Controlware Security Day 2022

Der sichere Arbeitsplatz in einer modernen Welt mit Microsoft 365

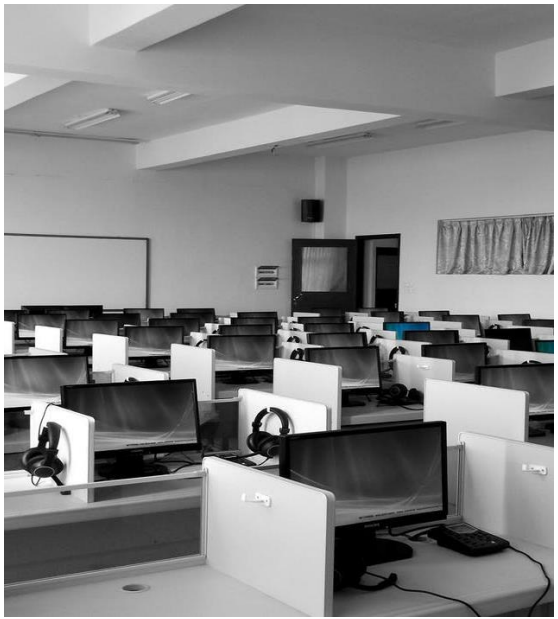
Patrick Benesch, Controlware GmbH, Team Lead – Competence Center Cloud|Modern Workplace
Mischa Rohleder, Controlware GmbH, Cloud Security Consultant
Hermann Karsten, Controlware GmbH, Senior Cloud Consultant

Controlware Security Day
22. - 23. September 2022
Congress Park Hanau

© 2022 Controlware GmbH

Unser Arbeitsplatz

früher



vor nicht all zu langer Zeit…

Heute

© 2022 Controlware GmbH

Ist das der neue und moderne Arbeitsplatz?

© 2022 Controlware GmbH

Mein persönliches Ziel eines modernen Arbeitsplatzes

© 2022 Controlware GmbH

Der moderne Arbeitsplatz

Wie wird dieser durch Microsoft definiert?

Kreativität

© 2022 Controlware GmbH

Der moderne Arbeitsplatz

Wie wird dieser durch Microsoft definiert?

Kreativität

Teamwork

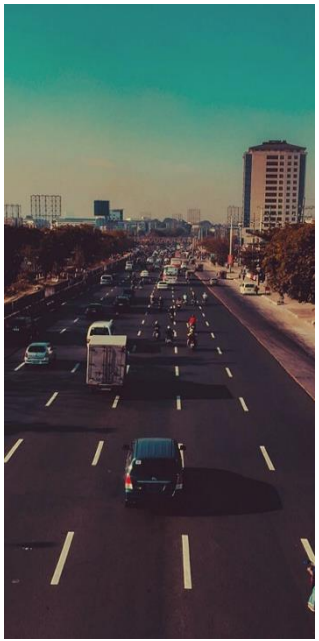
© 2022 Controlware GmbH

Der moderne Arbeitsplatz

Wie wird dieser durch Microsoft definiert?

Kreativität

Teamwork



Mobilität

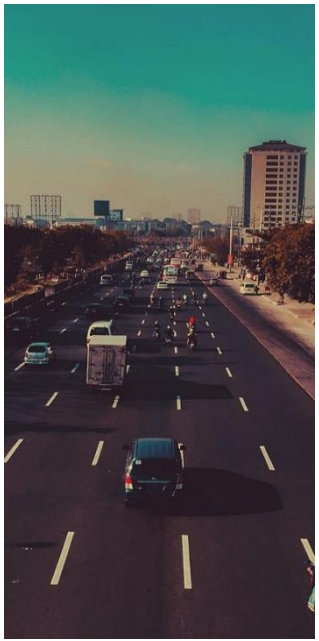
© 2022 Controlware GmbH

Der moderne Arbeitsplatz

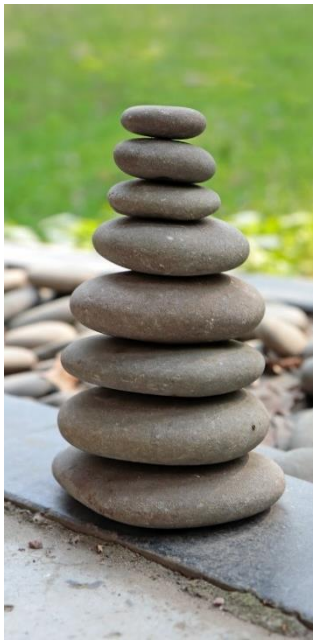
Wie wird dieser durch Microsoft definiert?

Kreativität

Teamwork



Mobilität



Einfachheit

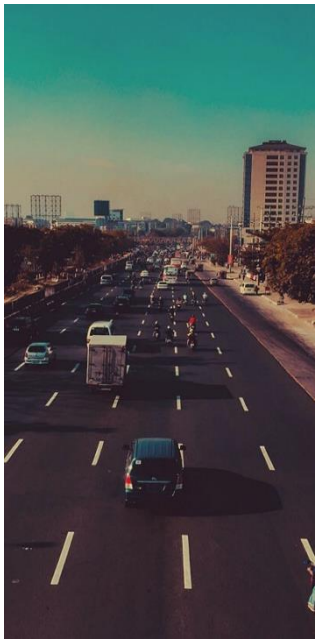
© 2022 Controlware GmbH

Der moderne Arbeitsplatz

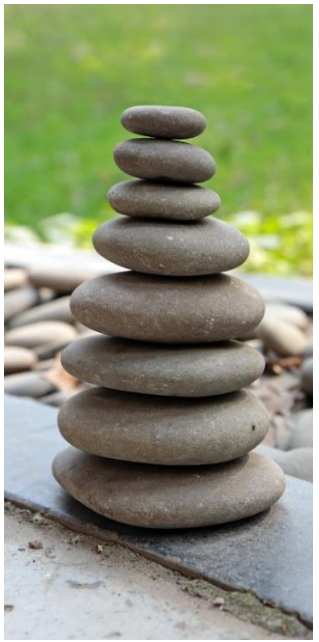
Wie wird dieser durch Microsoft definiert?

Kreativität

Teamwork



Mobilität



Einfachheit

Sicherheit

© 2022 Controlware GmbH

Das Sicherheitsperimeter hat sich verändert!

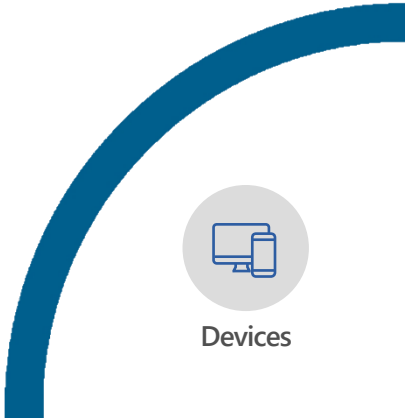
© 2022 Controlware GmbH

Das Sicherheitsperimeter hat sich verändert!

