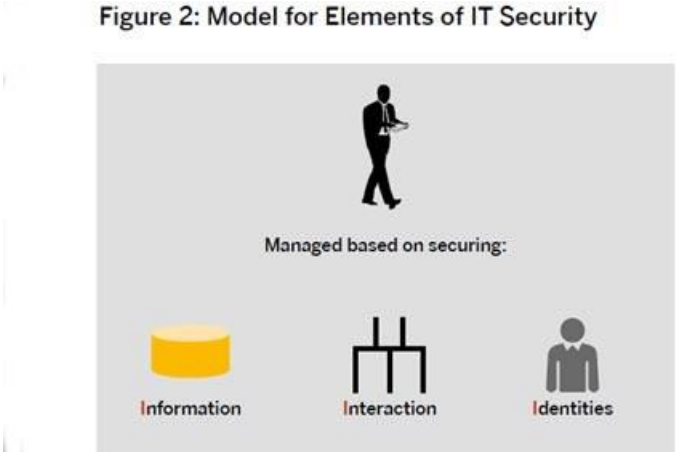
Link: https://www.computerwoche.de/a/so-entwickeln-cios-das-passende-it-security-konzept,2553586

Neuer CIO Guide

So entwickeln CIOs das passende IT-Security-Konzept

Datum: 18.02.2014
Autor(en): Andreas Schaffry

SAP gibt in einem neuen CIO Guide Empfehlungen zur Absicherung von Informationen, Interaktionen und Identitäten in hybriden und mobilen IT-Umgebungen sowie in der Cloud.



Die drei Kernelemente bei der Umsetzung einer IT-Security-Strategie sind: Information, Interaktion und Identität
Foto: SAP

In der stark vernetzten Geschäftswelt heute müssen Unternehmen effizient agieren. Eine wichtige Voraussetzung dafür bildet eine IT-Infrastruktur, die Anwendern überall und jederzeit den Zugriff auf Geschäftsanwendungen und -daten ermöglicht. CIOs wiederum treibt dies den Schweiß auf die Stirn, denn sie müssen IT-Sicherheitskonzepte entwickeln, um Applikationen, sensible Geschäftsdaten und Mobilgeräte vor fremdem Zugriff zu schützen.

Hierbei sind vielfältige Fragestellungen zu beachten. Wie lassen sich zum Beispiel geschäftliche und personenbezogene Daten, die in einer **Cloud**[1]-Umgebung lagern, bestmöglich schützen? Wie können sensible Informationen, die Anwender aus den Back-End-Systemen auf ihr Mobilgerät holen und sie dort speichern, abgesichert werden? Welche Sicherheitsrisiken entstehen in hybriden und mobilen IT-Umgebungen oder in der Cloud? Wie können diese bereits im Vorfeld erkannt und minimiert werden? Auf diese und viele weitere Fragen müssen CIOs die passenden Antworten finden und im Rahmen von Security-Konzepten die IT-Prozesse, die Ausbildung der Mitarbeiter und die IT-Architekturen an der jeweiligen Situation ausrichten.

Die drei Elemente bei IT-Security

SAP stellt in dem neuen CIO Guide "IT Security in Cloud and Mobile Environments" herstellerneutral konkrete Empfehlungen und Referenzkonzepte vor, die CIOs als Entscheidungshilfe bei der Umsetzung ihrer IT-Sicherheitsanforderungen und -konzepte nutzen können. Die einzelnen Aspekte rund um das Thema IT-Sicherheit in der Cloud sowie in hybriden und mobilen Umgebungen werden anhand eines **IT-Security**[2]-Modells veranschaulicht, dessen drei Kernelemente "Information", "Interaktion" und "Identität" bilden.

1. Die Absicherung von Informationen adressiert die Themen Datensicherheit in der Cloud und den Schutz geschäftlicher Informationen.

