Herausforderungen für die digitale Forensik in Cloud-Umgebungen

BLICK IN DIE GROSSEN „VERSTECKE“ VON CYBERKRIMINELLEN

Serviceangebote aus der Public Cloud schießen derzeit förmlich durch die Decke. Obwohl Corona in einzelnen Bereichen Cloud-Projekte verzögert, gehören die Digitalisierung und damit auch Cloud Services zu den eindeutigen Gewinnern in der Krise. Doch mit der Auslagerung von IT-Services im großen Maßstab in die Cloud, nehmen auch Cyberkriminelle dieses Umfeld mehr und mehr ins Visier. Cloud Service Provider sind zwar in der Regel sicherheitstechnisch immer auf dem neuesten Stand – aber auch sie sind angreifbar. Damit Cyberkriminelle in Cloud-Umgebungen keine Chance haben, den Blicken von Unternehmen und Strafverfolgungsbehörden zu entgehen, ist eine umfassende digitale Forensik erforderlich. In der Praxis bestehen dafür jedoch große Hürden. Deshalb müssen hier jetzt schnell neue, kreative Ansätze gefunden werden.

Cloud Computing bietet zahlreiche Vorteile. So werden dem Cloud-Kunden je nach Wunsch verschiedene Servicemodelle gegen Bezahlung zur Verfügung gestellt. Im Kern spielen sich diese Dienste auf drei Ebenen ab:

- Cloud-Computing, Infrastructure as a Service (IaaS),
- Platform as a Service (PaaS) und
- Software as a Service (SaaS).

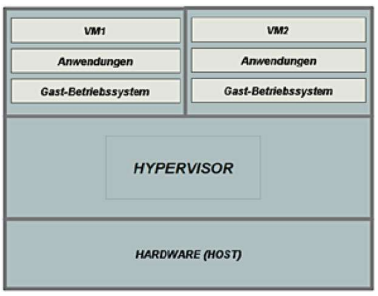
Da die gesamte Infrastruktur, die Plattform oder die Software bereitgestellt wird – oder jeweils Teile davon, spart der Nutzer erheblich an Kosten bei einem höheren Level an Qualität des Dienstes. Zu nennen sind vor allem die fixen Investitionskosten und -risiken, die wegfallen und zu variablen Kosten werden, die sehr feinteilig am tatsächlichen Bedarf ausgerichtet sind. Dazu kommen die weiteren Vorteile der zeitnahen Skalierbarkeit von IT-Leistungen (nach oben und unten): der reduzierte Administrationsaufwand und eine verbesserte Verfügbarkeit der Dienste. Wegen all dieser Vorzüge nutzen immer mehr Unternehmen die Möglichkeit, ganz oder teilweise IT-Infrastruktur, Plattformen und Software out zu sourcen oder von Beginn der Unternehmung an von dieser Alternative Gebrauch zu machen.

WO LICHT IST, IST AUCH SCHATTEN

Da nun immer mehr geschäftskritische Aufgaben und Daten in die Cloud ausgelagert werden, und das an einer oder wenigen zentralen Stellen, werden diese immer attraktiver für Angreifer. Generell sind alle in der IT möglichen Angriffsszenarien bei Cloud Service Provider (CSP) denkbar. Durch Maßnahmen wie dem Einsatz von cloudbasierten VPNs und stabilen HTTPS-URLs

Bild: ©alphaspirit - stock.adobe.com

für Cloud-Run-Dienste lässt sich bereits einem großen Teil der Angriffsvektoren ein wirksamer Riegel vorschieben.[1] Somit konzentrieren sich die meisten Angreifer die schwächsten verbleibenden Stellen der IT-Infrastruktur. Dazu gehört nach wie vor die Fehlkonfiguration der Cloud-Plattform, die Verwendung unsicherer Schnittstellen zwischen Programmen und die Entwendung von Accounts, Services und Datenverkehr. Durch den Einsatz der Hypervisor-Technologie, welche erst das eigentliche Cloud Computing ermöglicht, entstehen zusätzliche Schwachstellen. Als Single Point of Failure stellt diese Abstraktionsschicht eine besonders kritische Komponente dar. Auch hier sind eine Reihe möglicher Angriffsvektoren denkbar, wie zum Beispiel Seitenkanalangriffe, Privilegien-Eskalation oder der unerlaubte Zugriff auf Speicher. Zurzeit sind zwar kaum Angriffe öffentlich bekannt, dass dies aber theoretisch möglich ist, zeigen die über 130 bekannten Schwachstellen in Hypervisor Software. Diese Verwundbarkeiten sind in öffentlichen CVE-Datenbanken (Common Vulnerabilities and Exposures) zu finden. Mittels falscher Identitäten oder entwendeter Accounts verschaffen sich Angreifer Zugang zu den Cloud-Servern.



Native Virtualisierung auf der Hardwareebene (Quelle: ifis)

WARUM IST DIGITALE CLOUD-FORENSIK NOTWENDIG?

Digitale Forensik ist die Grundlage, auf der Straftaten im Cyberraum verfolgbar sind. Sie bildet damit eine unverzichtbare Disziplin sowohl für die Strafverfolgungsbehörden, als auch für Unternehmen. Cyberkriminelle müssen verfolgbar bleiben und zur Rechenschaft gezogen werden. Gleichzeitig ist es wichtig, Angriffsmethoden und -Tools zu erkennen, um im Sinne eines besseren Schutzes aus Angriffen zu lernen. In besonderem Maße gilt das etwa für Advance Persistent Threats (APTs), die einen komplexen, zielgerichteten und effektiven Angriff auf IT-Infrastrukturen durchführen. Durch Manipulation und Diebstahl wichtiger Daten können Unternehmen finanziell in Bedrängnis geraten, oder ihre reale Infrastruktur könnte mit unvorhersehbaren Folgen kollabieren (Elektrizitätswerke, Chemiewerke etc.).

