universität wien

Strategien und Werkzeuge zur Sicherung von Cloud Diensten: ”Entwicklung eines umfassendes Sicherheits-Wikis”

Bachelorarbeit von Florian Chocholka

Inhaltsverzeichnis

Introduction

universität wien

Bedeutung der Cloud-Technologie:

- Ermöglicht Bereitstellung und Nutzung von Daten und Anwendungen über das Internet.
- Vorteile: Flexibilität, Skalierbarkeit, Effizienz, keine lokalen Hardware-Ressourcen.

Sicherheitsstrategien

- Mehrschichtige Sicherheitsstrategien erforderlich (technisch und organisatorisch).

Zielsetzung der Arbeit

- Entwicklung eines umfassenden Cloud Security Wikis.
- Entwicklung eines interaktiven Tools zur Unterstützung bei der Erlernung und Umsetzung von Sicherheitsanforderungen.

Motivation

universität wien

Problemstellung

- Bestehende Cloud Security Wikis konzentrieren sich hauptsächlich auf technische Konfiguration.
- Vernachlässigung der Behandlung spezifischer Sicherheitsbedrohungen und Integration von Prinzipien und Richtlinien führender Sicherheitsorganisationen (z.B. NCSC).

Notwendigkeit und Relevanz

- Wachsende Abhängigkeit von Cloud-Diensten in verschiedenen Organisationen.
- Beispiel: In Schweden nutzten 2021 etwa 75,4% der Unternehmen mit mehr als zehn Mitarbeitern kostenpflichtige Cloud-Computing-Dienste.

Bedeutung eines verbesserten Verständnisses

- Das Cloud Security Wiki beleuchtet aktuelle und zukunftsorientierte Sicherheitsstrategien und behandelt spezifische Empfehlungen detailliert.
- Ziel: Leichte Wartbarkeit und einfache Benutzbarkeit zur schnellen Aktualisierung bei Änderungen in der Bedrohungslandschaft.

Einführung in die Cloud Modelle (IaaS)

universität wien

Bereitstellung: Netzwerk, Speicher und Rechenleistung.

Vorteile: Keine hohen Vorabinvestitionen, keine Wartungskosten.

Architektur: Globale Rechenzentren, Zugriff über virtuelle Maschinen.

Abgrenzung: Fokus auf Grundinfrastruktur, nicht auf Anwendungsstacks (wie PaaS und SaaS).

Flexibilität: Skalierbar, ideal für Start-ups und keine Kapitalinvestitionen für teure physische Infrastruktur.

Einführung in die Cloud Modelle (PaaS)

universität wien

Bereitstellung: Hardware, Software und Infrastruktur für Anwendungsentwicklung, -ausführung und -verwaltung.

Vorteile: Verkürzte Entwicklungszeit, Kosteneffizienz, keine Installation oder Wartung.

Architektur: Rechenzentren mit Betriebssystemen, Datenbanken und Entwickler-Tools, integriert über eine GUI.

Flexibilität: Zugriff auf Tools von überall, fördert globale Teamarbeit.

Anwendungsbereiche: API-Entwicklung, IoT, agile Entwicklung, DevOps, Cloud-Migration, cloudnative Entwicklung, Hybrid-Cloud-Strategien.

Einführung in die Cloud Modelle (SaaS)

