Security & Privacy
Incident Roadmap

VanDoorne Advocaten • Notarissen • Fiscalisten

ZURICH

Zurich Security & Privacy Incident Roadmap

De afgelopen jaren zijn IT faciliteiten van cruciaal belang geworden voor de meeste organisaties. Een veelvoud aan gegevens wordt digitaal verwerkt. Met de groei van de digitaal opgeslagen gegevens en de waarde die de gegevens zijn gaan vertegenwoordigen, nemen ook de risico's op beveiligingsincidenten toe. Beveiliging van de IT faciliteiten is dan ook onontbeerlijk. Voor elke organisatie geldt helaas dat geen enkele beveiliging waterdicht is. Gegevens kunnen verloren gaan of op straat komen te liggen. Dat kan komen door een menselijke fout, maar ook kan de beveiliging worden doorbroken door een geavanceerde aanval van buitenaf.

praktijkvoorbeeld 1

Op zondagnacht breken hackers in op uw computersysteem. Zij weten zich de toegang te verschaffen tot de creditcard- en incassogegevens van uw klanten. U wordt hierover ingelicht via uw IT afdeling die de hack heeft ontdekt. Hoe kunt u ervoor zorgen dat de schade wordt beperkt?

praktijkvoorbeeld 2

Eén van uw medewerkers verliest een USB stick met 100.000 klantgegevens tijdens een zakenreis in Zuid Afrika. Welke stappen dienen ondernomen te worden om de gegevens veilig te stellen en de klanten te informeren?

praktijkvoorbeeld 3

Het automatiseringssysteem van uw ziekenhuis blijkt onvoldoende beveiligd. Naast de medische dossiers van enkele tientallen patiënten is het bestand van 500.000 patiëntgegevens in te zien. Hoe zorgt u ervoor dat de beveiliging wordt hersteld en uw patiënten vertrouwen blijven houden in uw ziekenhuis?

Elk bedrijf moet rekening houden met het risico van een beveiligingsincident. Het is raadzaam proactief hiermee om te gaan. Om u daarbij te helpen, heeft Zurich deze Security & Privacy Incident Roadmap opgesteld.

Deze Roadmap bevat de stappen die u kunt nemen ter voorkoming van incidenten, en voor het nadien omgaan met incidenten. Drie fasen kunnen worden onderscheiden:

- voordat het incident zich voordoet (pre-incident);
- het moment dat het incident zich voordoet (incident);
- nadien (post-incident).

1 Pre-incident

Diverse preventieve maatregelen zijn denkbaar om incidenten zoveel mogelijk te voorkomen. Een aantal voorbeelden van preventieve maatregelen staan hieronder omschreven.

1.1 Analyseer uw IT faciliteiten en technische voorzieningen.

Gegevens worden doorgaans op verschillende IT faciliteiten verwerkt. Om incidenten te voorkomen, dient u een goed beeld te hebben van uw IT faciliteiten en wat de verschillende eigenschappen zijn van deze faciliteiten. Maak daarbij onderscheid tussen de cruciale en minder belangrijke faciliteiten. Check de kwaliteit van uw IT faciliteiten en de technische voorzieningen. Vergeet daarbij niet te kijken naar welke afspraken u met uw toeleveranciers heeft gemaakt, met name ook over de mogelijke noodfaciliteiten.

Aspecten die hierbij meegenomen dienen te worden, zijn:

a) beschikbaarheid;
b) integriteit;
c) vertrouwelijkheid.

1.2 Analyseer en categoriseer de soorten gegevens.

U zult verschillende soorten gegevens verwerken. Het is raadzaam om de categorieën van gegevens die u verwerkt in kaart te brengen.

Bijvoorbeeld:

a) algemeen bekende bedrijfsinformatie;
b) vertrouwelijke informatie;
c) algemene persoonsgegevens, bijvoorbeeld naam, geboortedatum of geslacht;
d) bijzondere persoonsgegevens, zoals medische gegevens of godsdienst;
e) financiële gegevens, zoals creditcard gegevens of gegevens over schulden;
f) gebruikersnamen, wachtwoorden en andere inloggegevens;
g) gegevens die kunnen worden misbruikt voor (identiteits)fraude, zoals iemands burgerservicenummer (BSN).

1.3 Aard, inhoud en omvang van de gegevensverwerking.

Check met name:

a) hoe vertrouwelijk de gegevens zijn;
b) hoeveel gegevens er worden verwerkt;
c) om hoeveel en wat voor betrokkenen het gaat;
d) voor welke doeleinden de gegevens worden verwerkt;
e) wie toegang heeft tot de gegevens;
f) of de gegevens ook naar het buitenland gaan;
g) of er sprake is van een bewaarbeleid.

1.4 Persoonsgegevens.

Zorg er voor dat de IT faciliteiten en technische voorzieningen voldoen aan de wettelijke eisen die gelden voor het verwerken van persoonsgegevens. Check hierbij of er ook sprake is van het verwerken van gevoelige persoonsgegevens, zoals gezondheidsgegevens, waarvoor nog strengere regels gelden.