Auch die Technologie als solche kann in Verruf geraten. Daher sollten alle Angriffe zeitnah erkannt, umgehend analysiert und ausgewertet werden. Hierbei müssen Kenntnisse zu den Gründen, Quellen und Auswirkungen des Vorfalls gesammelt werden. Schädliche Anwendungen, korrumpierte Dateien und gefährliche Malware müssen unverzüglich analysiert werden. Dies dient auch der schnellen Wiederherstellung des Normalbetriebs. Ein Schließen der Sicherheitslücken ist so umgehend möglich. Mittels maschinellen Lernens können Komponenten, wie das Intrusion-Detection- und das Intrusion-Prevention-System, mit Mustern trainiert werden, damit sie rechtzeitig alarmieren. Ermittelte Angriffsadressen können anhand von Filtern (Paket, Ingress, ...) in einer Firewall oder einem Router gesperrt werden, um das Netzwerk nach innen und außen zu schützen. Bei der Netzwerkanalyse werden Anomalien schneller identifiziert. Im Handumdrehen ist das Incident Response Management detailliert informiert und kann eine Bedrohungslage augenblicklich erkennen.

DIE KLASSISCHE DIGITALE FORENSIK

Daher ist es unentbehrlich, digitale Spuren, die in IT-Systemen gespeichert oder übertragen worden sind, zu sammeln, um den Angreifer, die Angriffsmethode, das Angriffsziel und den Schaden zu identifizieren. Diese Spureninformationen, die auf Daten basieren, können in verschiedenen Abstraktionsebenen vorliegen (Bit, Zeichenkodierung, Datei etc.). Dabei werden zwei fundamentale Analysemethoden unterschieden, um digitale Spuren zu sichern und auszuwerten.[2] Die Post-mortem-Analyse meint die Auswertung von Datenträgern ausgeschalteter IT-Systeme. Dies sind Daten auf Festplatten oder USB-Sticks, die auch ohne Stromzufuhr noch vorhanden sind. Das andere Verfahren ist die Live-Analyse. Dabei werden flüchtige Daten live oder mithilfe einer Forensik-Protokolldatei gespeichert. Zum einen sind dies Daten, die dauerhaft bei Stromzufuhr gespeichert werden können (RAM) und andererseits temporär zu speichernde Daten bei Stromzufuhr, wie beispielsweise Netzwerkdaten.

Beide Arten von Spuren sind zudem fragil. Daher muss bei der Sicherung und Auswertung stets darauf geachtet werden, dass die Spureninformationen nicht verändert, manipuliert oder zerstört werden können. Das heißt, die Integrität und die Authentizität der gesicherten Daten müssen gewährleistet sein.

Damit bestimmte Verfahrensweisen und Kriterien standardisiert werden können, haben sich verschiedene, jedoch ähnliche Vorgehensmodelle entwickelt. Der forensische Prozess nach Casey korreliert hierbei am ehesten mit der Vorgehensweise in der Cloud-Forensik. Zu Beginn erfolgt die operative Vorbereitung. Dieser Punkt spielt eine eher untergeordnete Rolle, wird oft weggelassen und in der Beschreibung der Cloud-Forensik gar nicht erwähnt. Er verlangt einen Aktionsplan und die Beschaffung der Werkzeuge, welche zur Sammlung, Sicherung und Analyse der Daten benötigt werden. Dann folgen die Umfrage und Identifikation. Potenzielle Quellen für digitale Beweise müssen an einem Tatort, zum Beispiel innerhalb der Organisation, festgestellt und gesammelt werden. Als Nächstes folgt die Bewahrung. Relevante Protokolldateien werden gesichert und das IT-System sollte vom Netzwerk isoliert werden. Zuvor müssen die flüchtigen Daten vor dem Abschalten aktiv bewahrt werden. Die Untersuchung und Analyse der gesicherten digitalen Beweise schließen sich daran an. Als letzte Maßnahme erfolgt eine Präsentation, die dem Kontext der Untersuchung gerecht wird.

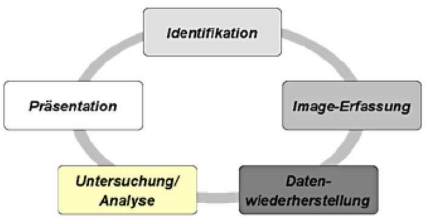
DIE DIGITALE FORENSIK IN GETEILTEN VERANTWORTUNGEN

Nicht nur die Verantwortung für die Sicherheit liegt im geteilten Modell des Cloud Computings je nach Service-Modell teilweise beim Cloud Provider und partiell beim Kunden, sondern auch die Kontrolle über die IT-Infrastruktur. Beim Software-as-a-Service-Modell hat der Kunde keine Möglichkeit, den forensischen Prozess zu unterstützen. Die Kontrolle der Hardware, des Betriebssystems, der Anwendung und der Daten

liegt im vollen Umfang beim CSP. Bei der Lösung Platform as a Service gibt der Cloud Provider lediglich die Kontrolle über die Anwendung und teilweise über die Daten ab. Es besteht oftmals die Möglichkeit, die eigenen Daten zu verschlüsseln. Dies erschwert die Reaktionszeit eines forensischen Teams erheblich, beziehungsweise macht eine Analyse ohne Entschlüsselung bestimmter Daten unmöglich. Dieses Problem besteht auch beim Modell Infrastructure as a Service. Allerdings hat der Kunde hier die Kontrolle über das Betriebssystem und die Anwendung. