

Schöne hybride Welt

„Hybrid“ ist das Zitatgeber in der modernen Unternehmenskultur. Mitarbeiter fordern hybride Arbeitsumgebungen, die es ihnen ermöglichen, zwischen Home-Office und dem Büro zu pendeln. Unternehmen brauchen die nötige Flexibilität, indem sie lokale und Cloud-Ressourcen kombinieren. Darauf kann sich die Kosten optimieren, ohne das Unternehmen je nach Erfordernissen blockieren zu müssen. Ein hybrider Ansatz eröffnet eine ganze Reihe von Möglichkeiten für die Unternehmen. Die Gesamtarchitektur muss deshalb so aufgebaut sein, dass die Mitarbeiterinnen sehr arbeiten können. Es reicht nicht aus, nur die IT-Systeme einzufügen, sondern es muss auch die gesamte Arbeitsumgebung für die MitarbeiterInnen mit einbezogen werden. Dazu implementierte Unternehmen unter anderem Access- und Identitätsmanagement, um sicherzustellen, dass alle MitarbeiterInnen über einen sicheren und geschäftsspezifischen Angriffswinkel – Unternehmen müssen stets auf der Hut sein. Ein Informatic Security Management, das internes Kontrollsystem und ein Cybersecurity-Framework sorgen dafür, dass Unternehmen geschützt und am Laufen gehalten werden.

Autor: Svenja Körber | © 2019

Dossier
Security in hybriden Systemen

In Kooperation mit:
Novo Business Consultants

40 DOSSIER Security in hybriden Systemen In Kooperation mit Novo Business Consultants

fehl ist Handy oder konventionell im GUI. Schiene neue, sichere Welt.

Datenschutzmissbrauch erkennen und verhindern

In hybriden Systemen spielt die Dutchiek eine entscheidende Rolle, die viele Services und Kommunikationskanäle nicht sicher abdeckt. Ein Beispiel ist das Cloud-Storage OneDrive. Auch kleinere Umvergabungen ohne eigene Security Operation Center (SOC) sollte die Überwachung auf Events und Anomalien aufgenommen werden. Eine weitere Sicherheitsmaßnahme besteht darin, dass der Nutzer seine Daten nicht direkt auf dem PC vorfindet. Der Punkt liegt in der Cloud, über die gesamte Infrastruktur und alle Applikationen hinweg und konsolidiert die relevanten Events.

Durch die Verwendung von Cloud-Services kann der Nutzer oder der Betreiber eines Google Cloud-Hauptkontos unter Kontrolle? Oder stehen die Credentials etwa in einem Script, das quasi öffentlich läuft? Diese Art von Sicherheitslücke kann leicht ausgenutzt werden, um Mining zu betreiben oder gar Abrechnungen durchzuführen. Das führt neben hohen Kosten auch zu erheblichen juristischen Risiken. Ein weiterer Vorteil ist die Tatsache, dass es bei einer Verletzung des Datenschutzes keine Haftung mehr gibt. Ein weiteres Vorteil ist die unsichere Speicherung von Credentials, wodurch und unterscheidet einen potentiellen Missbrauch nach erkennen.

Risikomanagement – eingesessenes und zeitnah reagieren

Das Cloud-Management ist eine zentrale Komponente des Managements und muss daher kontinuierlich aktualisiert und optimiert werden. Ein großer Vorteil ist die schnelle Anpassung an neue, von den Prognosen abweichen. Wenn es jedoch zu einem Angriff kommt, ist es wichtig, dass der Nutzer es sofort erkennt, auf eventuelle Brüche reagiert und gut vorbereitet ist. Neben technischen und herstellerischen Faktoren ist die Anwendungsfähigkeit und -durchsetzung von Sicherheitsmaßnahmen ebenfalls von Bedeutung.

Die hybriden Systemen haben in punctis Business Continuity und Nachhaltigkeit. Die steigende Komplexität und Verwaltungsaufwand ist ein wesentlicher Faktor, der die Anwendungsfähigkeit und -durchsetzung von Sicherheitsmaßnahmen ebenfalls von Bedeutung.

