Cloud-Computing: Sicherheitsrisiken digitaler Dateiablagen

Anthes, Florian **Dakkak, Mohanad**

Fischer, Fiona Rose **Gesch, Susann**

Kubegenov, Almat

VORWORT

Unter Weisung von Prof. Dr. Ulrich Meissen, Chief Executive Officer (CEO) der Ships-Without-Diesel-Solution (SWDS), wurde eine Untersuchung potenzieller interner Sicherheitsrisiken durch die IT-Administration in Auftrag gegeben. Ein relevanter Sicherheitsvorfall wurde gegenwärtig durch den führenden Sicherheitsbeauftragten Herrn Sebastian Breu (CISO) gemeldet. Die IT-Administration dankt für die zielführende Zusammenarbeit und stellt im Folgenden die gewonnenen Erkenntnisse bereit.

ABSTRACT

Ein potenzieller Angriff auf interne Systeme der Dateiablage der SWDS via Cloud-Computing wird untersucht, um die Sicherheitsrisiken zu beurteilen. Es wird der denkbare Ablauf des Vorfalls betrachtet sowie empfohlene Schutzmaßnahmen abgeleitet. Mögliche Auswirkungen des Angriffs werden analysiert.

Ein schadhafter Angriff ist in aktiver Form durch Cracker zu erwarten, etwa als DDoS- oder Ransomware-Attacke. Unter Berücksichtigung allgemeingültiger Verschlüsselungsstandards, Security-Monitoring sowie Verwaltung der Zugriffsrechte kann das Sicherheitsrisiko verringert werden. Im fatalen Fall können sämtliche Daten der SWDS entwendet und vernichtet werden.

Das Risiko wird durch die IT-Administration als hoch eingestuft. Zur Folge-Untersuchung der Verschlüsselungsform in der Dateiablage des Cloud-Systems wird geraten. Die Implementierung eines Security-Monitoring durch den CISO ist zu empfehlen.

Schlüsselwörter

Cloud-Computing, Dateiablage, Datenschutz, Sicherheitsrisiko, Sicherheitsvorfall

Inhaltsverzeichnis

1. ANGRIFFSMETHODIK

Cloud-Storage ist ein Service zur Speicherung von Daten, welche über das Internet oder ein anderes Netzwerk an ein externes Speicherungssystem übermittelt werden, das von Dritten betrieben wird. Mit der steigenden Nachfrage nach Möglichkeiten zur effizienten sowie praktischen Übermittlung und Speicherung von Daten wachsen auch die Nutzerzahlen von Cloud-Systemen. Trotz der attraktiven Vorteile dieser Art des Outsourcings von Daten ergeben sich konträr dazu vielseitige Sicherheitsrisiken: Die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit sind bedroht, da sich die Daten der direkten Kontrolle durch den eigentlichen Besitzer entziehen (Zhang et al., 2020).

1.1 Angriffsarten

Es wird zwischen verschiedenen Arten von Angriffen unterschieden, welche bei der Nutzung von Cloud-Computing-Systemen bedacht werden müssen. Die Angriffsmöglichkeiten lassen sich zwischen passiv und aktiv unterteilen (Ruppel und Schmitz, 2020).

1.1.1 Passive Angriffe

Ein passiver Angriff kennzeichnet sich durch einen Angreifer, welcher sich Zugriff auf Informationen verschafft, ohne in das dazugehörige Cloud-System selbst einzugreifen. Da der Angreifer in diesem Fall lediglich passiv an Informationen gelangt, statt aktiv in die Dateiablage einzugreifen, fällt es in den meisten Fällen sehr schwer, diese Angriffsart zu erkennen (Ruppel und Schmitz, 2020).

Bei der Durchführung eines passiven Angriffs werden die Schutzziele der Vertraulichkeit sowie der Authentizität bedroht. Es ist somit möglich, dass Informationen von unbefugten Personengruppen abgerufen werden. Dabei ist es denkbar, dass ein Kommunikationspartner unter Vortäuschung falscher Identität Zugriff auf die Daten erhält. Ein Beispiel für einen passiven Angriff stellt das Mithören oder Mitschneiden von Informationen über das Netzwerk dar (Harkut, 2020).

