Arbeitsgruppe 4
Vertrauen, Datenschutz und Sicherheit im Internet

Nationaler IT Gipfel

UAG 1 • Sicheres Cloud Computing

Sicherheitsprofil für Cloud Computing
Schwerpunkt: CRM-Software nach dem SaaS-Modell

Impressum

Dokumentation der Ergebnisse der AG 4,
Unterarbeitsgruppe 1 · Sicheres Cloud Computing
zum Nationalen IT Gipfel 2013/2014

Leitung der Arbeitsgruppe:
Deutsche Telekom AG

Ansprechpartner Leitung der Arbeitsgruppe:
T-Systems International GmbH
80995 München
http://www.t-systems.de

Mitgliederliste der Unterarbeitsgruppe 1
Alle Mitglieder auf der Umschlagrückseite

Gestaltung und Produktion:
Im Auftrag von:
Deutsche Telekom AG
Hewlett-Packard GmbH
Microsoft Deutschland GmbH

Inhalte:
Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63 · 53133 Bonn
https://www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Sicheres Cloud Computing am Beispiel CRM (SaaS)

Inhalt

Arbeitsgruppe 4

Die Arbeitsgruppe 4 „Vertrauen, Datenschutz und Sicherheit im Internet“ stellt sich den Herausforderungen, die mit der Durchdringung unseres Alltags mit dem Internet verbunden sind. Sicherheit und Datenschutz sind die wesentlichen Grundlagen für die Schaffung von Vertrauen im Internet. Etwa 80 Prozent aller Deutschen nutzen das Internet für geschäftliche und für private Aktivitäten. Auch die wirtschaftliche Prosperität unseres Landes ist zunehmend mit dem Internet verbunden: Die Geschäfte von 50 Prozent aller Unternehmen in Deutschland sind heutzutage mittel bis stark vom Internet abhängig.

Nicht zuletzt aus diesen Erwägungen heraus folgt die gemeinsame Verantwortung von Staat und Wirtschaft, den Cyber-Raum sicher zu gestalten. Die unterjährige Arbeit der AG 4 erfolgt dabei zum großen Teil in den jeweiligen Unterarbeitsgruppen (UAG), die sich mit Fragen des Cloud Computing, der Sicherheit elektronischer Identitäten im Internet, mit der Stärkung der Providerverantwortung und mobiler Sicherheit beschäftigen.

Co-Vorsitzende

- Dr. Thomas de Maizière · Bundesminister des Innern
- Dr. Walter Schlebusch · Vorsitzender der Geschäftsführung, Giesecke & Devrient GmbH

UAG 1 · Sicheres Cloud Computing (Leitung Deutsche Telekom AG)

Die Potenziale des Cloud Computing sind sowohl aus Anwendersicht als auch als Sicht der Industrie immens. Dabei kommt es zunehmend darauf an, das geeignete regulatorische Umfeld für Cloud Computing zu definieren. Über technische Standards hinaus werden dabei im Wesentlichen Fragen des Datenschutzes und der IT-Sicherheit – und damit auch die Akzeptanz durch den Nutzer – berührt.

In der Unterarbeitsgruppe 1 wurde am Beispiel der Kundenbetreuung die Sicherheitsthematik im Cloud Angebot durchleuchtet. Insbesondere kleinen und mittleren Unternehmen wird zusätzlich durch die Bereitstellung eines elektronischen Portals (technisches) Wissen in gebündelter Form zugänglich gemacht.

Dieses Infoblatt dient einer schnellen Übersicht und Abbildung der erarbeiteten 13 Steckbriefe.

Sicheres Cloud Computing am Beispiel CRM (SaaS)

Sicherheitsprofil für Cloud Computing: Inhalte und Vorgehen

Die UAG1 hat sich bei der Erarbeitung des Sicherheitsprofils der CRM-Software nach dem Software-as-a-Service-Modell als exemplarische Cloud-Computing-Anwendung gewidmet.

Als Customer Relationship Management (kurz: CRM, dt. Kundenbeziehungsmanagement) bezeichnet man die Software, Daten und Services, die ein Unternehmen nutzt, um die Kundenbeziehungsprozesse abzubilden und zu gestalten. CRM integriert unternehmensweit alle kundenbezogenen Prozesse in Marketing, Vertrieb, Kundendienst sowie Forschung und Entwicklung.

CRM-Systeme basieren meist auf Standardsoftware: einer zugrundeliegenden Datenbank mit den Kundendaten plus fest definierten Prozessen für die Arbeitsabläufe (Workflow). Für spezielle Anforderungen werden CRM-Systeme auch als Individuallösungen realisiert.

CRM-Systeme zählen zu den ersten Anwendungen, die als SaaS-Dienstleistungen angeboten wurden (nach Webmail und Online-Speicher). Die Vorteile des Cloud Computing liegen hier auf der Hand: Schnelle Skalierbarkeit auch in Spitzenlastzeiten (zum Beispiel im Weihnachtsgeschäft) und bei raschem Wachstum des Unternehmens; gleichzeitig ist der Zugriff auf das CRM-System auch bei verteilten Standorten und für Unternehmen mit hoher Zahl von Außendienst- und externen Mitarbeiten (Vertrieb, Kundendienst, Dienstleister) möglich.

Vorgehensweise und berücksichtigte Sicherheitsstandards

Bei der Betrachtung der Bedrohungen für SaaS-Systeme am Beispiel eines CRM-Systems wurden – aufbauend auf der Betrachtung, dass der CRM-Prozess in die 3 grundsätzlichen Schritte **LogIn > Aktion > LogOut** zu unterteilen ist, – über 30 Prozesse analysiert und insgesamt 60 Angriffsmöglichkeiten ermittelt. Diese hohe Zahl ergibt sich aus der Komplexität der Bezugsgrößen:

- 5 berücksichtigte Sicherheitsstandards
- den 6 Angriffsarten aus dem STRIDE-Modell
- den insgesamt 5 Bereichen (Schichten), in denen es zu Angriffen kommen kann
- sowie den 4 unterschiedlichen Akteuren, die angegriffen werden können und die es zu schützen gilt

Ausgehend von den Bedrohungsarten wurde ein spezielles Schichtmodell abgeleitet.

Die Arbeitsgruppe selektierte dann in einem weiteren Verfahrensschritt ein Profil von 13 Bedrohungen, welches in diesem Heft vorliegt.

Die Akteure

In CRM-Anwendungen nach dem SaaS-Modell sind Akteure beteiligt, die man zum einen nach dem Schichtenmodell des IETF Cloud Stack unterscheidet und zum anderen danach, ob es sich um Provider (Serviceanbieter) oder Subscriber (Serviceabonnenten) handelt.

Zu den Serviceabonnenten zählt man die tatsächlichen Endnutzer und die IT-Administratoren bei dem Unternehmen, das das SaaS-Angebot in Anspruch nimmt. Auf Seiten des Serviceanbieters sind hauptsächlich IT-Administratoren sowie Sub-Dienstleister beteiligt, die die erforderliche Cloud-Umgebung bereitstellen und überwachen.

Die folgenden Schichten des IETF Cloud Stack sind von den Bedrohungen betroffen:

Architektur

Access and Delivery Layer

Das Access and Delivery Layer (ADL) ist die Schicht der Cloud Architektur, über die Verbindungen zur „Außenwelt“ (alle Akteure außerhalb des Cloud Service Providers) hergestellt werden. Aber auch interne Akteure loggen sich über diese Schicht ein. Diese Schicht ist eine kritische Komponente, da über sie berechtigte Subscriber und Provider auf die CRM-Anwendung zugreifen genauso wie unberechtigte. Auf dieser Schicht können alle sechs Angriffsarten des STRIDE-Modells stattfinden; Angriffe auf dieser Schicht können alle Akteure betreffen.

Externe Kommunikation

Darunter versteht man sämtliche Netzverbindungen. Sie sind kritisch für die Nutzung der Cloud-Services, schließlich ist ein Zugriff auf die Cloud ohne Netzverbindung nicht möglich.

Cloud Service Layer

Das „Cloud Service Layer“ bestimmt den Bedarf an Ressourcen, die für die zuverlässige Bereitstellung des Service benötigt werden (Art und Umfang der benötigten Ressourcen, Art, Zeitpunkt und Dauer der Bereitstellung). Hier drohen Manipulationen, Rechteeskalation sowie Vertraulichkeitsverlust.

Cloud Management Layer

Auf der Cloud-Management-Ebene werden Funktionen für die Administration und Überwachung der Cloud-Umgebung bereitgestellt. Dazu gehören u. a. die Einbindung der Cloud-Komponenten auf der Basis der Einsatzrichtlinien, die Verwaltung und Registrierung von Service, die Überwachung des operativen und Alarmfunktionen bei sicherheitsrelevanten Ereignissen. Außerdem werden hier die Sicherheitsservices der Cloud selbst verwaltet – Manipulationen und Rechteeskalation haben auf dieser Ebene besonders gravierende Folgen.

Ressource Control

Der Ressourcen-Layer ist für die Verwaltung der verschiedenen Ressourcen des Ressourcenpools und die Zugriffe auf physikalische sowie virtuelle Komponenten zuständig. Angriffe darauf können zu Vertraulichkeitsverlust (Information Disclosure, Stichwort: Industriespionage) oder auch Manipulation (Tampering) führen – Ausfälle von Hardwarekomponenten zu Betriebsunterbrechungen.

Den Analysen zu Grunde liegen die Attacken des sogenannten STRIDE-Modells. Die Buchstaben stehen für die sechs wichtigsten Bedrohungsarten:

Spoofing (Vortäuschen und Missbrauch fremder Identitäten)

Spoofing gilt als eine der gravierendsten Bedrohungen für Computernetze und Cloud Computing. Spoofing ist meist Ausgangspunkt für weiterreichende Angriffe, insbesondere auf dem Access and Delivery Layer (ADL) – das typische Einfallstor für Angriffe.

Ein externer Angreifer versucht beim Spoofing, Nutzer durch gefälschte E-Mails, kompromittierte Webseiten oder auch Anrufe dazu zu verleiten, entweder Informationen weiterzugeben, mit Schadsoftware versehene Dokumente oder Webseiten zu öffnen und so sein System mit Schadsoftware zu infizieren. Alternativ kann der Angreifer versuchen, über unbemerkte Man-in-the-Middle-Attacken die Kontrolle über Kommunikationswege und/oder Zugriff auf Ressourcen zu erlangen. Mit den beim Spoofing erlangten Authentifikationsdaten (Benutzername und Kennwort) kann er sich Zugriff auf die Infrastruktur und Daten verschaffen.

Tampering (Manipulieren von Daten)

Von Tampering spricht man, wenn ein Angreifer unberechtigterweise Daten verändert. Das kann die Manipulation von Daten sein, die in einer Datenbank oder einem Dokument gespeichert sind; das kann aber auch die Manipulation von Daten sein, die über ein Netzwerk übertragen werden. Häufig wird die Manipulation erst erheblich später bemerkt.

Repudiation (Abstreiten)

Repudiation bedeutet, dass ein Angreifer eine nicht erlaubte Operation in einem System durchführt, ohne dass der Nachweis geführt werden kann, dass **a)** die Operation stattgefunden hat und **b)** er der Verursacher war – zum Beispiel, weil die Möglichkeit fehlt, die Operation nachzuverfolgen. So kann er, sofern die Aktion doch entdeckt wird, die Tat abstreiten (daher der Begriff Repudiation).

Information Disclosure (Vertraulichkeitsverlust)

Dabei erlangen Personen Zugriff auf vertrauliche Daten, die dazu nicht berechtigt sind. Zwei Beispiele: Nutzer können Dokumente einsehen, für die sie keine Leseberechtigung haben; ein Angreifer erlangt Zugriff auf Daten, während diese von einem System zu einem anderen übertragen werden. Anders als bei Tampering erhält der Angreifer „nur“ Lesezugriff; der Angriff wird häufig nicht bemerkt. Typischer „Anwendungsfall“: Industriespionage.

Denial of Service (Dienstverweigerung)

Denial-of-Service-Angriffe (DoS) bedrohen die Verfügbarkeit und verhindern, dass berechtigte Nutzer Zugriff auf Ressourcen erhalten. Typischerweise wird dazu ein Webserver durch eine sehr hohe Anzahl von (nicht gültigen) Zugriffsversuchen überlastet und ist so für andere Nutzer nicht zugänglich. Gleichzeitig versucht der Angreifer häufig, sich unberechtigten Zugriff auf den Server zu verschaffen, um dort zum Beispiel Daten einzusehen oder sich höhere Zugriffsrechte zu verschaffen.

Elevation of Privilege (unzulässige Erweiterung von Rechten)

Dabei verschafft sich ein Angreifer erweiterte Zugriffsrechte und kann so unrechtmäßig auf Ressourcen zugreifen und das System kompromittieren oder stören. Im schlimmsten Fall durchbricht ein Angreifer auf diese Weise sämtliche Schutzsysteme und wird Teil des vertrauenswürdigen Systems.

ECKPUNKTE

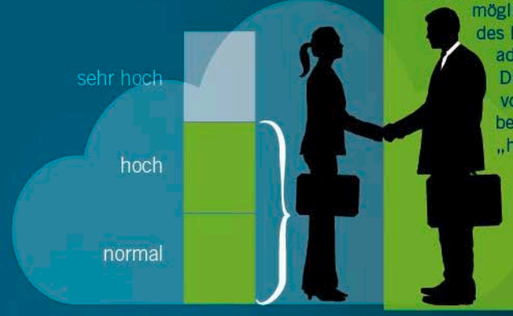
Herausforderung
Cloud Sicherheit im CRM (SaaS)

ISO 27001
Sicherheitsempfehlungen für Cloud Computing Anbieter
NIST SP 800-53 rev3
Cloud Security Alliance Cloud Control Matrix
IETF

BSI-Sicherheits-empfehlungen

Die Ansprüche der berücksichtigten Standards, Empfehlungen und Anforderungen von staatlichen Behörden und sonstiger Konsortien unterscheiden sich zum Teil.

Schutzbedarf
für CRM-SaaS



Dieses Sicherheitsprofil ist für den gesamten Markt CRM-SaaS gedacht und es wurde mit der Wahl des Schutzbedarfs versucht, einen möglichst großen Teil des Marktes zu adressieren. Die UAG geht von einem Schutz-bedarf bis „hoch" aus.

4 Gefährdungs-typen

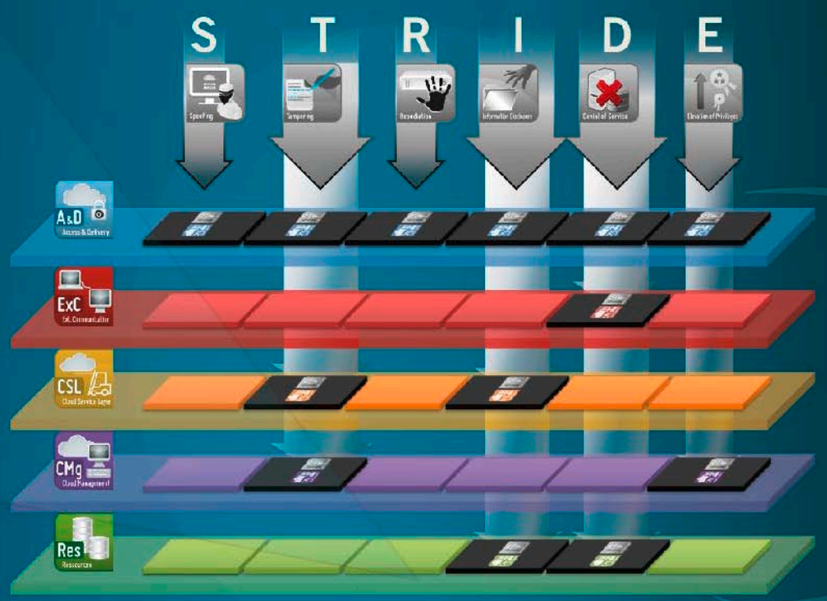
5 Schichten

Angelehnt an den IETF Cloud Stack entstanden 5 relevante Komponenten im Modell.

- A&D Access & Delivery
- ExC Ext. Communication
- CSL Cloud Service Layer
- CMg Cloud Management
- Res Ressourcen

6 Attacken

Bedrohungen werden nach den 6 STRIDE Attacken abgebildet.