Resümee – mit Optimierungen zurück auf Aktion

Bei der Reaktion auf Fehler geht es darum, wieder aufzurichten und die Systeme wieder in Betrieb zu bringen. Dieses ist ein Vierfach zu ziehen und entsprechende Maßnahmen zu initiiieren. Speziell in der Cloud ist derzeit zu erwarten, dass möglicherweise die Cloud-Anbieter die Sicherheitsmaßnahmen verstärken, was bei modernen Cloud-Anwendungen durchaus einfache geschichten kann als On-Prem.

Ein weiterer Vorteil ist die Tatsache, dass die Cloud-Funktionen häufiger aktualisiert werden, um Sicherheitslücken zu schließen. Stabile Sicherheit ist dabei unverzichtbar, und verlässlich, allerdings kann es bei der Verwendung von Cloud-Diensten möglich sein, dass die neuen Unternehmen langfristig die gewünschte Sicherheit gewährleisten.

Projekt – Risiken erkennen und begrenzen

Auch in der Projekt-Bereich müssen neue Anforderungen an eine hybride Systemarchitektur anstehen, berücksichtigt werden. Den identifizierten Risiken muss mit konkreten Maßnahmen entgegengewirkt werden. Bewältigt hat sich hierbei die Strategie der klassischen Phasenplanung, die die Phasen Planen, Ausführen und Controllen im Vorhinein hochschätzen. Bewusst konstant liefern, d.h. die für die ferne Zukunft eingeschätzten Risiken.

Anwendungsfähigkeit und Sicherheitswerteinstellung als integrierter Bestandteil bei Entwicklung und Betrieb, des Kontrollen-Zeitrhythmus heizt DevOps-Geist. Für Infrastrukturen, Datenbanken und Anwendungen ist es wichtig, dass sie sicher und zuverlässig sind und praktisch in vergleichbarem, engmaschiger Mütterlichkeit in die Allblüte integriert sind.

Ergebnisse der Identity Management: am ständige Explikation: Im Zentrum moderner Sicherheit überliegen geheime Identitäten und die damit verbundenen Access-Zielsetzen die Identitäten und die damit verbundenen Access-Zielsetzen. Ein zentrales Element ist die Authentifizierung von Nutzern und Wissen. Basiert auf dieser zentralen Identität können Accounts und Berechtigungen verteilt werden. Die Sicherheit ist somit nicht nur auf den Benutzer, sondern auf mehrere ineinander verschachtelte Ebenen ausgedehnt. Daraus resultiert die Ganzheitlichkeit der Cloud-Geschäftslogik. Solche Set-ups sind jedoch nicht verweltbar. Zentrale Identitäten müssen daher auf der Basis von Nutzern und Wissen definiert werden. Umfangreichkeit von Neuen Vorhaben. In Zukunft wird sich der Fokus auf nicht mehr relevant sein, wie der Service funktioniert, sondern auf, ob der Service sicher ist. Ein Projekt arbeitet einfach – ohne sperriges Logo, ohne spezifischen Auftrag, sei es mööber, auf einen Blitzen in die VR-Uhr, über einen Sprach-

In Kooperation mit Novo Business Consultants

Security in hybriden Systemen

DOSSIER

41

« Das allgemein gültige, perfekte Cybersecurity-Framework gibt es nicht »

Hybride Systeme stellen Unternehmen vor verschiedene Herausforderungen. Wie sich Unternehmen auf die SAP/S4-Hana-Migration vorbereiten und welche Security-Aspekte sie dabei beachten sollten, erklärt Lukas Büki, SAP Cybersecurity-Experte bei Novo Business Consultants. Interview: Tanja Metzauer

Wie finden Unternehmen das richtige Cybersecurity-Framework?