1.1.2 Aktive Angriffe

Aktive Angriffe sind gefährlicher als passive Angriffe einzuordnen. Bei dieser Angriffsform wird der Angreifer selbst durch sein Handeln aktiv. Es erfolgt ein Eingriff auf die Daten des Unternehmens, indem die Data etwa modifiziert oder gelöscht werden. Es können zudem vorhandene Schwachstellen im System wie Sicherheitslücken offenbart und ausgenutzt werden. Auch die Sabotage hinsichtlich der Verfügbarkeit von Diensten oder beteiligten Diensten für das Unternehmen durch den Angreifer ist denkbar (Zhang et al., 2020).

Im Gegensatz zu passiven Angriffen kann ein aktiver Angriff jedoch leichter aufgedeckt werden. Häufig werden bei der Ausführung des Angriffs Spuren hinterlassen, sodass der Angriff oder sogar der ausführende Angreifer selbst enttarnt werden kann. Aktive Angriffe können zusätzlich auch als Vorbereitung auf einen passiven Angriff des Cloud-Systems dienen. Dazu wird beispielsweise der Datenstrom in der Art umgelenkt, dass der ausführende Angreifer schließlich passiv die Informationen Mitschneiden kann (Ruppel und Schmitz, 2020).

In der Folge sind bei einem aktiven Angriff alle drei primären Schutzziele der Informationssicherheit bedroht: Die Vertraulichkeit, Integrität und Verfügbarkeit. Es Daten werden unbefugt an Dritte preisgegeben (Vertraulichkeit), können in der Folge manipuliert und verändert werden (Integrität) und stehen schließlich nicht mehr wie vorhergesehen für berechtigte Nutzer zur Verfügung (Verfügbarkeit). Im besonderen Maße ist zudem auch die Authentizität bedroht, da ein Dritter sich unvermittelt unter falscher Identitätsangabe Zugriff auf vertrauliche Daten verschafft. Die Vertrauenswürdigkeit der Nutzer wird somit maßgeblich bedroht (Ruppel und Schmitz, 2020).

1.2 Bedrohungstypen

Man unterscheidet verschiedene Formen von Bedrohungen und Angreifern, welche bei der Nutzung von Cloud-Computing-Systemen auftreten können. Gefahren für Cloud-Systeme lassen sich als Bedrohungen internen und externen Ursprungs klassifizieren (Zhang et al., 2020).

Tiefergehend kann auch hinsichtlich der entsprechend maßgeblichen Intention des Angreifers unterschieden werden. Häufig erfolgen Angriffe etwa aus „Spaß, Interesse, Unzufriedenheit oder auch aus kommerziellen oder terroristischen Gründen“ (Ruppel und Schmitz, 2020). Das Cloud-Computing-System kann dabei sowohl

als Ziel des Angriffs selbst oder auch als Werkzeug zur Ausführung des eigentlichen Angriffs Anwendung finden. Letzteres ist etwa bei der Verwendung von Botnetzen durch den Angreifer denkbar, da die dafür entsprechend nötigen Ressourcen in Form von Cloud-Systemen potenziell nutzbar sind (Ruppel und Schmitz, 2020).

1.2.1 Interne Bedrohungen

Ein häufig unterschätztes Risiko für die Sicherheit der firmeneigenen Daten stellen die internen Stakeholder des Cloud-Providers selbst dar. Zu den internen Angreifern zählen etwa die „(temporären oder externen) Mitarbeiter [...], Dienstleister [...], Kooperationspartner oder Praktikanten des Cloud-Computing-Anbieters [sowie] auch die Kunden des Cloud-Computing-Anbieters“ (Ruppel und Schmitz, 2020).

Die Intention der Mitarbeiter kann sich dabei unterscheiden. Ist das Ziel des Angriffs etwa eine Schädigung des Kunden selbst oder die des Cloud-Computing-Anbieters? Entsprechend kann eine Verärgerung, Unzufriedenheit oder vorangehende Kündigung des Mitarbeiters die Ursache sein. Auch eine Fremdmotivation, beispielsweise mittels Erpressung oder Bestechung durch externe Parteien, ist ein denkbarer Anlass, dass ein Mitarbeiter zum internen Angreifer wird (Harkut, 2020).