© 2022 Controlware GmbH

Kernbereiche bei der Sicherheit in der Cloud

controlware

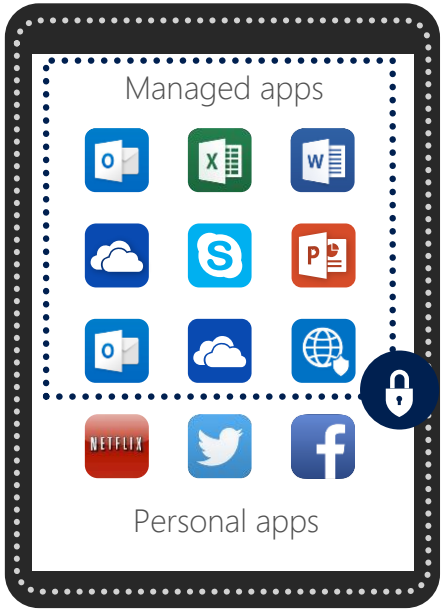


© 2022 Controlware GmbH

Devices

Mobile Device Management

Mobile Application Management

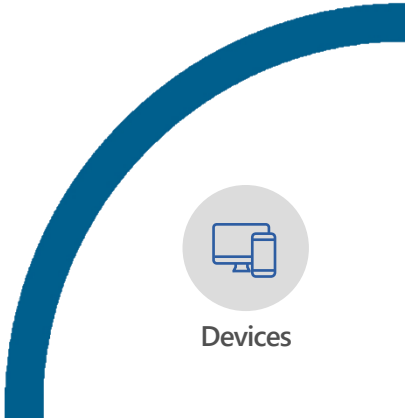


Verschlüsselung

EDR / XDR

© 2022 Controlware GmbH

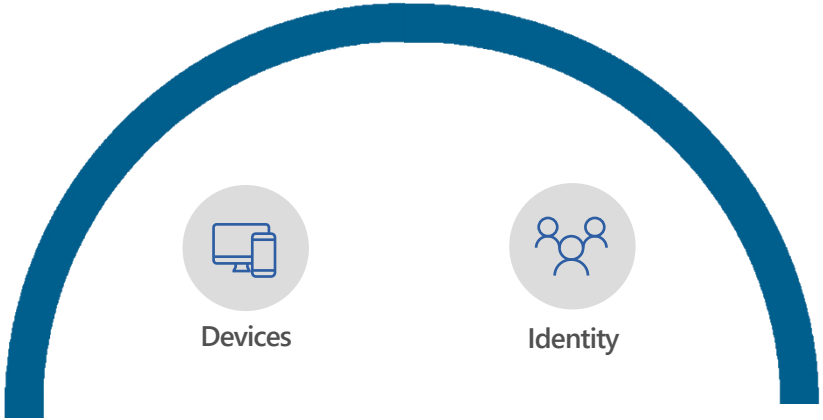
Kernbereiche bei der Sicherheit in der Cloud



© 2022 Controlware GmbH

Kernbereiche bei der Sicherheit in der Cloud

controlware



© 2022 Controlware GmbH

Identity - Basics

controlware

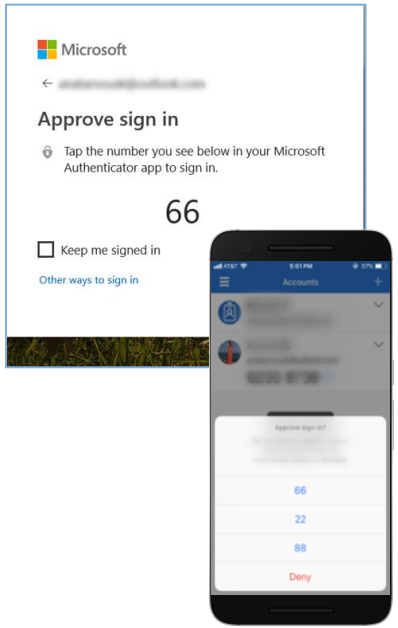
Multi-Faktor-Authentifizierung

- SMS
- Anruf
- Soft Token
- Hard Token / FIDO2

Bedingter Zugriff

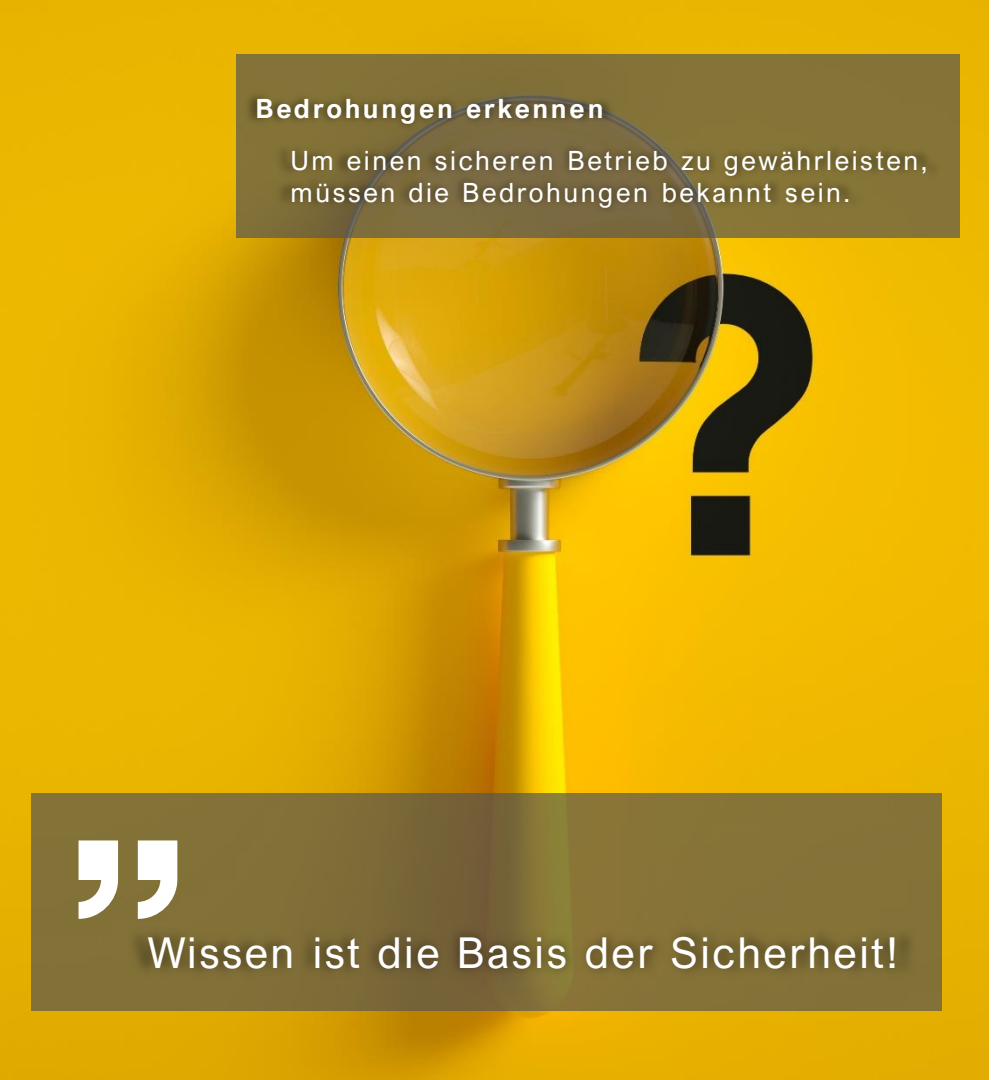
- Anwender & Standort
- Endgerät
- Echtzeit Risiko
- Applikation

Passwortlose Authentifizierung



Privileged Identity Management

© 2022 Controlware GmbH



controlware

Bedrohungen

Mögliche Ursachen für erfolgreiche Angriffe

- Kompromittierte Accounts
- Insider Risk
- Fehlkonfiguration
- Daten sind nicht geschützt
- Schwache Passwörter
- Kein MFA
- User Awareness
- Malware / Phishing
- ...