4 Akteure

Je 2 Akteure beim Kunden und bei den Anbietern (Provider) sind von den Gefährdungen unmittelbar betroffen. In einer zweistufigen Bewertung zeigt die Studie die Relevanz bzw. Wahrscheinlichkeit auf.

SEU: Subscriber End User

Kunde Nutzer

SAD: Subscriber Administration

Kunde Admin

CSP: Cloud Service Provider

Anbieter Admin

Sub-Provider Admin

In der Regel gibt es mehrere Sub-Provider und auch Ketten von Sub-Providern. Die Risiken werden als vernachlässigbar eingeschätzt, wenn eine entsprechende Vertragsgestaltung vorliegt.

3 Phasen

Eine 3-Phasen-Struktur umfasst LogIn, Aktionen im System und LogOut

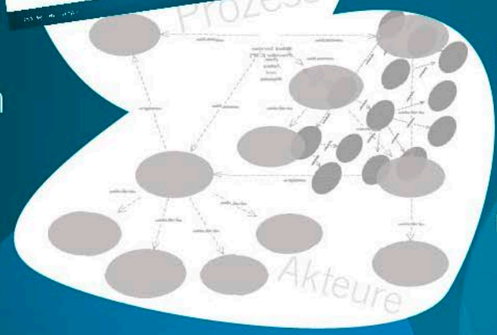
Jede Tätigkeit des Endbenutzers am CRMS beginnt mit einem LogIn und endet mit einem LogOut. Im Falle eines erfolg-reichen LogIn kann der End-nutzer im CRMS neue Kunden-daten hinzuzufügen, vorhandene Kundendaten bearbeiten und analysieren.

13 Bedrohungen

Als Steckbrief zusammengefasst

Komplexität

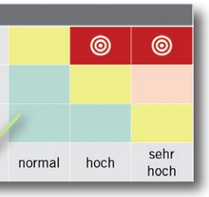
Konfrontiert mit den 6 STRIDE Bedrohungen ergaben sich 60 Bedrohungs-Szenarien, die priorisiert und auf 13 Hauptbedrohungen konsolidiert wurden.



In kurzen Steckbriefen behandeln und bewerten die folgenden Seiten diese Szenarien. Im Anhang finden Sie die betroffenen Sicherheitsanforderungen und Prozesse im Detail.

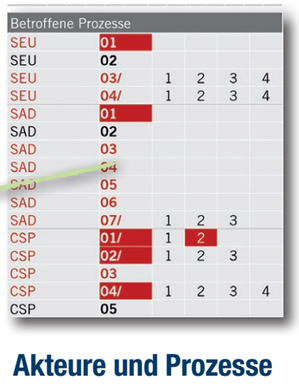
Sicherheits-anforderungen

Die betroffenen Normen sind rot hervorgehoben. Eine erste Übersicht dazu finden Sie im Anhang Seite 24-26.



Vereinfachter ALARP

Wahrscheinlichkeit und Schadenshöhe in einer kompakten Übersicht



Akteure und Prozesse

Betroffene Prozesse sind mit roter Zahl, besonders wahrscheinliche Angriffsflächen mit rotem Hintergrund gekennzeichnet.

Die einzelnen Akteure sind auf der Schaugrafik Seite 8/9 erkennbar (SAD, SEU, CSP)

Eine Übersicht zu den hier referenzierten Prozessen finden Sie auf Seite 27 dieser Broschüre.

Beispiele für die Benutzung und Zuordnung des Anhangs:

AES-03: Die Anwendung setzt eine sichere Identifikation und Authentisierung externer Zugriffe durch. (...)

PIM-03: Der CS-Anbieter legt die Schnittstellen für den Datenaustausch und die Datenspeicherung offen.

Spoofing im Access & Delivery Layer

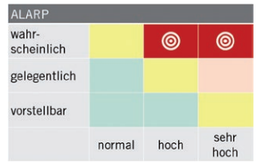
Spoofing stellt für das Access & Delivery Layer (ADL) eine der größten Bedrohungsflächen dar. Für Cloud-Systeme ist die erfolgreiche Verwendung „vorgetäuschter“ oder manipulierter Identitäten eine Methode, um an Kunden oder Konfigurationsdaten zu gelangen. Sobald ein Angreifer im ADL erfolgreich spoofen konnte, ist er imstande Aktivitäten und Transaktionen zu belauschen und Daten zu manipulieren. Erfolgreiches Spoofing ist überdies Ausgangspunkt für weitere Bedrohungen.

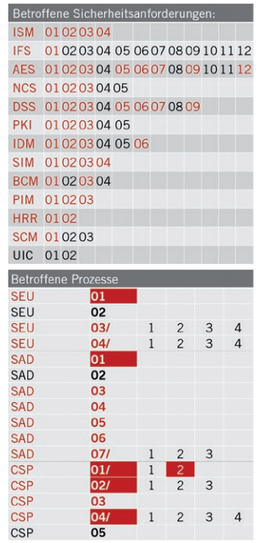
Im einfachsten Fall wird ein externer Angreifer versuchen, mittels vorgetäuschter Kommunikationsverbindungen, wie zum Beispiel durch falsche E-Mails, (Support-) Websites oder Anrufe, den jeweiligen Akteur zur Aufdeckung bzw. Weitergabe dieser Informationen zu bewegen. Eine weitere Möglichkeit für Spoofing ist, mittels unbemerkter „Man-In-The-Middle“-Attacken die Kontrolle über die Datenwege bzw. den Zugriff auf entscheidende Systemkomponenten zu erlangen.

Besondere Spoofing-Attacken auf ADL für SaaS CRM

Für das Szenario „SaaS CRM“ kommen alle Akteure dieses Profils in Betracht. Dabei lassen sich vor allem folgende Spoofing-Einzelbedrohungsszenarien für das Access & Delivery Layer erkennen:

1. Missbrauch von Zugriffsrechten mittels fremder bzw. gefälschter Authentifikationsdaten bei der Anmeldung (Login) der SaaS CRM-Anwendung
   01. die Anmeldung als „gespoofter“ SEU könnte den Zugriff auf einzelne, nicht zuletzt auch vertrauliche Daten zur Folge haben
   02. die Anmeldung als „gespoofter“ SAD hat zusätzlich den Zugriff auf die Benutzerverwaltung des SaaS CRM zur Folge
   03. die Anmeldung als „gespoofter“ CSP Administrator hat die mögliche Kompromittierung des gesamten SaaS CRM aller Kunden zur Folge
   04. der Internet Service Provider (ISP) und der CSP Sub-Provider sollten in der Regel über keine SaaS CRM-Benutzerkonten verfügen und werden daher hier nicht weiter betrachtet.
2. Missbrauch ungeschützter bzw. nicht beendeter Sitzungen (Sessions)
   01. Abgefangene Cookies (z. B. mit Wireshark) werden neu im Browser platziert, um SaaS Sessions neu zu laden, oder
   02. es wird mit einem solchen Cookie unbemerkt auf Komponenten in der Cloud Architektur zugegriffen.
3. Abfangen des Datenverkehrs
   01. durch Vortäuschung einer gefälschten Login-Website oder
   02. durch Vortäuschung eines legitimierten Empfängers und somit Um- bzw. Weiterleitung des Datenverkehrs in Richtung einer gefälschten Identität (z. B. mit SSL Strip).
4. Weiterleitung des zuvor abgefangenen Datenverkehrs unter Verwendung von gefälschten Identifikations- / Absendermerkmalen
   01. Dieses Szenario stellt gegebenenfalls den bedrohlichsten zu erwartenden Fall dar, da es sich hierbei um einen unerkannten Teilnehmer auf dem Kommunikationsweg handelt. Dieser Angriff lässt sich allerdings nur sehr aufwendig realisieren, wenn die Verbindung nicht hinreichend kryptografisch abgesichert ist. Bei nicht ausreichender Verschlüsselung besteht allerdings das Risiko des Spoofings für alle Nutzer der SaaS CRM Anwendung und kann zur Offenlegung aller Daten aller Nutzer führen.





Noch näher zu betrachtende Bereiche

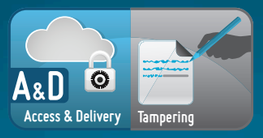
In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

1. Überprüfung der Sicherheitskonzepte und -richtlinien aller Akteure auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage. Dies beinhaltet die Funktionen des Portal Gateways, Inter-Cloud Funktionalitäten mit Sub-Provider und die SLAs mit dem ISP.
2. Etablierte Maßnahmen zur Reduzierung der Möglichkeiten für Angreifer, erfolgreich zu spoofen. Dies beinhaltet unter anderem:
   01. Der sichere Umgang von Kennwörtern und Benutzerkennungen. E-Mails, in denen zum Zugriff auf das CRM aufgefordert wird oder die nach den Zugangsdaten fragen, sollten gelöscht werden.
   02. Die strikte Trennung von Nutzern und die Beschränkung auf die die nötigsten Berechtigungen, sichere und zuverlässige Benutzer- und Berechtigungsverwaltung sowie sicheres Session Handling.

Trotz umgesetzter technischer und organisatorischer Sicherheitsmaßnahmen, kann nicht endgültig verhindert werden, dass einzelne Spoofing Attacken wie Blind Spoofing, Non-Blind Spoofing (aus dem gleichen Sub-Netzwerk), Referrer-Spoofing, Content-Spoofing (Pishing, DHTML Spoofing, Website Spoofing, URL Spoofing) erfolgen und Man-in-the-middle-Attacken oder Denial of Service Attacken ausgeführt werden.

Restrisiken

- unsicherer Umgang mit Benutzerkennung auf der Seite des Subscribers und des Sub-Providers
- fahrlässiges sowie vorsätzlich böswilliges Verhalten auf der Seite des Subscribers, des Sub-Providers, des ISP und durch die CSP Administrator
- ungenügend bzw. unzureichend gesicherte Kommunikationsverbindungen in der Verantwortung des Subscribers, des Sub-Providers und des ISP
- ungenügend bzw. unzureichend gesicherte Systemkomponenten auf der Seite des Subscribers, des Cloud Service Providers, des Sub-Providers und des ISP



Tampering im Access & Delivery Layer

Tampering stellt für das Access & Delivery Layer (ADL) eine kritische Bedrohungsfläche dar, da es eine Gefährdung aller auf dem ADL befindlichen Konfigurations- und ggf. auch Authentifikationsdaten der Access- und Sicherheitssysteme, wie beispielsweise der Service Gateways und der durch das ADL ermöglichten Verwaltungsportale, wie beispielsweise das User Portal, bedeutet.

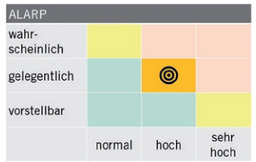
Tampering ist vor allem eine Folge erfolgreicher →Spoofing-Attacken. Externe wie interne Angreifer erlangen unter Nutzung gefälschter Identitäten Zugriff auf Kommunikationsverbindungen, Cloud-Systeme, Komponenten und Anwendungen und sind anschließend in der Lage, Daten im ADL bzw. über das ADL in der nachgelagerten Cloud-Infrastruktur zu manipulieren oder manipulierte Daten einbringen zu können. Innentäter mit Administratorrechten können im Access und Delivery Layer insbesondere durch Manipulation der Konfigurationsdaten und der Sicherheitskomponenten Schaden anrichten. Ferner können Sie die Benutzerverwaltung im ADL manipulieren.

Die Bedrohung durch Tampering wird seitens der Cloud Security Alliance im aktuellen Dokument „The Notorious Nine Cloud Computing Top Threats 2013“ als eine kritische Bedrohung benannt.

Besondere Tampering-Attacken bzgl. des ADL für SaaS CRM

Für das Szenario „SaaS CRM“ kommen als privilegierte Tampering-Akteure der Subscriber End User (SEU), der Subscriber Administrator (SAD) und der Cloud Service Provider Administrator (CSA) oder auch Innentäter des ISP in Betracht. Dabei lassen sich vor allem folgende Tampering Einzelbedrohungsszenarien für das Access & Delivery Layer erkennen

1. Veränderung der Konfigurationsdaten der ADL Komponenten bzw. der Anwendungen
   01. Ein Angreifer erhält nach einer erfolgreichen Spoofing-Attacke Zugriff auf Konfigurationsdaten der ADL-Komponenten oder Anwendungen.
   02. Er ist in der Folge in der Lage, mit einer Veränderung (Manipulation) von Konfigurationsdaten nachfolgendes →Spoofing zu erleichtern, und damit auch ein erneutes, ggf. auch wirkungsvolleres Tampering (gestützt auf →Elevation of Privilege mit ggf. nachfolgendem →Information Disclosure), aber auch die korrekte Ausführung bzw. die Verfügbarkeit des Service insgesamt zu beeinträchtigen (→Denial of Service).
2. Datenmanipulation durch Hacking der CSP Architektur
   01. Ein Angreifer gelangt entweder nach erfolgreichem →Spoofing oder über eine unzureichend gesicherte Architektur/Infrastruktur des CSP direkt an die Datenhaltungsschichten der einzelnen Layer (Hacking einer ungenügend gesicherten und ohne ausreichende Identitätsprüfung von Außen erreichbaren Datenhaltungsschicht),
   02. Dadurch ist es dem Angreifer möglich, Kenntnis von Kundendaten zu erhalten (→Information Disclosure) und/oder Kundendaten zu manipulieren (→Tampering).
3. Datenmanipulation durch Abhören der Verbindungen
   01. ein Angreifer gelangt auf Grund einer unsicheren Verbindung zwischen dem SEU, dem ADL und nachgelagerter Schichten des CSP an die übermittelten Daten (→Information Disclosure).
   02. Dadurch ist es dem Angreifer nicht nur möglich, Kenntnis von Kundendaten zu erhalten (→Information Disclosure), sondern ggf. darüber hinaus, den Datenverkehr zwischen dem SEU und der Datenhaltungsschicht des CSP umzuleiten. Dadurch könnte der Angreifer mit einer falschen Identität (→ Spoofing) eines SEU die Daten anderer SEUs (in der Zeit, in der diese inaktiv sind) manipulieren und so großen Schaden anrichten.



Betroffene Sicherheitsanforderungen:												
ISM	01	02	03	04								
IFS	01	02	03	04	05	06	07	08	09	10	11	12
AES	01	02	03	04	05	06	07	08	09	10	11	12
NCS	01	02	03	04	05							
DSS	01	02	03	04	05	06	07	08	09			
PKI	01	02	03	04	05							
IDM	01	02	03	04	05	06						
SIM	01	02	03	04								
BCM	01	02	03	04								
PIM	01	02	03									
HRR	01	02										
SCM	01	02	03									
UIC	01	02										

Betroffene Prozesse						
SEU	01					
SEU	02					
SEU	03/	1	2	3	4	
SEU	04/	1	2	3	4	
SAD	01					
SAD	02					
SAD	03					
SAD	04					
SAD	05					
SAD	06					
SAD	07/	1	2	3		
CSP	01/	1	2			
CSP	02/	1	2	3		
CSP	03					
CSP	04/	1	2	3	4	
CSP	05					

4. Datenmanipulation auf Grund einer ungenügenden Trennung der Mandanten
   01. Eine unsichere Trennung der Systeme und Daten auf der Seite des CSP ermöglicht oder erleichtert Mandanten die Einsichtnahme (→Information Disclosure) und den Zugriff auf die Daten eines anderen Mandanten.
   02. Ein Angreifer gelangt aufgrund einer nicht hinreichend gesicherten Verbindung mit dem SEU und der Datenhaltungsschicht des CSP an die übermittelten Daten.
5. Datenmanipulation durch nicht kommunizierte, nicht abgestimmte Prozesse
   01. Im erweiterten Sinne kann auch ein nicht vorher mit dem Subscriber vereinbarte Datenwiederherstellung (im Rahmen eines Backup und Recovery Verfahrens) durch den CSP den Anschein des Tamperings erwecken. Dadurch erscheint dem SEU beim nächsten Login ein alter Sachstand, der dem SEU zunächst wie ein veränderter Sachstand erscheint.

