Diligent

5 best practices voor governance van informatiebeveiliging

In 2020 was er een recordaantal van 3950 datalekken waardoor honderden miljoen persoonlijke dossiers op straat kwamen te liggen. Het is de hoogste tijd voor de juiste governance van informatiebeveiliging. Lees onze vijf best practices.

Op steeds grotere schaal worden data gedeeld. Data zijn overal: op mobiele apparaten, in de cloud, tijdens overdracht. Het risico op datalekken neemt hierdoor ieder jaar weer toe. Er zijn steeds meer en steeds nieuwere bedreigingen. Cybercriminaliteit vormt een steeds grotere bedreiging voor het internationale bedrijfsleven. In 2020 was er volgens het gezaghebbende Data Breach Report van ITRC een recordaantal van 3950 datalekken waardoor honderden miljoenen persoonlijke dossiers op straat kwamen te liggen.

Governance van informatiebeveiliging moet dan ook onderdeel zijn van ieder bedrijfsbeleid. Beleid dat is gericht op een sterk strategische leiding, het signaleren van risico's en het bewaken van state of the art databeveiliging.

In deze informatie leest u welke best practices en richtlijnen er zijn om een zo effectief mogelijke governance van informatiebeveiliging binnen uw organisatie te implementeren. Centraal daarbij staat de vraag hoe de beschikbare bedrijfsmiddelen binnen uw organisatie zo doeltreffend mogelijk kunnen worden ingezet om uw bedrijfsgegevens zo optimaal mogelijk te beschermen.

WAT GOVERNANCE VAN INFORMATIEBEVEILIGING NIET IS

Governance van informatiebeveiliging mag niet worden verward met IT-management. Dat is voornamelijk gericht op het nemen van tactische beslissingen om beveiligingsrisico's te beperken.

WAT IS GOVERNANCE VAN INFORMATIEBEVEILIGING DAN WEL?

Governance van informatiebeveiliging gaat over het aanwijzen van personen die de bevoegdheid en verantwoordelijkheid hebben voor het nemen van beslissingen over het beveiligingsbeleid. Het gaat niet om de implementatie, maar om het opstellen van en het toezien op het beleid. Het is niet het afdwingen van het beveiligingsbeleid (dat is een taak van het IT-management), maar de bekrachtiging ervan. Kort gezegd, governance van informatiebeveiliging is gericht op de strategische en niet de tactische kant.

WAAROM IS GOVERNANCE VAN INFORMATIEBEVEILIGING BELANGRIJK?

Data spelen steeds grotere rol binnen organisaties. Of het nu gaat om financiële en juridische informatie, klantspecifieke informatie, informatie over onderzoek en ontwikkeling of bedrijfsspecifieke informatie; veel data bevatten zeer vertrouwelijke gegevens. Deze data mogen volgens wet- en regelgeving en vanwege concurrentiegevoeligheid niet naar buiten komen. Het is daarom van wezenlijk belang

Diligent

dat iedere organisatie de juiste governance van informatiebeveiliging voert en daarmee strategische maatregelen bepaalt om alle data te beschermen tegen concurrenten of erger nog cybercriminelen.

Een datalek kan zelfs lang na het incident nog schadelijke gevolgen hebben, zoals juridische aansprakelijkheid, reputatieschade, verminderd vertrouwen van klanten en partners en een verminderde omzet. Volgens een onderzoek van IBM uit 2019 bedragen de gemiddelde kosten van een datalek USD 4 miljoen.

WIE IS VERANTWOORDELIJK VOOR DE BEPALING VAN GOVERNANCE VAN INFORMATIEBEVEILIGING?

Beveiliging van data is uiteindelijk de verantwoordelijkheid van iedereen die voor een organisatie werkt. Alle werknemers moeten bewust zijn van het risico op een datalek. De governance van informatiebeveiliging, het opstellen van beleid over informatiebeveiliging, ligt echter in handen van het bestuur, de bedrijfsleiding of een stuurgroep. Immers, voor een effectieve governance is strategische besluitvorming vereist.

TOP VIJF VAN BEST PRACTICES VOOR GOVERNANCE VAN INFORMATIEBEVEILIGING

Hierna staan de vijf strategische oplossingen waarmee een organisatie het beveiligingsbeleid effectief en succesvol kan uitzetten.

1. Voer een holistische strategie

Voordat u governance van informatiebeveiliging implementeert, bekijkt u vanuit een breed perspectief welke invloed beveiliging heeft op uw organisatie. Met een brede visie op de gehele organisatie kan het best worden bepaald welke data moeten worden beschermd.

Stel de volgende vragen:

- Welke data moeten worden beschermd?
- Wat zijn de beveiligingsrisico's?
- Welk strategisch beleid moet er worden ontwikkeld?
- Welke teams moeten de verantwoordelijkheid dragen voor het handhaven van het veiligheidsbeleid?

Een beveiligingsstrategie moet ook worden afgestemd op zakelijke en IT-doelstellingen. Vraag alle stakeholders in de hele organisatie, dus de IT-, de verkoop- en marketingafdeling, operations en de juridische afdeling, om input.

