IRISONE ICT

Bescherm je data met Azure Information Protection

Bescherm de gevoelige bedrijfsinformatie beter, waar en wanneer je ook werkt. Van eenvoudige classificaties tot ingesloten labels en machtigingen: verbeter de gegevensbescherming met Azure Information Protection.

Documenten reizen meer tussen gebruikers, apparaten, apps en services dan ooit tevoren. Helaas geeft het beschermen van je netwerk, gebruikers of apparaten geen garantie dat je gegevens niet in handen van ongewenste lezers komen.

Azure Information Protection (AIP) is een cloud-gebaseerde oplossing waarmee organisaties documenten en e-mails kunnen ontdekken, classificeren en beschermen door labels op de inhoud toe te passen. Met Azure Information Protection kunnen IT-beheerders:

- E-mails en documenten automatisch classificeren op basis van ingestelde regels,
- Markeringen toevoegen aan de inhoud, als aangepaste watermerken, kop- en voettekst,
- Vertrouwelijke bestanden beschermen van de organisatie met Rights Management, waardoor:
    - De bestanden worden vergrendeld voor specifieke ontvangers, zowel binnen als buiten de organisatie;
    - Specifieke rechten worden toegepast om de bruikbaarheid van het bestand te beperken;
    - De inhoud wordt gedecodeerd op basis van de identiteit van de gebruiker en autorisatie in het rechtenbeleid.

Deze mogelijkheden stellen organisaties in staat om meer end-to-end controle over hun gegevens te hebben. In deze context speelt Azure Information Protection een belangrijke rol bij het beveiligen van de bedrijfsgegevens.

De huidige staat van bedrijfsbescherming

Veel ondernemingen beschikken nog niet over enige beveiligingstechnologie. Documenten en e-mails worden in gewone teksten gedeeld. De IT-beheerders hebben geen duidelijkheid wie toegang heeft tot welke documentatie.

Hoewel de beveiliging een voortdurend onderwerp is en geen enkele organisatie 100% garantie kan claimen, vergroot AIP de beveiligingsvoetdruk van de organisatie.

Beveiligingsafspraken voor het delen van documentatie

In een situatie waarin de IT-beheerder geen controle heeft over het apparaat of de identiteit, heeft IT dus ook geen inzichten meer over wat er met de beschermde informatie gebeurt.

Je vertrouwt de ontvanger erop dat hij zich houdt aan het beleid dat op de inhoud is geplaatst. Azure Information Protection helpt bij het vaststellen van deze grenzen.

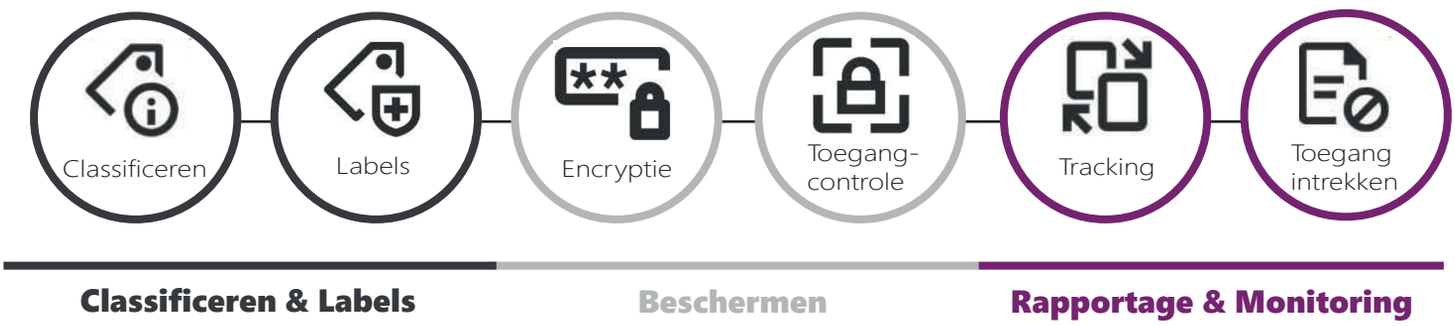
Door gebruik te maken van AIP, hebben IT-beheerders volledige controle over het beheer van de gebruikersidentiteiten.