Gäste

Häufig werden Gäste in Microsoft 365 unterschätzt

> Normalerweise gehen Gäste irgendwann wieder...

controlware

Bedrohungen durch Gäste

Mögliche Bedrohungen

- Zugriff auf Kontakte
- Zugriff auf Dateien
- Social Engineering
- „Schläfer“ / verwaiste Account
- Malware
- Phishing

Gäste

Sicherheitsrisiken

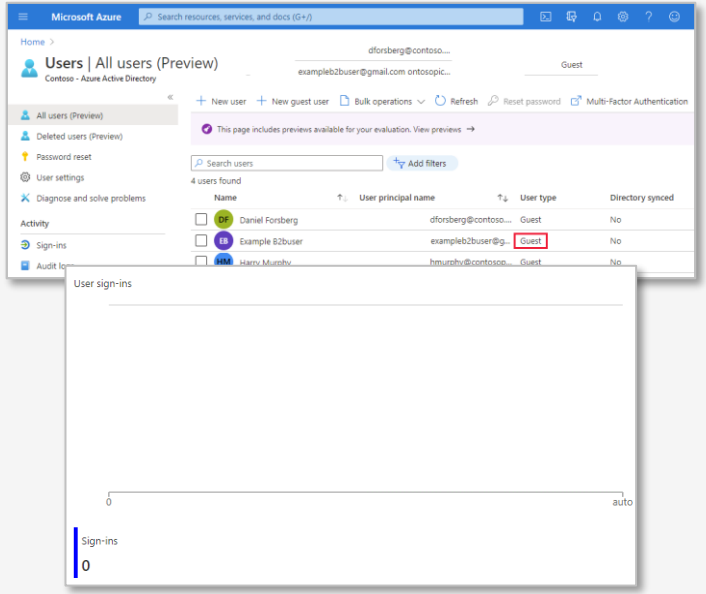
- Kein Überblick über Gäste
- Gäste können weitere Gäste einladen (Standardeinstellung)
- Daten oft nicht geschützt (Sensitivity Labels)
- Verwaiste Gäste
- Keine Kontrollen, ob Gäste weiterhin Zugriff haben dürfen
- Zugriff auf sensible Projektdaten, auch über das Projekt hinaus
- Geräte von Gästen entsprechen ggf. nicht den Sicherheitsstandards
- Zugriff auf sensible Daten (z.B. Telefonnummern) (Standardeinstellung)
- Admins haben normalerweise keine Informationen zu Gästen

Was kann man tun?

- Einschränken, wer einladen darf
- Regelmäßig überprüfen
- Bei Inaktivität deaktivieren
- Deaktivierungsdatum schon direkt bei der Anlage festlegen

Wie kann man das umsetzen?

- Graph API
- Azure Functions
- Custom Security Attributes (noch in Preview)



© 2022 Controlware GmbH

Gäste

Sicherheitsrisiken

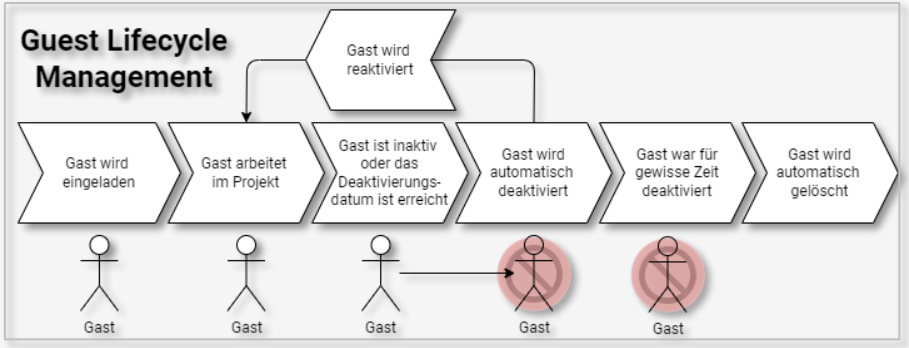
- Kein Überblick über Gäste
- Gäste können weitere Gäste einladen (Standardeinstellung)
- Daten oft nicht geschützt (Sensitivity Labels)
- Verwaiste Gäste
- Keine Kontrollen, ob Gäste weiterhin Zugriff haben dürfen
- Zugriff auf sensible Projektdaten, auch über das Projekt hinaus
- Geräte von Gästen entsprechen ggf. nicht den Sicherheitsstandards
- Zugriff auf sensible Daten (z.B. Telefonnummern) (Standardeinstellung)
- Admins haben normalerweise keine Informationen zu Gästen

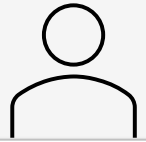
Was kann man tun?

- Einschränken, wer einladen darf
- Regelmäßig überprüfen
- Bei Inaktivität deaktivieren
- Deaktivierungsdatum schon direkt bei der Anlage festlegen

Wie kann man das umsetzen?

- Graph API
- Azure Functions
- Custom Security Attributes (noch in Preview)

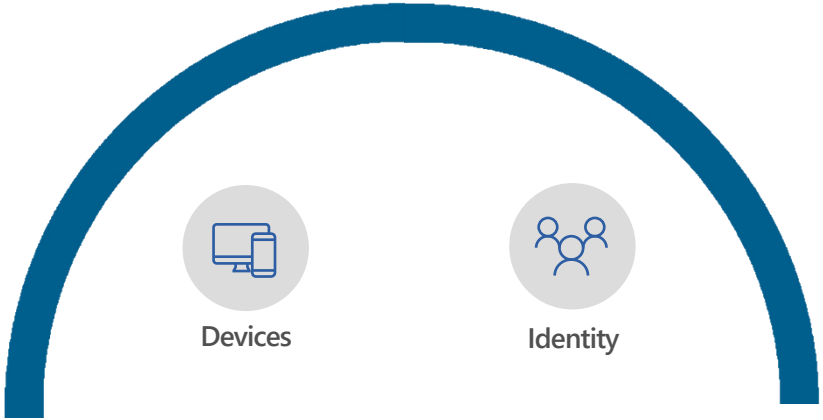




Attribute name	Attrib...	Data type	Multi-valu...	Assigned values
justification	[text]|B...	String	No	Benötigt, da er im Projekt X mit arbeitet
allowAutomatedDeletion	[true/fa...	Boolean	No	false
deactivationDate	[YYYY-...	String	No	2022-10-01
responsibles	[email]|...	String	Yes	1 value
allowAutomatedDeactivation	[true/fa...	Boolean	No	false

© 2022 Controlware GmbH

Kernbereiche bei der Sicherheit in der Cloud



© 2022 Controlware GmbH

Kernbereiche bei der Sicherheit in der Cloud

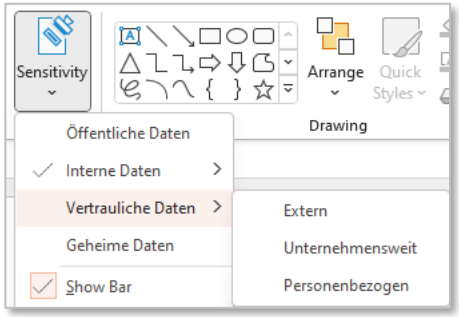
© 2022 Controlware GmbH

controlware

Datenklassifizierung

Ziel

- Überblick der eigenen Daten
- Schutz der Daten
- Datenverlust vermeiden
- Unabhängigkeit vom Speicherort
- Erkennen/Verhindern das Teilen von bestimmten Daten
- Markierungen von schützenswerten Daten
- Schutz von Daten vor Gästen und innerhalb des Unternehmens vor unberechtigten Zugriffen



Was ist bei der Einführungen zu beachten?

- Was kennen die Benutzer schon?
- Die Bezeichnungen sollten auf ein Minimum begrenzt und einfach aufgebaut sein
- Verwenden von unterschiedlichen Bezeichnern für Gruppen und Sites
- Sollten Data Loss Prevention (DLP) Richtlinien eingesetzt werden, dann sollten neue Elemente zunächst standardmäßig als sensibel markiert werden, da ggf. eine Prüfung durch DLP noch nicht stattgefunden hat

Microsoft 365 Security

Wie hilft Microsoft diese neuen Anforderungen zu erfüllen?