Noch näher zu betrachtende Bereiche

In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

1. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure, d. h.:
   01. das Cloud Architekturkonzept des CSP, insbesondere bzgl. des User Portals und der Service Gateways sowie der Inter-Cloud Funktionalitäten,
   02. die Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP, des Subscribers und Sub-Providers, einschl. Berechtigungs- und Rollenkonzepte
   03. die Vertrags- und SLA-Gestaltung mit dem ISP durch die einzelnen Akteure.
2. Überprüfung der technischen Maßnahmen zur Validierung und Integritätsprüfung von persistenten Daten, sowie von Daten während des Transports
3. Authentifizierungs- und Autorisierungskonzepte des Subscribers und des CSP
4. Logging- und Log-Daten-Auswertungskonzepte (Aggregation und Monitoring sicherheitsrelevanter Ereignisse) des CSP

Restrisiken

- unzureichende Integritätsprüfungen von Daten auf der Seite des Subscribers,
- ungenügende Sicherung der Architektur und Kommunikation auf der Seite des Subscribers zum Übergabepunkt des CSP,
- unsicherer Umgang mit Benutzerkennung auf der Seite des Subscribers und des Sub-Providers,
- fahrlässiges Fehlverhalten der Mitarbeiter des Subscribers, des Sub-Providers, des ISP und der CSP Administratoren,
- Konfigurationsfehler der SAD und CSP Administroren,
- Szenarien „Höherer Gewalt“, welche den CSP zum sofortigen Handeln (Recovering von Daten) zwingen.

Repudiation im Access & Delivery Layer

Repudiation stellt eine nicht zu unterschätzende Bedrohungsfläche für das Access & Delivery Layer (ADL) dar. Im ADL wird der maßgeblich vom Subscriber aufkommende Datenverkehr angenommen. Im ADL erfolgt die Authentifizierung sowie nach erfolgreicher Anmeldung auch die Autorisierung der Nutzer bzgl. der Funktionalitäten und Zugriffe auf die SaaS CRM Anwendungen und den darin verarbeiteten/gespeicherten Daten. Werden diese Aktionen nicht ausreichend protokolliert (durch Logging der einzelnen Aktionen und den handelnden Akteuren), ist ein Angreifer ggf. in der Lage, seine eigentliche Identität und damit fahrlässige oder auch böswillige Handlungen (→Tampering, →Information Disclosure oder →Denial of Service) zu verschleiern.

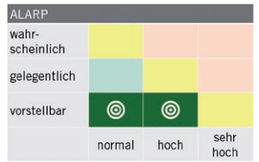
Repudiation wird möglich durch erfolgreiches →Spoofing bzw. wenn es einem Angreifer gelingt das Logging oder Log-Protokolle zu manipulieren oder durch Manipulation zu umgehen, beispielsweise durch →Tampering der Konfiguration relevanter ADL-Komponenten. Ist kein lückenloser Nachweis bzgl. erfolgter Anmeldungen, Zugriffe und erteilter Berechtigungen mittels eines geeigneten und strikten Loggings sichergestellt, so kann nicht nachgewiesen werden, welcher Benutzer in der SaaS CRM Anwendung welche Tätigkeiten wann durchgeführt hat und damit für welche Daten / Datenveränderungen verantwortlich ist. Das unzureichende oder gar fehlende Logging und die ggf. nicht ausreichende Trennung der Systeme und Anwendungen auf der Seite des CSP erleichtern es einem externen oder internen Angreifer nach erfolgreichem →Spoofing unerkannt und ggf. auch unbemerkt, Daten zu manipulieren (→Tampering) oder gar zu löschen (→Denial of Service).

Die Bedrohung durch Repudiation werden auch durch die Cloud Security Alliance unter die „Notorious Nine Cloud Computing Top Threats 2013“ eingeordnet.

Besondere Repudiation-Gefährdungen bzgl. des ADL für SaaS CRM

Für das Szenario „SaaS CRM“ kommen als privilegierte Repudation-Akteure der Subscriber End User (SEU), der Subscriber Administrator (SAD), der Cloud Service Provider Administrator (CSA), der Sub-Provider Administrator (SPA) oder auch ein Innentäter des ISP in Betracht. Dabei lassen sich vor allem folgende Repudiation-Einzelbedrohungsszenarien für das Access & Delivery Layer erkennen.

1. Unsichere Authentisierung
   01. Eine unsichere oder auch nur unzureichende Authentisierung erleichtert →Spoofing, ggf. auch →Elevation of Privilege und damit die verschleierte oder abstreitbare Ausführung unzulässiger oder auch böswilliger Aktionen.
   02. Eine unsichere oder auch nur unzureichende Authentisierung erleichtert die Umgehung von Sicherheitsmaßn. im Zugriff auf das ADL.
   03. Eine unsichere oder auch nur unzureichende Authentisierung beteiligter Komponenten, erleichtert den unbemerkten Austausch falsch oder auch böswillig konfigurierter Komponenten.
2. Unzureichende Protokollierung
   01. Eine unzureichende Protokollierung von Zugriffen erleichtert die Bestreitung fahrlässiger oder auch böswilliger Aktionen.
   02. Eine unzureichende Protokollierung und Auswertung der Protokolle erschwert die unverzügliche und angemessene Reaktion auf Sicherheitsvorfälle.
3. Unzureichender Schutz von Authentifikationsdaten
   01. Er erleichtert →Spoofing und damit die Verschleierung fahrlässiger oder auch böswilliger Aktionen.



Betroffene Sicherheitsanforderungen:												
ISM	01	02	03	04								
IFS	01	02	03	04	05	06	07	08	09	10	11	12
AES	01	02	03	04	05	06	07	08	09	10	11	12
NCS	01	02	03	04	05							
DSS	01	02	03	04	05	06	07	08	09			
PKI	01	02	03	04	05							
IDM	01	02	03	04	05	06						
SIM	01	02	03	04								
BCM	01	02	03	04								
PIM	01	02	03									
HRR	01	02										
SCM	01	02	03									
UIC	01	02										

Betroffene Prozesse						
SEU	01					
SEU	02					
SEU	03/	1	2	3	4	
SEU	04/	1	2	3	4	
SAD	01					
SAD	02					
SAD	03					
SAD	04					
SAD	05					
SAD	06					
SAD	07/	1	2	3		
CSP	01/	1	2			
CSP	02/	1	2	3		
CSP	03					
CSP	04/	1	2	3	4	
CSP	05					

4. Unzureichender Schutz von Protokolldaten
   01. Ein unzureichender Schutz von Protokolldaten erleichtert deren Manipulation und damit die Verschleierung fahrlässiger oder böswilliger Manipulationen.

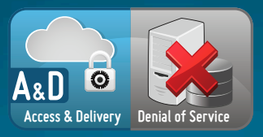
Noch näher zu betrachtende Bereiche

In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

1. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure, d. h.:
   01. das Cloud Architekturkonzept des CSP, insbesondere bzgl. des User Portals und der Service Gateways sowie der Inter-Cloud Funktionalitäten,
   02. die Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP, des Subscribers und Sub-Providers, einschl. Berechtigungs- und Rollenkonzepte,
   03. die Vertrags- und SLA-Gestaltung mit dem ISP durch die einzelnen Akteure.
2. Überprüfung der Logging- und der Protokollierungs Konzepte bzgl. aller in Frage kommender Verbindungs-, System- (einschließlich relevanter Dienste) und Nutzererereignissen, einschließlich der Konzepte und Prozesse bzgl. der Auswertung dieser Log-Daten und Protokolle, sowie bzgl. der bei Feststellung definierter, sicherheitsrelevanter Ereignisse erforderlichen Maßnahmen
3. Logging- und Log-Daten-Auswertungskonzepte (Aggregation und Monitoring sicherheitsrelevanter Ereignisse) des CSP
4. Überprüfung der Umsetzung und der Funktionsweise des Loggings und der Protokollierung auf den Systemen und Komponenten des Access & Delivery Layers
5. Authentifizierungs- und Autorisierungskonzept des Subscribers und des CSP

Restrisiken

- menschliches Fehlverhalten durch ungenügende Schulung oder Sensibilisierung hinsichtlich sicherheitsrelevanter Sachverhalte der Mitarbeiter des Subscribers, des Sub-Providers, des ISP und des CSP,
- Konfigurationsfehler der SAD und CSP Administratoren,
- unsicherer Umgang mit Benutzerkennung auf der Seite des Subscribers und des Sub-Providers.

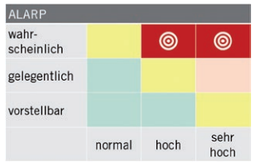


Denial of Service im Access & Delivery Layer

Denial of Service stellt in zweierlei Hinsicht eine kritische Bedrohungsfläche für das Access & Delivery Layer (ADL) dar. Einerseits wird es bzgl. der stetig wachsenden und immer komplexer werdenden Anforderungen für Cloud Service Provider immer schwerer, dass Business Modell / den Business Case „Cloud“ in betriebswirtschaftlich sinnvollem Umfang mit der jeweils erforderlichen Hardware zu betreiben (hier wären zu nennen: Ausfälle auf Grund von Überlastung oder Inkompatibilität der Hardware) und andererseits sind Cloud Infrastrukturen zunehmend Ziel möglicher Angriffe (beispielsweise Ausfälle auf Grund von DoS Attacken). Davon betroffen sind im Umfeld des Access & Delivery Layers insbesondere Netzwerkkomponenten und Kommunikationsendpunkte bzw. Web-Komponenten (Webserver und Webanwendungen) auf der Seite des CSP.

Abseits des Denial of Service auf Grund von Fehlkonfiguration bzw. Fehlverhalten durch Innentäter oder logischer Attacken durch externe Angreifer (entweder als reine DoS-Attacken oder Folge eines erfolgreichen →Spoofings), sind hierbei insbesondere auch Aspekte des physikalischen Zugriffs auf involvierte und relevante Komponenten sowie die ausreichende dynamische Bereitstellung ausreichender Ressourcen durch den CSP zu betrachten. Hinzu kommen mögliche Störungen oder Ausfälle der in der Verantwortung des ISP befindlichen Kommunikationswege. Insbesondere Innentäter mit Administratorrechten sind in besonderer Weise für den Zutritt und den Zugriff auf die entsprechenden Komponenten des ADL privilegiert.

Die Dienstverhinderung und der Datenverlust auf Grund von Denial of Service-Bedrohungen sind auch seitens der Cloud Security Alliance in „The Notorious Nine Cloud Computing Top Threats 2013“ als zunehmende und häufig auftretende Bedrohung benannt.



Betroffene Sicherheitsanforderungen:												
ISM	01	02	03	04								
IFS	01	02	03	04	05	06	07	08	09	10	11	12
AES	01	02	03	04	05	06	07	08	09	10	11	12
NCS	01	02	03	04	05							
DSS	01	02	03	04	05	06	07	08	09			
PKI	01	02	03	04	05							
IDM	01	02	03	04	05	06						
SIM	01	02	03	04								
BCM	01	02	03	04								
PIM	01	02	03									
HRR	01	02										
SCM	01	02	03									
UIC	01	02										

Betroffene Prozesse						
SEU	01					
SEU	02					
SEU	03/	1	2	3	4	
SEU	04/	1	2	3	4	
SAD	01					
SAD	02					
SAD	03					
SAD	04					
SAD	05					
SAD	06					
SAD	07/	1	2	3		
CSP	01/	1	2			
CSP	02/	1	2	3		
CSP	03					
CSP	04/	1	2	3	4	
CSP	05					

Besondere Denial of Service-Gefährdungen bzgl. des ADL für SaaS CRM

Für das Szenario „SaaS CRM“ kommen als privilegierte Denial of Service-Akteure der Subscriber End User (SEU), der Subscriber Administrator (SAD), der Cloud Service Provider Administrator (CSA), der Sub-Provider Administrator (SPA) oder auch Innentäter des ISP in Betracht. Dabei lassen sich vor allem folgende Denial of Service-Einzelbedrohungsszenarien für das Access & Delivery Layer erkennen:

1. Ausfall/Störung beim ISP
   01. Ein Ausfall oder eine Störung technischer Komponenten beispielsweise durch Unwetter oder Wartungsarbeiten, führt bei einer unzureichenden redundanten Auslegung der Netzinfrastruktur zwangsläufig zu einer Nichterreichbarkeit des SaaS CRM Service,
   02. Eine unzureichende kryptographische Sicherung von Kommunikationswegen und -endpunkten erleichtert DoS-Angriffe oder andere böswillige Störungen der Kommunikation mit zwischen Serviceprovider und Subscriber.
   03. Eine unzureichende Bereitstellung von Netzwerkkapazitäten (beispielsweise Bandbreite, Router, etc.) kann bei einem erhöhten Zugriff von Nutzern und/oder Mandanten des SaaS CRM Service zumindest zu einer partiellen Nichtverfügbarkeit des Dienstes führen.
2. Ausfall von Komponenten im ADL
   01. Störungen oder der Ausfall der Funktion von Gateways oder Anwendungen im ADL durch Konfigurationsfehler, Wartungsarbeiten, Programmfehler oder auch erfolgreich ausgeführte Attacken haben für den Subscriber eine unerwartete Nichterreichbarkeit der SaaS CRM Dienstes zur Folge.
3. Unsichere, nicht redundant gestaltete Architektur
   01. Eine unsichere (nicht ausreichend vor DoS-Attacken etc. geschützte) sowie nicht ausreichend redundant gestaltete Architektur/Infrastruktur auf der Seite des CSP führen bereits bei einem einfachen technischen Ausfall zu einer zumindest partiellen Nichterreichbarkeit des SaaS CRM Service.
4. Dienstverweigerung durch Sperrung von Benutzerkonten
   01. Fahrlässiges Fehlverhalten der SEU, beispielsweise ein mehrfach fehlerhaftes Login, kann für den SEU einen technischen «Denial of Service» durch die Sperrung seines SaaS CRM-Benutzerkontos zur Folge haben.
   02. Fahrlässiges Fehlverhalten durch Administratoren des Subscribers oder CSP, beispielsweise bei einer Änderung vom Konfigurationsdaten, kann zu einer Sperrung von Benutzerkonten führen.
   03. Ebenso können böswillige Innentäter (des Subscribers wie des CSP), auf der Basis eines erfolgreichen →Spoofings und in der Folge eines →Elevation of Privilege eine Sperrung von Benutzerkonten und damit eine Nichtverfügbarkeit des Service herbeiführen.
5. Ausfall durch nicht kommunizierte, nicht abgestimmte Prozesse
   01. Die Durchführung von nicht vorher mit dem Subscriber abgestimmten und vereinbarten Wartungsarbeiten durch den CSP haben können die Nichtverfügbarkeit von Komponenten und Funktionen sowie ggf. der kompletten SaaS CRM-Anwendung für den SEU zur Folge haben.

Noch näher zu betrachtende Bereiche

In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

1. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure, d. h.:
   01. das Cloud Architekturkonzept des CSP, insbesondere bzgl. des User Portals und der Service Gateways sowie der Inter-Cloud Funktionalitäten,
   02. die Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP, des Subscribers und Sub-Providers, einschl. Berechtigungs- und Rollenkonzepte,
   03. die Vertrags- und SLA-Gestaltung mit dem ISP durch die einzelnen Akteure.
2. Disaster Recovery- und Notfallkonzepte des CSP,
3. Konzepte des CSP bzgl. des Einsatzes von IDS- und IPS Systemen,
4. Konzepte des CSP hinsichtlich der Aggregation und des Monitoring sicherheitsrelevanter Ereignisse.

Restrisiken

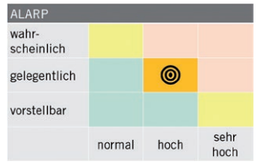
- unsichere Kommunikationsendpunkte auf der Seite des Subscribers (DoS Angriffe können sich auch gegen den Subscriber richten),
- unzureichende Schulung von Mitarbeitern beim CSP und Subscriber,
- unsichere oder fehlerhafte Konfiguration von Sicherheitskomponenten,
- unzureichende Aggregation sicherheitsrelevanter Ereignisse beim CSP,
- unzureichende oder fehlende Maßnahmen bzgl. Szenarien „Höherer Gewalt“,
- unzureichende Kommunikation zwischen CSP und Subscriber bezüglich Wartungsmaßnahmen oder Änderung von Zugangsmechanismen.