Mit dem Ziel, einen möglichst großen Schaden anzurichten, können zahlreiche Methoden Anwendung finden. Denkbare Handlungen sind etwa „die Modifikation oder das Herunterfahren von virtuellen Maschinen, Herunterfahren von Hosts, Löschung von Daten, Dekonnektierung wichtiger Netzelemente oder die Manipulation von Konfigurationsdateien“ (Ruppel und Schmitz, 2020).

Auch die Kunden eines Cloud-Computing-Anbieters können eine mögliche Bedrohung darstellen. Potenziell ähnliche Motive sind etwa „Verärgerung, Unzufriedenheit oder auch [...] Spaß oder Interesse am Stören der Verfügbarkeit des Systems“ (Ruppel und Schmitz, 2020). Als Gefahren für die SWDS sollten demnach vor allem Angriffe auf die firmeninternen Daten in Erwägung gezogen werden: Ein unberechtigter Zugriff auf gespeicherter Daten sowie eine Modifikation oder Löschung von Daten der SWDS sind denkbar. Ferner sind auch eine Übernahme der Kontrolle virtueller Maschinen, ihrer Kommunikation oder der Zugriff auf Dateisysteme des Hosts potenziell möglich (Zhang et al., 2020).

1.2.2 Externe Bedrohungen

Ein allgemein besonders bekannter Typus der Bedrohung auf IT-Systeme sind externe Angreifer. Man unterscheidet zwischen Hackern, Crackern und Script Kiddies, welche jeweils verschiedene Merkmale hinsichtlich Motivation und Ziel des Angriffs aufweisen (Harkut, 2020).

Als Hacker werden Personen bezeichnet, die aus ihrem starken Interesse für Technik folgend auch ein umfangreiches Wissen im Bereich computertechnischer Systeme und ihrer Vorgänge besitzen. Im Bezug auf die Sicherheit von Systemen weisen sie zudem einen hohen Kenntnisstand sicherheitstechnischer Themen auf. Ihr Ziel liegt in der Überwindung von Sicherheitsmechanismen, um Schwachstellen zu erkennen. Dies ermöglicht ihnen den Zugriff auf Netzwerke, virtuelle Maschinen oder auch fremde Daten, zu dem sie nicht autorisiert sind. Hacker greifen ihr Ziel folglich nicht direkt an, sondern verschaffen sich Zugang dazu. Ein sogenannter „Hackerangriff“ wäre somit für die SWDS als vergleichsweise eher geringes Risiko einzustufen, da keine Intention zur Verursachung von Schaden besteht. Trotzdessen befinden sich Hacker zweifelsohne bei vergleichbaren Handlungen im illegalen Strafraum, da sie sich etwa unautorisierten Zugriff zu Daten verschaffen, was nicht im Sinne der SWDS ist (Ruppel und Schmitz, 2020).

Eine große Sicherheitsbedrohung stellen Cracker dar. Diese besitzen technisch vergleichbare Fähigkeiten zu den Hackern, weisen jedoch eine bewusste Motivation auf, sich durch ihr Handeln Vorteile zu verschaffen oder Schaden zu verursachen. Es besteht eine kriminelle Handlungsabsicht. Es können Angriffe auf Webserver, eine Manipulation von Daten oder DDoS-Angriffe stattfinden, um Schaden am Cloud-Computing-System zu verursachen. Letztere Angriffsart zielt darauf ab, die Verfügbarkeit des Cloud-Systems einzuschränken. Bei einem DDoS-Angriff auf das Cloud-System der SWDS ist es möglich, dass auf die Cloud und damit auch die darin gespeicherten Daten nicht mehr zugegriffen werden kann. Dies wird erreicht, indem der Server mittels Botnetz, gekaperten Systemen durch Malware-Infektion, mit Anfragen überlastet wird, bis er jene nicht mehr bewältigen kann. Schlussendlich bricht das Netzwerk zusammen (Petrosyan, 2022).

