Vijf best practices voor beleid inzake informatiebeveiliging

In 2015 zijn ruim 169 miljoen persoonlijke dossiers blootgesteld uit meer dan 700 gepubliceerde datalekken in de financiële wereld, de zakelijke wereld, het onderwijs, de overheid en de gezondheidszorg.

INTRODUCTIE

Data is overal: op mobiele apparaten, in de cloud, tijdens overdracht. De aanwas van data en het toenemend aantal bedrijven dat zijn processen optimaliseert op basis van data veranderen snel, naarmate data afkomstig is uit meer en meer platforms, in uiteenlopende indelingen. Datagroei, nieuwe technologieën en het toenemend aantal cyberbedreigingen vormen een uitdaging voor bedrijven bij het inrichten van hun strategieën, maatregelen en beleidsregels die al hun informatie moeten beveiligen.

Bedreigingen zijn er steeds meer en ontwikkelen zich snel naarmate criminelen steeds meer nieuwe manieren ontdekken om beveiligingssystemen te omzeilen en waardevolle data aan te vallen. Volgens het Data Breach Report[1] van ITRC zijn in 2015 ruim 169 miljoen persoonlijke dossiers blootgesteld uit meer dan 700 gepubliceerde datalekken in de financiële wereld, de zakelijke wereld, het onderwijs, de overheid en de gezondheidszorg.

Het IT Governance Institute[2d] definieert beleid inzake informatiebeveiliging als “een onderdeel van bedrijfsbeleid dat voorziet in strategische leiding, erop toeziet dat doelstellingen worden behaald, risico’s opvangt en de verantwoordelijkheid van organisatiebronnen bepaalt, en meet in hoeverre de bedrijfsbeveiliging slaagt of mislukt.”

Alles bij elkaar vereist beleid inzake informatiebeveiliging een organisatiestructuur, het toewijzen van rollen en verantwoordelijkheden, en duidelijk omschreven maatregelen en taken. Deze moeten allemaal strategisch worden ontwikkeld en gedefinieerd door de directieleden en het uitvoerend management.

Diligent

"Hoe kan een bedrijf zijn resources zo doeltreffend mogelijk inzetten om risico's verband houdend met cyberbeveiliging te beperken tot een acceptabel niveau?" is de vraag die gesteld wordt in een artikel in het blad Bloomberg Government[3]. Alleen besluitvormers in de raad van bestuur kunnen deze vraag beantwoorden.

Dit whitepaper beoogt best practices en richtlijnen te bieden om strategisch beleid inzake informatiebeveiliging met succes te implementeren. De volgende vragen komen aan bod:

- Hoe luidt de definitie van beleid inzake informatiebeveiliging?
- Welke misvattingen zijn er over beleid inzake informatiebeveiliging?
- Waarom is beleid inzake informatiebeveiliging belangrijk?
- Wie draagt de verantwoordelijkheid voor het beleid inzake informatiebeveiliging?

WAT BELEID INZAKE INFORMATIEBEVEILIGING NIET IS

Beleid inzake informatiebeveiliging mag niet worden verward met IT-management, dat hoofdzakelijk is gericht op het nemen van tactische beslissingen om beveiligingsrisico's te beperken.

U kunt beleid zien als het aanwijzen van personen die gemachtigd en verantwoordelijk zijn voor het nemen van beslissingen gerelateerd aan het informatiebeveiligingsbeleid. Het is niet de implementatie van het beleid, maar het bewaken en definiëren van het programma. Het is niet het afdwingen van het beleid (dat is een taak van het IT-management), maar de bekrachtiging van het beveiligingsbeleid. Kort gezegd is beleid inzake informatiebeveiliging gericht op de strategische kant, niet de tactische.

WAAROM IS BELEID INZAKE INFORMATIEBEVEILIGING BELANGRIJK?

Beleid inzake informatiebeveiliging beoogt strategische maatregelen te bepalen om de informatie van een organisatie te beschermen. Die informatie kan bestaan uit zeer vertrouwelijke data en informatie: financiële en juridische informatie, klant- of partnerspecifieke informatie, informatie met betrekking tot onderzoek en ontwikkeling, proprietary informatie en meer. Organisaties slaan meer en meer data op die concurrenten, of erger nog, criminelen, goed van pas zou kunnen komen.

In de afgelopen jaren hebben cybercriminelen het nieuws gehaald met grootschalige hacks en datalekken. Deze variëren van de hack bij Sony Pictures Entertainment, waarbij criminelen naar schatting 100 terabyte aan vertrouwelijke data[4] hebben gestolen, tot het datalek bij Anthem Medical[5]. Alle sectoren zijn kwetsbaar voor aanvallen. Een datalek kan zelfs lang na het incident nog schadelijke gevolgen hebben: juridische aansprakelijkheid, een beschadigde merkreputatie, wegvallend vertrouwen van klanten en partners, en verminderde omzet als gevolg hiervan. Volgens een Ponemon-onderzoek uit 2016[6] bedragen de gemiddelde kosten van een datalek $ 4 miljoen.