Identity & Access Management

Azure Active Directory
Microsoft Cloud App Security
Windows Hello
Windows Credential Guard

Information Protection

Azure Information Protection
Office 365 Data Loss Prevention
Microsoft Cloud App Security
Windows Information Protection
Microsoft Intune
BitLocker

Threat Protection

Azure Advanced Threat Protection
Windows Defender Advanced Threat Protection
Office 365 Advanced Threat Protection
Office 365 Threat Intelligence
Microsoft Cloud App Security

Security Management

Microsoft Security Center
Microsoft Compliance Center
Windows Defender Security Center
Microsoft Secure Score
Microsoft Compliance Score

© 2022 Controlware GmbH

Wir schaffen die Grundlagen für Ihr Sicherheit!

Unsere standardisierten Dienstleistungen geben ihnen die Basis für einen sicheren Einsatz ihrer Microsoft 365 Lösung

Security Checkup

Wir prüfen Ihren Microsoft 365 Mandanten auf über 80 Sicherheitsempfehlungen. Hierbei betrachten wir sowohl technische als auch organisatorische Maßnahmen. Etwaige Findings werden gemeinsam mit Ihnen priorisiert und eine mögliche Auswirkung auf Infrastruktur oder Endanwender besprochen.

Compliance Checkup

Wir bewerten Ihre derzeitige Konfiguration von Microsoft 365 im Hinblick auf Compliance Fragenstellungen. Hierzu werden wir einschlägige Rechtsvorschriften aus der DSGVO, dem BDSG und weiteren Gesetzgebungen gegen Ihre aktuelle Konfiguration prüfen.

Backup

Wir richten für Sie Backups ein und sorgen dafür, dass Ihre Daten geschützt und regelmäßig gesichert werden. Damit verlieren Sie selbst im äußersten Notfall nicht Ihre wertvollen Daten und stellen sicher, dass Sie schnell wieder einsatzfähig sind.

© 2022 Controlware GmbH

Unsere Workshops

Secure Identities and Access

Identitäten benötigen in der Cloud besondere Schutzmaßnahmen. Der Zugriff zu einem Microsoft 365 Dienst wird im Standard nur durch E-Mail und Kennwort verifiziert. Dieser Workshop soll Kunden dabei helfen, den Sicherheitszustand Ihrer Cloudidentitäten zu bewerten. Wir sprechen Empfehlungen aus und definieren konkrete Schritte und die besten Möglichkeiten zur Risikominderung zu erreichen

Defend Against Threats with SIEM Plus XDR

Wie kann man sich vor Bedrohungen in der Cloud, im Unternehmen und am Arbeitsplatz im Homeoffice schützen? Dieser Workshop stellt Microsoft 365 Sicherheitsdienste vor und wir entwickeln mit Ihnen gemeinsam Schutzziele sowie eine Roadmap, um Ihre Umgebung vollständig abzusichern.

Protect and Govern Sensitive Data

Die Ablage von sensiblen Unternehmensdaten in der Cloud ist möglich, bedarf jedoch zusätzlichen Schutzmaßnahmen. Dieser Workshop wurde entwickelt, um Ihnen darzustellen, welche Typen von sensiblen Daten Sie in Ihrem Unternehmen verarbeiten und wie Sie damit umgehen sollten.

Mitigate Compliance and Privacy Risks

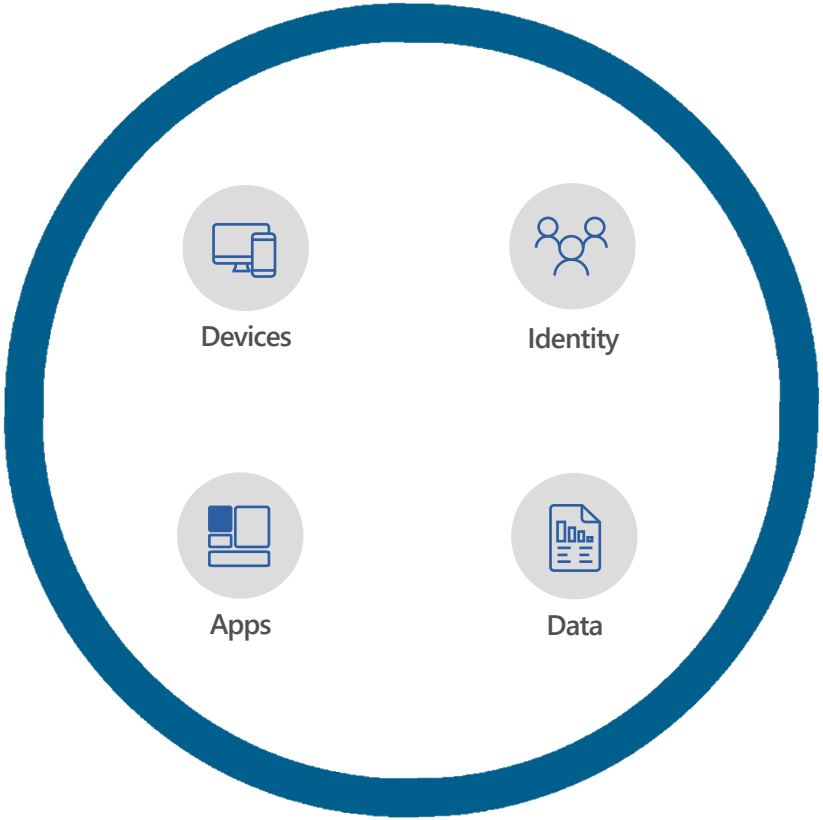
Der Workshop "Mitigate Compliance and Privacy Risks " wurde entwickelt, um Kunden Beispiele für potenzielle Datenlecks und Datendiebstahl in ihren Modern Work-Umgebungen zu geben. Diese Datenlecks treten vermehrt durch interne Mitarbeitende auf, dies stellt ein hohes Risiko für Ihr Unternehmen dar, da Sie solche Angriffe zunächst nicht erkennen können. Wir helfen Ihnen diese Risiken zu erkennen und Gegenmaßnahmen zu treffen.