1.5 Voer een privacy impact assessment (PIA) uit.

Het uitvoeren van een PIA is nodig om inzicht te krijgen in de rechten en plichten van de betrokkenen, waarvan u de persoonsgegevens verwerkt.

1.6 *Analyseer de juridische positie van uw organisatie.*

Aan welke regelgeving is de organisatie onderworpen in verband met de verwerking en beveiliging van gegevens? Ook de daarmee verband houdende contractuele verplichtingen van de organisatie zijn relevant voor de positie van uw organisatie. Is de organisatie de verantwoordelijke of bewerker van de persoonsgegevens in de zin van de toepasselijke privacyregelgeving? Verder kan van belang zijn om te bepalen wie gerechtigd is tot de betreffende gegevens.

1.7 *Check of uw organisatie privacy compliant is.*

Beschikt u over de documentatie om dat te onderbouwen? Het gaat om zaken zoals meldingen, privacy statements, bewerkersovereenkomsten, en documenten die de doorgifte van de persoonsgegevens naar landen buiten de EER rechtvaardigen, bijvoorbeeld data transfer agreements, Safe Harbor certificaten en/of vergunningen.

1.8 *Is er een functionaris voor de gegevensbescherming (FG)?*

U kunt in de toekomst mogelijk verplicht zijn om een FG aan te stellen. Naar huidig recht is dat nog een vrije keuze. Indien u al een FG heeft aangesteld, betrek deze dan bij uw actieplan.

1.9 *Rol Ondernemingsraad.*

Als het gaat om het verwerken van HR gerelateerde persoonsgegevens, check ook of u de instemming van uw ondernemingsraad nodig heeft (indien van toepassing op uw organisatie).

1.10 *Houd rekening met internationale aspecten.*

Als uw organisatie vestigingen in het buitenland heeft, dient u ermee rekening te houden dat de toepasselijke regels in de verschillende landen kunnen verschillen en dat u hiervoor lokaal advies moet inwinnen. Check in dit verband ook welke afspraken er op concernniveau zijn of moeten worden gemaakt.

1.11 *Implementeer een beveiligingsbeleid.*

Het is van belang dat de technische en organisatorische beveiligingsmaatregelen binnen de organisatie in kaart worden gebracht, worden uitgewerkt in een beveiligingsbeleid en dat zij steeds up-to-date zijn. Hierbij dient tevens aan de orde te komen welke beveiligingsstandaarden er worden gehanteerd, hoe medewerkers moeten omgaan met gegevens en IT faciliteiten om de beveiliging ook op dat vlak te waarborgen. Ook dienen er reglementen te zijn geïmplementeerd op grond waarvan de organisatie de mogelijkheid heeft om IT systemen te monitoren, opdat beveiligingsissues direct gesignaleerd kunnen worden. Het is verder verstandig de beveiliging van de IT systemen regelmatig aan een audit te onderwerpen.

1.12 *Maak een incidentenbeleid.*

Dit beleid zou ten minste de volgende elementen moeten omvatten:

1.12.1 *Kwalificatie als incident.*

Het moet duidelijk zijn wanneer sprake is van een incident, waarbij actie moet worden ondernomen. U kunt hierbij bijvoorbeeld denken aan de volgende situaties:

a) schending van toepasselijk beleid;
b) doorbreking van de beveiligingsmaatregelen;
c) constatering van een zwakke plek in de beveiliging.

1.12.2 Classificatie van de aard en ernst van de incidenten.

Aan de hand van verschillende factoren kan de classificatie worden vastgesteld, bijvoorbeeld verwerkt in een matrix. Hierin dient u in ieder geval de volgende elementen op te nemen:

a) de omvang en aard van getroffen gegevens;
b) impact op het systeem;
c) soort beveiligingsincident (intern/extern);
d) ernst en duur van het incident;
e) de betrokken personen.

1.12.3 Strategie voor het omgaan met incidenten.

Per type incident en afhankelijk van de ernst daarvan kan een standaard strategie ontwikkeld worden voor de aanpak. Hierbij kunnen onder andere de volgende elementen worden verwerkt:

a) welke processen zijn geraakt door het incident;
b) wie dient op de hoogte te worden gesteld;
c) welke maatregelen moeten genomen worden en op welke termijn;
d) is het verstandig te overleggen met ketenpartners.

1.12.4 Instellen van een Incidententeam.

Binnen dit team dienen de verschillende relevante competenties aanwezig te zijn, zoals IT, Legal, HR, Finance en Marketing. Daarnaast dient er, ten behoeve van de slagvaardigheid, een persoon met beslissingsbevoegdheid in het team te zitten.

Ook dienen contactpersonen te worden aangesteld, waarbij incidenten 24/7 kunnen worden gemeld en die de verschillende informatiestromen en contacten binnen de organisatie en extern coördineren. Binnen de organisatie dient duidelijk gecommuniceerd te worden wie deze contactpersonen zijn en hoe en wanneer zij gecontacteerd moeten worden.