Strategisch beleid inzake informatiebeveiliging is essentieel voor alle organisaties. Hierdoor kunnen zij hun klanten, partners en werknemers garanderen dat zij met en bij een veilig bedrijf werken. En omdat bedrijfsdata meer en meer toegankelijk wordt voor werknemers via mobiele apparaten en de cloud, is het uitermate belangrijk dat bedrijven hun beveiligingspraktijken up-to-date houden om te kunnen waarborgen dat de juiste werknemers toegang hebben tot die data. Want uiteraard moet worden voorkomen dat vertrouwelijke data in handen valt van criminelen.

WIE DRAAGT DE VERANTWOORDELIJKHEID VOOR DE BEPALING VAN BELEID INZAKE INFORMATIEBEVEILIGING?

Alle teams en werknemers moeten beveiliging als hun eigen verantwoordelijkheid beschouwen, maar de bedrijfsleiding is verantwoordelijk voor het opzetten en onderhouden van een beleidskader inzake informatiebeveiliging. Ongeacht of het de directie is, executives of een bestuurscommissie, of dat zij hier allemaal aan meewerken, voor beleid inzake informatiebeveiliging is strategische planning en besluitvorming vereist.

TOP VIJF VAN BEST PRACTICES VOOR BELEID INZAKE INFORMATIEBEVEILIGING

Wat nu volgt zijn strategische oplossingen om een organisatie beter in staat te stellen haar beveiligingsbeleid met succes uit te voeren:

1. Een holistische strategie voeren: Voordat u beleid inzake informatiebeveiliging implementeert, bekijkt u de impact van beveiliging op uw organisatie vanuit een uniform perspectief. Een onderzoek in het hele bedrijf kan helpen bepalen welke data moet worden beschermd. Hierdoor kunt u ook in een vroeg stadium al de bijval krijgen van uw belangrijkste stakeholders. Denk aan de volgende vragen:

- Welke data moet worden beschermd?
- Wat zijn de risico's?

- Welke strategische beleidsregels zouden moeten worden ontwikkeld?

- Welke teams moeten de verantwoordelijkheid dragen voor het handhaven van de beleidsregels?

Een beveiligingsstrategie moet ook in lijn gebracht worden met en afgestemd op de zakelijke en IT-doelstellingen. Vraag alle stakeholders in de organisatie, dus de IT-, de verkoop- en de marketingafdeling, de bedrijfsvoering en de juridische afdeling, om input. Zo kunt u hun zorgen en uitdagingen in kaart brengen en kunt u hun vaardigheden en expertise beoordelen.

Vermijd doorsneeoplossingen en silovorming. Dit kan leiden tot meer obstakels en van elkaar gescheiden beveiligingsoplossingen. Een holistische aanpak zorgt ervoor dat uw bedrijfsleiding (de bedenkers van het beleid inzake informatiebeveiliging) meer controle en inzicht krijgen.

2. Bewustzijn realiseren en training binnen de hele organisatie implementeren: Als u het beleid inzake informatiebeveiliging wel instelt maar vervolgens niet opvolgt, kunnen er negatieve resultaten ontstaan, zoals onvoldoende acceptatie, onduidelijkheden over beleidsregels, rollen en verantwoordelijkheden, en kwetsbaarheden in de beveiliging. Voor het continu opvolgen van het beveiligingsbeleid moeten alle betrokken partijen zijn geïnformeerd, opgeleid zijn en getraind blijven.

Beveiliging is niet alleen de verantwoordelijkheid van IT. Iedereen is verantwoordelijk. Iedereen is verantwoordelijk.

- Nemen uw werknemers hun eigen apparaten mee naar het werk?

- Werken zij met goedgekeurde apps?

- Hoe gaan zij om met de vertrouwelijke data van het bedrijf?

Regelmatige bedrijfsonderzoeken, seminars over beveiliging en training op basis van best practices inzake beveiliging zijn manieren om te zorgen dat beveiliging onder de aandacht blijft bij alle werknemers.

Hoewel beleid inzake informatiebeveiliging wordt ontwikkeld door de directie, executives en bestuurscommissies, geldt het beleid voor alle werknemers van de organisatie. Het bepaalt weliswaar de richtlijnen en de accountability. Elk teamlid is echter verantwoordelijk voor het opvolgen van de beveiligingsstandaard.

Bewustzijn, training en opleiding voor best practices inzake beveiliging moeten worden voortgezet. Een organisatie kan bepaalde teamleden bijvoorbeeld laten deelnemen aan een conferentie over beveiliging om op de hoogte te blijven van de nieuwste technieken in de sector. Aan de hand van de nieuw verworven kennis kunnen zij dan hun inzicht delen met de rest van de organisatie.

3. Bewaken en meten: Voor beleid inzake informatiebeveiliging moeten processen continu worden beoordeeld en gemeten.

- Welke beleidsregels werken wel?

- Welke beleidsregels werken niet?

- Welke teams of personen houden zich niet aan de beleidsregels?

- Is het aantal beveiligingsincidenten van invloed op de reputatie die het bedrijf heeft opgebouwd bij klanten en partners?

Het meten van de naleving van het beleid inzake informatiebeveiliging zorgt ervoor dat doelstellingen worden behaald en resources op de juiste manier worden beheerd.