Elevation of Privilege im Access & Delivery Layer

Elevation of Privilege ist eine Bedrohungsfläche für das Access & Delivery Layer (ADL) deren Risikopotenzial maßgeblich von der Durchsetzung ausreichender und zuverlässiger Authentisierungs- und Autorisierungskonzepte und -maßnahmen, sowie der strikten Trennung von Zuständigkeiten (Separation of Duties) bestimmt wird. Erfolgr. Elevation of Privilege ermöglicht oder erleichtert den unbefugten und unbemerkten Zugriff auf beispielsweise Authentifikationsdaten von Nutzern, Kundendaten oder auch Konfigurationsdaten von Komponenten des ADL und damit →Spoofing, →Tampering, →Information Disclosure oder →Denial of Service . Für externe Angreifer ist Elevation of Privilege vornehmlich Folge erfolgreichen →Spoofings. Für Innentäter kommen sowohl böswillige und mittels →Spoofing verschleierte Angriffe, aber auch fahrlässiges Verhalten in Betracht. Zu Letzterem gehört insbesondere die unzureichende Kontrolle der Zuweisung von Nutzerkonten und Zugriffsberechtigungen. Nicht auszuschließen ist beispielsweise die nicht erfolgte Löschung der Benutzerkonten ausgeschiedener Mitarbeitern oder auch die fahrlässige Preisgabe von Authentifikationsinformationen.

Eine unzulässige oder unbemerkte Erweiterung von Berechtigungen im ADL kann dazu führen, dass ein Angreifer auf sicherheitsrelevante Komponenten und Daten zugreifen kann. Eine solche Erweiterung von Berechtigungen erleichtert oder ermöglicht also weitere Attacken wie beispielsweise →Tampering, →Information Disclosure oder → Denial of Service.

Elevation of Privilege wird auch seitens der Cloud Security Alliance mehrfach in „The Notorious Nine Cloud Computing Top Threats 2013“ als eine ernstzunehmende Bedrohung für Cloud-Umgebungen benannt.



Betroffene Sicherheitsanforderungen:												
ISM	01	02	03	04								
IFS	01	02	03	04	05	06	07	08	09	10	11	12
AES	01	02	03	04	05	06	07	08	09	10	11	12
NCS	01	02	03	04	05							
DSS	01	02	03	04	05	06	07	08	09			
PKI	01	02	03	04	05							
IDM	01	02	03	04	05	06						
SIM	01	02	03	04								
BCM	01	02	03	04								
PIM	01	02	03									
HRR	01	02										
SCM	01	02	03									
UIC	01	02										

Betroffene Prozesse						
SEU	01					
SEU	02					
SEU	03/	1	2	3	4	
SEU	04/	1	2	3	4	
SAD	01					
SAD	02					
SAD	03					
SAD	04					
SAD	05					
SAD	06					
SAD	07/	1	2	3		
CSP	01/	1	2			
CSP	02/	1	2	3		
CSP	03					
CSP	04/	1	2	3	4	
CSP	05					

Besondere Elevation of Privilege-Gefährdungen bzgl. des ADL für SaaS CRM

Für das Szenario „SaaS CRM“ kommen als privilegierte Elevation of Privilege-Akteure der Subscriber End User (SEU), der Subscriber Administrator (SAD), der Cloud Service Provider Administrator (CSA), der Sub-Provider Administrator (SPA) in Betracht. Dabei lassen sich vor allem folgende Elevation of Privilege Einzelbedrohungsszenarien für das Access & Delivery Layer erkennen:

1. Missbrauch von Berechtigungen
   01. Ein unbemerkter Missbrauch von Berechtigungen kann die Manipulation von Benutzerkonten (→Tampering) oder die unbefugte Kenntnisnahme Kundendaten (→Information Disclosure) ermöglichen oder erleichtern.
   02. Ein unbemerkter Missbrauch von Berechtigungen kann den Zugriff auf Authentifikations- oder Konfigurationsdaten (→Information Disclosure) ermöglichen, ein →Tampering dieser Daten erleichtern und in der Folge zu einer Beeinträchtigung des Service (→Denial of Service) führen.
   03. Sollte ein SEU Zugriff auf die Benutzerverwaltung des (Self-Service) User Portals haben oder erlangen und somit die eigenen Berechtigungen verwalten können bzw. sich selber weitere Berechtigungen zuweisen können, so kann dieser SEU dann ggf. auf alle SaaS CRM-(Kunden)-Daten zugreifen und die diese verändern (→Tampering), veröffentlichen (→Information Disclosure) oder löschen (→Denial of Service).
2. Aneignung unbegründeter Berechtigungen durch Social Engineering
   01. Ein Innentäter kann unter Benennung fiktiver Begründungen den Helpdesk/User-Support davon überzeugen, dass ihm erweiterte Rechte zugewiesen werden und somit der unbefugte Zugriff auf sensible Kundendaten bzw. andere sicherheitsrelevante Daten im ADL möglich wird.

Noch näher zu betrachtende Bereiche

In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

3. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure, d. h.:
   01. das Cloud Architekturkonzept des CSP, insbesondere bzgl. des User Portals und der Service Gateways sowie der Inter-Cloud Funktionalitäten,
   02. die Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP, des Subscribers und Sub-Providers, einschließlich der Berechtigungs- und Rollenkonzepte,
   03. die Vertrags- und SLA-Gestaltung mit dem ISP durch die einzelnen Akteure.
4. Prozesse bzgl. der Verwaltung von Subscriber Mandanten, insbesondere bzgl. der Änderung, Anpassung und Kontrolle von Nutzerautorisierungen,
5. Überprüfung der Logging- und der Protokollierungs Konzepte bzgl. aller in Frage kommender Verbindungs-, System- (einschließlich relevanter Dienste) und Nutzereignissen, einschließlich der Konzepte und Prozesse bzgl. der Auswertung dieser Log-Daten und Protokolle, sowie bzgl. der bei Feststellung definierter Ereignisse erforderlichen Maßnahmen,
6. Logging- und Log-Daten-Auswertungskonzept (Aggregation und Monitoring sicherheitsrelevanter Ereignisse) des CSP,
7. Überprüfung der Umsetzung und der Funktionsweise des Loggings und der Protokollierung auf den Systemen und Komponenten des Access & Delivery Layers,
8. Authentifizierungs- und Autorisierungskonzept des Subscribers und des CSP.

Restrisiken

- menschliches Fehlverhalten des SEU bzw. des SAD des Subscribers
- fehlende bzw. ungenügende Prozesse zur Erteilung, Genehmigung und Kontrolle von Nutzerkonten und Autorisierungen beim Subscriber,
- fehlende bzw. ungenügende Prozesse zur Erteilung, Genehmigung und Kontrolle von Nutzerkonten und Autorisierungen beim CSP,
- unzureichende Schulung des Personals bezüglich Social Engineering,
- unzureichende Trennung und Kontrolle von Zuständigkeiten (→Separation of Duties).

Information Disclosure im Access & Delivery Layer

Information Disclosure ist hinsichtlich der zu erwartenden Risiken die wohl schwerwiegendste Bedrohungsfläche für das Access & Delivery Layer (ADL). Denn, obgleich gemäß der Definition der IETF im ADL keine Kunden- bzw. Produktivdaten vorgehalten werden sollten, befinden sich im Access & Delivery Layer Konfigurationsdaten der ADL-Komponenten und des User Portals. Diese Informationen sind, nicht nur hinsichtlich Information Disclosure, als besonders schützenswert zu definieren. Eine unbefugte Kenntnisnahme darf nicht möglich sein, da die Kenntnis und das Wissen um diese Informationen als Grundlage für weitere Bedrohung und Gefährdungen dienen kann (beispielsweise →Tampering oder gezieltes →Information Disclosure, →Repudiation, →Denial of Service, →Elevation of Privilege), um den Zugriff auf die (Kunden) Daten in der Datenhaltungsschicht zu erlangen.

Information Disclosure / Data Breaches wird durch die Cloud Security Alliance in „The Notorious Nine Cloud Computing Top Threats 2013“ als schwerwiegendste und stark zunehmende Bedrohung auf Platz 1 geführt.

Besondere Information Disclosure-Gefährdungen bzgl. des ADL für SaaS CRM

Für das Szenario „SaaS CRM“ kommen als privilegierte Information Disclosure-Akteure alle Administratoren (der Subscriber Administrator (SAD), der Cloud Service Provider Administrator (CSA), der Sub-Provider Administrator (SPA)) in Betracht, da diese auf Grund der den Administratoren-Konten zugeordneten Berechtigungen das Ausmaß dieser Gefährdung auf alle Daten in der SaaS CRM Anwendung auszudehnen vermögen. Das schließt natürlich nicht gezielte Angriffe durch Subscriber End User (SEU) oder externe Täter aus, sofern es ihnen gelingt, sich mit einem erfolgreichen →Spoofing-Angriff besondere Zugriffsrechte anzueigenen (→Elevation of Privilege). Es lassen sich vor allem folgende Information Disclosure-Einzelbedrohungsszenarien für das Access & Delivery Layer erkennen:

1. Einsatz von ungeeignetem, nicht sicherheitsüberprüftem Personal

01. Der Einsatz von fachlich ungeeignetem und/oder unzureichend geschultem und/oder unzureichend sicherheitsüberprüftem Personal an Schlüsselpositionen (Administration von Hard- und Softwarekomponenten oder Kommunikationsverbindungen) birgt ein großes Gefahrenpotential und Risiko beispielsweise im unsichereren Umgang mit vertraulichen, schützenswerten Daten, und
02. erleichtert böswillige interne Angriffe.
03. Hinzu kommt, dass böswillige interne Angreifer ausgerüstet mit Administratorrechten viel leichter imstande sind, sich unbefugt zusätzliche Rechte anzueignen (→Elevation of Privilege) oder Angriffe zu verschleiern (→Repudiation).

2. Unsichere Datenhaltungsnetzwerke und -systeme

01. Ein Angreifer erlangt auf Grund unsicherer Datenhaltungsnetzwerke und -systeme des CSP, entweder unter Ausnutzung einer unwahren Identität (→Spoofing) oder durch Hacking bzw. Hijacking, Kenntnis von Kundendaten (→Information Disclosure).
02. Angreifern ist es auf Grund unzureichender bzw. unsicherer Authentisierungs und Autorisierungsmaßnahmen durch →Spoofing möglich, unbefugt Kenntnis von Kundendaten zu erlangen (→Information Disclosure), Daten zu verändern (→Tampering), oder gar zu löschen (→Denial of Service).

ALARP

	normal	hoch	sehr hoch
wahrscheinlich			
gelegentlich			
vorstellbar		◎	

Betroffene Sicherheitsanforderungen:

ISM	01	02	03	04							
IFS	01	02	03	04	05	06	07	08	09	10	11	12
AES	01	02	03	04	05	06	07	08	09	10	11	12
NCS	01	02	03	04	05							
DSS	01	02	03	04	05	06	07	08	09			
PKI	01	02	03	04	05							
IDM	01	02	03	04	05	06						
SIM	01	02	03	04								
BCM	01	02	03	04								
PIM	01	02	03									
HRR	01	02										
SCM	01	02	03									
UIC	01	02										

Betroffene Prozesse

SEU	01				
SEU	02				
SEU	03/	1	2	3	4
SEU	04/	1	2	3	4
SAD	01				
SAD	02				
SAD	03				
SAD	04				
SAD	05				
SAD	06				
SAD	07/	1	2	3	
CSP	01/	1	2		
CSP	02/	1	2	3	
CSP	03				
CSP	04/	1	2	3	4
CSP	05				

3. Ungeeignetes Rechte- und Rollenkonzept

01. Auf Grund unzureichender oder unsicherer Rollen- und Berechtigungskonzepte, unzureichender Trennung von Zuständigkeiten, erlangt ein Innentäter bzw. nach erfolgreichem →Spoofing auch ein externer Angreifer Nutzerberechtigungen, welche die uneingeschränkte Kenntnisnahme und Veröffentlichung von Kundendaten gestützt auf gestohlene oder gefälschte Identitäten erlauben.

4. Fehlende Verschlüsselungsverfahren

01. Durch fehlende oder unzureichende Verschlüsselungsverfahren auf der Kommunikations- oder Datenebene wird es Angreifern ermöglicht, Daten auf diesen Ebenen abzugreifen und für weitere Angriffe auf andere Komponenten zu benutzen.
02. Dies betrifft insbesondere Administratoren des CSP und des Sub-Providers, da diese ggf. einen privilegierten Zugriff auf Endgeräte und Datenspeicher im Physical Resource Layer haben.

Noch näher zu betrachtende Bereiche

1. In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

01. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure, d. h.:
02. das Cloud Architekturkonzept des CSP, insbesondere bzgl. des User Portals und der Service Gateways sowie der Inter-Cloud Funktionalitäten,
03. die Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP, des Subscribers und Sub-Providers, einschl. Berechtigungs- und Rollenkonzepte,
04. die Vertrags- und SLA-Gestaltung mit dem ISP durch die einzelnen Akteure.

2. Verschlüsselungskonzepte des Subscribers und des CSP

3. Authentifizierungs- und Autorisierungskonzepte des Subscribers und des CSP

4. Logging- und Log-Daten-Auswertungskonzepte (Monitoring und Aggregation von Zugriffen und anderen sicherheitsrelevanten Ereignissen) des CSP

Restrisiken

- unsicherer Umgang mit Benutzerkennung auf der Seite des Subscribers und des Sub-Providers,
- fahrlässiges sowie vorsätzlich böswilliges Verhalten auf der Seite des Subscribers, des Sub-Providers, des ISP und durch CSP Administratoren,
- nicht aufgelöste Konflikte zwischen Compliance-Anforderungen und Datenschutzrichtlinien auf der Seite des Subscribers und den etablierten Sicherheitsmaßnahmen des CSP,
- fehlende bzw. ungenügende Anweisungen und Schulungen bzgl. des Umgangs mit sensiblen Daten auf der Seite des Subscribers und des CSP,
- technisches Versagen der für die Verschlüsselung verantwortlichen Komponenten auf der Seite des Subscribers und des CSP.

Ausfall der externen Kommunikationsverbindung

Fällt die externe Kommunikationsverbindung zum Cloud-Service aus, können die Akteure des Kunden (SEU und SAD) nicht auf den Cloud-Service zugreifen, auch wenn dieser selbst einwandfrei funktioniert. DoS ist dabei in mehrerer Hinsicht eine ernstzunehmende und mehrdimensionale Bedrohungsfläche für eine SaaS CRM Lösung. Einerseits müssen für eine valide Risikobewertung alle relevanten Aspekte bzgl. der Sicherheit der Netzwerkkomponenten und Kommunikationsendpunkte auf den Seiten des Subscribers und des CSP betrachtet werden, andererseits sind alle in Frage kommenden Aspekte bzgl. der durch den ISP bereitgestellten Kommunikationslösung von gleichrangiger Bedeutung. Hierzu zählen nicht nur die Themen wie Redundanz und Hochverfügbarkeit, Einsatz ausreichender und bzgl. der Kommunikationsbedürfnisse geeigneter Hardware, Schutz und Überwachung der relevanten Kommunikationskomponenten, sondern auch die Details bzgl. der Vertrags- und SLA-Gestaltung für die genutzte Kommunikationslösung durch die jeweiligen Akteure (Vertragspartner).

Denial of Service kann sowohl eine Folge von logischen Attacken externer Angreifer (entweder als reine DoS-Attacken oder Folge eines erfolgreichen →Spoofings) auf die relevanten Komponenten des Subscribers, CSP oder ISP sein, aber auch auf Grund von Fehlkonfiguration bzw. Fehlverhalten durch Innentäter, einschließlich der Berücksichtigung des physikalischen Zugriffs dieser auf involvierte und relevante Komponenten hin, auftreten. Darüberhin. kann DoS auch das Ergebnis von Szenarien höherer Gewalt bzw. nicht zu erwartenden Ereignissen sein (beispielsweise ein Erdarbeitsgerät zerstört eine Verbindungsader des ISP oder durch Umwelterereignisse sind relevante Verteilerknoten nicht mehr in Betrieb bzw. einzelne Komponenten des ISP entlang dieser Kommunikationsverbindung weisen eine Störung / einen Defekt auf oder fallen aus unterschiedlichsten Gründen aus).