universität wien

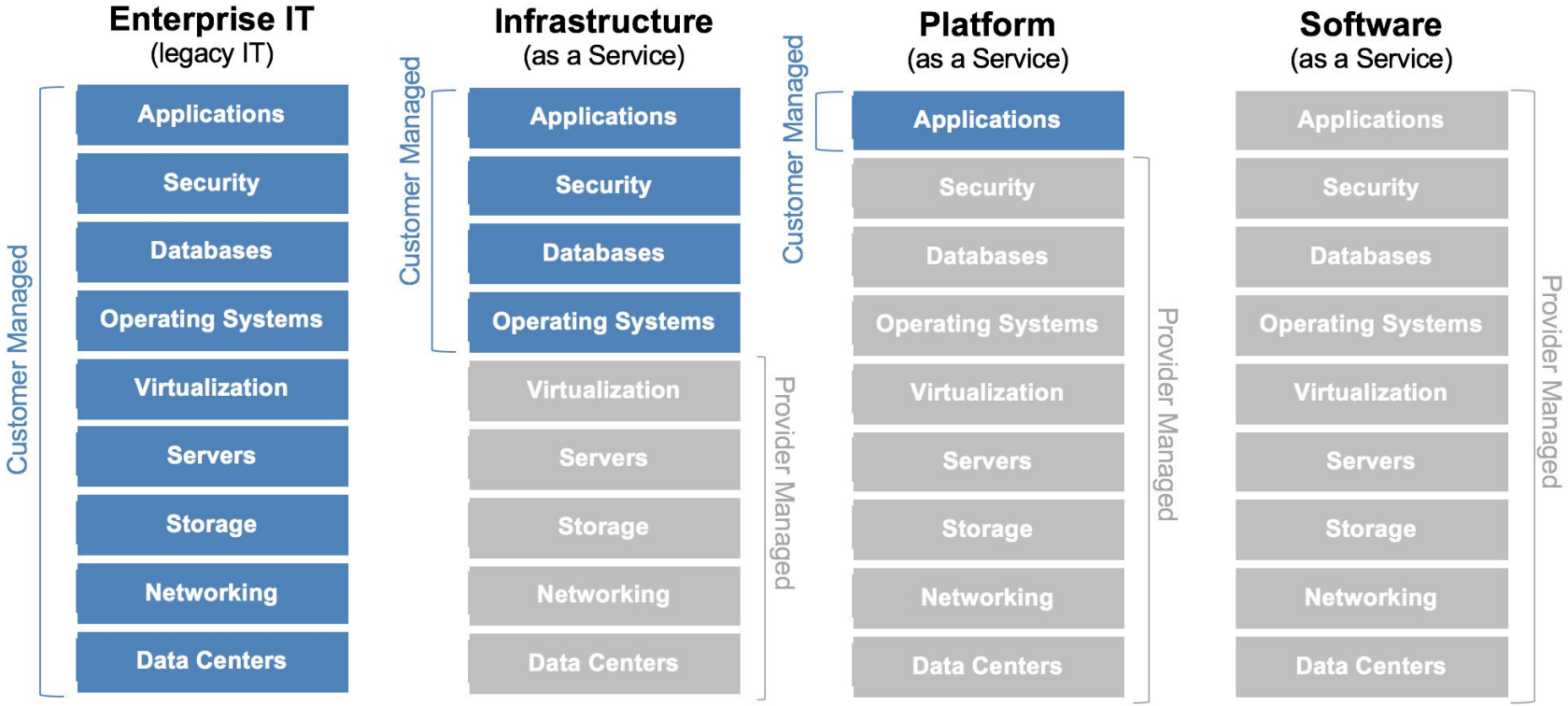
Bereitstellung: Anwendungssoftware über das Internet, betrieben und gewartet vom Dienstanbieter.

Vorteile: Minimale Kundenaufwand, skalierbar, effiziente Nutzung, keine Entwicklungskosten, keine Wartungskosten.

Architektur: Rechenzentren mit Betriebssystemen, Datenbanken und Entwickler-Tools, integriert über eine GUI.

Kosten-Effizient: Schnellere Implementierung, geringere Vorlaufkosten.

Überblick



Quelle: David Chou. Cloud Service Models (IaaS, PaaS, SaaS) Diagram. https://dachou.github.io/2018/09/28/cloud-service-models.html

Deployment-Modelle in der Cloud

universität wien

Public Cloud:

Öffentlich zugänglich über das Internet, zahlungspflichtig

Flexibel, kosteneffizient, keine Investition in eigene Hardware

Multinational, wählbare Datenregionen

Hochentwickelt, zusätzliche Maßnahmen für höhere Sicherheitsstufen erforderlich

Edge Computing für niedrige Latenzzeiten, ideal für IoT-Geräte

Private Cloud:

Exklusiv für eine Organisation auf privatem Netzwerk

Hohe Kontrolle und Sicherheit, ideal für vertrauliche Daten und strenge Datenschutzregelungen

Leichter umsetzbar, physischer Datenstandort kontrollierbar.

Community Cloud für gemeinsame Nutzung unter ähnlichen Organisationen

Hybrid Cloud:

Kombination von lokalen Diensten und Cloud-Diensten (Private und Public)

Nahtlose Interaktion, Erweiterung bestehender Infrastrukturen

Datenschutz bei Datenkommunikation

Multi Cloud:

Nutzung mehrerer Cloud-Anbieter

Hohe Flexibilität, beste Angebote verschiedener Anbieter

erhöhte Komplexität und Angriffsfläche, Datenflüsse überwachen, Schnittstellen absichern

Service Level Agreements (SLAs)

Definition: Verträge zwischen Cloud-Anbietern und Kunden über Servicequalität und Maßnahmen bei Abweichungen.

Bedeutung: Bietet Klarheit, Sicherheit und setzt Unternehmensanforderungen durch.

Typen von SLAs:

1. **Kundenbasiert:** Spezifisch für einzelne Kunden und deren genutzte Services.
2. **Servicebasiert:** Standardisierte Services mit gleichen Metriken für alle Kunden.
3. **Mehrstufig:** Kombination verschiedener Service-Levels in einem Vertrag.

Inhalte eines SLA: Start-/Enddatum, beteiligte Parteien, genutzte Services. Servicebeschreibung: Klare Festlegung der erbrachten Leistung. Service-Level-Ziele (SLOs): Leistungskriterien wie Reaktionszeiten und Verfügbarkeit.

Durchsetzung für Entscheidungsträger: Regelmäßige Überprüfung von Verfügbarkeit und Reaktionszeiten → Vertragsstrafen, Gutschriften oder andere Wiedergutmachungen bei Nichteinhaltung.

Zweck: Minimiert Risiken, bietet rechtliche Sicherheit, setzt präzise Erwartungen an die Servicequalität.

Auswahl und Überprüfung von Cloud-Anbietern nach NCSC-Richtlinien

universität wien

Prinzip 1: Schutz von Daten während der Übertragung

Datenverschlüsselung während der Übertragung, um Abhörung und Manipulation zu verhindern.

Prinzip 2: Schutz und Resilienz von Vermögenswerten

Sicherstellung des Schutzes physischer und digitaler Assets.

Prinzip 3: Trennung zwischen den Benutzern

Trennungstechniken, um den Zugriff und Missbrauch von Daten durch verschiedene Nutzer zu verhindern.

Prinzip 4: Governance und Betriebsmanagement

Einbindung eines Governance-Rahmenwerks zur Koordination und Verwaltung des Cloud-Dienstes.

Prinzip 5: Betriebssicherheit

Maßnahmen zur Erkennung, Verhinderung und Reaktion auf Sicherheitsvorfälle.

Auswahl und Überprüfung von Cloud-Anbietern nach NCSC-Richtlinien

universität wien

Prinzip 6: Personalsicherheit

Einschränkung und Überwachung des Zugriffs durch Servicepersonal auf System- und Benutzerdaten.

Prinzip 7: Sichere Softwareentwicklung

Sichere Gestaltung, Entwicklung und Implementierung von Cloud-Services.

Prinzip 8: Sicherheit der Lieferkette

Sicherstellung der Sicherheitsanforderungen auch bei Drittanbieter-Lieferketten.

Prinzip 9: Sicheres Benutzermanagement

Bereitstellung von Werkzeugen zur sicheren Verwaltung und Konfiguration des Services

Prinzip 10: Identität und Authentifizierung

Beschränkung des Zugangs zu Serviceschnittstellen auf authentifizierte und autorisierte Identitäten.

Auswahl und Überprüfung von Cloud-Anbietern nach NCSC-Richtlinien

universität wien

Prinzip 11: Schutz externer Schnittstellen

Sicherheit aller internen und externen Schnittstellen des Cloud-Services gegen Angriffe.

Prinzip 12: Sichere Dienstverwaltung

Robuste Maßnahmen zur Sicherung der Verwaltungssysteme des Cloud-Anbieters.

Prinzip 13: Auditinformationen und Sicherheitswarnungen

Bereitstellung notwendiger Protokolle zur Überwachung und Reaktion auf Sicherheitsvorfälle.

Prinzip 14: Sichere Nutzung des Dienstes

Unterstützung der Kunden bei der sicheren Verwaltung und Nutzung ihrer Daten.

Leitfaden zur sicheren Nutzung von SaaS-Anwendungen

universität wien

Verständnis der Anwendung und ihres Zwecks:

Bevor mit der Konfiguration begonnen wird, ist es wichtig, den Zweck der SaaS-Anwendung und die Art der verarbeiteten Daten zu verstehen.

Gestaltung des Benutzer-Lebenszyklusmanagements:

Effektives Management des Benutzerlebenszyklus durch rechtzeitiges Onboarding und Offboarding. Zugriffsrechte sollten auf das notwendige Minimum beschränkt und ein zentrales Identitätssystem genutzt werden.