2. Bewustzijn creëren en training binnen de hele organisatie

Een goede beveiliging van data stopt niet bij de governance ervan. Voor het continu opvolgen van het beveiligingsbeleid moet iedereen binnen de organisatie blijvend zijn geïnformeerd, opgeleid en getraind. Regelmatige bedrijfsonderzoeken, seminars over beveiliging en training over best practices zijn mogelijkheden om te zorgen dat databeveiliging bij alle werknemers onder de aandacht blijft.

Hoewel governance van informatiebeveiliging wordt ontwikkeld door het bestuur, het uitvoerend management en stuurgroepen, geldt dit beleid voor alle werknemers van de organisatie. Het beleid bepaalt de richtlijnen en de accountability, maar iedereen binnen de organisatie is verantwoordelijk voor het opvolgen van de beveiligingsnormen.

Stel de volgende vragen:

- Nemen werknemers eigen apparaten mee naar het werk?
- Werken zij met goedgekeurde apps?
- Hoe gaan zij om met de vertrouwelijke data?

3. Bewaken en meten

Voor governance van informatiebeveiliging moeten continu beoordelingen en metingen worden uitgevoerd.

Stel de volgende vragen:

- Welke beleidsregels werken wel?
- Welke beleidsregels werken niet?
- Welke teams of personen houden zich niet aan het beveiligingsbeleid?

Diligent

- Is het aantal beveiligingsincidenten van invloed op de reputatie die het bedrijf heeft opgebouwd?

Het meten van de werking van de governance van informatiebeveiliging zorgt ervoor dat doelstellingen worden behaald en middelen op de juiste manier worden beheerd.

Stel de volgende vragen:

- Hoe vaak worden de beveiligingsmaatregelen getest?
- Hoe vaak komen datalekken voor?
- Hoe snel wordt er gereageerd op incidenten?
- Welke regels voor beveiliging werken wel en welke niet?

Om te testen hoe goed uw organisatie is voorbereid op een datalek kan er een simulatie uitgevoerd worden. Uit de evaluatie kan blijken wat er nog verbeterd kan worden.

4. Open communicatie tussen alle stakeholders

Het is van cruciaal belang dat stakeholders rechtstreeks met de bedrijfsleiding kunnen communiceren. Als werknemers langs elkaar heen werken, kan dat belangrijke communicatie over het beveiligingsbeleid in de weg staan.

Een werknemer in de IT-beveiliging kan bijvoorbeeld praktijkervaring en vakspecifieke inzichten hebben in de doeltreffendheid van een bepaald beveiligingsbeleid. Als de bedrijfsleiding openstaat voor de feedback en suggesties van teamleden, zullen zij ook gunstiger tegenover het doorvoeren van die veranderingen staan.

Een open communicatie draagt bij aan het onderlinge vertrouwen en leidt tegelijkertijd tot meer zichtbaarheid in de volledige organisatie. Overweeg het instellen van een stuurgroep bestaande uit executives en belangrijke teamleiders om de betrokkenheid verder te verbeteren, zodat actuele beveiligingsrisico's kunnen worden beoordeeld.

De stuurgroep kan bestaan uit afdelingshoofden van de IT-afdeling, de financiële afdeling, de PR- en marketingafdeling, de juridische afdeling en operations. Periodieke vergaderingen van de stuurgroep kunnen ervoor zorgen dat het beveiligingsbeleid voortdurend wordt opgevolgd. Als bijvoorbeeld een nieuw beveiligingsbeleid wordt ingesteld, kunnen afdelingshoofden, die deelnemen aan de stuurgroep, ervoor zorgen dat hun teams zich aan dat beleid houden.

Flexibiliteit en aanpassingsvermogen promoten

Het digitale landschap verandert snel omdat nieuwe technologieën steeds meer invloed hebben op onze manier van zakendoen. Uw governance van informatiebeveiliging moet bestaan uit deugdelijke beleidsregels en richtlijnen, maar moet ook kunnen worden aangepast. Organisaties moeten het algehele effect van het beveiligingsbeleid bewaken en meten.

Stel de volgende vragen:

- Wat werkt wel?
- Wat werkt niet?
- Wat kunnen we veranderen?

CONCLUSIE

Een geslaagde governance van informatiebeveiliging gaat niet over één nacht ijs. Het is een continu proces van leren, herzien en aanpassen. Er zullen altijd nieuwe technologieën en cyberdreigingen blijven komen. En er zullen datalekken en beveiligingsincidenten voorkomen. Na een beveiligingslek moeten organisaties een proactief en strategische governance van informatiebeveiliging voeren. Alle bedrijven moeten zich ten doel stellen informatiebeveiliging te implementeren en ongewenste gevolgen en veiligheidsrisico's te beperken tot een acceptabel niveau. Bedreigingen en incidenten zullen zich blijven voordoen, maar als u ervoor zorgt dat uw bedrijf een strategische governance van informatiebeveiliging heeft, is uw organisatie beter beveiligd en tegelijkertijd uw waardevolle data beter beschermd.

Heeft u vragen? Dan horen we het graag!
www.diligent.com/nl | +31(0)20 299 6769 | info@diligent.com