Darüber hinaus sind Innentäter mit Administratorrechten in besonderer Weise für den Zutritt und den Zugriff auf die entsprechenden Komponenten des ADL privilegiert.

Die Dienstverhinderung und der Datenverlust auf Grund von Denial of Service-Bedrohungen sind auch seitens der Cloud Security Alliance in „The Notorious Nine Cloud Computing Top Threats Is häufig auftretende kommende Bedrohung benannt.

Besondere Denial of Service-Gefährdungen bzgl. der Kommunikationsverbindung SEU-ADL

Für das Szenario „SaaS CRM“ kommen als privilegierte Denial of Service-Akteure der Subscriber Administrator (SAD), der Cloud Service Provider Administrator (CSA) oder auch Innentäter des ISP in Betracht. Dabei lassen sich vor allem folgende Denial of Service-Einzelbedrohungsszenarien für die Kommunikationsverbindung SEU-ADL erkennen:

1. Ausfall/Störung beim ISP

01. Ein Ausfall oder eine Störung techn. Komponenten (beispielsweise durch technisches Versagen, Unwetter oder Wartungsarbeiten), führt bei einer unzureichenden redundanten Auslegung der Netzinfrastruktur zwangsläufig zu einer Nichterreichbarkeit des SaaS CRM Service.
02. Eine unzureichende kryptographische Sicherung von Kommunikationswegen und -endpunkten erleichtert DoS-Angriffe oder andere böswillige Störungen der Kommunikation mit zwischen Serviceprovider und Subscriber.
03. Eine unzureichende Bereitstellung von Netzwerkkapazitäten (beispielsweise Bandbreite, Router, etc.) kann bei einem erhöhten Zugriff von Nutzern und/oder Mandanten des SaaS CRM Service zumindest zu einer partiellen Nichtverfügbarkeit des Dienstes führen.
04. Darüberhin. können auch fehlerhafte Konfigurationen auf den Komponenten bzgl. der durch den ISP bereitgestellten Kommunikationslösung verursacht durch unbewusst oder auch bewusst fahrlässiges Fehlverhalten seitens der Administratoren des ISP zu Ausfällen führen.

2. Unsichere, nicht redundant gestaltete Architektur

01. Eine unsichere (nicht ausreichend vor DoS-Attacken etc. geschützte) sowie nicht ausreichend redundant gestaltete Architektur/Infrastruktur bzgl. der durch den ISP bereitgestellten Kommunikationslösung für den Subscriber und/oder CSP führen bereits bei einem einfachen technischen Ausfall zu einer zumindest partiellen Nichterreichbarkeit des SaaS CRM Service.
02. Darüberhin. kann auch eine ungeeignete Verkabelung zu einem DoS Bedrohungsszenario führen. So ist beispielsweise eine zweite, separate Hauseinführung als Backup bzgl. der primär genutzten Kommunikationsverbindung unzweckmäßig, wenn diese Backup-Leitung auf dem gleichen APN der Primärverbindung angeschlossen ist und keine eigene, von der Primärleitung getrennte Trassen- bzw. Wegführung aufweist, da bei Ausfall dieses Anschlusspunktes des ISP dann auch die Backup-Leitung betroffen wäre.

3. Ausfall durch nicht kommunizierte, nicht abgestimmte Prozesse

01. Die Durchführung von Wartungsarbeiten etc. durch den ISP, welche vorher nicht mit den die bereitgestellte Kommunikationslösung nutzenden Akteuren abgestimmt und vereinbart worden sind. h.ben ggf. die Nichtverfügbarkeit der für den Subscriber entfernten Cloud-Services zur Folge.

ALARP

	normal	hoch	sehr hoch
wahrscheinlich			
gelegentlich		◎	
vorstellbar			

Betroffene Sicherheitsanforderungen:

ISM	01	02	03	04							
IFS	01	02	03	04	05	06	07	08	09	10	11	12
AES	01	02	03	04	05	06	07	08	09	10	11	12
NCS	01	02	03	04	05							
DSS	01	02	03	04	05	06	07	08	09			
PKI	01	02	03	04	05							
IDM	01	02	03	04	05	06						
SIM	01	02	03	04								
BCM	01	02	03	04								
PIM	01	02	03									
HRR	01	02										
SCM	01	02	03									
UIC	01	02										

Betroffene Prozesse

SEU	01				
SEU	02				
SEU	03/	1	2	3	4
SEU	04/	1	2	3	4
SAD	01				
SAD	02				
SAD	03				
SAD	04				
SAD	05				
SAD	06				
SAD	07/	1	2	3	
CSP	01/	1	2		
CSP	02/	1	2	3	
CSP	03				
CSP	04/	1	2	3	4
CSP	05				

Noch näher zu betrachtende Bereiche

In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

1. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure, d. h.:

01. das Cloud Architekturkonzept des CSP, insbesondere bzgl. der Kommunikationsendpunkte im ADL,
02. die Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP und des Subscribers bzgl. Redundanz, Hochverfügbarkeit und Ausfallsicherheit der Kommunikationsverbindungen,
03. die Vertrags- und SLA-Gestaltung mit dem ISP durch die einzelnen Akteure

2. Disaster Recovery- und Notfallkonzepte des CSP und des ISP,

3. Konzepte des ISP bzgl. Redundanz und Hochverfügbarkeit bzw. Ausfallsicherheit

Restrisiken

- unsichere Kommunikationsendpunkte auf der Seite des Subscribers (DoS Angriffe können sich auch gegen den Subscriber richten),
- unsichere oder auch fehlerhafte Konfiguration von Sicherheits- und Kommunikationskomponenten,
- unzureichende oder fehlende Maßnahmen bzgl. Szenarien „Höherer Gewalt“,
- unzureichende Kommunikation zwischen ISP und CSP, sowie Subscriber bezüglich Wartungsmaßnahmen oder Änderung von Zugangsmechanismen.

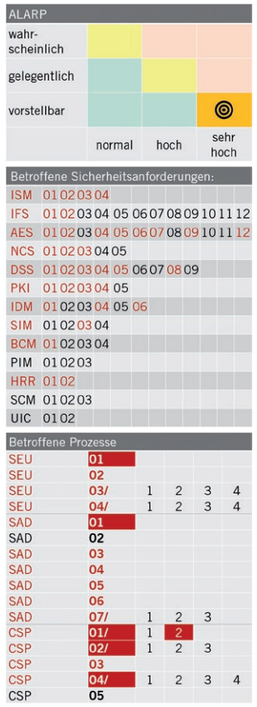
Tampering im Cloud Service Layer

Tampering stellt für das Cloud Service Layer (CSL) eine schwerwiegende Bedrohungsfläche dar, da es eine Gefährdung aller auf dem CSL befindlichen Konfigurationsdaten der in die Bereitstellung des Service involvierter Ressourcen bedeutet. Ein erfolgreicher Tampering-Angriff kann sich maßgeblich auf sämtliche in den Kommunikationsfluss im orchestrierten SaaS CRM Service involvierten Ressourcen auswirken. Ausgenommen fahrlässige Handlungen, ist ein erfolgreiches →Spoofing für externe wie für interne Angreifer Voraussetzung für Tampering. Dabei sind natürlich mit Administratorrechten ausgestattete Innentäter in besonderer Weise für den Zugriff auf Konfigurationsdaten des CSL und damit mittelbar die Orchestration der für die Ausführung des SaaS CRM Service erforderlichen Ressourcen privilegiert.

Die Bedrohung durch Tampering wird seitens der Cloud Security Alliance in „The Notorious Nine Cloud Computing Top Threats 2013 grundsätzlich als eine der großen, weil kritischen Bedrohungen benannt.

Besondere Tampering-Attacken bzgl. des CSL für SaaS CRM

Für das Szenario „SaaS CRM“ kommen als privilegierte Tampering-Akteure der Subscriber End User (SEU) bzgl. der Kundendaten, der Subscriber Administrator (SAD) und der Cloud Service Provider Administrator (CSA) bzgl. der Konfigurationsdaten involvierter der Anwendungen und Ressourcen, sowie der Sub-Provider Administrator (SPA) bzgl. der im CSL zur Verwendung kommenden und durch den Sub-Provider bereitgestellten Ressourcen in Betracht. Dabei lassen sich vor allem folgende Tampering Einzelbedrohungsszenarien für das Cloud Service Layer erkennen:



1. Datenmanipulation durch unsichere Schnittstellen

Unsichere Schnittstellen bedeuten in diesem Zusammenhang, dass

01. diese unzureichend kryptographisch gesichert sind,
02. diese nicht überwacht werden bzw. ihre auf einem Dienst basierende Funktion und die über die Schnittstelle erfolgende Kommunikation nicht selbst überwachen od.,
03. dass diese Schnittstellen unsicher konfiguriert sind (beispielsweise ein unsicheres Protokoll für die Kommunikation nutzen) od.
04. weil diese Schnittstellen nicht im Sicherheitskonzept des CSP vorkommen, imstande sind, Daten an der Sicherheitsarchitektur vorbei direkt mit den durch sie angebundenen Anwendungen kommunizieren.
05. Sollte eine solche Schnittstelle also beispielsweise jeden ankommenden Datenverkehr, welcher das zur Kommunikation benötigte Protokoll aufweist, direkt an die dahinter betriebene Anwendung oder Datenbank mit Lese- und Schreibberechtigung weiterleiten, ohne an Hand von detaillierten, sehr anwendungsspezifischen Kriterien (beispielsweise ob es sich um einen erlaubten Absender handelt, welche Lese- oder Schreibberechtigungen dem Absender zugeordnet sind etc.) zu überprüfen, wie mit diesem Daten verfahren werden soll, könnte ein potenzieller Angreifer über diese Schnittstelle manipulierte Daten nahezu unbemerkt in die dahinter befindliche Anwendung oder Datenbank einbringen.
06. Sollte eine solche Schnittstelle den relevanten Datenverkehr zudem unverschlüsselt kommunizieren (Verschlüsselung hier beispielsweise via XML-Encryption), so ist es einem potentiellen Angreifer einfach möglich, Schnittstellen-spezifische Anforderungen an Hand einer Analyse des übermittelten Datenverkehrs festzustellen.

2. Datenmanipulation durch Hacking der CSP Architektur

01. Ein Angreifer gelangt entweder nach erfolgreichem →Spoofing oder über die unzureichend gesicherte Architektur des CSP direkt an die Datenhaltungsschichten der einzelnen Layer (→Hacking),
02. Dadurch ist es dem Angreifer möglich, Kenntnis von Kundendaten zu erhalten (→Information Disclosure) und/oder Kundendaten zu manipulieren (→Tampering).

3. Datenmanipulation auf Grund einer ungenügenden Trennung der Mandanten

01. Eine unsichere Trennung der Ressourcen und Daten auf der Seite des CSP ermöglicht oder erleichtert ggf. Administrator eines Subscribers die Einsichtnahme (→Information Disclosure) und den Zugriff auf sowie die Manipulation (→Tampering) von Daten eines anderen Mandanten.

4. Datenmanipulation durch Eskalation von Zugriffsrechten

01. Eine unzureichende Trennung von Zugriffsrechten und/oder Autorisierung beim Zugriff auf eine Managementkonsole für das CMP erleichtert Innentätern den Zugriff auf Kundendaten →Elevation of Privilege.

Noch näher zu betrachtende Bereiche

In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

1. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure, d. h.:

01. das Cloud Architekturkonzept des CSP, insbesondere bzgl. der genutzten Schnittstellen und Kommunikationsverbindungen zwischen den in die Bereitstellung des Service involvierten Ressourcen
02. Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP, des Subscribers und Sub-Providers, einschließlich Berechtigungs- und Rollenkonzepte auf Managementkonsolen des CSP, sowie des Konzepts zur sicheren Kommunikation über Schnittstellen

2. Überprüfung der Prozesse bzgl. der Validierung und bzgl. der Integritätsprüfung von persistenten Daten, sowie Daten während des Transports, einschließlich dazugehörender API und anderer Schnittstellen

3. Authentifizierungs- und Autorisierungskonzept des Subscribers und des CSP

4. Logging- und Log-Daten-Auswertungskonzept (Aggregation und Monitoring sicherheitsrelevanter Ereignisse) des CSP

Restrisiken

- unzureichende Integritätsprüfungen und Schutz transportierter (kommunizierter) Daten,
- unsicherer Umgang mit Benutzerkennung auf der Seite des Subscribers und des Sub-Providers,
- fahrlässiges Fehlverhalten von mit Administratorrechten ausgestatteten Mitarbeitern des Subscribers, des Sub-Providers, des ISP und des CSP,
- Konfigurationsfehler der SAD und CSL, beispielsweise nach Wartungsarbeiten, Updates oder dem Austausch von Komponenten,
- Szenarien „Höherer Gewalt“, die zum Ausfall oder Störung des CSL führen.

Information Disclosure im Cloud Service Layer

Information Disclosure stellt für das Cloud Service Layer (CSL) die größte Bedrohungsfläche dar. Gemäß Cloud-Stack der IETF befinden sich im CSL die durch den Subscriber genutzten Cloud Anwendungen und deren Schnittstellen zu weiteren Anwendungen und/oder Datenbanken. Damit betrifft die Gefährdung durch Information Disclosure im CSL nicht nur Konfigurations- und Prozessdaten involvierter Anwendungen und Schnittstellen, sondern auch die in den Anwendungen verarbeiteten und über die Schnittstellen kommunizierten Kundendaten. Erfolgr. Information Disclosure im CSL wird möglich oder erleichtert

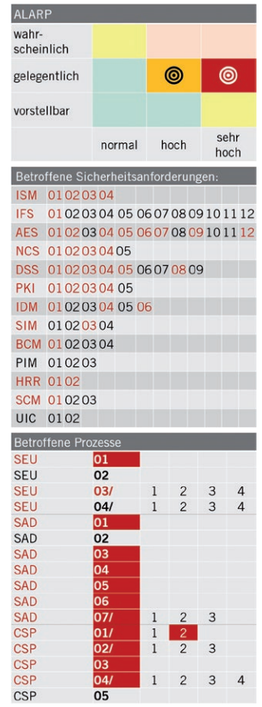
- nach einem erfolgreichen →Spoofing,
- durch privilegierte, d. h. mit Administratorrechten ausgestattete Innentäter,
- durch unzureichende oder unsichere Trennung von Mandanten sowie
- aufgrund von Konfigurationsfehlern im CSL.

Das Information Disclosure wird durch die Cloud Security Alliance in „The Notorious Nine Cloud Computing Top Threats 2013 als schwerwiegendste und eine stark zunehmende Bedrohung genannt.

Besondere Information Disclosure-Gefährdungen bzgl. des CSL für SaaS CRM

Für das Szenario „SaaS CRM“ kommen als privilegierte Information Disclosure-Akteure vor allem die Administratoren in Betracht, wobei der Subscriber Administrator (SAD) nur eingeschränkt Zugriff auf die Anwendungskonfigurationen im CSL und in der Regel wohl kaum Zugriff auf die Schnittstellenkonfigurationen und die Middleware des CSL haben dürfte, ein Administrator des CSP hingegen entweder bereits im Besitz eines vollen Zugriffs auf Anwendungen, Schnittstellen und eingesetzte Middleware hat oder sich diesen ggf. leichter beschaffen könnte. In Frage kommt auch ein Sub-Provider Administrator (SPA), dem ggf. im Rahmen der Bereitstellung externer Ressourcen ein weitgehendes Zugriffsrecht auf Komponenten und Ressourcen des CSL eingeräumt wird. Letztlich können natürlich auch Information Disclosure Angriffe durch Subscriber End User (SEU) oder externe Angreifer nicht gänzlich ausgeschlossen werden, sofern sie sich nach einem erfolgreichen →Spoofing in den Besitz von Administratorrechten bringen können (→Elevation of Privilege).

