

Inhaltsverzeichnis

Danksagungen	xvii
Vorwort	xix
Einleitung	xxi

Teil 1: Sicherheitsgrundsätze

Kapitel 1

Prozesse für sichere Entwicklungszyklen	3
Entwickler sind die Hauptursache für Kompromittierungen	3
Einführung in den Microsoft Security Development Lifecycle	4
Qualität $\neq$ Sicherheit	4
Sicherungsmerkmale vs. Sicherheitsmerkmale	5
SDL-Komponenten	5
Sicherheitsschulung	6
Definieren Ihrer Bug Bar, Ihres Klassifizierungsschemas	7
Analyse der Angriffsfläche	11
Modellierung von Bedrohungen	12
Definieren Ihrer Toolchain	12
Verbotene Funktionalität vermeiden	13
Werkzeuge zur statischen Analyse verwenden	15
Dynamische Analysetools verwenden	18
Code-Review unter Sicherheitsaspekten	19
Reaktionsplan bei Zwischenfällen haben	21
Penetrationstests durchführen	21
SDL-Aufgaben nach Sprint	22
Das menschliche Element	24
Zusammenfassung	24

Kapitel 2

Sicherer Entwurf	25
Die Cloud, DevOps und Sicherheit	25
IaaS vs. PaaS vs. SaaS und die gemeinsame Verantwortung	26
Zero Trust für Entwickler	30
Nachdenken über sicheres Design	34
Azure-Entwurfsprinzipien für sichere Systeme	36
Angriffsfläche reduzieren	36
Vollständige Zugriffskontrolle	37
Sicherheit in der Tiefe – Defense in Depth	38
Einfachheit der Mechanismen	42
Sichere Standardeinstellungen	43
Fail Safe und Fail Secure	44
Minimale gemeinsame Ressourcen	45
Minimale Berechtigungen	46
Vorhandene Komponenten nutzen	48
Offener Entwurf	49
Psychologische Akzeptanz	51
Funktionstrennung	52
Single Point of Failure	53
Schwächstes Glied	54
Zusammenfassung	56

Kapitel 3

Sicherheitsmuster	57
Was ist ein Muster?	57
Unsere Meinung zu Azure-Sicherheitsmustern	58
Das Azure Well-Architected Framework	59
Authentifizierungsmuster	59
Zentralisierten Identitätsanbieter für die Authentifizierung verwenden ..	60
Autorisierungsmuster	62
Einführung einer Just-in-Time-Administration	62
Rollen an Gruppen zuweisen	64
Vom Internet isolieren	66
Isolieren mit einem Identitätsperimeter	67
Rollenbasierte Zugriffssteuerung (RBAC) verwenden	68
Muster für die Verwaltung von Geheimnissen	71
Verwaltete Identitäten verwenden	71
Geheimnisse mit Azure Key Vault schützen	74

Muster für die Verwaltung vertraulicher Informationen	77
Sichere Kanäle schaffen	77
Daten clientseitig verschlüsseln	80
Bring Your Own Key (BYOK) einsetzen	82
Verfügbarkeitsmuster	83
Entwurf für Denial of Service	84
Zusammenfassung	86

Kapitel 4

Bedrohungsmodellierung	87
TL;DR	87
Was ist Bedrohungsmodellierung?	88
Die vier Hauptphasen der Bedrohungsmodellierung	90
Der STRIDE-Ansatz zur Klassifizierung von Bedrohungen	94
Das Problem mit der Bedrohungsmodellierung	96
Auf der Suche nach einem besseren Prozess zur Modellierung von Bedrohungen	98
Ein besserer Weg, Bedrohungsmodelle zu erstellen: Die fünf Faktoren	100
Tools zur Bedrohungsmodellierung	102
Bewertung der fünf Faktoren	103
CAIRIS	103
Microsoft Threat Modeling Tool	105
OWASP Threat Dragon	106
pytm	108
Threagile	109
Threats Manager Studio	110
Wie man ein Bedrohungsmodell erstellt: Ein Praxisbeispiel	112
Analysieren Sie die Lösung: Das erste Meeting	113
Analysieren Sie die Lösung: Das zweite Meeting	115
Identifizierung spezifischer Bedrohungen und Gegenmaßnahmen	119
Angabe des Schweregrads	122
Gegenmaßnahmen festlegen	123
Automatisch zusätzliche Bedrohungen und Gegenmaßnahmen identifizieren	125
Roadmap erstellen	128
Das Dashboard verwenden	131
Ausgewählte Gegenmaßnahmen in das Backlog pushen	132
Zusammenfassung	136