© 2022 Controlware GmbH

Kernbereiche bei der Sicherheit in der Cloud

© 2022 Controlware GmbH

Kernbereiche bei der Sicherheit in der Cloud

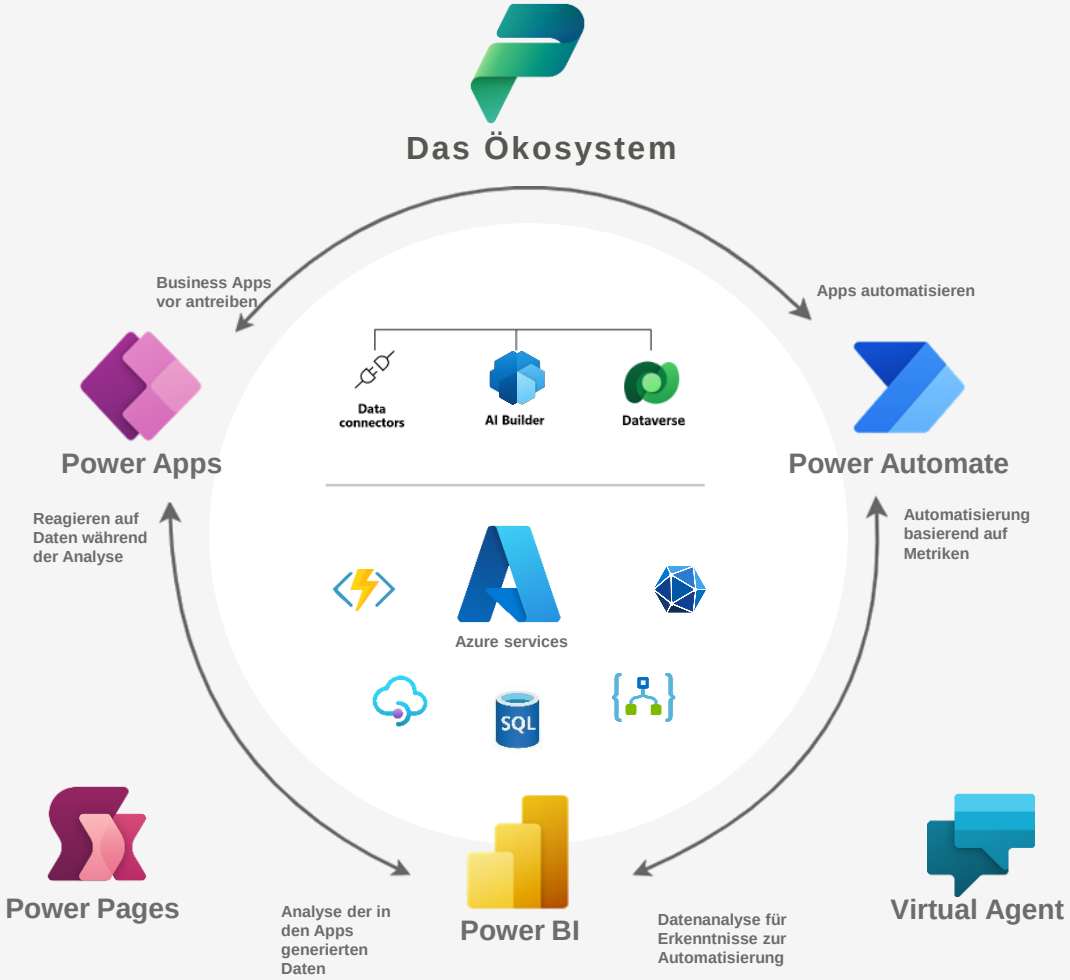


© 2022 Controlware GmbH

Power Platform

Ein Teil des modernen Arbeitsplatzes

- Stabile, skalierbare und sichere (Low-Code) Unternehmensplattform
- API-First-Model – Integration der Power Platform mit externen Diensten zur einheitlichen-Lösung
- Treibt (Guided) Citizen Development
- Lösungen, Prozessautomatisierungen Reporting für die Administration und Governance
- Enterprise Governance – Best Practices aus der Software-Entwicklung + Center of Excellence
- Power BI Pro in E5-Lizenzen
- Standard-Features Power Apps und Automate in M365-Lizenzen



© 2022 Controlware GmbH

Compliant Teams

Herausforderung

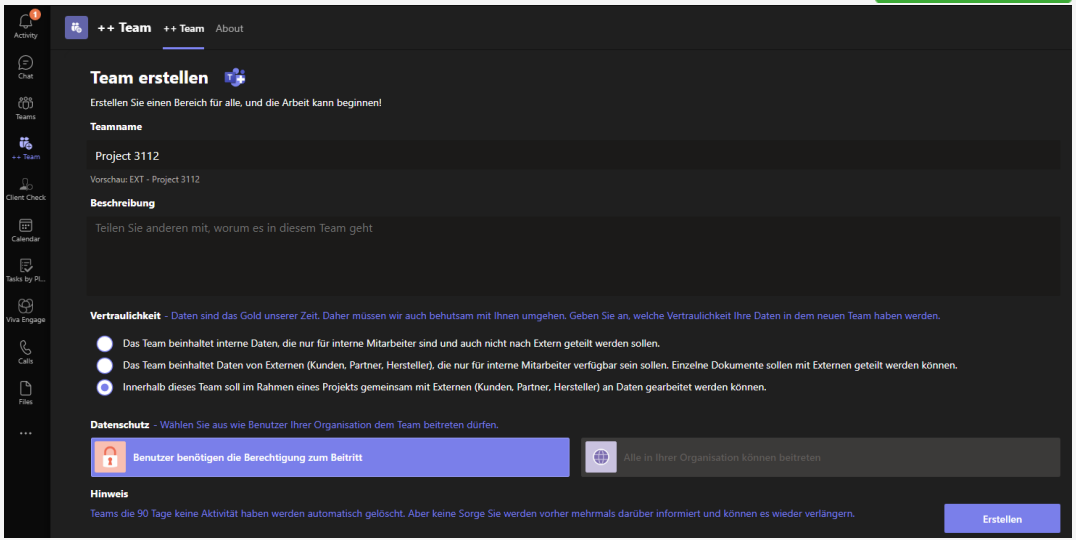
- Einhaltung von Namenskonventionen für Teams
- Anwendung von Klassifizierungsbezeichnungen
- Native Integration in MS Teams
- Benutzerfreundliche Führung

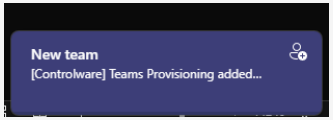
Eingesetzte Technologie

- Power Platform Solution
- GUI per Power Apps
- Automatisierung per Power Automate
- Service Principal & Technical Account

++ Teams

- In MS Teams integriert
- Darkmode/Lightmode Unterstützung
- Responsive Design





© 2022 Controlware GmbH

Compliant Teams

Herausforderung

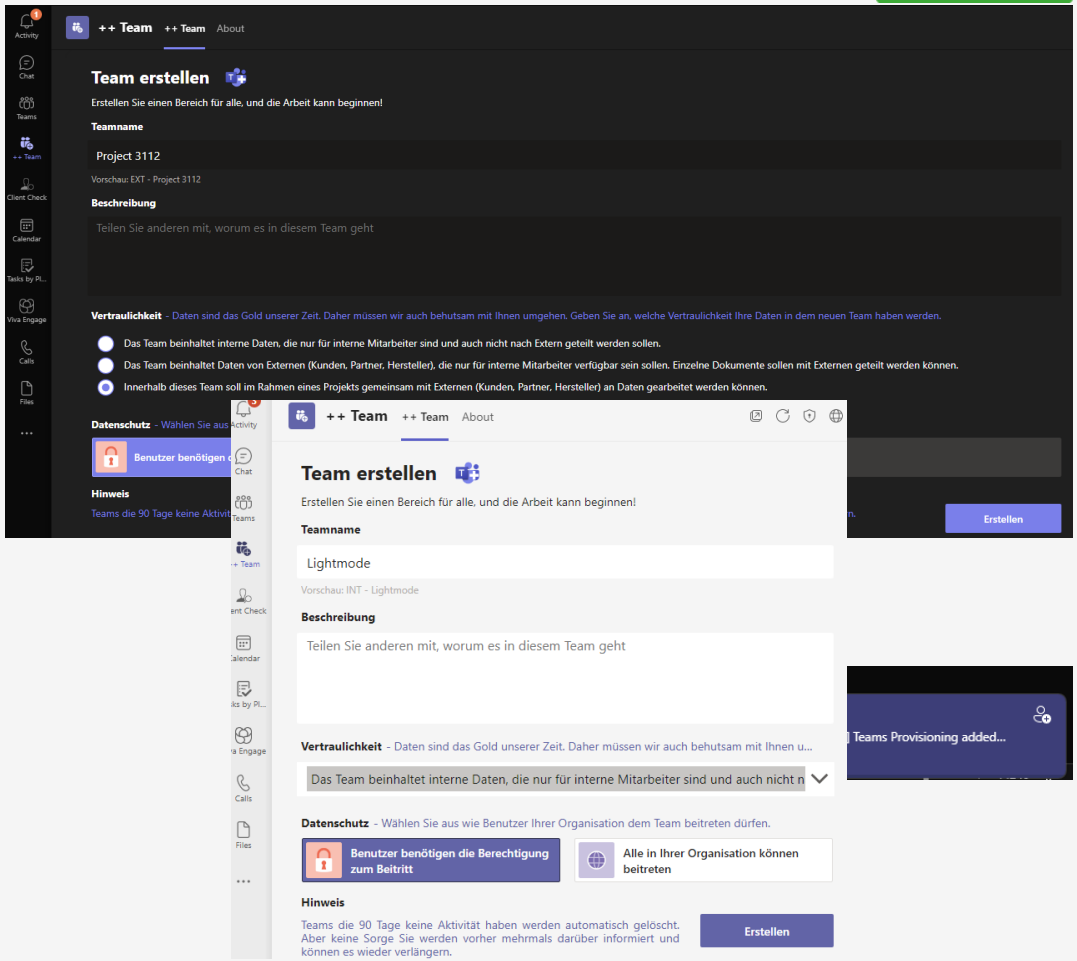
- Einhaltung von Namenskonventionen für Teams
- Anwendung von Klassifizierungsbezeichnungen
- Native Integration in MS Teams
- Benutzerfreundliche Führung