Daher lassen sich vor allem folgende Information Disclosure Einzelbedrohungsszenarien, zusätzlich zu den unter dem ADL aufgeführten Bedrohungen, für den Cloud Service Layer erkennen:



1. Unsicherer Datenaustausch

01. Ein unzureichend geschützter (beispielsweise durch unsichere Kommunikationsprotokolle oder unzureichende Verschlüsselung) Datenaustausch zwischen den Komponenten des CSL ermöglicht oder erleichtert die unbefugte Kenntnisnahme und ggf. sogar die Manipulation von Daten (→Tampering) während des Austauschs,
02. dieses gilt insbesondere für Import- / Exportfunktionen, sowie Up- und Downloads von Informationen durch den Subscriber, aber auch bzgl. einer durch die Anwendungen initiierten Inter-Cloud Kommunikation beispielsweise über Schnittstellen oder Netzwerk- und Middleware Komponenten.

2. Ungenügende Mandantentrennung

01. Vor dem Hintergrund, dass in der Cloud Datenflüsse, Anwendungen und Ressourcen unterschiedlicher Mandanten virtualisiert, d. h. nicht mehr strikt physikalisch voneinander getrennt werden, ermöglichen oder erleichtern ungeschützte oder fehlerhaft konfigurierte (virtuelle) Firewalls, Zugriffskontrollen, VLANs und virtualisierte Speicherressourcen die unbefugte Kenntnisnahme verarbeiteter oder gespeicherter Daten.

3. Ungeeignete Technologien

01. Der Einsatz von im Cloud-Umfeld ungeeigneten oder unsicheren Technologien, insbesondere für sicherheitsrelevante Komponenten oder Schnittstellen, ermöglicht oder erleichtert die Nutzung von Schwachstellen für erfolgreiche Information Disclosure Angriffe.

4. Unzureichende Erfahrung

01. Unzureichend ausgebildete oder erfahrene Administratoren erhöhen das Risiko fahrlässigen Fehlverhaltens in der Konfiguration und Kombination sicherheitsrelevanter Komponenten und der Bewertung sicherheitsrelevanter Ereignisse oder Schwachstellen.

Noch näher zu betrachtende Bereiche

In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

1. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure, d. h.:

01. das Cloud Architekturkonzept des CSP, insbesondere bzgl. der genutzten Schnittstellen und Kommunikationsverbindungen zwischen den Anwendungen und den involvierten (virtualisierten) Ressourcen,
02. die Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP, des Subscribers und Sub-Providers, einschl. Berechtigungs- und Rollenkonzepte, sowie des Konzepts zur sicheren Kommunikation über Schnittstellen und der Konzeption bzgl. einer konsequenten Mandantentrennung.

2. Verschlüsselungskonzepte des Subscribers und des CSP

3. Authentifizierungs- und Autorisierungskonzepte des Subscribers und des CSP

4. Logging- und Log-Daten-Auswertungskonzept (Aggregation und Monitoring sicherheitsrelevanter Ereignisse) des CSP

5. Wissenslücken der CSP Administratoren bzgl. sicheren Konfiguration von Multi-Mandanten-Anwendungen und derer Schnittstellen

6. Einsatz von Softwareprodukten (im Rahmen der Anwendungen, Datenbanken und Schnittstellen), welche nur bedingt geeignet bzw. ungenügend bzgl. der Trennung von Mandanten sind

Restrisiken

- unsicherer oder fahrlässiger Umgang mit Benutzerkennung
- fahrlässiges sowie vorsätzlich böswilliges Verhalten auf der Seite des Subscribers, des Sub-Providers und durch CSP Administratoren
- nicht aufgelöste Konflikte zwischen den Datenschutz- und Datensicherheitsanforderungen des Subscribers und des Providers bzw. Sub-Providers
- fehlende bzw. ungenügende Anweisungen und Schulungen bzgl. des Umgangs mit sensiblen Daten auf der Seite des Subscribers

Tampering in der Cloud Management Plane

Tampering stellt für die Cloud Management Plane eine äußerst kritische Bedrohungsfläche dar, denn über die in der CMP vorhandenen Funktionalitäten ist die Kontrolle, die Überwachung und Konfiguration aller relevanten Cloud Dienste, einschließlich der Sicherheitsdienste möglich.

Tampering in der CMP ist vor allem als eine Folge erfolgreicher →Spoofing-Attacken möglich. Externe wie interne Angreifer erhalten dabei unter Nutzung gefälschter Identitäten und Ausnutzung unzureichender oder unsicherer Authentifizierungsmaßnahmen sowie ungenügender Überwachung von Zugriffen und Schnittstellen der CMP die Möglichkeit, selbst sicherheitskritische Funktionen, wie beispielsweise das Monitoring von Cloud Komponenten und Services oder die Konfiguration von Sicherheitsdiensten über die Funktionalitäten der CMP zu kompromittieren. Damit wird es ihnen zweifellos erleichtert, nicht nur weitere und ggf. umfangreichere Attacken vorzubereiten, sondern ebenso unbemerkt auf die Kundendaten oder andere Cloud Systeme bzw. Inter-Cloud Funktionen zugreifen zu können →Information Disclosure.

Innentäter mit Administratorrechten sind dabei natürlich in besonderer Weise für den Zugriff auf die Funktionalitäten der Cloud Management Plane privilegiert.

Die Bedrohung durch Tampering wird auch seitens der Cloud Security Alliance in „The Notorious Nine Cloud Computing Top Threats 2013“ als eine große Bedrohung benannt.

Besondere Tampering-Attacken auf die Cloud Management Plane bei SaaS

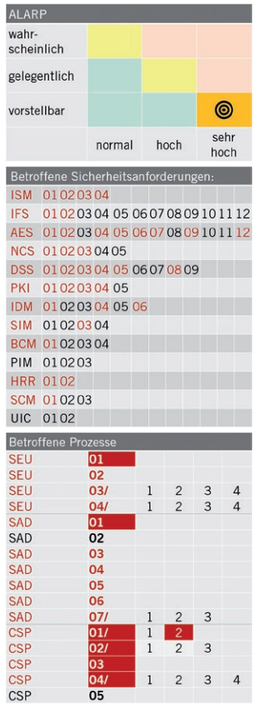
Für das Szenario „SaaS CRM“ kommen als privilegierte Tampering-Akteure der Subscriber Administrator (SAD), der Cloud Service Provider Administrator (CSA) und die Administratoren des Cloud Sub-Providers in Betracht. Dabei lassen sich zusätzlich zu den für das ADL aufgezeigten Bedrohungen vor allem folgende Tampering-Einzelbedrohungsszenarien für die Cloud Management Plane erkennen:

1. Datenmanipulation auf Grund einer ungenügenden Trennung des Zugriffs auf die Funktionalitäten in der CMP

01. Eine unzureichende Trennung der Systeme, Schnittstellen und Kommunikationsverbindungen der CMP in Bezug auf die Komponenten anderer Schichten und weitere, ggf. sogar externe Kommunikationsverbindungen hin, sowie ein ungenügender Authentifizierungszwang zur Nutzung der Dienste und der CMP (unsichere Managementkonsole mit unzureichender Mehr-Faktoren-Authentifizierung und ungenügende Trennung separater Benutzerkonten), ermöglichen einem Angreifer nach einer erfolgreichen →Spoofing-Attacke den Zugriff auf die Funktionalitäten der CMP.
02. In der Folge ist dieser in der Lage, mit einer Veränderung (Manipulation) →Tampering von Konfigurationsdaten oder Einstellungen der Cloud (Sicherheits) Dienste nachfolgendes →Spoofing zu erleichtern, und damit auch ein erneutes, ggf. auch wirkungsvolleres →Tampering gestützt auf →Elevation of Privilege mit ggf. nachfolgendem →Information Disclosure), aber auch die korrekte Ausführung bzw. die Verfügbarkeit von Cloud-Service insgesamt zu beeinträchtigen (→Denial of Service).

2. Datenmanipulation durch Hacking der CSP Architektur

01. Ein Angreifer gelangt entweder nach erfolgreichem →Spoofing oder über eine unzureichend gesicherte Architektur/Infrastruktur des CSP direkt an die CMP bzw. das Management-Netzwerk des CSP (Hacking einer ungenügend gesicherten und ohne ausreichende Identitätsprüfung von Außen erreichbaren Administrationsschicht).



02. Dadurch ist einem Angreifer die Veränderung (Manipulation) →Tampering von Konfigurationsdaten oder Einstellungen der Cloud-(Sicherheits-)Dienste möglich, um nachfolgendes →Spoofing zu erleichtern und damit auch ein erneutes, ggf. auch wirkungsvolleres →Tampering (gestützt auf →Elevation of Privilege mit ggf. nachfolgendem →Information Disclosure), aber auch die korrekte Ausführung bzw. die Verfügbarkeit von Cloud-Service insgesamt zu beeinträchtigen (→Denial of Service).

Noch näher zu betrachtende Bereiche

In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

1. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure, d. h.:

01. das Cloud Architekturkonzept des CSP, insbesondere bzgl. der Trennung / Alleinstellung der CMP,
02. die Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP, des Subscribers und Sub-Providers, einschl. der Durchsetzung von Berechtigungs- und Rollenkonzepten,
03. die Vertrags- und SLA-Gestaltung zwischen CSP und Subscriber bzgl. administrativer Kompetenzen, Monitoring, Logging und Audits.

2. Authentifizierungs- und Autorisierungskonzepte des Subscribers und des CSP (hier insbesondere von Managementkonsolen in der CMP)
3. Logging- und Log-Daten-Auswertungskonzept (Aggregation und Monitoring sicherheitsrelevanter Informationen) des CSP

Restrisiken

- unzureichende Authentifizierung und Autorisierung der SAD bzgl. des Zugriffs auf die Elemente der CMP (unsichere Managementkonsolen)
- ungenügende Sicherung der CMP Architektur und Kommunikation durch den CSP,
- unsicherer Umgang mit Benutzerkennung auf der Seite des Subscribers und des Sub-Providers
- fahrlässiges Fehlverhalten der Mitarbeiter des Subscribers und der CSP Administratoren
- Konfigurationsfehler der CSP Administratoren

Elevation of Privilege in der Cloud Management Plane

Elevation of Privilege ist eine Bedrohungsfläche für die CMP deren Risikopotenzial maßgeblich von der Durchsetzung ausreichender und zuverlässiger Authentisierungs- und Autorisierungskonzepte und -maßnahmen (beispielsweise in Managementkonsolen) sowie der strikten Trennung der CMP von anderen Cloud Schichten und externen Kommunikationsverbindungen, als auch innerhalb der CMP (Managementkonsole) durch die strikte Trennung von Zuständigkeiten (Separation of Duties) bestimmt wird.

Erfolgr. Elevation of Privilege ermöglicht oder erleichtert den unbefugten Zugriff auf die Funktionalitäten der CMP, beispielsweise auf die Sicherheitsdienste der Cloud-Umgebung oder auch Konfigurationsdaten von Komponenten des CMP-Monitoring bzw. des CMP-Accounting und damit →Tampering, →Information Disclosure oder →Denial of Service .

Für externe Angreifer ist Elevation of Privilege vornehmlich die Folge eines erfolgreichen →Spoofings. Für Innentäter kommen sowohl böswillige und mittels →Spoofing verschleierte Angriffe (→Repudiation), aber auch fahrlässiges Verhalten in Betracht. Zu Letzterem gehört insbesondere die unzureichende Kontrolle der ggf. versehentlichen Zuweisung von Administratorenberechtigungen und (erweiterten) Zugriffsberechtigungen. Nicht auszuschließen ist beispielsweise die nicht erfolgte Löschung oder Deaktivierung eines Administratoren-Kontos von nicht mehr unter Vertrag stehenden Sub-Providern oder die fahrlässige Preisgabe von Authentifikationsinformationen. Vor dem Hintergrund, dass eine unzulässige oder auch nur unbemerkte Erweiterung von Berechtigungen ggf. den Zugriff auf die Cloud-Sicherheitsdienste in der CMP gestattet, erleichtert oder ermöglicht erfolgreiches Elevation of Privilege die Vorbereitung und Ausführung weiterer Attacken, wie beispielsweise →Tampering, →Information Disclosure oder →Denial of Service.

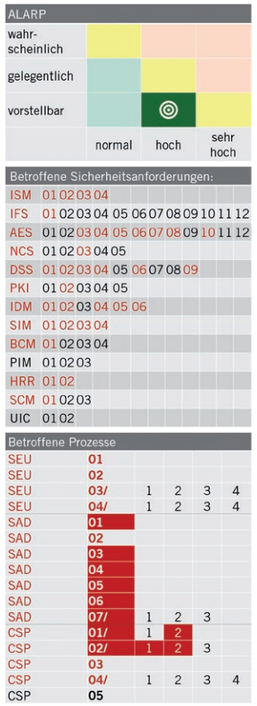
Elevation of Privilege wird auch seitens der Cloud Security Alliance mehrfach in „The Notorious Nine Cloud Computing Top Threats 2013“ als eine ernstzunehmende Bedrohung für Cloud-Umgebungen benannt.

Besondere Elevation of Privilege-Gefährdungen bzgl. der CMP für SaaS CRM

Für das Szenario „SaaS CRM“ kommen als privilegierte Elevation of Privilege-Akteure der Subscriber Administrator (SAD), der Cloud Service Provider Administrator (CSA) und der Sub-Provider Administrator (SPA) in Betracht. Dabei lassen sich zusätzlich zu den für das ADL aufgezeigten Bedrohungen vor allem folgende Elevation of Privilege-Einzelbedrohungsszenarien für die Cloud Management Plane erkennen:

1. Missbrauch von Berechtigungen

01. Ein unbemerkter Missbrauch von Berechtigungen kann den Zugriff auf Authentifikations- oder Konfigurationsdaten (→Information Disclosure) ermöglichen, ein →Tampering dieser Daten und in der Folge weitere unbemerkte, weil verschleierte (→Repudiation) Attacken erleichtern (beispielsweise →Denial of Service),
02. Der unbemerkte Missbrauch von Berechtigungen für die Manipulation von Benutzerkonten und/oder Konfigurationsdaten (→Tampering) sowie einen verschleierten (→Repudiation) Zugriff auf Funktionen der Cloud Management Plane wird erleichtert durch die Möglichkeit der unbefugten und unbemerkten Kenntnisnahme von Authentifizierungsinformationen (→Spoofing).
03. Durch den unbemerkten oder auch verschleierten Zugriff auf die Cloud-Dienste in der CMP ist ein Angreifer in der Lage die Einstellungen der Überwachungs- und Sicherheitsdienste der relevanten Cloud Umgebung zu verändern (→Tampering), um so dann mittels weiterer Zugriffe oder Attacken (unerkannt) ggf. auf alle SaaS CRM-(Kunden)-Daten zuzugreifen und die diese zu verändern (→Tampering), zu veröffentlichen (→Information Disclosure) oder zu löschen (→Denial of Service).



Noch näher zu betrachtende Bereiche

In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

1. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure, d. h.:

01. das Cloud Architekturkonzept des CSP, insbesondere bzgl. der Trennung / Alleinstellung der CMP,
02. die Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP, des Subscribers und Sub-Providers, einschl. Berechtigungs- und Rollenkonzepte, sowie erforderl. Prozesse zur Berechtigungs- und Zugriffsvergabe,
03. die Vertrags- und SLA-Gestaltung zwischen CSP und Subscriber bzgl. administrativer Kompetenzen, Monitoring, Logging und Audits

2. Prozesse bzgl. der Verwaltung von Subscriber Mandaten, insbesondere bzgl. der Änderung, Anpassung und Kontrolle von Nutzerautorisierungen
3. Überprüfung der Logging- und der Protokollierungs Konzepte bzgl. aller in Frage kommender Verbindungs-, System- (einschließlich relevanter Dienste) und Nutzereignissen, einschließlich der Konzepte und Prozesse bzgl. der Auswertung dieser Log-Daten und Protokolle, sowie bzgl. der bei Feststellung definierter Ereignisse erforderlichen Maßnahmen
4. Logging- und Log-Daten-Auswertungskonzept (Aggregation und Monitoring sicherheitsrelevanter Ereignisse) des CSP
5. Überprüfung der Umsetzung und der Funktionsweise des Loggings und der Protokollierung bzgl. der Dienste und Funktionalitäten der Cloud Management Plane
6. Authentifizierungs- und Autorisierungskonzept des Subscribers und des CSP insbesonder beim Zugriff auf die CMP

Restrisiken

- fehlende bzw. ungenügende Prozesse zur Erteilung, Genehmigung und Kontrolle von Nutzerkonten und Autorisierungen beim Subscriber und beim CSP,
- unzureichende Trennung und Kontrolle von Zuständigkeiten beim CSP (→Separation of Duties),
- unzureichende Authentifizierung und Autorisierung der SAD und der Administrator des CSP bzgl. des Zugriffs auf die Elemente der CMP,
- ungenügende Sicherung der CMP Architektur und Kommunikation durch den CSP,
- fahrlässiges Fehlverhalten der Mitarbeiter des Subscribers und der CSP Administratoren,
- Konfigurationsfehler der CSP Administratoren.