Identität, Authentifizierung und Autorisierung	137
Identität, Authentifizierung und Autorisierung unter dem Aspekt der Sicherheit	137
Authentifizierung vs. Autorisierung vs. Identität	138
Moderne Identität und Zugriffsmanagement	139
Identität: Grundlagen von OpenID Connect und OAuth2	140
OpenID Connect und OAuth2	143
Anwendung registrieren	144
Microsoft-Authentifizierungsbibliothek	145
Rollen in OAuth2	149
Flows	150
Clienttypen	153
Token	154
Gültigkeitsbereiche, Berechtigungen und Zustimmung	155
Anatomie eines JSON Web Token (JWT)	158
OAuth2 in Ihren Azure-Anwendungen verwenden	163
Authentifizierung	167
Etwas, das Sie wissen	168
Etwas, das Sie besitzen	169
Etwas, das Sie sind	170
Multi-Faktor-Authentifizierung	170
Wer authentifiziert wen?	171
Erstellen einer eigenen Authentifizierungslösung	173
Die Rolle des einmaligen Anmeldens (Single Sign-On)	174
Zugriff ohne Authentifizierung erhalten	176
Authentifizierung von Anwendungen	177
Autorisierung	180
Microsoft Entra ID-Rollen und -Bereiche	181
Integrierte Azure-RBAC-Rollen für die Steuerungsebene	182
Integrierte Azure-RBAC-Rollen für die Datenebene	183
Rollenzuweisungen verwalten	184
Benutzerdefinierte Rollendefinitionen	184
Zuweisungen ablehnen	187
Bewährte Verfahren für die Rollenzuweisung	187
Microsoft Entra ID Privileged Identity Management	188
Attributbasierte Zugriffssteuerung in Azure	189
Zusammenfassung	192

Kapitel 6

Überwachung und Überprüfung	193
Überwachung, Überprüfung, Protokollierung. Ach du meine Güte!	193
Die Möglichkeiten der Azure-Plattform nutzen	195
Diagnoseeinstellungen	195
Log-Kategorien und Kategoriegruppen	197
Log Analytics	198
Kusto-Abfragen	199
Warnungen auslösen	204
Schutz von Überwachungsprotokollen	210
Richtlinien zum Hinzufügen von Überwachungsprotokollen verwenden	213
Eindämmung der Kosten	213
Die Notwendigkeit einer gezielten Sicherheitsüberwachung und -überprüfung	214
Die Rolle der Bedrohungsmodellierung	215
Benutzerdefinierte Ereignisse	217
Warnungen für benutzerdefinierte Ereignissen auf Azure Sentinel	222
Zusammenfassung	225

Kapitel 7

Governance	227
Governance und der Entwickler	227
Microsoft Cloud Security Benchmark Version 1	228
Netzwerksicherheit	228
Identitätsmanagement	229
Privilegierter Zugriff	229
Datenschutz	230
Asset-Management	230
Protokollierung und Bedrohungserkennung	231
Reaktion auf Vorfälle	231
Status- und Sicherheitsrisikoverwaltung	231
Endpunktsicherheit	232
Sicherung und Wiederherstellung	232
DevOps-Sicherheit	232
Governance und Strategie	232
Durchsetzung der Governance	232
Durchsetzung durch Prozesse	232
Governance-Dokumentation und Sicherheitsschulung	232
Rollenbasierte Zugriffssteuerung	233
Automatisierte Durchsetzung während der Bereitstellung	233

Microsoft Defender für Cloud	233
Sicherheitsbewertung	234
Überprüfung des Konformitätsstatus für die Lösung	235
Azure Policy	236
Azure-Initiativen und Frameworks für die Einhaltung von Vorschriften ...	236
Auswirkungen von Azure Policy	237
Durchsetzungsebenen (Effekte) und RBAC nach Umgebung	237
Richtlinienzuweisungen	238
Richtliniendefinitionen als Code	239
Zusammenfassung	239

Kapitel 8

Compliance und Risikomanagement	241
Vorweg: Mögliche Missverständnisse ausräumen	241
Was ist Compliance?	241
HIPAA	244
HITRUST	244
DSGVO (GDPR)	245
PCI DSS	246
FedRAMP	247
NIST SP 800-53	248
NIST Cybersecurity Framework	249
FIPS 140	250
SOC	253
ISO/IEC 27001	254
ISO/IEC 27034	255
Center for Internet Security Benchmarks	255
Microsoft Cloud Security Benchmark (MCSB)	256
OWASP	258
MITRE	259
Übersicht zu weiteren Compliance-Programmen	261
Verwendung von Bedrohungsmodellen zur Erstellung von Compliance-Artefakten	263
Zusammenfassung	265