Robuste Nutzerauthentifizierung:

Implementierung von Single Sign-On (SSO) und Multi-Faktor-Authentifizierung (MFA) zur Sicherstellung, dass Benutzer sicher und eindeutig authentifiziert werden.

Absicherung administrativer Zugänge:

Minimierung der Anzahl administrativer Benutzer und Anwendung des Prinzips der minimalen Rechtevergabe. Nutzung von rollenbasierter Zugriffskontrolle (RBAC) und Protokollierung aller administrativen Aktivitäten.

Leitfaden zur sicheren Nutzung von SaaS-Anwendungen

universität wien

Berechtigungsmanagement für Standardnutzer:

Gewährung von Zugriffsrechten nur im notwendigen Umfang durch rollenbasierte Zugriffskontrolle. Implementierung eines Zero-Trust-Modells, um den Zugriff nur von vertrauenswürdigen Geräten und Netzwerken zu erlauben.

Nutzung vertrauenswürdiger Geräte:

Sicherstellung, dass der Zugriff nur von vertrauenswürdigen Geräten wie Firmenlaptops erfolgt, insbesondere beim Zugriff auf hochsensible Daten.

Datenschutz und Datensicherheit gewährleisten:

Verschlüsselung von Daten sowohl in Transit als auch in Ruhe und Speicherung in rechtskonformen Rechtsräumen. Sicherstellung, dass auf die Daten nur mit Einwilligung zugegriffen werden kann.

Prüfung auf Schadsoftware und gefährliche Inhalte:

Implementierung von Sicherheitsmechanismen, die Daten auf bösartige Komponenten untersuchen, um die Verbreitung von Malware und Phishing-Versuchen zu verhindern.

Leitfaden zur sicheren Nutzung von SaaS-Anwendungen

universität wien

Management von Dienstidentitäten:

Kontinuierliche Überwachung und Verwaltung von Dienstidentitäten zur Vermeidung von Missbrauch. Regelmäßige Überprüfung der Zugriffsrechte und Integration in Überwachungsprozesse.

Reaktionsstrategien für Sicherheitsvorfälle und Notfälle:

Implementierung gut definierter und getesteter Reaktionsstrategien für Sicherheitsvorfälle. Sicherstellung aktueller Kontaktinformationen und robuster Wiederherstellungsverfahren.

Überwachung von Sicherheitsereignissen:

Kontinuierliche Überwachung und Analyse von Aktivitätenprotokollen zur frühzeitigen Erkennung und Reaktion auf Sicherheitsvorfälle.

Aufrechterhaltung der Sicherheitsstandards:

Regelmäßige Überprüfung und Anpassung der Sicherheitsstrategien und -konfigurationen an neue technologische Entwicklungen und Sicherheitsanforderungen.

Praxisteil 1: Cloud Security Wiki in Moodle

universität wien

Einleitung: Entwicklung eines Cloud Security Wikis in Moodle als umfassendes Nachschlagewerk für Entscheidungsträger und Einzelpersonen, die Cloud-Dienste nutzen möchten.

Ziele: Bereitstellung von Informationen zu Cloud-Modellen, Deployment-Modellen, häufigen Bedrohungen und Maßnahmen, basierend auf den 14 NCSC-Sicherheitsprinzipien.

Anforderungen: Nutzung von Moodle für die dauerhafte Aktualität der Inhalte und für die Implementierung einer rollenbasierten Zugriffskontrolle (RBAC).

Implementierungsschritte:

1. Installation und Konfiguration: Moodle lokal mittels Docker aufgesetzt, HTML und Styling zur Strukturierung genutzt.
2. Migration von Informationen: Klar strukturierte und aufbereitete Inhalte aus der Bachelorarbeit in ein Wiki-Leseformat überführt.
3. Benutzerverwaltung: Einstellungen durch einen Admin-User vorgenommen, Wiki auf Moodle der Universität Wien migriert.
4. Benutzerverwaltung lokal: Admin-Rolle mit vollem Zugriff erstellt, um Aktualität der Inhalte zu gewährleisten.

Testing und Bereitstellung:

Lokales Testing der Suchfunktion, Menüführung und rollenbasierten Benutzergruppen. Bereitstellung über Moodle der Lehrveranstaltung "051061 VU Informationssicherheit".