Information Disclosure im Resources Control Layer

Da das Resources Control Layer (ROCL) die Bindung u. Koordination der Ressourcen im Cloud Computing für alle Mandanten übernimmt, ist das ROCL ein lukratives Ziel für →Information Disclosure. Von Information Disclosure bedroht sind im ROCL vornehmlich Konfigurationsdaten (von FC Switches oder HBAs), weil durch sie die Segmentierung der (virtuellen) Ressourcen bestimmt wird und über sie ein direkter Zugriff auf Kundendaten möglich wird. Im Kontext vernetzter Datenspeicher beispielsweise genügt der Snapshot eines SANs um Kenntnis einer LUN und damit die Adresse gespeicherter Daten zu erhalten. Werden Daten zudem standortübergreifend transferiert (Replikation oder Spiegelung) kann bei fehlender kryptografischer Sicherung auf alle transferierten Daten zugegriffen werden.

Information Disclosure im RCOL wird in der Regel neben →Spoofing vor allem von →Tampering und →Elevation of Privilege begleitet.

Besondere Information Disclosure-Gefährdungen

Offenlegung von Informationen auf dem RCL geschieht in der Regel nur über die Administratoren des CSP oder Sub-Providers. Andere Akteure müssten erfolgreich Sicherheitssysteme mehrerer Schichten überwunden werden, was für dieses Sicherheitsprofil als vernachlässigbar angesehen wird. Ursachen für diese Gefährdung sind:

1. Fehlendes Sicherheitsbewusstsein

01. Der ggf. wirtschaftlich begründete Einsatz ungeeigneter Segmentierungsinstrumente (beispielsweise Soft- statt Hardware-Zoning) erleichtert Angreifern den Zugriff auf und die Manipulation (→Tampering) von logisch segmentierten Ressourcen.

02. Eine unzureichende Trennung von Zuständigkeiten ermöglicht Angreifen über eine erfolgreiche →Rechteeskalation den unzulässigen Zugriff auf Konfigurationsdaten des RCOL.

2. Unsichere oder fehlerhafte Konfiguration der Segmentierung

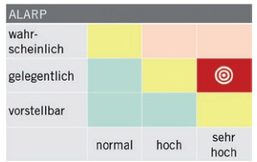
01. Der Einsatz Software-basierter Segmentierung (World Wide Number Zoning) im SAN erleichtert Angreifern das →Spoofing der WWN u. damit den Zugriff auf Geräte in anderen Segmenten.

02. Da die Zugriffsberechtigung zu einem konfigurierten Ressourcensegment beim Einsatz Software-basierter Segmentierung nicht auf Hardwareniveau validiert wird, ist es für kompromittierte HBAs (Host Bus Adapter) möglich, den Namenserver zu umgehen, und direkt mit einer Ressource zu kommunizieren, die nicht im konfigurierten (zugelassenen) Segment liegt.

03. Die fehlerhafte Konfiguration (LUN Maskierung) von WWNs auf HBA-Level erleichtert einem Angreifer das→Spoofing v. LUN Gruppen u. den Zugriff auf andere Segmente.

3. Fehlendes bzw. ungenügendes Storage Security Konzept

01. Durch ungenügende Verschlüsselung, für gespeicherte und bewegte Daten ist es einem Angreifer möglich, die Administration von virtualisierten Ressourcen im Netz (In-Band-Management) zu beeinflussen.



Betroffene Sicherheitsanforderungen:												
ISM	01	02	03	04								
IFS	01	02	03	04	05	06	07	08	09	10	11	12
AES	01	02	03	04	05	06	07	08	09	10	11	12
NCS	01	02	03	04	05							
DSS	01	02	03	04	05	06	07	08	09			
PKI	01	02	03	04	05							
IDM	01	02	03	04	05	06						
SIM	01	02	03	04								
BCM	01	02	03	04								
PIM	01	02	03									
HRR	01	02										
SCM	01	02	03									
UIC	01	02										

Betroffene Prozesse					
SEU	**01**				
SEU	**02**				
SEU	**03/**	1	2	3	4
SEU	**04/**	1	2	3	4
SAD	**01**				
SAD	**02**				
SAD	**03**				
SAD	**04**				
SAD	**05**				
SAD	**06**				
SAD	**07/**	1	2	3	
CSP	**01/**	1	2		
CSP	**02/**	1	2	3	
CSP	**03**				
CSP	**04/**	1	2	3	4
CSP	**05**				

Noch näher zu betrachtende Bereiche

1. Fortentwicklung der Konzepte und Richtlinien in Bezug auf die aktuell gegebene Risiko- u. Bedrohungslage aller Akteure, d. h.:

01. das Cloud Architekturkonzept des CSP, wie z. B. die Anbindung von Speicherlösungen und deren Virtualisierung,

02. das Konzept zur Storage-Virtualisierung (SAN Zoning, LUN Masking, VSANs)

03. Block- u. File-orientierte Virtualisierung

04. In-Band-Virtualisierung (symmetrische Virtualisierung)

05. Out-of-Band-Virtualisierung (asymmetrische Virtualisierung

06. das Server Virtualisierungskonzept

07. die Integration der Speichernetze in die Sicherheitskonzepte des CSP, des Subscribers u. Sub-Providers hier insbesondere

08. Storage Security (mit Fokus auf Datenschutz und Disaster Recovery)

09. Umgang mit schützenswerten Daten in einem (virtualisierten) SAN Systemen wie beispielsweise WWN u. LUN Masken

10. Abspaltung eines Spiegels (mit dem Kopierbefehl werden beide Spiegel getrennt und sind unabhängig von einander benutzbar)

11. Snapshots (im SAN Umfeld bezeichnet das die virtuelle Kopie einer LUN bzw. einer LUN-Gruppe innerhalb eines Speichersystems)

12. Spiegelung und Replikation der Daten

13. Disaster Recovery / Failover Konzept

14. Verwaltung und Monitoring von Komponenten

15. In-Band-Management (die Administration der Geräte eines Netzwerkes aus selbigem heraus)

16. Out-Band-Management

2. Verschlüsselungskonzept des Subscribers und des CSP, welches die Sicherung v. Daten in Speichernetzen (beispielsweise durch eine Dateiverschlüsselung) beinhaltet

3. Einsatz von Hard- u. Softwareprodukten, welche die separate Behandlung von unterschiedlichen Speicherbereichen in Speichernetzen verlässlich gewährleisten

4. Einsatz von Fibre Channel Security Protokollen

Restrisiken

- Fahrlässiges Verhalten der Admins des CSP und des Subproviders hervorgerufen durch fehlende bzw. ungenügende Schulungen bzgl. des Umgangs mit sensiblen Konfigurationsdaten des RCOLs,
- Vorsätzliches Verhalten auf der Seite des CSP Admins oder des Sub-Providers (Innentäter),
- nicht aufgelöste Konflikte zwischen den Datenschutz- u. Datensicherheitsanforderungen der Vertragsparteien.

Denial of Service im Resources Control Layer

Aufgrund der Tatsache, dass das Resources Control Layer (ROCL) die Bindung und Koordination der (virtualisierten, gleichwohl aber physikalisch mehreren Mandanten bereitgestellten) Ressourcen im Cloud Computing übernimmt, ist das ROCL eine durch →Denial of Service stark bedrohte Schicht.

Gegeben ist dieses durch die bereits bestehende und stetig anwachsende Komplexität (beispielsweise durch neue Produkte, Protokolle und dadurch entstehender, heterogener Umgebungen) bzgl. der Konzeption, der Verwaltung und des Betriebs von virtualisierten Multi-Mandanten-Umgebungen (Shared Resources) mit permanent steigendem Speicherplatzbedarf für Kundendaten. Insbesondere bzgl. der nicht immer vorhandenen Interoperabilität von Speichersystemen und den an diese angeschlossenen Sub-Systeme unterschiedlicher Anbieter, sind beispielsweise viele Arrays und Switche «Inseln» und müssen als solche individuell administriert und überwacht werden, da es hierfür kaum hersteller- und plattformunabhängige bzw. -übergreifende Managementwerkzeuge gibt. Dieses hat auch zur Folge, dass die Konfiguration von Aspekten wie Hochverfügbarkeit und Failover, insbesondere bzgl. der Anbindung von Speicher Host Systemen, nicht immer sicher und vollautomatisch gewährleistet werden kann.

Somit gestaltet sich die Bedrohungsfläche Denial of Service für das RCOL einerseits aus dem für den Cloud Service Provider immer schwerer werdenden, im betriebswirtschaftlich sinnvollem Umfang und mit der jeweils erforderlichen Hardware zu betreibenden Business Modell / Business Case „Cloud“ (= Ausfälle auf Grund von Inkompatibilität der Hardware verschiedener Anbieter in heterogenen iSCSI FC Umgebung) und andererseits sind Cloud Infrastrukturen zunehmend Ziel möglicher Angriffe (beispielsweise Ausfälle auf Grund von DoS Attacken). Abseits des Denial of Service auf Grund von Fehlkonfiguration bzw. Fehlverhalten durch Innentäter oder logischer Attacken durch externe Angreifer (entweder als reine DoS-Attacken oder Folge eines erfolgreichen →Spoofings), sind hierbei insbesondere auch Aspekte des physikalischen Zugriffs auf involvierte und relevante Komponenten sowie die ausreichende dynamische Bereitstellung ausreichender Ressourcen durch den CSP zu betrachten. Innentäter mit Administratorrechten sind in besonderer Weise für den fahrlässigen oder böswilligen Zugriff auf die Ressourcen des RCOL privilegiert. Die Dienstverhinderung und der Datenverlust auf Grund von Denial of Service-Bedrohungen sind auch seitens der Cloud Security Alliance in „The Notorious Nine Cloud Computing Top Threats 2013“ als häufige und wachsende Bedrohung benannt.

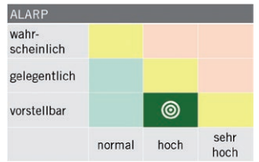
Besondere Denial of Service-Gefährdungen bzgl. des RCOL für SaaS CRM

Für das Szenario „SaaS CRM“ kommen als privilegierte Denial of Service-Akteure der Cloud Service Provider Administrator (CSA) und der Sub-Provider Administrator (SPA) in Betracht. Dabei lassen sich zusätzlich zu den unter dem ADL aufgeführten Bedrohungen für den Sachverhalt Information Disclosure vor allem folgende Denial of Service-Einzelbedrohungsszenarien für das Resources Control Layer erkennen:

1. Ausfall/Störung durch den Einsatz zueinander inkompatibler Hardware

01. Speichersysteme und daran anzuschließende Sub-Systeme, welche nicht vom gleichen Anbieter stammen, sind nicht immer kompatibel zu einander bzw. unterstützen und keine automatischen HA oder Failover Szenarien.

02. Erschwerend kommt hinzu, dass es für heterogene Umgebungen nur wenige herstellerunabhängige bzw. plattformübergreifenden Managementwerkzeuge gibt und somit eine effiziente Kontrolle und Überwachung dieser Komponenten fast nicht möglich ist.



Betroffene Sicherheitsanforderungen:												
ISM	01	02	03	04								
IFS	01	02	03	04	05	06	07	08	09	10	11	12
AES	01	02	03	04	05	06	07	08	09	10	11	12
NCS	01	02	03	04	05							
DSS	01	02	03	04	05	06	07	08	09			
PKI	01	02	03	04	05							
IDM	01	02	03	04	05	06						
SIM	01	02	03	04								
BCM	01	02	03	04								
PIM	01	02	03									
HRR	01	02										
SCM	01	02	03									
UIC	01	02										

Betroffene Prozesse					
SEU	**01**				
SEU	**02**				
SEU	**03/**	1	2	3	4
SEU	**04/**	1	2	3	4
SAD	**01**				
SAD	**02**				
SAD	**03**				
SAD	**04**				
SAD	**05**				
SAD	**06**				
SAD	**07/**	1	2	3	
CSP	**01/**	1	2		
CSP	**02/**	1	2	3	
CSP	**03**				
CSP	**04/**	1	2	3	4
CSP	**05**				

2. Unsichere oder fehlerhafte LUN Maskierung

01. Eine unsichere oder fehlerhafte LUN Maskierung kann zu einem Datenverlust →Denial of Service führen

3. Kompromittierung von Host Bus Adaptern (HBA)

01. Die Kompromittierung von HBAs erleichtert das →Spoofing von WWN und damit den Zugriff auf andere Segmente →Information Disclosure sowie die Löschung von Daten mit dem Ergebnis eines →Denial of Service.

Noch näher zu betrachtende Bereiche

In Abhängigkeit von den Architekturkonzepten, Sicherheitskonzepten und -richtlinien der einzelnen Akteure, sowie deren Umsetzung und Kontrolle, lassen sich die noch genauer zu betrachtenden Bereiche wie folgt priorisieren:

1. Überprüfung und ggf. Anpassung der Sicherheitskonzepte und -richtlinien auf der Grundlage einer validen Schutzbedarfsfeststellung und in Bezug auf die aktuell gegebene Risiko- und Bedrohungslage durch die betroffenen Akteure:

2. das Cloud Architekturkonzept des CSP, insbesondere bzgl. der Infrastruktur und des Betriebs von der Speichersystemen und Speichernetzen (Storage Konzept),

3. Sicherheitskonzepte und IT-Sicherheitsrichtlinien des CSP, des Subscribers und Sub-Providers, einschl. Berechtigungs- und Rollenkonzepte und des Storage Security Konzepts

4. Vertrags- und SLA-Gestaltung zwischen Subscriber und CSP

5. Disaster Recovery- und Notfallkonzepte des CSP

6. Konzepte des CSP bzgl. des Einsatzes von IDS- und IPS-Systemen

Restrisiken

- unzureichende Schulung von Mitarbeitern beim CSP und Sub-Provider
- unsichere oder fehlerhafte Konfiguration von Speicherkomponenten
- unzureichende oder fehlende Maßnahmen bzgl. Szenarien „Höherer Gewalt“
- unzureichende Kommunikation zwischen CSP und Subscriber bezüglich Wartungsmaßnahmen oder Änderung von Zugangsmechanismen

Anhang: Sicherheitsanforderungen

In den Steckbriefen werden die Sicherheitsanforderungen aus verschiedenen Standards (ISO 27001 und NIST SP 800-53 rev3) sowie aus Anforderungen und Empfehlungen von staatlichen Behörden und industriellen Verbänden (BSI-Eckpunktepapier, FedRAMP, Cloud Control Matrix) aufgeführt, wie sie für das SaaS-Sicherheitsprofil ausformuliert wurden.Die Definitionen von Sicherheitsanforderungen an ein als SaaS bereitgestelltes CRM-System folgen dem Eckpunktepapier des BSI „Sicherheitsempfehlungen für Cloud Computing Anbieter“. Nachfolgend die Kurzfassung der Definitionen, wie sie zum Verständnis der Steckbriefe notwendig sind – ausführliche Erläuterungen sind dem Eckpunktepapier des BSI zu entnehmen. (CS = Cloud Service)

ISM: Information Security Management

ISM-01: Der CS-Anbieter hat ein anerkanntes Informationssicherheits-Management-System etabliert und implementiert.

ISM-02: Das ISM-System etabliert und setzt eine klare Trennung von Aufgaben, Rollen und Verantwortlichkeiten durch und benennt dem CS-Abonnenten Ansprechpartner für Sicherheitsfragen.

ISM-03: Der CS-Anbieter hat ein zuverlässiges Risikomanagement etabliert, das in regelmäßigen Abständen Bedrohungs- und Risikoanalysen für Daten, Anwendungen und Ressourcen durchführt. Die Ergebnisse werden dokumentiert, vor Verlust und Manipulation geschützt und dem CS-Abonnenten auf Anforderung zur Kenntnis gebracht.