Eingesetzte Technologie

- Power Platform Solution
- GUI per Power Apps
- Automatisierung per Power Automate
- Service Principal & Technical Account

++ Teams

- In MS Teams integriert
- Darkmode/Lightmode Unterstützung
- Responsive Design



© 2022 Controlware GmbH

Enterprise Application Monitoring

Herausforderung

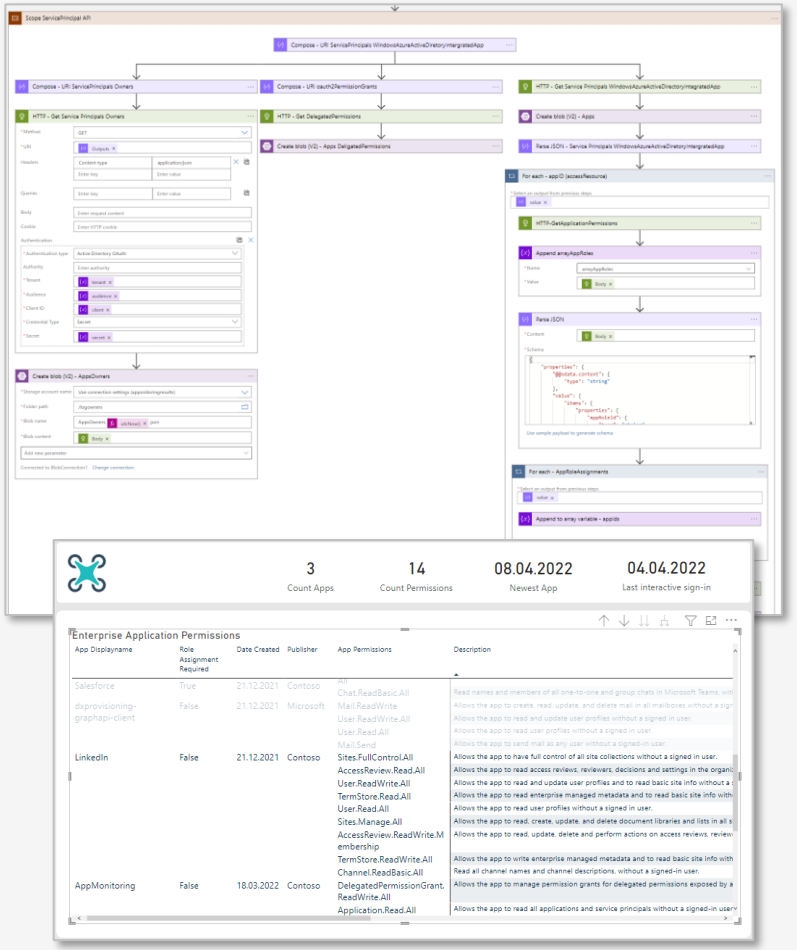
Im Azure Active Directory werden eine Vielzahl von Enterprise Applications, viele davon von Dritt-Anbietern, durch Nutzer angefragt und Administratoren hinzugefügt. Die Enterprise Application benötigen häufig viele Zugänge zu den Ressourcen des eigenen Mandanten. Über ein Application-Monitoring soll eine Übersicht der vorhanden Enterprise Application erstellt werden, welches an einer einzigen Stelle alle wichtigen Informationen zu Berechtigungen, Besitzern und Verwendung aggregiert, sodass die Notwendigkeit der Applikationen leichter, zielführenden und wiederkehrend bewertet werden können.

Eingesetzte Technologie

- Azure AD – Service Principal
- Graph API
- Power Automate/Logic App
- Azure Storage/SharePoint Online
- Power BI

Implementierung

- Power Automate/Logic App – Workflow startet periodisch
- Abfrage der Enterprise Application Informationen per Graph API
- Ablage der gesammelten Daten in Azure Storage und SharePoint Online als JSON
- Einlesen und modellieren der Reports mittels Power BI



© 2022 Controlware GmbH

Herausforderungen beim Einsatz der Power Platform

Governance und Security

- Power Platform ist in M365 aktiviert – Default Environment
  - https://make.powerapps.com / https://make.powerautomate.com
  - https://admin.powerplatform.com
- Keine Lizenzen/Dienste ≠ Zero Trust ≠ Zero Problems
- Sicherheitsrisiken in der Power Platform
  - Unzureichende Awarness und kein Training
  - Wildwuchs ohne Umgebungsstrategie
  - Trial-Lizenzen aktivieren, mangelnde Data Loss Prevention Policies, Custom-Components, Berechtigungen und Teilen (in Umgebungen/Gäste)
  - Mitarbeiter verlässt Unternehmen

Sicherheit in der Power Platform

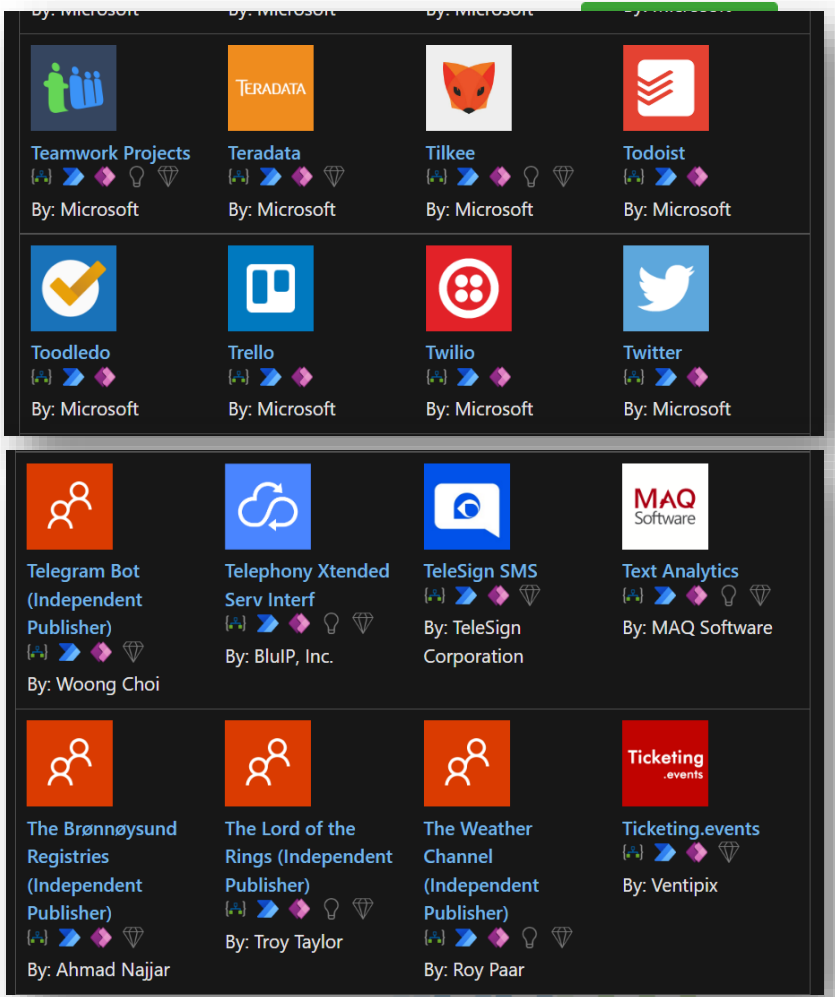
Data Loss Prevention

- Hunderte von Microsoft und Third-Party Connectors
- Interne Daten verlassen das Unternehmen