Eine weitere potenzielle Bedrohung für die SWDS stellen Script Kiddies dar. Auch wenn diese unerfahren und planlos in ihrem Vorgehen sind, besteht dennoch die Intention zur Verursachung von Schaden am System. Ein konkreter Angriff auf Daten der SWDS ist als eher gering einzustufen, sollte aber dennoch in Erwägung gezogen werden (Ruppel und Schmitz, 2020).

2. SCHUTZMAßNAHMEN

Um die vielfältigen Vorteile des Cloud-Computings unter möglichst hohen Sicherheitsstandards zu nutzen, sind entsprechende Sicherheitsvorkehrungen erforderlich. Zum Entgegenwirken der erfassten Methoden zum Angriff des Cloud-Systems lassen sich zahlreiche Abwehrmaßnahmen definieren. Unter Befolgung dieser Empfehlungen kann die Bewahrung der Schutzziele der Informationssicherheit für die SWDS sichergestellt werden (Harkut, 2020).

2.1 Verschlüsselung von Daten

Ein maßgeblicher Standard zum Datenschutz in Cloud-Systemen stellt die Verschlüsselung von Daten dar. Zur Bewahrung der Schutzziele der Vertraulichkeit sowie der Authentizität lässt sich somit beispielsweise ein passiver Angriff abwehren. (Ruppel und Schmitz, 2020).

Das Ziel der Verschlüsselung ist es, das Mithören von Informationen für potenzielle Angreifer zu erschweren. Die übertragenen Daten werden dazu verschlüsselt oder mittels weiterer Maßnahmen geschützt (Zhang et al., 2020).

Allgemein ist in Cloud-Computing-Systemen ein gewisser Sicherheitsstandard maßgeblich. Eine verschlüsselte Übertragung von Konsumentendaten zum Cloud-Service-Provider ist weit verbreitet und sollte stets sowie für alle Daten der SWDS Anwendung finden. Sofern die Möglichkeit zur unverschlüsselten und zur verschlüsselten Übertragung von Daten besteht, kann durch Konfiguration der Firewall eine SSL-Verbindung über HTTPS erzwungen werden. Diese Verschlüsselungsform endet jedoch in den meisten Fällen beim Übergang des öffentlichen Netzwerks in das private Netzwerk des Cloud-Providers. Im privaten Netzwerk des Anbieters selbst sind die Daten folglich meist unverschlüsselt und werden ebenso in dieser Form gespeichert. In diesem Netzwerk wäre somit die Möglichkeit für einen passiven Angriff gegeben. Es ist entsprechend ratsam, dass die SWDS bei der Wahl des Cloud-Providers darauf achtet, dass dieser vergleichbare Vorkehrungen trifft, etwa durch Isolierung des Datenverkehrs einzelner Benutzer (Ruppel und Schmitz, 2020).

Bei einem unverschlüsselten privaten Netzwerk des Cloud-Providers ist zudem denkbar, dass Netzwerkadministratoren auf den Servern des Anbieters Zugriff auf sensible Unternehmensdaten erhalten. Entsprechend wird von der IT-Administration geraten, eine Folgeuntersuchung der Verschlüsselungsform des derzeitig genutzten firmeninternen Cloud-Systems der SWDS durch den CISO in Auftrag zu geben. Es ist maßgeblich abzuklären, ob die momentanen Systeme eine Verschlüsselung etwa via SSL vorweisen sowie ebenso erforderlich festzustellen, ob eine Verschlüsselung auf Server-Seite oder Client-Seite erfolgt. Sollten die Vorkehrungen nicht den beschriebenen Standards entsprechen, wird ein dringendes Handeln durch den CISO angeraten (Steiner, 2013).

Eine weitere, tiefergreifende Maßnahme zur Verschlüsselung stellt das Ersetzen wichtiger Daten durch Platzhalter dar. Es ist zudem denkbar, dass die SWDS gänzlich darauf verzichtet, eine Übertragung sensibler Daten an den Cloud-Anbieter durchzuführen (Ruppel und Schmitz, 2020).

