

Microsoft Azure Security

Bewährte Methoden, Prozesse und Grundprinzipien für das Entwerfen und Entwickeln sicherer Anwendungen in der Cloud

Sichere Anwendungen und Workloads in der Cloudpraktisches Tutorial und hilfreiches Referenzwerk in einem behandelt die Azure-Sicherheitsdienste sowohl auf Anwendungs- als auch auf Netzwerkebene sowie deren Zusammenarbeit inkl. kostenloser Code-Beispiele zum Download Wenn wichtige Anwendungen und Workloads eines Unternehmens in die Microsoft Azure-Cloud verlagert werden, müssen sie gegen eine Vielzahl von ebenso unterschiedlichen wie gefährlichen Bedrohungen gewappnet werden. Um ihre Sicherheit zu optimieren, ist es erforderlich, dass Sie diese bereits zuverlässig in Ihre Entwürfe einbauen, bewährte Best Practices über die gesamte Entwicklung hinweg anwenden und verschiedene Azure-Dienste kombinieren. In diesem Buch zeigen Ihnen drei führende Azure-Sicherheitsexperten, wie Sie genau das tun. Auf der Grundlage ihrer umfangreichen Erfahrungen mit der Absicherung von Azure-Workloads geben die Autoren Ihnen eine praktische Anleitung zur Bewältigung unmittelbarer Sicherheitsherausforderungen an die Hand sowie eine umfassende Referenz, auf die Sie sich über Jahre hinweg verlassen können. Egal ob Softwarearchitektin, Softwareentwickler oder beim Testen: Integrieren Sie die wichtigsten Azure-Sicherheitstechnologien – von Entwurf und Entwicklung über Tests und Bereitstellung bis hin zu Governance und Compliance. In diesem Buch werden folgende Themen behandelt: Verbesserung der Anwendungs-/Workload-Sicherheit, Verringerung der Angriffsflächen und Implementierung von Zero Trust im Cloud-Code Anwendung von Sicherheitsmustern zur einfacheren Lösung gängiger Probleme Frühzeitige Modellierung von Bedrohungen, um wirksame Abhilfemaßnahmen zu planen Implementierung moderner Identitätslösungen mit OpenID Connect und OAuth2 Azure-Monitoring, Protokollierung und Kusto-Abfragen optimal nutzen Absicherung von Workloads mit den Best Practices von Azure Security Benchmark (ASB) Prinzipien für sicheren Code, defensiven Code schreiben, unsicheren Code reparieren und Codesicherheit testen Nutzung von Azure-Kryptographie und Technologien für verschlüsselte Datenverarbeitung Verstehen von Compliance- und Risikoprogrammen Sichere automatisierte CI/CD-Workflows und - Pipelines Verstärkung der Container- und Netzwerksicherheit

Sichere Anwendungen und Workloads in der Cloud

- praktisches Tutorial und hilfreiches Referenzwerk in einem
- behandelt die Azure-Sicherheitsdienste sowohl auf Anwendungs- als auch auf Netzwerkebene sowie deren Zusammenarbeit
- inkl. kostenloser Code-Beispiele zum Download

Wenn wichtige Anwendungen und Workloads eines Unternehmens in die Microsoft Azure-Cloud verlagert werden, müssen sie gegen eine Vielzahl von ebenso unterschiedlichen wie gefährlichen Bedrohungen gewappnet werden. Um ihre Sicherheit zu optimieren, ist es erforderlich, dass Sie diese bereits zuverlässig in Ihre Entwürfe einbauen, bewährte Best Practices über die gesamte Entwicklung hinweg anwenden und verschiedene Azure-Dienste kombinieren.

In diesem Buch zeigen Ihnen drei führende Azure-Sicherheitsexperten, wie Sie genau das tun. Auf der Grundlage ihrer umfangreichen Erfahrungen mit der Absicherung von Azure-Workloads geben die Autoren Ihnen eine praktische Anleitung zur Bewältigung unmittelbarer Sicherheitsherausforderungen an die Hand sowie eine umfassende Referenz, auf die Sie sich über Jahre hinweg verlassen können. Egal ob Softwarearchitektin, Softwareentwickler oder beim Testen: Integrieren Sie die wichtigsten Azure-Sicherheitstechnologien – von Entwurf und Entwicklung über Tests und Bereitstellung bis hin zu Governance und Compliance.



59,90 €
55,98 € (zzgl. MwSt.)

sofort versandfertig, Lieferzeit: 1-3
Werktage

Artikelnummer: 9783864909856
Medium: Buch
ISBN: 978-3-86490-985-6
Verlag: dpunkt.verlag
Erscheinungstermin: 01.12.2023
Sprache(n): Deutsch
Auflage: 1. Auflage 2023
Serie: Microsoft Press
Produktform: Kartoniert
Gewicht: 1050 g
Seiten: 546
Format (B x H): 170 x 241 mm