- *„Sollen der Saleforce Connector und der Twitter/Telegram Connector wirklich im gleichen Workflow nutzbar sein?“*

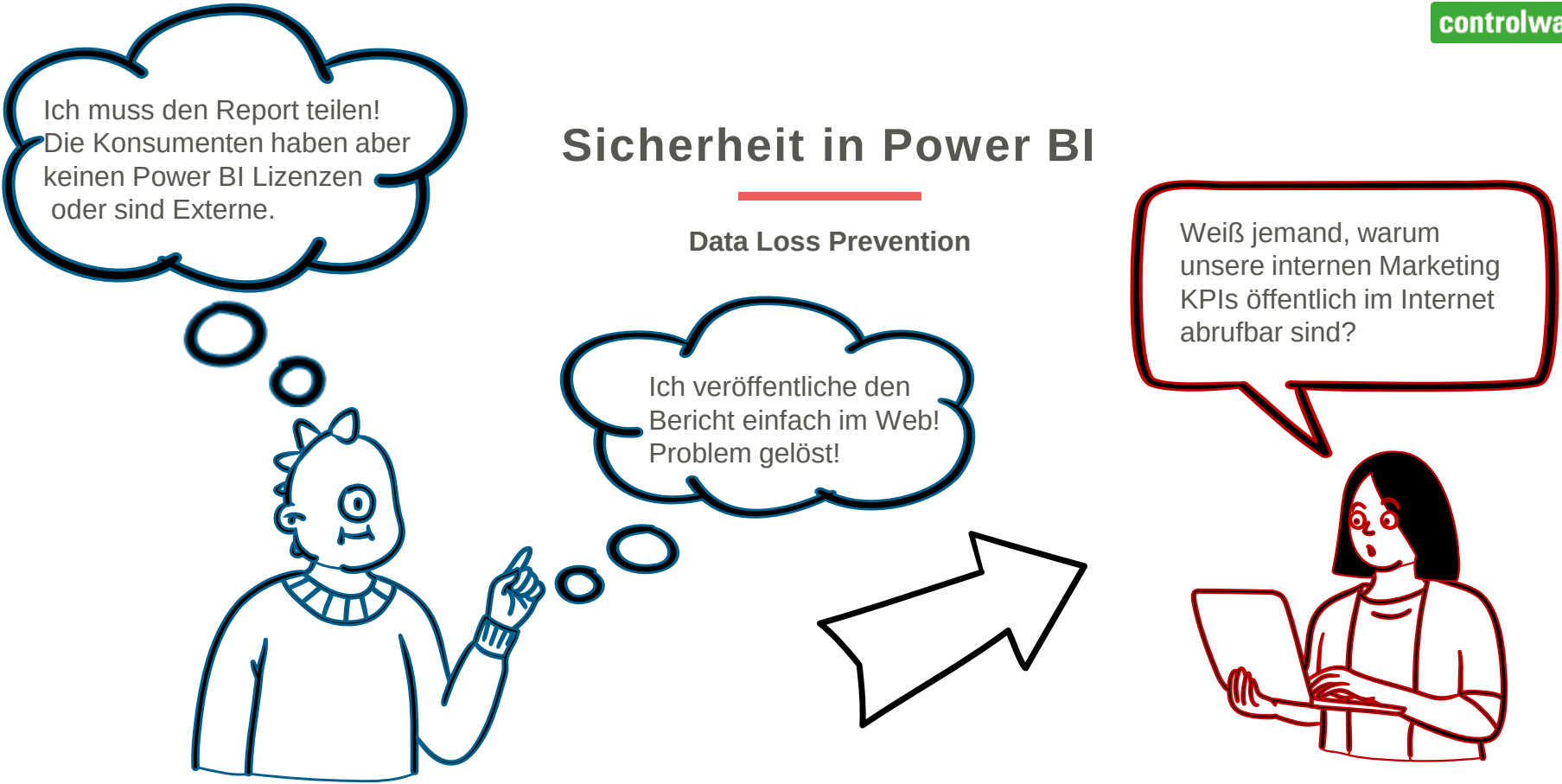
Mitigation

- Umgebungsstrategie
- Wo welche Connectors bllocken, erlauben, miteinander erlauben
- Mitarbeiter schulen
- Mitarbeiter auf Umgebungen freischalten
- Apps logisch in Umgebungen gruppieren
- Default-Umgebung einschränken
- Gateways prüfen



Sicherheit in Power BI

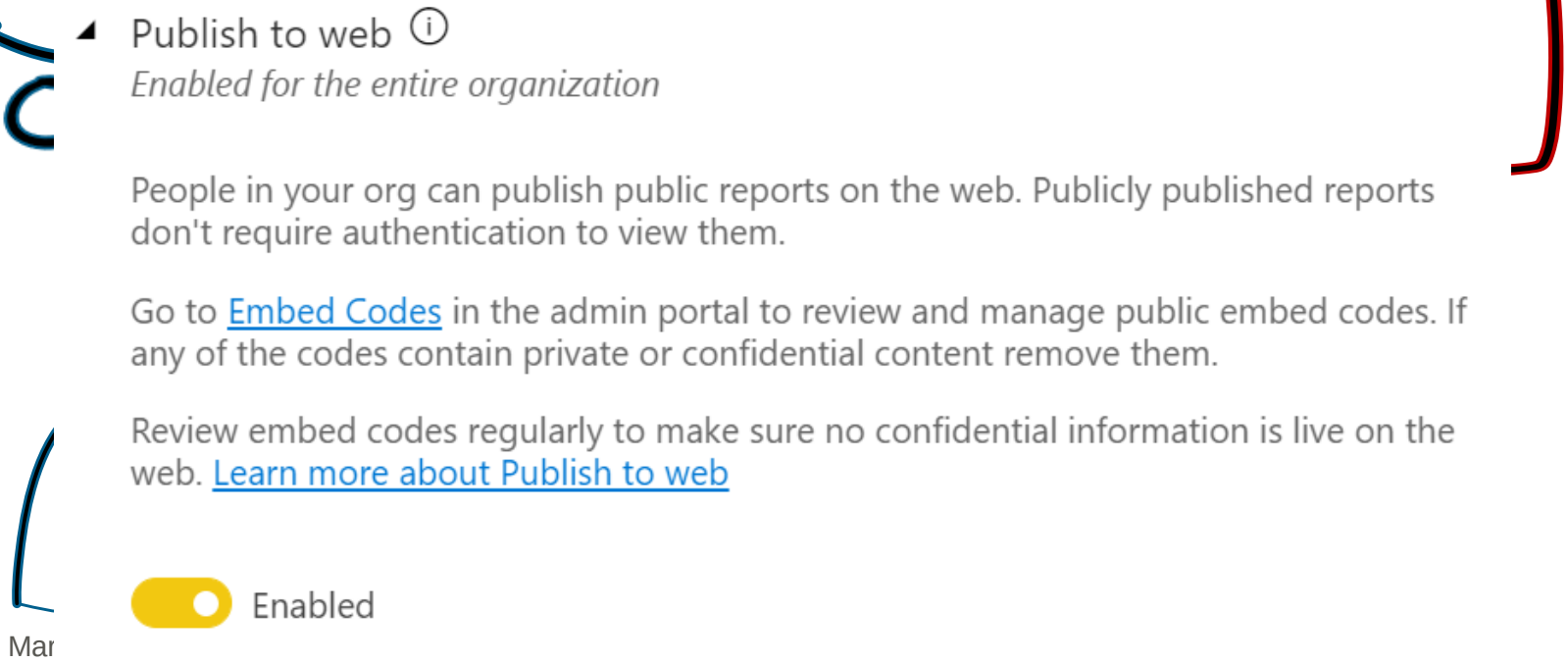
Data Loss Prevention



© 2022 Controlware GmbH

Ich muss den Report teilen!
Die Konsumenten haben aber keinen Power BI Lizenzen oder sind Externe.