2.2 Security-Monitoring

Vor allem für die Erkennung aktiver Angriffe, aber auch für den Erhalt eines allgemeinen Sicherheitsstandards ist die Durchführung eines Security-Monitoring durch den Cloud-Provider sowie den Kunden selbst von Bedeutung. Zur Erkennung von Angriffen sind etwa Firewalls, Honeypots, IDS oder IPS verbreitete Technologien (Ruppel und Schmitz, 2020).

Durch eine vergleichbare regelmäßige Untersuchung und Überwachung des Cloud-Systems können in der Folge passive als auch aktive Angriffe bereits frühzeitig entdeckt sowie im Idealfall gänzlich verhindert werden. Dazu können zusätzlich automatisierte oder manuelle Tests genutzt werden. Mittels dieser kann eine stetige Überprüfung der Sicherheit des Cloud-Systems gewährleistet sowie potenzielle Sicherheitsbedrohungen aufgeklärt werden. Dieses Vorgehen wird etwa vom Sicherheitslabor des Fraunhofer SIT angewandt. Folglich wird von der IT-Administration eine entsprechende Empfehlung für ein ständiges Security-Monitoring gegeben, um einen umfassenden Schutz der Daten der SWDS im Cloud-System zu gewährleisten (Zhang et al., 2020).

2.2.1 Firewall

Eine Firewall ist eine Vorrichtung, die den ein- und ausgehenden Netzwerkverkehr überwacht. Auf Grundlage zuvor definierter Sicherheitsregeln entscheidet sie, ob ein Datenverkehr jeweils zugelassen oder blockiert wird. Eine Firewall fungiert als Trennwand zwischen geschützten und kontrollierten Bereichen des internen

Netzwerks sowie nicht vertrauenswürdigen, äußeren Netzwerken. Sie sichert dadurch den Schutz des Netzwerks ab (Berkenkopf, 2022).

Erweiterungsformen zu einer komplexeren Art der Firewall bieten verschiedene Module. Ein Intrusion Detection System (IDS) ermöglicht die Erkennung unerlaubter Eingriffe. Ein Intrusion Prevention System (IPS) realisiert die Prävention dieser unerlaubten Eingriffe (Berkenkopf, 2022).

2.2.2 Honeypot

Ein sogenannter „Honigtopf" dient als Art Lockmittel für potenzielle Angreifer. Dieser kann die Sicherheit des Netzwerks erhöhen, indem er bestimmte Dienste oder Verhaltensweisen simuliert. Im Vergleich zum realen Netzwerk, das hohe Sicherheitsstandards erfüllt, ist der Honeypot von diesem abgetrennt und schlechter gesichert. Dadurch fungiert er als Ablenkung für Angreifer, deren Aktionen entsprechend erkannt und gespeichert werden können (Lauterschlag, 2022).

In der Folge können mithilfe eines Honeypots Daten zum Verhalten und Muster von Angreifern gesammelt werden. Im Falle eines Angriffs werden die entsprechenden Informationen protokolliert und an den Administratoren weitergegeben. Dadurch bleibt im Idealfall das reale Netzwerk geschützt und vor einem Angriff bewahrt. Ferner können wertvolle Daten über die im System existierenden Schwachstellen offengelegt und für ein weiteres Security-Monitoring genutzt werden (Lauterschlag, 2022).

2.3 Zugriffsrechte

Es ist von Bedeutung, dass sowohl vom Cloud-Computing-Anbieter als auch der SWDS selbst die Zugriffsrechte aller Personen überprüft werden.

2.3.1 Zugriffsrechte durch den Cloud-Computing-Anbieter

Die Handhabung der Konfigurationsrechte durch den Cloud-Provider ist essenziell bei der Wahl des Anbieters für die SWDS.