2. Die Absicherung von Interaktionen verfolgt das Ziel, eine sichere On-Premise-Landschaft zu garantieren, wenn diese mit Cloud- und Mobility-Technologien kombiniert wird.

3. Bei der Absicherung von Identitäten werden die Themen Identity Management" und Single-Sign-On (**SSO**[3]) innerhalb hybrider IT-Infrastrukturen adressiert.

Welche Relevanz die drei Elemente für das eigene Business und die IT-Sicherheit haben, hängt von verschiedenen Faktoren ab, die von Unternehmen zu Unternehmen variieren. Zum einen wäre das die bestehende IT-Infrastruktur, ob Cloud-, Hybrid- oder Mobil-Umgebung, dann die Priorität der einzelnen Elemente für die IT-Sicherheit und nicht zuletzt die Qualität der jeweils verfügbaren IT-Security-Lösungen. Anhand dieser Kriterien stellt der CIO Guide für jedes Element konkrete Referenzkonzepte für die IT-Sicherheit vor und beschreibt deren Nutzen.

Datensicherheit in der Cloud

Bei der Informationssicherheit etwa müssen die Anforderungen an die Datensicherheit in einer **Cloud-Umgebung**[4] an den aktuellen gesetzlichen Regelungen ausgerichtet werden. Agiert eine Firma international, sind auch noch die Vorschriften der jeweiligen Länder zu beachten. Des Weiteren ist zu berücksichtigen, ob der beauftragte Cloud Service Provider (CSP) geschäftliche Informationen an mehreren Standorten speichert. Schließlich ist zu evaluieren, ob die Rechenzentren des CSP den gewünschten Sicherheitsanforderungen genügen. Ein wichtiges Gütesiegel bilden hier Zertifizierungen, etwa nach DIN ISO 27001.

Die typische Basismaßnahme bei der Absicherung von Interaktionen ist die Unterteilung einer IT-Systemlandschaft in mehrere **Netzwerkzonen**[5] oder -schichten, die jeweils durch eine eigene **Firewall**[6] geschützt ist. Dabei müssen die einzelnen Zonen oder Schichten technisch den risikolosen Zugriff auf Daten und deren Transport innerhalb des Netzwerkes ermöglichen.

Single-Sign-On: Ein Schlüssel für Alles

In hybriden Umgebungen oder bei heterogenen IT-Systemlandschaften ist die sichere Authentifizierung und eine SSO-Funktionalität eine Kernanforderung beim Zugriff auf Cloud-Anwendungen und mobile Apps. In einer **Identity-Management**[7]-Lösung können Benutzerdaten wie auch die Berechtigungen zentral verwaltet und jederzeit zugeteilt oder entzogen werden.

IT-Verantwortliche erfahren im CIO Guide darüber hinaus, wie sie die speziellen Security-Anforderungen in Cloud- und Mobility-Umgebungen erfüllen, mobile Geräte schützen oder Interaktionen in Cross-Company-Prozessen absichern können. Nicht zuletzt beinhaltet das Dokument zahlreiche Links, die zu weiterführenden Informationen über die einzelnen Themen führen.

Der aktuelle CIO Guide "IT Security in Cloud and Mobile Environments" kann **hier**[8] als PDF-Datei heruntergeladen werden.

Links im Artikel:

[1] **https://www.computerwoche.de/a/datensicherheit-in-und-aus-der-cloud%2C2550657**
[2] **https://www.computerwoche.de/p/security%2C332**
[3] **https://www.computerwoche.de/a/worauf-es-bei-sso-loesungen-ankommt%2C2539134**
[4] **http://global.sap.com/germany/solutions/technology/cloud/overview/index.epx**
[5] **https://www.computerwoche.de/a/netzwerke-schuetzen%2C2363301**

[6] **https://www.computerwoche.de/a/zwoelf-security-mythen-entlarvt%2C2505799%2C12**
[7] **https://www.computerwoche.de/a/identity-management%2C2549607**
[8] **https://www.computerwoche.de/ueb/24218**