Sicherheit in Power BI



Mar

© 2022 Controlware GmbH

Center of Excellence

Governance und Security

Von Microsoft bereitgestellte Lösung

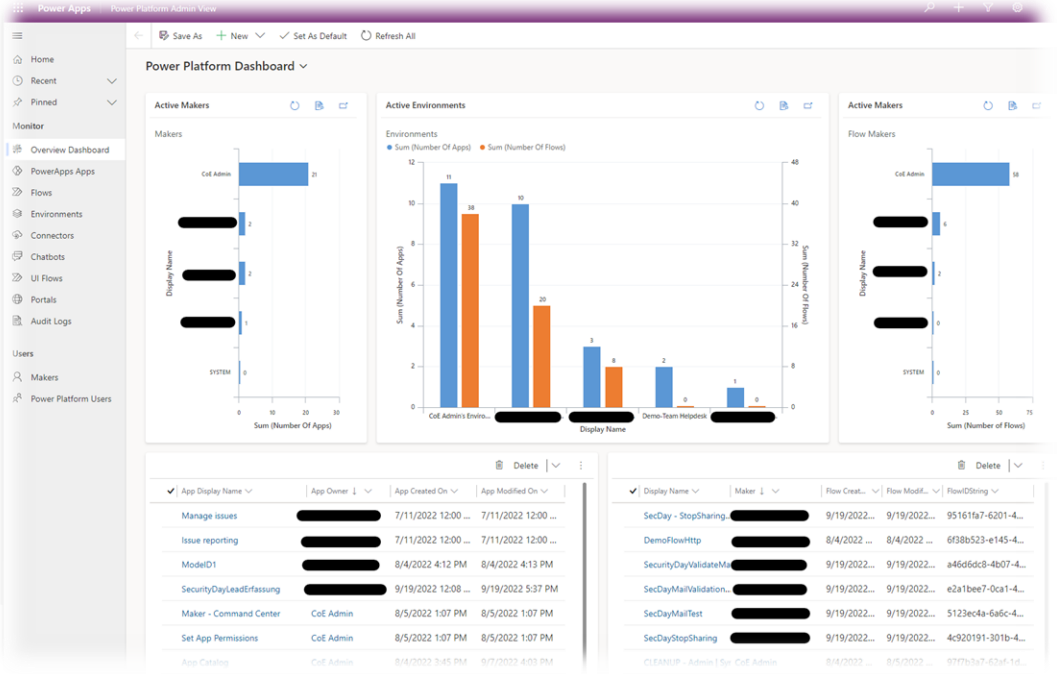
Muss für jeden Mandanten konfiguriert werden

→ Erfordert mindestens 1 Premium-Lizenz

Teil der Microsoft Power Platform-Strategie

Governance: Wer Apps erstellt, welche Apps erstellt werden und wie sie verwendet werden.

Organisches Wachstum



Wir führen die initialen Einrichtung durch und unterstützen Ihre Mitarbeiter bei den weiteren Konfigurationen!

Center of Excellence

Governance und Security

Von Microsoft bereitgestellte Lösung

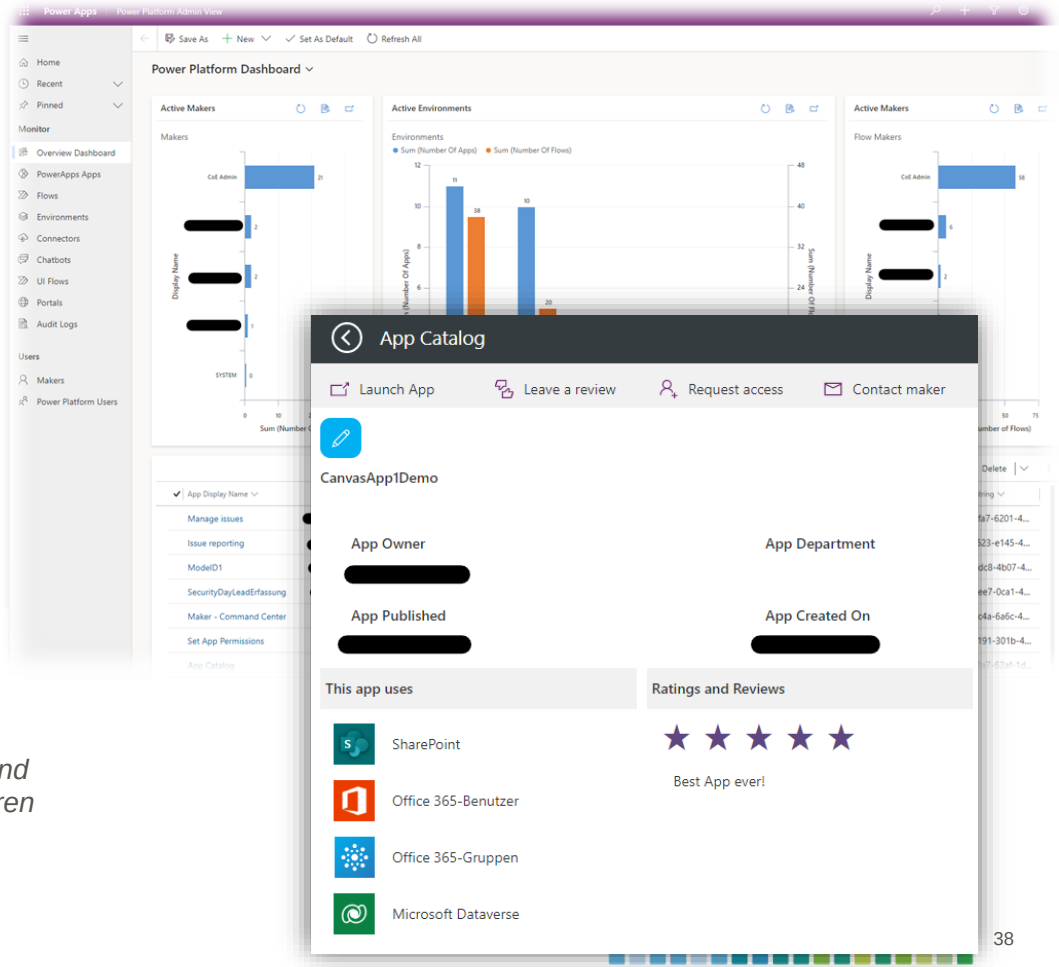
Muss für jeden Mandanten konfiguriert werden

→ Erfordert mindestens 1 Premium-Lizenz

Teil der Microsoft Power Platform-Strategie

Governance: Wer Apps erstellt, welche Apps erstellt werden und wie sie verwendet werden.

Organisches Wachstum



Wir führen die initialen Einrichtung durch und unterstützen Ihre Mitarbeiter bei den weiteren Konfigurationen!

controlware

Das richtige Toolset

Inspirierende Workshops

Das notwendige Skillset

Managed Services

secure by controlware

© 2022 Controlware GmbH

zu guter Letzt…

Ist der moderne Arbeitsplatz wirklich so modern?

Tomorrow's World - BBC Archive (1979)

© 2022 Controlware GmbH


controlware
Controlware, Ihr Partner für den modernen Arbeitsplatz
Sprechen Sie uns an!
Unsere Partner:
Microsoft 365
Google Workspace