkocht of aan andere medewerkers ter beschikking wordt gesteld.

Incident management – Incident management is een cruciaal proces om de detectie en afhandeling van incidenten te sturen. Zeker nu bij een inadequate afhandeling van privacy-incidenten een hoge boete geriskeerd wordt, is het van belang dit proces op orde te krijgen en te houden. Een belangrijk aspect bij het afhandelen van datalekken is de tijdige melding (binnen 72 uur) van het incident bij de AP en, in specifieke gevallen, bij de getroffen personen. Dit moet dus vooraf goed georganiseerd worden door middel van een meldingstraject dat deel uitmaakt van het reguliere proces voor het afhandelen van incidenten.

Ethical hack – Een periodieke ethical hack is raadzaam voor het boven tafel krijgen van mogelijke technische kwetsbaarheden. Het vormt een proef op de som op de effectiviteit van het geheel van getroffen maatregelen. Als social engineering hier deel van uitmaakt, komen bovendien de menselijke kwetsbaarheden boven tafel. De ervaring leert dat het verschillende ethical hacks vergt om de infrastructuur en de organisatiecultuur op een voldoende niveau van beveiliging te krijgen en te houden.

Mensen

Houding en gedrag – Aangezien mensen van nature geen belangstelling hebben voor informatiebeveiliging en privacy maatregelen, zijn zij een zwakke schakel in het totaal aan maatregelen. Er moet dus expliciet aandacht geschonken worden aan het vormen van de gewenste houding en gedrag. Uitgangspunt hierbij is bewustwording van het management voor risico's en noodzakelijke maatregelen. Dit levert draagvlak op voor de nodige gedragsregels voor gebruikers en beheerders van privacygevoelige gegevens. Een belangrijke gedragsregel is bijvoorbeeld het geheimhouden van de eigen wachtwoorden. Een andere gedragsregel is het voorkomen van verlies en diefstal van apparatuur. Het is belangrijk laptops, tablets, smartphones en USB-sticks adequaat te beveiligen en bij je houden.

Training – Het best kan houding en gedrag worden beïnvloed door middel van training. Deze is gericht op alle medewerkers, waarbij het onderscheid tussen eigen medewerkers en inhuurmedewerkers van belang is. De inhuurmedewerkers hebben initieel niet zo'n band met de organisatie, zijn ook niet vertrouwd met de regels en gewoonten en verdienen dus extra aandacht. Bij de training van medewerkers zijn de volgende aandachtspunten van belang:

- belang van gegevensverzamelingen;
- risico's met betrekking tot de gegevensverzamelingen;
- gewenst gedrag gebaseerd op een gezond wantrouwen;
- ongewenst gedrag gebaseerd op onkunde en desinteresse;
- sancties voor de organisatie en medewerkers.

Een basistraining kan plaatsvinden in de vorm van reguliere e-learning. Raadzaam is de training dan te voorzien van een toetsmodule, zodat aantoonbaar is dat de training gevolgd en voldoende begrepen is. Het is handig als zo'n toetsmodule gekoppeld is aan het hrm-systeem, waardoor de toetsresultaten van de training gerapporteerd worden aan de managers, die erop toezien dat al hun medewerkers de toets positief afronden. Medewerkers moet duidelijk gemaakt worden welke incidenten met betrekking tot privacygevoelige gegevens gemeld moeten worden en dat dit tijdig en volgens een afgesproken meldingstraject moet gebeuren. Medewerkers hebben de neiging problemen zelf op te willen lossen, maar juist in het geval van privacy moet de organisatie voor het afhandelen van incidenten zo snel mogelijk geïnformeerd worden.

Gedragscode en afspraken – Andere formele manieren om privacy onder de aandacht van de medewerkers te brengen zijn het opnemen van privacy in de Gedragscode van de organisatie, met een getekende verklaring van medewerkers dat zij deze gelezen en begrepen te hebben. En aspecten van privacy deel laten uitmaken van afspraken in de hr-cyclus. De ritueelwerking ervan is groot omdat medewerkers hierop beoordeeld worden.

Tweede natuur – Het is raadzaam om geregeld aandacht te schenken aan privacy, gecombineerd met andere aspecten van informatiebeveiliging. Door afwisseling in inhoud en presentatievorm beklijft de inhoud beter. Het veilig omgaan met privacygevoelige gegevens wordt dan meer een tweede natuur. De meeste impact heeft het aangaan van de dialoog en het leren van incidenten, bijvoorbeeld:

- speciale voorlichtingscampagnes in de vorm van een spel, of bespreking van dilemma's, waarbij de interactie tussen medewerkers wordt gefaciliteerd;
- lessons learned van incidenten, deze kunnen bijvoorbeeld op het intranet aan de medewerkers medegedeeld worden. Hierdoor beseffen de medewerkers dat incidenten niet alleen bij andere organisaties plaatsvinden en dat er voortdurend aandacht voor moet zijn.

Levend houden kennis – Het is raadzaam de kennis en kunde levend te houden. Bij het beheer van privacygevoelige gegevens gaat er namelijk zelden iets fout. Beheerders lopen daarom de reële kans om na verloop van tijd minder aandacht voor de bedreigingen te hebben en bij hun werkzaamheden onbewust risico's te nemen. Bij de opleiding van beheerders is het daarom belangrijk om steeds aandacht te schenken aan die risico's en voorbeelden aan te dragen waar het fout is gegaan. Daarnaast kan ook controle en rapportage zorgen voor het scherp blijven van de beheerders.

Conclusies

Het voorkomen van datalekken vergt een inspanning op meerdere fronten: het totaal aan maatregelen, inclusief controles en rapportages, vormt een samenhangend geheel waardoor het mogelijk falen op een bepaald gebied elders wordt opgevangen. Goed functionerende en aantoonbare maatregelen zorgen voor het voorkomen van hoge boetes door de AP, mocht zich onverhoopt toch een incident hebben voorgedaan. Maar wat waarschijnlijk belangrijker is, zij beperken mogelijke reputatieschade. Het succesvol voorkomen van datalekken blijkt vooral afhankelijk te zijn van mensenwerk: de organisatie van de processen en houding en gedrag van medewerkers. Het startpunt is de besluitvorming op managementniveau om de omgang met privacygevoelige gegevens serieus op te pakken en op niveau te brengen en te houden. De mens vraagt daarbij voortdurend aandacht. <<

Paul Bloemen is expert op het gebied van informatiebeveiliging en heeft ruim dertig jaar ervaring op het gebied van informatiebeveiliging als information security officer bij Gasunie.

Ivo Kouters en Ad Meeuwesen werken bij KoutersVanderMeer, bureau voor prestatieverbetering. Zij hebben studie verricht naar de vraag hoe bedrijven informatiebeveiliging organiseren en invloed kunnen uitoefenen op menselijk gedrag.