1.13 Check uw verzekeringen en polissen.

Check welke verzekeringen zijn afgesloten, en of aanvullende verzekeringen nodig zijn. De juiste verzekering kan niet alleen de financiële consequenties afdekken, maar ook de toegang waarborgen tot de expertise binnen de benodigde competenties die nodig zijn om een incident situatie effectief en snel aan te pakken.

2 Incident

Als u het vermoeden heeft dat een incident heeft plaatsgevonden, dient u over te gaan tot maatregelen ter detectie van het incident. Het voor handen hebben van een duidelijk crisis management plan is op dat moment cruciaal. De ervaring leert dat de eerste 24 uur na een incident meestal de belangrijkste fase is voor 'damage control' en onderzoek. Indien een incident wordt gesignaleerd, dienen in ieder geval de volgende stappen te worden genomen:

- Identificeer het incident.
- Kwalificeer aard en ernst van incident.
- Informeer onmiddellijk de contactpersoon voor incidenten.
- De contactpersoon dient het Incidententeam in te schakelen.
- Schakel noodvoorzieningen in.
- Informeer het management.
- Draag zorg voor de vertrouwelijke behandeling van het incident.

3 Post-incident

Nadat het incident zich heeft voorgedaan, dienen onmiddellijk repressieve en herstelmaatregelen te worden genomen om de schade te beperken. In een latere fase is het van belang om de gang van zaken te evalueren ter voorkoming van nieuwe incidenten en ter verbetering van de strategie.

3.1 Isoleer en conserveer.

Isoleer en conserveer zo snel mogelijk het getroffen systeem en de informatie daarop. Maak back-ups. Indien nodig kunnen forensische experts worden ingeschakeld.

3.2 Audit.

Het incident dient onmiddellijk onderzocht te worden door het Incidententeam, eventueel met assistentie van anderen, zoals forensische en juridische experts. In dit onderzoek dienen de feiten en omstandigheden te worden vastgesteld en te worden uitgewerkt.

Stel vast:

a) welke en wat voor gegevens getroffen zijn;
b) wanneer en waar het incident plaatsvond;
c) wat de consequenties zijn;
d) wat de classificatie en ernst van het incident is.

3.3 Maatregelen.

Op grond van het onderzoek dient zo snel mogelijk te worden vastgesteld welke maatregelen precies nodig zijn. De benodigde maatregelen zullen grotendeels volgen uit de uitgewerkte strategie voor het omgaan met incidenten, maar het Incidententeam zal ook altijd moeten bekijken of gelet op de specifieke situatie additionele acties nodig zijn, dan wel of bepaalde acties beter achterwege kunnen worden gelaten. Hierbij dient ook gedacht te worden aan de continuïteit van de bedrijfsactiviteiten.

3.4 Check of er een wettelijke meldplicht is en aan wie.

Beoordeel of het incident gemeld moet worden aan autoriteiten, betrokkenen of contractspartijen.
Let op: in de toekomst geldt er een plicht om het lekken van persoonsgegevens te melden aan de bevoegde privacytoezichthouder, mogelijk moet dat binnen 72 uur en zo snel mogelijk aan de gedupeerden. Schakel voor een juiste beoordeling juridische expertise in en verricht vervolgens de vereiste meldingen.

3.5 Media.

Bepaal de mediastrategie, mede in overleg met een juridisch expert, als een incident in de publiciteit komt of zou kunnen komen.

3.6 Schade en kosten.

Breng de aan het incident gerelateerde schade en kosten in kaart. Neem alle andere maatregelen die uit het incident voortvloeiende schade zoveel mogelijk zouden kunnen beperken.

3.7 Documenteer.

Verifieer of alle relevante maatregelen uit het incidentenbeleid zijn genomen. Draag er zorg voor dat het onderzoek en de genomen maatregelen gedocumenteerd zijn. Documenteer daarbij ook de oorzaken van het incident en de details van het incident zelf. Op basis van de documentatie kan het incident en de handelwijze rondom het incident onderzocht en geëvalueerd worden. Verbeterpunten die hieruit volgen, dienen in het bestaande beleid en in de beveiligingsmaatregelen te worden verwerkt.

3.8 Communicatie.

Zorg ervoor dat alle relevante partijen afdoende op de hoogte worden gehouden over de afhandeling van het incident, en maak afspraken over de vertrouwelijkheid.

3.9 Updaten en bijstellen van reglementen, procedures en policies.

Pas waar nodig uw reglementen, procedures en policies aan naar aanleiding van een incident.

3.10 Claims.

Zorg voor een adequate afhandeling van eventuele claims en juridische procedures.

Voor nadere informatie kunt u contact opnemen met:

Erik Wolper / Richard Bakker
Underwriters Security & Privacy
Zurich Insurance Plc, Netherlands Branch

Zurichtoren
Muzenstraat 31
2511 VW DEN HAAG

Tel: 0031 (0)70 418 4108
Email: erik.wolper@zurich.com
richard.bakker@zurich.com

ZURICH®

VanDoorne

Advocaten • Notarissen • Fiscalisten