- Hoe vaak test u uw beveiligingsmaatregelen?

- Hoe vaak komen datalekken voor?

- Hoe snel worden incidenten opgevolgd?

- Welke beleidsregels werken wel en welke niet?

Een organisatie kan bijvoorbeeld een datalek simuleren om te testen hoe goed de teams zijn voorbereid. Uit de resultaten kan blijken wat de actiepunten zijn en wat het bedrijf wel of niet onder controle heeft.

4. Open communicatie tussen alle stakeholders bevorderen: Het is cruciaal dat stakeholders rechtstreeks met de bedrijfsleiding kunnen communiceren. Een verzuilde aanpak kan belangrijke communicatie met betrekking tot beveiligingsbeleid in de weg staan.

Durven werknemers overal in de organisatie een eventueel datalek aan te kaarten bij de bedrijfsleiding? Of zullen ze eventuele negatieve berichten achterhouden voor de top?

Een open communicatie draagt bij aan vertrouwen en leidt tegelijkertijd tot meer inzicht in de volledige organisatie. Overweeg een bestuurscommissie bestaande uit executives en belangrijke teamleiders in te stellen om de betrokkenheid verder te verbeteren, zodat u actuele beveiligingsrisico's kunt beoordelen. De commissie kan bestaan uit afdelingshoofden van de IT-afdeling, de financiële afdeling, de PR- en marketingafdeling, de juridische afdeling en de operations. Periodieke vergaderingen van de bestuurscommissie kunnen ervoor zorgen dat de beleidsregels doorlopend worden opgevolgd. Bijvoorbeeld: als een nieuw beveiligingsbeleid wordt ingesteld, kunnen afdelingshoofden, die deel uitmaken van de commissie, ervoor zorgen dat hun teams zich aan het beleid houden.

5. Flexibiliteit en aanpassingsvermogen promoten: Het digitale landschap verandert snel, omdat nieuwe platforms onze manier van zaken steeds meer beïnvloeden. Uw beleid inzake informatiebeveiliging moet bestaan uit deugdelijke beleidsregels en richtlijnen, maar moet ook kunnen worden aangepast. Organisaties moeten het algehele effect van de beleidsregels bewaken en meten. Denk aan de volgende vragen:

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

Bijvoorbeeld: een werknemer in de IT-beveiliging kan praktijkervaring en inzicht hebben in de doeltreffendheid van een bepaald beveiligingsbeleid. Als de bedrijfsleiding open staat voor de feedback en suggesties van het teamlid, moet er ook flexibiliteit zijn met betrekking tot het doorvoeren van die veranderingen.

CONCLUSIE

Een geslaagd beleid inzake informatiebeveiliging gaat niet over één nacht ijs. Het is een continu proces waarbij men blijft leren, herzien en aanpassen. Elk bedrijf heeft specifieke behoeften, maar de beveiliging van de data hebben alle organisaties gemeen. Er zullen altijd nieuwe technologieën en cyberbedreigingen zijn. Datalekken en beveiligingsincidenten zullen ook voorkomen. Na een inbreuk in de beveiliging moeten organisaties niet bij de pakken neerzitten, maar een proactief en strategisch beleid inzake informatiebeveiliging voeren. Alle bedrijven moeten zich ten doel stellen informatiebeveiliging te implementeren en ongewenste gevolgen en risico's te beperken tot een acceptabel niveau. Bedreigingen en incidenten zullen zich blijven voordoen. Als u uw bedrijf echter bewapent met een strategisch beleid inzake informatiebeveiliging, kunt u uw organisatie beter beveiligen en tegelijkertijd uw waardevolle informatie beschermen.

BRONNEN:

1. "Data Breach Reports", ITRC, 29 december 2015, http://www.idtheftcenter.org/images/breach/ DataBreachReports_2015.pdf
2. "Information Security Governance: Guidance for Boards of Directors and Executive Management" 2e editie, IT Governance Institute, 2006, http://www.isaca.org/knowledge-center/research/documents/information-security- govenance-for-board-of-directors-and-executive-management_res_eng_0510.pdf
3. "Why cyber is a boardroom issue", Tom Skypek, 21 april 2016. Bloomberg Government, http://about.bgov.com/blog/why-cyber-is-a-boardroom-issue/
4. "The Sony Hackers Still Have A Massive Amount of Data that Hasn't Been Leaked Yet", Business Insider, James Cook, 16 december 2014, http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of- data-that-hasnt-been-leaked-yet-2014-12
5. "Insurance Giant Anthem Hit by Massive Data Breach", CNN Money, Charles Riley, 4 februari 2015, http://money.cnn.com/2015/02/04/technology/anthem- insurance-hack-data-security/
6. "2016 Cost of Data Breach Study", Ponemon-onderzoek 2016, http://www-03.ibm.com/security/data-breach/

Beleid inzake informatiebeveiliging bepaalt de strategische maatregelen om de informatie van een organisatie te beschermen.

Telefoon: +31 (0) 621 552 222
Email: jthiel@diligent.com
Bezoek: www.diligent.com