Praxisteil 2: Interaktives Fallbeispiel-Tool

universität wien

Einleitung: Entwicklung eines interaktiven Tools, um die 14 NCSC-Sicherheitsprinzipien durch Quizzes zu vermitteln.

Ziele: Förderung des Verständnisses und der Anwendung der NCSC-Sicherheitsprinzipien durch eine benutzerfreundliche Plattform und ein dynamisches Lernumfeld.

Anforderungen: Verwendung von React für die Entwicklung, Fokus auf intuitive Navigation und Benutzerfreundlichkeit, Integration von MUI-Komponenten.

Implementierungsschritte:

1. Einrichtung der React App: Aufsetzen des Projekts mit Create React App, Installation notwendiger Bibliotheken, Unterteilung in modulare Komponenten.
2. Entwicklung der Szenarien: Erstellung interaktiver Szenario-Komponenten für jedes der 14 Sicherheitsprinzipien.
3. Entwicklung der App-Komponente: Navigation zwischen Szenarien mittels MUI-Cards, ohne herkömmliche Menüleiste.
4. State Management: Verwendung von React State zur Verwaltung des aktuellen Zustands der App und zur Verarbeitung von Benutzereingaben.

Testen und Bereitstellung:

Bereitstellung über Vercel mit kontinuierlicher Integration durch GitHub-Repository. Intensives Testing zur Fehlerbehebung vor endgültiger Bereitstellung.

Evaluierung der beiden Praxisteile

Methodik:

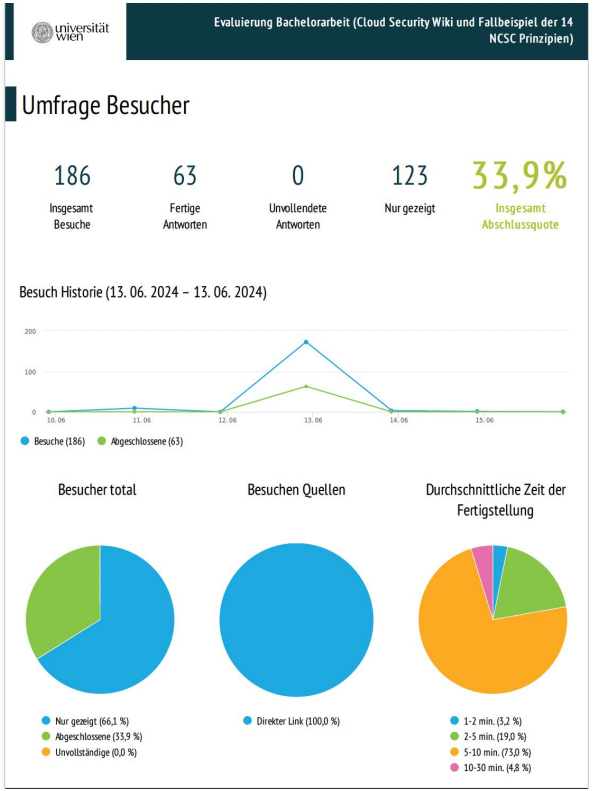
Onlinefragebogen: Erstellt mit Survio, enthielt offene und Single-Choice-Fragen.

Ziele: Bewertung von Effektivität, Benutzerfreundlichkeit und Qualität der Informationen.

Fragen bezüglich Usability, Struktur und Organisation, Qualität der Inhalte, Feedback

Durchführung: 13. Juni 2024, Universität Wien

Auswertung: Qualitative und quantitative Analyse.



Ergebnisse

Verbesserungsvorschläge:

Cloud Security Wiki

- Verbesserung der Suchfunktion (keine Unterscheidung zwischen Groß- und Kleinschreibung).
- Detailliertere Erklärungen für spezifische Themen (z.B. softwaredefinierte Netzwerke).
- Hinzufügen einer Seite mit weiterführenden externen Links.

Interaktives Fallbeispiel-Tool:

- Erhöhung des Schwierigkeitsgrades der Fragen
- Deutliche Hinweise auf die Art der Fragen (Multiple Choice oder Single Choice).
- Sofortige Anzeige der richtigen Antwort mit Erklärung nach jeder Frage.

Gesamtzufriedenheit:

Cloud Security Wiki: 84.1% der Teilnehmer insgesamt zufrieden.

Interaktives Fallbeispiel-Tool: 81% der Teilnehmer insgesamt zufrieden.