Zum Schutz vor Angriffen ist es für den Cloud-Computing-Anbieter maßgeblich, eine Trennung von Funktionen und Rollen der Mitarbeiter einzuhalten. Dadurch können interne Angriffe durch Mitarbeiter verhindert beziehungsweise erschwert werden, da der Zugriff auf gewisse Kundendaten jeweils nur auf beschränkte Bereiche des Cloud-Systems ermöglicht wird. Auch die Einhaltung allgemeiner Sicherheitsrichtlinien sowie die Umsetzung des „4-Augen-Prinzips" erhöht die Sicherheit: Vor jedem Datenzugriff sind dabei weitere Bestätigungen von Nöten, die wiederum durch andere Mitarbeiter autorisiert werden müssen. Entsprechend kann die Gefahr zu einem durch Einzelmotivation entstehenden internen Angriff verringert werden (Ruppel und Schmitz, 2020).

Auch die Kunden von Cloud-Computing-Anbietern können eine Bedrohung darstellen. Zum Schutz vor Angriffen auf virtuelle Maschinen sollten zudem sichere Hypervisoren genutzt sowie die Netzwerkverbindungen durch Nutzung von VPN, VLAN und Firewall sicher getrennt und geschützt sein. Auch das Härten von Betriebssystemen und Anwendungen ist von Bedeutung, indem nicht benötigte Funktionalitäten entfernt werden. Maßgeblich ist ebenso die Trennung von Daten, damit die Kunden nicht auf andere verwandte Daten Zugriff erhalten, welche nicht für sie bestimmt sind (Ruppel und Schmitz, 2020).

2.3.2 Zugriffsrechte durch die SWDS

Es ist von essenzieller Bedeutung, dass die SWDS die Konfiguration der Zugriffsrechte auf das Cloud-System innerhalb des Unternehmens möglichst durchdacht gestaltet. Es ist etwa möglich, dass ein interner, autorisierter Benutzer auf zu viele Daten zeitgleich zugreifen kann. Dadurch besteht, bewusst oder unbewusst, die Gefahr, dass durch diesen Benutzer eine Manipulation von Daten erfolgt (Harkut, 2020).

Mittels Nutzung von Produkten zur Identitäts- und Zugriffsverwaltung kann genauer verfolgt werden, welcher Benutzer auf welche Daten der Cloud Zugriff erhält. Entsprechend können die Benutzer autorisiert werden sowie unbefugte Benutzer eine Zugriffsverweigerung erhalten. Dies ist im Falle der digitalen Dateiablage essenziell, da allein die Identität und die Zugriffsrechte der Benutzer bestimmen, auf welche Daten sie zugreifen können (Cloudflare, Veröffentlichungsdatum unbekannt).

Es wäre somit tendenziell einfach für einen möglichen Angreifer, sich Zugang zu Daten zu beschaffen, wenn die Verwaltung der Zugriffsrechte nicht ernsthaft verfolgt wird. Dazu ist es erforderlich, dass die Zugriffsrechte möglichst kompakt gestaltet werden. Ein Benutzer sollte jeweils nur Zugriff zu genau den Daten erhalten, die er

benötigt. Konträr erhöht ein weites Zugriffsfeld die Menge der Daten, auf die zugegriffen werden kann, was einen potenziellen Angriff begünstigt (Harkut, 2020).

Um die Accounts der Benutzer jeweils entsprechend abzusichern, ist es wichtig, allgemeingültige Sicherheitsstandards für Passwörter zu nutzen. Diese sollten regelmäßig geändert werden und eine möglichst komplexe Struktur aufweisen, um den Zugang zu Daten der Cloud im Falle eines Angriffs möglichst schwierig zu gestalten (Harkut, 2020).

Auch Systeme zur Authentifizierung der Identität von Benutzern können hilfreich sein. Man unterscheidet zwischen verschiedenen Diensten zur Identitäts- und Zugriffsverwaltung. *Identitätsanbieter (IdP)* bewerkstelligen das Authentifizieren der Identität von Benutzern. *Single-Sign-On-Dienste (SSO)* dienen der Authentifizierung der Identität von Benutzern über mehrere Anwendungen hinweg. Ein Benutzer muss sich folglich lediglich einmal anmelden, um einen Zugriff auf alle Cloud-Dienste zu erhalten. *Multifaktor-Authentifizierungsdienste (MFA)* verstärken weiterhin den Vorgang der Benutzerauthentifizierung, indem verschiedene Mittel zur Erkennung des Benutzers genutzt werden. *Zugriffskontrolldienste* ermöglichen die Zulassung oder Einschränkung des Zugriffs durch einen Benutzer (Cloudflare, Veröffentlichungsdatum unbekannt).

