



Consulting services: Security

Sensitive Data Assessment

Weet u waar uw gegevens zich bevinden?

Tegen 2024 zal het jaarlijks volume aan dataconsumptie naar verwachting groeien tot 149 zettabytes (ZB), een verdubbeling ten opzichte van de in 2021 geconsumeerde hoeveelheid*. In het verleden hielden organisaties zich voornamelijk bezig met documenten en e-mails. Maar nu hebben ze ook te maken met instant messaging, tekstberichten, videobestanden en afbeeldingen. En het internet of Things (IoT), zal deze gegevensexplosie alleen maar in de hand werken.

De bescherming van informatie is essentieel om het vertrouwen te waarborgen, maar ook om te voldoen aan de interne en externe regelgeving. Gegevensbescherming wordt een nog grotere uitdaging, nu mensen op nieuwe manieren werken en over de grenzen heen gegevens creëren en delen. Terwijl mobiliteits- en clouddiensten gebruikers hebben geholpen om productiever te worden en beter samen te werken, is het moeilijker geworden om de gegevens te beveiligen en te controleren. Klanten moeten nu gevoelige informatie beschermen over apparaten, SaaS-toepassingen en clouddiensten heen, alsook op fysieke omgevingen.

Voordat een organisatie haar gegevens kan beschermen, moet ze weten waar deze zich bevinden, hoe ze worden gebruikt en gedeeld, wat de bijbehorende risico's zijn op het gebied van privacy en regelgeving, en zelfs of de gegevens nog wel nodig zijn.

Leer uw gegevens kennen

De Sensitive Data Assessment is een klantenengagement van Proximus, waarbij gegevens van organisaties worden gescand op privacy- en regelgevingsrisico's. Naast het scannen van organisatiegegevens op risico's inzake privacy en regelgeving omvat de Sensitive Data Assessment ook een activiteit om de Microsoft 365-omgeving (waaronder Teams, Sharepoint, Exchange...) van uw organisatie te toetsen aan de Data Protection Baseline. Deze beoordeling maakt gebruik van Microsoft Compliance Manager en geeft inzicht in hoe uw organisatie presteert ten opzichte van de belangrijkste normen en voorschriften voor gegevensbescherming. Ze wordt tevens gebruikt om een eerste Compliance Score te berekenen. Proximus zal de organisatie ook verbeteringsacties voorstellen.

Uiteindelijk zal de beoordeling van gevoelige gegevens u helpen te begrijpen hoe ze privacy- en regelgevingsrisico's die tijdens de opdracht zijn ontdekt, kan inperken en hoe u zich ertegen kan beschermen.

Vanaf het begin leidt Proximus u door de volledige workshop en implementatie, zodat de inspanningen nauw aansluiten bij uw bedrijfsbehoeften en -strategie.

* bron: Finances Online "How much data is created every day"

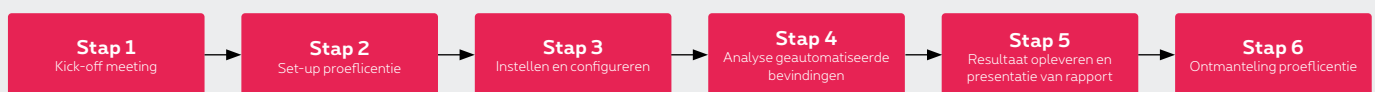
Sensitive Data Assessment

Service Description

Deze opdracht maakt gebruik van een subset van Microsoft 365-producten, -diensten en -functies om zicht te krijgen op mogelijke bestaande, en soms verborgen, privacy- en regelgevingsrisico's in de gegevens, die zich kunnen voordoen in de Microsoft 365-cloudomgeving en eventueel vestigingen van uw organisatie. De resultaten en bevindingen van de Data Risk Check dienen als input voor de algemene workshop en zullen worden gebruikt om bewustzijn te creëren en aanbevelingen te doen om de ontdekte risico's aan te pakken..

Scope

- Data Risk Check
 - Optioneel: Gegevensopslag op locatie
 - Optioneel: Windows 10 end points
- Compliance Manager Tenant Assessment
- Aanbevelingen en volgende stappen



Deliverables

De bevindingen van de Automated Discovery & Compliance Manager Tenant Assessment in het kader van de Data Risk Check worden verzameld, geanalyseerd en gekoppeld aan Microsoft-oplossingen voor risicobeperking. Tijdens een workshop worden de bevindingen en vastgestelde risico's op het gebied van privacy en regelgeving besproken, worden mogelijke oplossingen voor risicobeperking gepresenteerd en wordt een stappenplan met uitvoerbare volgende stappen en aanbevelingen opgesteld. Deze roadmap bevat aanbevelingen voor alle Microsoft Purview-tools die de klant al bezit en ontwikkelt. Het overzicht met next steps helpt de klant bij een bredere uitrol van Microsoft Purview.

- Activiteiten
- Doorlooptijd
- Resource capacity
- Technologische capaciteiten (oplossingen) indien van toepassing
- Begroting

64%

van de incidenten van gegevensdiefstal kan worden voorkomen door Data Loss Prevention.¹

85%

minder tijd besteed aan het identificeren, classificeren en labelen van gevoelige gegevens door organisaties dankzij automatisering en AI.²

1. McAfee: "Grand Theft Data: Data exfiltration study: Actors, tactics, and detection", 2017
2. Forrester Consulting, "The Total Economic Impact Of Microsoft 365 E5 Compliance", June 2021, commissioned by Microsoft.



Waarom Proximus?

- Meer dan vijftien jaar ervaring in cyberbeveiliging en het leiden van een security operations center
- Ervaring in alle sectoren: diensten, industrie, financiën, overheid, enz.
- Een Microsoft Gold-partner voor beveiliging, wat betekent dat u altijd verzekerd bent van de beste service en het beste advies
- Geavanceerde specialisatie in de bescherming tegen bedreigingen en het beheer van identiteit en toegang
- Onbeperkte ondersteuning bij alles van beoordeling, architectuur en implementatie tot en met beheerde diensten

Meer weten?

Neem contact op met uw Proximus-contactpersoon of praat met een expert:
proximus.be/securitycontact