Teil 2: Sichere Implementierung

Kapitel 9

Secure Coding	269
Unsicherer Code	269
Regel Nr. 1: All input is evil	270
Explizit überprüfen	275
Ermitteln Sie die Korrektheit	275
Bekannte fehlerhafte Daten ablehnen	287
Daten codieren	290
Weitverbreitete Schwachstellen	291
A01: Fehler in der Zugriffssteuerung	291
A02: Kryptografische Fehler	292
A03: Injection	292
A04: Unsicheres Design	293
A05: Sicherheitsrelevante Fehlkonfiguration	294
A06: Veraltete Komponenten mit bekannten Schwachstellen	299
A07: Fehler in der Identifizierung und Authentifizierung	300
A08: Integritätsfehler in Software und Daten	302
A09: Fehler bei der Sicherheitsprotokollierung und -überwachung	305
A10: Serverseitige Anforderungsfälschung (Server-Side Request Forgery, SSRF)	305
Anmerkungen zur Verwendung von C++	306
Schreiben Sie kein glorifiziertes C	307
Abwehrmaßnahmen im Compiler und Linker verwenden	307
Analysetools verwenden	308
Security Review	310
Ehrlichkeit der Entwickler durch Fuzz-Tests	311
Erzeugung völlig zufälliger Daten	313
Mutation vorhandener Daten	315
Intelligente Manipulation von Daten in Kenntnis ihres Formats	318
Fuzzing von APIs	318
Zusammenfassung	322

Kapitel 10

Kryptografie in Azure	323
Eine Wahrheit über Sicherheit	324
Schlüssel absichern	325
Zugriffssteuerung und Azure Key Vault	327
Key Vault Premium in der Produktion verwenden	339
Protokollierung und Auditing aktivieren	342
Netzwerkisolierung	344

Microsoft Defender für Key Vault verwenden	347
Sichern Sie Ihre Key Vault-Assets	347
Verwaltetes HSM und Azure Schlüsseltresor	349
Sichere Schlüssel mit Key Vault, eine kurze Zusammenfassung	354
Kryptografische Agilität	354
Wie man kryptografische Agilität erreicht	356
Implementierung von Krypto-Agilität	358
Krypto-Agilität, eine kurze Zusammenfassung	367
Das Microsoft Data Encryption SDK	368
Optionale Parameter	370
SDK-Schlüssel in Schlüsseltresor verwalten	371
Azure-Dienste und Kryptografie	373
Serverseitige Verschlüsselung mit plattformseitig verwalteten Schlüsseln	374
Serverseitige Verschlüsselung mit kundenseitig verwalteten Schlüsseln	374
Clientseitige Verschlüsselung	375
Azure Storage und Kryptografie	376
Azure VM und Kryptografie	381
Azure SQL-Datenbank sowie Cosmos DB und Kryptografie	383
Schlüsselrotation	383
Azure Key Vault Schlüsselrotation	385
Schutz von Daten bei der Übertragung	388
TLS und Krypto-Agilität	390
Ciphersuiten	390
TLS in Azure PaaS	392
Ciphersuiten einstellen	394
TLS in Azure IaaS	397
Ein häufiger TLS-Fehler im .NET-Code	402
TLS testen	402
Debugging von TLS-Fehlern	403
Unsichere Verwendung von SSH	405
Zusammenfassung	406

Kapitel 11

Confidential Computing	407
Was ist Confidential Computing?	407
Prozessoren für Confidential Computing	409
Intel Software Guard Extensions	409
AMD Secure Encrypted Virtualization-Secure Nested Paging	411
Arm TrustZone	412
VMs der DCsv3-Serie, SGX, Intel Total Memory Encryption und Intel Total Memory Encryption Multi-Key	412
Attestation	413

Vertrauenswürdiger Start für Azure-VMs	415
Azure-Dienste, die Confidential Computing nutzen	417
SQL Server Always Encrypted	417
Azure Confidential Ledger	418
Vertrauliche Container	419
Zusammenfassung	421