ISM-04: Sicherheitsrichtlinien, Sicherheitsarchitektur und Sicherheitsmaßnahmen des Service werden regelmäßig auf ihre Umsetzung und Wirksamkeit überprüft. Eine Überprüfung kann auf Verlangen des CS-Abonnenten auch durch zertifizierte externe Auditoren durchgeführt und dokumentiert werden.

IFS: Information Facility Security – Rechenzentrumssicherheit

IFS-01: Der Zutritt zu Betriebsräumen des CS-Anbieters ist nur authentisierten und autorisierten Personen möglich.

IFS-02: Der CS-Anbieter hat eine robuste und redundante Infrastruktur für die Bereitstellung des Services etabliert, die die Verfügbarkeit der Anwendung auch im Falle Störungen, Ausfall einzelner Komponenten und beherrschbarer Elementarschäden sicherstellt.

AES: Application and Environment Security – Sicherheit der Anwendung und der Anwendungsumgebung

AES-01: Die Anwendung wird in einer sicheren Betriebsumgebung ausgeführt, die Korrektheit und Integrität importierter und exportierter Daten ist sichergestellt.

AES-02: Die für den Betrieb erforderliche Anwendungsumgebung ist frei von Schadsoftware, ausreichend gegen interne oder externe netzbasierte Angriffe geschützt und sicher segmentiert und isoliert, so dass eine Eskalation von Zugriffsrechten über die operative Einsatzumgebung ausgeschlossen werden kann. In der Anwendungsumgebung sind geeignete Werkzeuge installiert, die zuverlässig das Eindringen und die Ausführung von Schadsoftware, Host- bzw. Netz-basierte Angriffe entdecken und verhindern.

AES-03: Die Anwendung setzt eine sichere Identifikation und Authentisierung externer Zugriffe durch. Ein Zugriff auf Informationen oder Daten der Anwendung ist nur für authentisierte und autorisierte Nutzer bzw. Anwendungen/Services möglich.

AES-04: Mandanten und Anwendungen und die ihnen zugewiesenen Ressourcen (Netze, Server, Speicher) sind sicher segmentiert und isoliert.

AES-05: Die Anwendung ist so in die Anwendungsumgebung integriert, dass eine Umgehung der Sicherungsmaßnahmen der Anwendungsumgebung nicht möglich ist.

AES-06: Verbindungen zwischen logischen oder physisch getrennten Komponenten kommen erst nach einer sicheren wechselseitigen Authentisierung zustande. Die Identifikation und Authentisierung wird durch zuverlässige und eindeutige Sicherheitsattribute durchgesetzt.

AES-07: Die Anwendung und die Anwendungsumgebung werden auf der Basis von Richtlinien und Handlungsanweisungen sicher konfiguriert und betrieben. Ein unbefugter Zugriff auf Daten, die für die Konfiguration und den Betrieb der Anwendungsumgebung erforderlich sind, ist nicht möglich.

AES-08: Konfigurationsänderungen oder Updates werden nur von autorisierten Mitarbeitern des CS-Anbieters durchgeführt. Sie werden kontrolliert und dokumentiert und vor Inbetriebnahme auf Bedrohungen getestet.

AES-09: Sicherheitslücken der Anwendung oder Anwendungsumgebung werden unverzüglich geschlossen, Sicherheitspatches werden unverzüglich implementiert.

AES-10: Der CS-Anbieter etabliert und implementiert sichere Prozesse für die Administration und Wartung der Anwendung und Anwendungsumgebung. Administration und Wartungsmaßnahmen dürfen nur von vertrauenswürdigen, erfahrenen und ausdrücklich autorisierten Mitarbeitern ausgeführt werden.

AES-11: Der CS-Anbieter hat sichere Prozesse für die Überwachung des Softwarelebenszyklus der Anwendung etabliert und implementiert. Neue Releases werden erst eingesetzt, nachdem sie qualitätsgesichert und ausführlichen Sicherheitstests unterzogen wurden.

AES-12: Der CS-Anbieter garantiert die Einhaltung von Sicherheits-Mindeststandards bei der Entwicklung und Bereitstellung von Web-Anwendungen.

NCS: Network Security – Netzsicherheit

NCS-01: Netzarchitekturen sind so entworfen, implementiert und konfiguriert, dass Verbindungen zwischen sicheren und unsicheren Netzen nicht möglich sind. Telekommunikations- und Netzverbindungen sind vor Abhören, Manipulation und Zerstörung geschützt. Virtualisierte Netzwerkkomponenten sind zuverlässig und sicher segmentiert und isoliert.

NCS-02: Der CS-Anbieter stellt auf Basis ausführlicher Richtlinien und Handlungsanweisungen die sichere Konfiguration und Segmentierung von Netzkomponenten sicher. Management-Netze sind strikt von Datennetzen getrennt.

NCS-03: Die Fernadministration des Service erfolgt über einen sicheren Kommunikationskanal. Der Ausfall oder die Kompromittierung von Management-Netzen wird zuverlässig verhindert.

NCS-04: Die Konfiguration der Netzkomponenten wird nur von autorisierten Mitarbeitern des CS-Anbieters ausgeführt. Änderungen an der Konfiguration von Netzkomponenten werden vor Inbetriebnahme ausführlichen Sicherheitstests unterzogen; die Tests werden protokolliert.

NCS-05: Im Falle verteilter Cloud-Computing-Ressourcen sind die Netzverbindungen zwischen den Rechen- oder Datenzentren redundant ausgelegt.

DSS: Data Safety and Security – Datenschutz und Datensicherheit

DSS-01: Der CS-Anbieter gewährleistet die Einhaltung der für den CS-Abonnenten geltenden datenschutzrechtlichen Regelungen.

DSS-02: Daten des CS-Abonnenten werden außerhalb der am Standort geltenden Gerichtsbarkeit nur mit ausdrücklicher, schriftlicher Zustimmung des CS-Abonnenten erfasst, verarbeitet und gespeichert; das gilt auch für Sub-Dienstleister des CS-Anbieters.

DSS-03: Personenbezogene Daten des CS-Abonnenten sind unter keinen Umständen unbefugten Dritten zugänglich.

DSS-04: Administratoren, Wartungspersonal oder andere Mitarbeiter des CS-Anbieters sowie seines Sub-Dienstleisters haben keinen Zugriff auf geschäftsbezogene Daten des CS-Abonnenten.

DSS-05: Verlust oder Diebstahl von Daten des CS-Abonnenten wird durch geeignete Sicherheitsmaßnahmen zuverlässig verhindert.

DSS-06: Der CS-Anbieter sorgt für eine regelmäßige, transparente und redundante Sicherung von Anwendungs- und anwendungsbezogenen Daten.

DSS-07: Datenträger mit den Daten und Informationen des CS-Abonnenten werden regelmäßig auf korrekte Funktion geprüft und vor Verlust und Zugriff unbefugter Dritter geschützt.

DSS-08: Der CS-Anbieter stellt die vollständige und nicht wiederherstellbare Löschung von Daten des CS-Abonnenten bei Vertragsende oder auf Anforderung des CS-Abonnenten sicher.

DSS-09: Ein Zugriff auf die Anwendung und Anwendungsdaten von mobilen Endgeräten erfolgt nur über sichere Kanäle und in Übereinstimmung mit den Sicherheitsrichtlinien des CS-Abonnenten.

PKI: Public-Key Infrastructure – Verschlüsselung und Schlüsselmanagement

PKI-01: Die Kommunikation zwischen CS-Anbieter und CS-Abonnenten, Standorten sowie Drittdienstleistern erfolgt verschlüsselt.

PKI-02: Der CS-Anbieter stellt ausreichend starke, standardisierte kryptografische Sicherheitsmaßnahmen und Services zur Verfügung, die eine unbefugte Kenntnisnahme oder Manipulation von Daten, Anwendungen, Komponenten und Services verhindern, die Korrektheit, die Integrität und Authentizität importierter und exportierter Daten zuverlässig gewährleisten und eine mögliche Aufdeckung oder Kompromittierung beim Import und Export verhindern.

PKI-03: Für den kryptografischen Schutz bewegter sowie gespeicherter Daten und von Kommunikationsverbindungen werden ausschließlich vertrauenswürdige kryptografische Komponenten eingesetzt.

PKI-04: Die Erzeugung, Verwaltung, Verteilung und Speicherung kryptografischen Materials wird nur in sicheren Umgebungen ausgeführt. Der Zugang zur Administration kryptografischen Materials erfordert eine separate Autorisierung.

PKI-05: Eine unbefugte Kenntnisnahme oder Kompromittierung sowie ein Verlust kryptografischen Materials wird zuverlässig verhindert.

IDM: ID and Rights Management – ID- und Rechtemanagement

IDM-01: Der CS-Anbieter stellt sicher, dass Zugriffe auf die Anwendung und Anwendungsumgebung nur auf der Basis eines sicheren Identitätsmanagements, Rollen- und Rechtekonzepts, einer starken Authentisierung und einer strikten Trennung von Aufgaben und Zuständigkeiten erfolgen können.

IDM-02: Die Umsetzung und Einhaltung des Identitätsmanagements und die Wirksamkeit der implementierten Maßnahmen werden regelmäßig überprüft.

IDM-03: Ein Diebstahl oder die Fälschung von Identitäten oder Zugriffsrechten wird unter Berücksichtigung erwartbarer Bedrohungsszenarien zuverlässig verhindert.

IDM-04: Mitarbeiter erhalten Zugriff nur auf die Funktionen, die sie für sie Erfüllung ihrer Aufgaben benötigen.

IDM-05: Eine Eskalation von Zugriffsrechten wird mit Blick auf erwartbare Bedrohungsszenarien zuverlässig verhindert. Kritische Administrationsaufgaben, wie das Einspielen von Sicherheitspatches oder die Änderung sicherheitskritischer Konfigurationsdaten werden besonders geschützt

IDM-06: Die Zugriffe werden protokolliert. Die Protokolle werden vor Verlust und Manipulation geschützt

SIM: Monitoring and Security Incident Management – Monitoring und Management von Sicherheitsereignissen

SIM-01: Der CS-Anbieter hat ein zuverlässiges Monitoring für das Konfigurationsmanagement etabliert und implementiert. Entsprechende Aktivitäten von Administratoren werden überwacht und protokolliert.

SIM-02: Der CS-Anbieter verfügt über klare Richtlinien sowie etablierte und bewährte Prozesse für die Behandlung sicherheitskritischer Ereignisse.

SIM-03: Der CS-Anbieter stellt die kontinuierliche (24/7) Erkennung, Identifikation und eine unverzügliche und angemessene Behandlung sicherheitskritischer Ereignisse durch ein handlungsfähiges Team und geeignete technische Maßnahmen sicher.

SIM-04: Sicherheitskritische Ereignisse werden dem CS-Abonnenten zur Kenntnis gebracht sowie umfassend, ausführlich und transparent dokumentiert.

BCM: Business Continuity Management – Notfallmanagement

BCM-01: Der CS-Anbieter hat ein zuverlässiges und sicheres Notfallmanagement implementiert. Die Maßnahmen und Prozesse werden regelmäßig auf ihre Funktion und Wirksamkeit überprüft.

BCM-02: Eine Störung oder ein Ausfall der Verfügbarkeit wird durch eine redundante Auslegung und dynamische Bereitstellung zusätzlicher Instanzen und Ressourcen verhindert.

BCM-03: Die Anwendung kann nach einem Systemfehler oder einem erfolgreichen Angriff wieder in einen sicheren und stabilen Zustand geführt werden.

BCM-04: Störungen der Verfügbarkeit, die Maßnahmen zur Wiederherstellung und die Zeitdauer der Störung werden zuverlässig und transparent protokolliert.

PIM: Portability and Interoperability Management – Management von Portabilität und Interoperabilität

PIM-01: Die Anwendung ist kompatibel und interoperabel mit den Systemen des CS-Abonnenten und auf der Basis akzeptierter und marktgängiger Standards implementiert.

PIM-02: Datenformate für den Austausch, die Verarbeitung und Speicherung von Daten basieren auf international anerkannten Standards. Der CS-Anbieter stellt die Plattformunabhängigkeit für den Austausch und die Speicherung von Daten sicher.

PIM-03: Der CS-Anbieter legt die Schnittstellen für den Datenaustausch und die Datenspeicherung offen.

HRR: Human Resources Requirements – Anforderungen an das Personal

HRR-01: Mitarbeiter des CS-Anbieters und der an der Bereitstellung des Service beteiligten Sub-Dienstleiter werden regelmäßig zu Sicherheitsbedrohungen und Sicherheitsmaßnahmen geschult.

HRR-02: Die Mitarbeiter werden regelmäßig einer Sicherheitsüberprüfung unterzogen und auf die Einhaltung der Bewahrung von Betriebsgeheimnissen von CS-Abonnenten verpflichtet.

SCM: Security Compliance Management – Sicherheitsüberprüfung und -nachweis

SCM-01: Der CS-Anbieter führt regelmäßige Sicherheitsrevisionen/ Audits auf der Basis international anerkannter und akzeptierter Standards durch.

SCM-02: Die Prüfergebnisse werden ausführlich dokumentiert und vor Verlust und Manipulation geschützt.

SCM-03: Unabhängige Auditoren führen regelmäßig Revisionen durch. Der CS-Abonnent kann die Dokumentation der Revisionen auf Verlangen einsehen.

UIC: User Information Control – Kontrollmöglichkeiten durch den Nutzer

UIC-01: Die Verfügbarkeit der Anwendung, die Performanz und die Auslastung werden ausreichend und transparent protokolliert.

UIC-02: Der CS-Abonnent hat die Möglichkeit, Monitoringinformationen zu Verfügbarkeit, Performanz und Auslastung über definierte Schnittstellen regelmäßig abzufragen.

Anhang
Prozessübersicht

Subscriber Enduser (SEU)

1. Login
2. Logout
3. Kundendaten verarbeiten
    1. Kundendaten hinzufügen
    2. Kundenspezifische Marketingaktivitäten und spezielle Angebote
    3. Vertragsübersicht
    4. Kundendaten löschen
4. Kundendaten analysieren
    1. Bestellhistorie
    2. Zahlungsbedingungen
    3. Zahlungsmoral & Liquidität
    4. Soziale Kontakte und Soziale Netzwerke

Subscriber Administrator (SAD)

1. Login
2. Logout
3. Anwendungskonfiguration
4. Nutzerkonto hinzufügen
5. Nutzerkonto ändern
6. Nutzerkonto löschen
7. Nutzerdatenverwaltung
    1. Rollenmanagement
    2. Identitäts- und Rechtemanagement
    3. Schlüsselverwaltung und Zugriffsrechteverwaltung

Cloud Service Provider (CSP)

1. Anwendungsbereitstellung
    1. Ressourcenmanagement (CPU, RAM, Storage)
    2. Segmentierung von physischen und logischen Ressourcen
2. Verwaltung der Cloud Nutzer
    1. Nutzer hinzufügen
    2. Verwaltung der Ressourcen für die Nutzer
    3. Nutzer löschen
3. Orchestrierung der Cloud und Cloudmanagement
4. Instanziierung, Steuerung und Überwachung von Anwendungsinstanzen
    1. Identitätsmanagement
    2. Bereitstellung kryptografischer Dienste
    3. Anwendungsüberwachung (Nutzung und Einhaltung der Dienstgüte)
    4. Sicherheitsüberwachung und Reaktion auf Sicherheitsvorfälle
5. Unterauftragsnehmerverwaltung

Nationaler IT Gipfel

Mitgliederliste der Unterarbeitsgruppe 1 · Sicheres Cloud Computing

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
- Bundesverband deutscher Banken e. V. (BDB)
- Bundesministerium des Innern
- Deutsche Telekom AG
- Deutschland sicher im Netz e. V.
- Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC)
- Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV)
- Giesecke & Devrient GmbH
- Hewlett-Packard GmbH
- Microsoft Deutschland GmbH
- SAP AG
- secunet Security Networks AG
- Symantec (Deutschland) GmbH
- T-Systems International GmbH
- TÜV Rheinland AG