EMPFEHLUNGEN ZU SICHERHEIT UND INFORMATIONSSCHUTZ FÜR MICROSOFT COPILOT FÜR MICROSOFT 365

Zu schützender Bereich	Erste Schritte mit E3	Nächste Schritte mit E5
Identität und Zugriff	Konfigurieren Sie mit Microsoft Entra ID P1 die folgenden Richtlinien für die Verwendung der Multi-Faktor-Authentifizierung (MFA): - MFA für Administratoren vorschreiben - MFA für alle Benutzer vorschreiben - Blockieren der Legacy-Authentifizierung Stellen Sie sicher, dass Microsoft 365 Services und Ihre anderen SaaS-Anwendungen in den Geltungsbereich dieser Richtlinien einbezogen sind. Wenn Ihre Umgebung hybride Identität umfasst, setzen Sie auch „vor Ort Microsoft Entra Password Protection für Active Directory Domain Services“ durch.	Konfigurieren Sie die empfohlenen Richtlinien für Zero Trust. Mit Microsoft Entra ID P1 konfigurieren Sie die folgenden Richtlinien für die Verwendung der Multi-Faktor-Authentifiierung (MFA): - Erfordern Sie MFA, wenn das Anmelderisiko mittel oder hoch ist - Blockieren der Legacy-Authentifizierung - Aufforderung an Benutzer mit hohem Risiko, ihr Passwort zu ändern Konfigurieren Sie auch Privileged Identity Management
Microsoft 365 Apps	**Implementierung von Intune App Protection Richtilinien (APP)** Mit APP schafft Intune eine Mauer zwischen Ihren Unternehmensdaten und persönlichen Daten. Richtlinien stellen sicher, dass Unternehmensdaten in den von Ihnen festgelegten Apps nicht in andere Apps auf dem Gerät kopiert und eingefügt werden können, selbst wenn das Gerät nicht verwaltet wird.	
Geräte	**Geräte verwalten** Nachdem die Geräte registriert sind, richten Sie Richtlinien zur Einhaltung der Vorschriften ein und verlangen dann gesunde und konforme Geräte. Stellen Sie schließlich Geräteprofile bereit, um Einstellungen und Funktionen auf den Geräten zu verwalten.	**Überwachung des Gerätsrisikos und der Einhaltung von Sicherheitsrichtlinien** Integrieren Sie Intune mit Defender for Endpoint, um das Geräterisiko als Bedingungen für den Zugriff zu überwachen. Überwachen Sie bei Windows-Geräten die Konformität dieser Gerät mit den Sicherheits-Baselines.
Schutz vor Bedrohungen	**Konfigurien Sie Exchange Online-Schutz und Endpunktschutz** Exchange Online Protection (EOP) hilft ihnen, ihre E-Mail- und Collaboration-Tools vor Phishing, Impersonation und anderen Bedrohung zu schützen. Sie können diese Schutzmaßnahmen schnell anwenden, indem Sie voreingestellte Sicherheitsrichtlinien konfigurieren. Microsoft Defender für Endpoint P1 umfasst Angriffs-flächenreduzierung und Schutz der nächsten Generation für Antimalware- und Antivirenschutz.	**Pilotprojekt und Bereitstellung von Microsoft 365 Defender** Für einen umfassenderen Schutz vor Bedrohungen können Sie Microsoft 365 Defender testen und einsetzen, einschließlich: - Verteidiger der Identität - Defender für Office 365 - Defender für Endpunkte - Defender für Cloud-Anwendungen
Daten zur Organisation	**Entwickeln Sie Ihr Klassifizierungsschema und beginnen Sie mit Sensitivitätskennzeichnungen und anderen Richtlinien** Sensibilitätskennzeichnungen sind der Grundstein für den Schutz Ihrer Daten. Bevor Sie die Kennzeichnungen für die Empfindlichkeit von Objekten und die anzuwendenden Schutzmaßnahmen erstellen, sollten Sie die bestehende Klassifizierungstaxonomie Ihres Unternehmens verstehen und wissen, wie diese den Kennzeichnungen zugeordnet wird, die Benutzer in Anwendungen sehen und anwenden. - Richtlinien zum Schutz vor Datenverlust erstellen - Erstellung von Aufbewahrungsrichtlinien - Kontext-Explorer verwenden	**Ausweitung der Richtlinien auf weitere Daten und Beginn der Automatisierung mit Datenschutzrichtlinien** Sensitivitätskennzeichnung wird auf den Schutz von mehr Inhalten und mehr Kennzeichnungsmethoden ausgeweitet. Zum Beispiel die Kennzeichnung von SharePoint-Sites und Teams mithilfe von Containern und die automatische Kennzeichnung von Elementen in Microsoft 365 und darüber hinaus. Weitere Informationen finden Sie in einer Liste gängiger Kennzeichnungsszenarien und deren Über-einstimmung mit den Unternehmenszielen.