Ferner kann es hilfreich sein, eine Schulung der Mitarbeiter der SWDS zum Umgang mit dem Cloud-System und generellen Sicherheitsstandards anzubieten. Häufig treten Sicherheitsvorfälle etwa aufgrund von Phishing-Angriffen auf, welche auf die internen Benutzer abzielen. Dabei wird unwissentlich Malware installiert, ein anfälliges Gerät genutzt oder ein unsicherer Umgang mit Passwörtern praktiziert. Eine entsprechende Aufklärung über die wichtigsten, durch die Mitarbeiter anzuwendenden Standards kann dabei Abhilfe schaffen, das Sicherheitsrisiko zu minimieren (Cloudflare, Veröffentlichungsdatum unbekannt).

3. AUSWIRKUNGEN DES ANGRIFFS

Sollte sich ein Sicherheitsvorfall in Bezug auf das Cloud-System ereignen, kann dies prekäre Nachwirkungen erzielen. Es sind dabei verschiedene Szenarien mit jeweils individuellen Folgen für die SWDS zu unterscheiden.

3.1 Datenleck

Es besteht die Möglichkeit, dass die Daten der SWDS nicht oder nicht hinreichend verschlüsselt sind und vollständig transparent in den Cloud-Speicher gesendet werden. Unter dieser Annahme sind alle übermittelten firmeninternen Informationen nicht nur den Netzwerkadministratoren auf Seiten des Cloud-Providers zugänglich, sondern zudem potenzielles Ziel eines passiven Angriffs auf die Cloud. Das Mithören von Informationen durch unbefugte Dritte wäre somit denkbar. Es besteht folglich die Möglichkeit, dass nicht nur die Schutzziele der Vertraulichkeit sowie der Authentizität gebrochen werden: Im fatalen Fall ist die Entwendung sämtlicher Daten der SWDS möglich. Eine Folgeuntersuchung wird in Anbetracht dieser Tatsache dringend von Seiten der IT-Administration empfohlen (Steiner, 2013).

3.2 Unbemerkter Angriff

Durch ein fehlendes Security-Monitoring können Angriffe auf das Cloud-System unbemerkt stattfinden. Eine reale Bedrohung stellt dabei eine Ransomware-Attacke dar (Posey, 2021).

Es können zwei Hauptfaktoren unterschieden werden, welche die Effektivität eines Angriffs mit Ransomware maßgeblich beeinflussen. Essenziell ist zum einen der genaue Typ der Ransomware. Je nach Aufbau unterscheiden sich auch die Funktionen; teilweise sind bestimmte Ransomware-Varianten effektiver auf Cloud-Systeme als andere. Einen zusätzlichen Faktor stellt das Maß an Berechtigungen dar, welcher dem Benutzeraccount gewährt wurde, durch welchen der Angriff unwissentlich initiiert wird. Je höher der Berechtigungsgrad, desto schädlicher kann der Angriff in der Folge sein (Posey, 2021).

Unter konkreter Fallbetrachtung kann das fatale Ausmaß eines Ransomware-Angriffs erkannt werden: Es wird angenommen, dass der Computer eines Mitarbeiters der SWDS als Initiator für eine Attacke fungiert. Das Gerät verfügt über ein Netzlaufwerk, einer Art lokalem Speicher, das mit dem Cloud-Speicher verbunden ist. Ein Ransomware-Angriff kann in diesem Fall alle Daten der Dateiablage, auf die der Nutzer Zugriff hat, verschlüsseln. Betroffen sind somit nicht nur die privaten Daten des Endnutzers: Da die Ransomware nicht zwischen lokalen und remote gespeicherten Daten unterscheidet, sind potenziell alle Daten auf der Cloud-Freigabe in Gefahr (Posey, 2021).