Kapitel 12

Containersicherheit	423
Was sind Container?	423
Hier brauchen Sie keine Container!	424
Wie geht es jetzt weiter?	425
Containerbezogene Dienste auf Azure	425
Container für IaaS-Angebote verwenden	426
Azure-Containerdienste im Vergleich	427
Probleme mit Containern	432
Komplexität	432
Unausgereiftheit	434
Fragmentierung	434
Containerdienste absichern	435
Entwicklung und Bereitstellung	435
Die Container Registry	437
Der Cluster	438
Die Knoten	438
Die Pods und Container	439
Die Anwendung	440
Zusammenfassung	441

Kapitel 13

Datenbanksicherheit	443
Warum Datenbanksicherheit?	443
Welche Datenbanken?	444
Über die Sicherheit von Datenbanken nachdenken	444
Die SQL Server-Familie	446
SQL Server	446
Azure SQL-Datenbank	447
Azure SQL Managed Instance	447
Sicherheit in der SQL Server-Familie	447
Authentifizierung auf der Steuerungsebene	449

Autorisierung auf der Steuerungsebene	451
Überwachung der Steuerungsebene	453
Verschlüsselung der Steuerungsebene bei der Übertragung	454
Netzwerkisolierung auf der Steuerungsebene	455
Authentifizierung auf der Datenebene	455
Autorisierung auf der Datenebene	457
Überwachung der Datenebene	458
Verschlüsselung auf der Datenebene während der Übertragung	459
Netzwerkisolierung auf der Datenebene	459
Kryptografische Maßnahmen für ruhende Daten	461
Sonstiges	463
Cosmos DB Sicherheit	467
Authentifizierung auf der Steuerungsebene	468
Autorisierung auf der Steuerungsebene	469
Überwachung der Steuerungsebene	470
Netzwerkisolierung auf der Steuerungsebene	470
Authentifizierung auf der Datenebene	470
Autorisierung auf der Datenebene	471
Überwachung der Datenebene	476
Verschlüsselung auf der Datenebene während der Übertragung	477
Netzwerkisolierung auf der Datenebene	477
Kryptografische Schutzmaßnahmen für ruhende Daten	478
Verschiedenes	479
Verschlüsselung der Daten während der Verarbeitung: Always Encrypted	479
Always Encrypted	480
Always Encrypted mit sicheren Enklaven	487
Cosmos DB und Always Encrypted	490
SQL Injection	493
Zusammenfassung	494

Kapitel 14

CI/CD-Sicherheit	495
Was ist CI/CD?	495
CI/CD-Tools	495
Quellcodesysteme und Lieferkettenangriffe	496
Sicherheits-Tooling	496
Ihre Entwickler schützen	497
Genehmigung von Pull Requests und PR-Hygiene	497
Funktionstrennung, Übersicht über die geringsten Privilegien	498
Geheimnisse und Dienstverbindungen	498
Schutz des Main-Branch in Azure DevOps und GitHub	499

Schutz der PROD-Bereitstellung in Azure DevOps und GitHub	500
Sicherung von Bereitstellungsagents	500
Absicherung von Azure DevOps-Agents	501
Absicherung von GitHub-Agents	501
Zusammenfassung	502
 Kapitel 15	
Netzwerksicherheit	503
Azure-Netzwerk-Grundlagen	503
IPv4, IPv6 in Azure	505
IPv4-Konzepte	505
IPv4-Adressen in Azure und die CIDR-Notation	506
Routing und benutzerdefinierte Routen	506
Netzwerksicherheitsgruppen	506
Anwendungssicherheitsgruppen	507
Zielzonen, Hubs und Spokes	508
Hubs, Spokes und Segmentierung	508
Trennung von Umgebungen, VNets und erlaubte Kommunikation	508
Ingress- und Egress-Kontrollen	509
Network Virtual Appliances und Gateways	510
Azure Firewall	510
Azure Firewall Premium SKU	510
Azure Web Application Firewalls	511
API-Management-Gateways	512
Azure Anwendungsproxy	512
PaaS und private Netzwerke	512
Private gemeinsam genutzte PaaS	513
Dedizierte PaaS-Instanzen	517
Verwaltete VNets	517
Agent-basierte Netzwerkbeteiligung	517
Netzwerke für Azure Kubernetes Service	518
Ingress-Controller	518
Egress-Controller mit benutzerdefinierter Route	518
Private Endpunkte für Kubernetes-API-Server	519
Cluster-Netzwerkrichtlinien	519
Das Problem der verwaisten DNS-Einträge	520
Ein Beispiel	521
Das Problem der verwaisten DNS-Einträge angehen	522
Zusammenfassung	522
 Index	523