Dit bouwt het juiste vertrouwensplatform op binnen de organisatie. Het verzenden van informatie buiten de organisatie is daarintegen minder betrouwbaar. Bij de benadering van informatiebescherming, zijn er enkele principes die je bij een risicobeoordeling moet uitvoeren.

Houdt bij het uitvoeren van deze risicobeoordeling rekening met de volgende punten:

- De ontvanger heeft fysiek toegang tot een onbeheerd apparaat en heeft daardoor de controle over alles wat er op het apparaat gebeurt.
- De ontvanger wordt geauthentiseerd met een zekere mate van vertrouwen die verband houdt met niet-nabootsen.

Hoe IRIS one jouw organisatie ondersteunt met AIP



Classificatie - Gegevens kunnen automatisch worden geclassificeerd op basis van inhoud, context en bron. Gebruikers kunnen het gevoeligheidslabel selecteren die van toepassing zijn op het document als ze een hoger coderingsniveau willen toekennen dan het standaard-beleid. Classificatie- en etikettingsinformatie wordt vervolgens in het document of e-mail ingebed en reist overal mee.

Labels - Labels zijn metagegevens die ingesloten zijn in een document of e-mail, een duidelijke tekst zodat andere systemen deze kunnen lezen. Etiketten zijn persistent en reizen met het document mee. Acties zoals visuele markering van het document en versleuteling kan worden afgedwongen op basis van het label.

Encryptie - Dit is de versleuteling van het document, plus de opname van de authenticatie-vereisten en een definitie van het gebruikersrechten op de gegevens. Dit zorgt ervoor dat alleen geautoriseerde gebruikers toegang hebben tot beschermde gegevens en dat ze alleen toegestane acties kunnen ondernemen.

Toegangscontrole - Alle e-mails en documenten kunnen veilig worden gedeeld, met het ingestelde beleid van classificeren en labelen. De organisatie behoudt de controle, ongeacht of ze intern/extern worden gedeeld.

Monitoring en rapportage - IT-beheerder kunnen activiteiten op alle bestanden volgen en de toegang intrekken in geval van onverwachte activiteiten. Volledige inzage in de details tot het intrekken van de toegang, helpen de organisatie bij het bewaken, analyseren en rapporteren van gegevens voor de naleving en regelgevende doeleinden.

De voordelen van Azure Information Protection

Volledige controle, ongeacht wie inzichten heeft in de documenten

Zelf in geval van een datalek, kunnen de gevoelige en vertrouwelijke gegevens niet worden benaderd zonder uitdrukkelijke toestemming van de gegevensbeheerders. Indien noodzakelijk, kan alle toegang direct ingetrokken worden.

De manier van werken hoeft niet te veranderen.

Met behulp van Microsoft's Azure Information Protection, is er nu een manier om de gegevens in te zetten en te beschermen, waar de documenten zich ook bevinden of wie ze ook heeft. De dagelijkse werkzaamheden gaan gewoon door.

Real-time informatie

Alle documenten en gegevens blijven beschermd, waar ter wereld ze zich ook bevinden. Met eenvoudige inzichten weet je ook welke teams of afdelingen regelmatig gevoelige informatie verzenden of ontvangen.

Lage eigendomskosten

IRIS one kan je organisatie goed en vakkundig ondersteunen bij de implementatie. Updates worden automatisch via de cloud geïmplementeerd en wijzigingen kunnen door de organisatie worden aangebracht zoals het gegevensbeleid en wijzigingen in de wetgeving.

Gemakkelijk te onderhouden en bij te werken

Met de introductie van Microsoft AIP, kan een getrainde gegevensbeheerder eenvoudig de beleidswijzigingen door de gehele organisatie toepassen.

Azure Information Protection is een goede stap om ervoor te zorgen dat je organisatie niet het slachtoffer wordt van cybercriminaliteit en om te voldoen aan de AVG-naleving.

Microsoft AIP zorgt ervoor dat je documenten en e-mails worden beschermd en versleuteld op het punt van creatie, en altijd beschermd blijven, waar ze ook staan.

Wil je meer weten hoe IRIS one de online beveiliging kan verbeteren? Neem dan contact met ons op:
073 523 2288

IRISONE ICT

Graafsebaan 111,
5248 NL Rosmalen
073 523 2288
iris@iris-one.nl
www.iris-one.nl

Het maximale uit jezelf halen, iedere dag.