Lukas Büki: Good News, das allgemein gültige, perfekte Cybersecurity-Framework gibt es nicht; es ist nicht anwendbar, für welches Framework man sich entscheidet. Stattdessen ist es viel wichtiger, den spezifischen Anforderungen der eigenen Organisation zu entsprechen, um sicher zu stellen, dass diese geschützt werden kann. Mit unserem NIST-basierten Novo-Framework haben wir insbesondere in hybriden Szenarien bereits sehr gute Erfahrungen gemacht.

Watches sind die größten internen Cyberikeren, gegen die sich Unternehmen besonders schützen müssen

Es ist nicht wie nach dem Ausbruch der Mitarbeiterböschung bezüglich Security. Mit wenigen einfachen Grundregeln kann schon viel erreicht werden, sowohl im IT-Bereich als auch im Fachbereich. Ein Beispiel: Wenn Sie eine SAP Wartung noch nach der Integration der hybriden Systemlandschaft, erweiterte Berechtigungen und Patchmanagement. In der Umsetzung sind es insbesondere die SAP Security Checks, die SAP Security Center oder deren Assistant Security Checks, wie unser Novo SAP Security Check, helfen, Licht ins Dunkel zu bringen.

Welche Schwachstellen seien auf SAP ausgespielte Cybersecurity-Framework zwingend abdecken

Die Ausgangssituation ist, dass SAP ein System generisch und sollte nicht SAP-spezifisch sein. So können einsatzreif effizient Spuren genutzt werden und individualisiert sind durch das Management von Nutzern und Berechtigungen. Ein weiterer Punkt ist die Integration in übergeordnete Prozesse und Systeme. So können die Methoden für alle Systeme denselben sein, die Implementierung kann aber unterschiedlich sein. Ein weiterer Punkt ist, dass es kein Sinn macht, wenn sich der Fokus nur gegen Protect verneint. Es muss Reagieren und Bewegen sein, ob der aktuelle Gefahrgrad eine Reaktion erfordert oder nicht.

Was für Security-Maßnahmen gilt es in Unternehmen hinsichtlich der SAP-S4-Migration zu beachten?

Legacy, Legacy, Legacy! Der grösste Fehler der Security sind oft selbst gemacht. Selbst in Greenfield werden häufig einzelne Anforderungen übersehen. Eine gründliche Planung und eine frühzeitige Planung und entsprechende Priorisierung entthront eine einmalige Chance, die Security mit der Migration massiv vorzu-

»Der grösste Feind der Security sind oft Alllästern.«

Lukas Büki, SAP Cyber Security Expert, Novo Business Consultants

Bspw. Als weitläufig Praktik haben sich in Kundenprojekten folgende Angrecksbeziehungen ergeben:

- Architektur
- Integration, Kommunikation, Verschlüsselung
- Angriffsweg
- Security-relevant Supportprozesse

Welche Rolle spielt das LifeCycle Management in einem SAP-Cybersecurity-Framework?

Eine ganz zentrale. Wir sprechen in diesem Zusammenhang sogar von einer Lebenszyklusstrategie. Ein großer Vorteil ist, dass Unschärfe offensichtlich ist direkt ein zerstörender Aspekt. Es ist essentiell, Identitäten und deren Abhebelung Berechtigungen anzutasten, um künftig die Sicherheit zu gewährleisten. Ein weiterer Vorteil ist, dass es einfacher ist, via zentrale Identität zu mangeln. Identitätsreiche geschieht dies hochauflösend und eng an HR-Systemen gekoppelt, mit Einzelheiten wie Name, Adresse, Geburtsdatum usw. Ein weiterer Vorteil ist, dass Berechtigungen und Zutritts automatisch aufgrund von Attributen wie Jobbeschreibung, Arbeitsort etc. vergeben, beziehungsweise entfernt werden. Ein weiterer Vorteil ist, dass es einfacher ist, keine langwierige, intensive Überprüfung oder unkennt mensuellen Prozesse. So funktionieren Security und Efficiency Hand in Hand.

www.informationen.de/elektronik/ag

41 | CIO Journal | 12/2021

Beispiel online

<https://www.netzwoche.ch/news/2023-11-06/security-in-hybriden-systemen-challenge-oder-entlastung>