Es besteht folglich die Möglichkeit, dass sämtliche Daten der SWDS verschlüsselt und dadurch unbrauchbar

gemacht werden. Die augenscheinliche Gefahr durch eine vergleichbare Ransomware-Attacke ist als sehr hoch einzustufen. Das Team der IT-Administration gibt eine dringende Empfehlung zur Einschränkung der internen Benutzerberechtigungen ab, um das Risiko zu minimieren (Posey, 2021).

3.3 Unautorisierter Zugriff

Aufgrund einer mangelhaften Verwaltung der Zugriffsrechte des Cloud-Anbieters, welche bei der Wahl des Providers nicht bedacht wurde, oder innerhalb der Mitarbeiterschaft der SWDS selbst kann eine Möglichkeit zur Durchführung eines unautorisierten Zugriffs auftreten. Bei einer entsprechend negativ motivierten Person, etwa einem kürzlich gekündigtem Mitarbeiter, kann in der Folge die Absicht entstehen, dem Unternehmen einen größtmöglichen Schaden zuzufügen. Konkret heißt das für die SWDS, dass etwa umfassende Daten gelöscht oder manipuliert werden. Auch wichtige Netzelemente können dekonnektiert, virtuelle Maschinen modifiziert oder Konfigurationsdateien manipuliert werden (Harkut, 2020).

Es besteht in der Folge ein umfassendes Risiko für die Systeme und Daten der SWDS, welches aus Sicht der IT-Administration durch den CISO mit hoher Priorität abgeklärt werden sollte. Für eine Zusammenarbeit steht das Team der IT-Administration zur Verfügung (Harkut, 2020).

4. REFERENZEN

4.1 Literatur

Harkut, D. G. (2020) - Cloud Computing Security - Concepts and Practice, IntechOpen, 1. Auflage, Kapitel 1-5 , London.

Zhang, Y., Xu, C. und Shen, X. (2020) - Data Security in Cloud Storage, Springer, 1. Auflage, Kapitel 1-6, Singapur.

4.2 Weitere Quellen

Berkenkopf, S. (2022, 26. September) - Was ist eigentlich eine Firewall?, G DATA, G DATA CyberDefense AG, Bochum, unter: www.gdata.de/ratgeber/was-ist-eigentlich-eine-firewall

Cloudflare (Veröffentlichungsdatum unbekannt) - Wie funktioniert Cloud-Sicherheit? | Sicherheit beim Cloud Computing, Cloudflare, Inc., San Francisco, unter: www.cloudflare.com/de-de/learning/cloud/what-is-cloud-security

Lauterschlag, E. (2022, 19. Mai) - Honeypot – Sicherheitssystem um Hacker in die Falle zu locken, Was ist Malware?, AlsterPixel, Winsen, unter: www.was-ist-malware.de/it-sicherheit/honeypot

Petrosyan, K. (2022, 12. August) - DDoS vs. DoS Attacks: What's the Difference?, EasyDMARC, unter: www.easydmarc.com/blog/de/ddos-vs-dos-attacks-whats-the-difference

Posey, B. (2021, 21. April) - So können Ransomware-Attacken auch Cloud Storage angreifen, ComputerWeekly.de, TechTarget, Inc., Newton, unter: www.computerweekly.com/de/tipp/So-koennen-Ransomware-Attacken-auch-Cloud-Storage-angreifen

Ruppel, A. und Schmitz, P. (2020, 11. März) - Cloud Security Teil 2: Sicherheitsrisiko Cloud Computing - Angriffsarten und Angreifertypen in Cloud-Computing-Systemen, Security Insider, Vogel Communications Group, Würzburg, unter: www.security-insider.de/angriffsarten-und-angreifertypen-in-cloud-computing-systemen-a-254228

Steiner, D. (2013, 29. April) - SSL, Server-seitig, Client-seitig: Cloud-Daten sicher verschlüsseln, Computer Woche, IDG Tech Media GmbH, München, unter: www.computerwoche.de/a/cloud-daten-sicher-verschluesseln,2536499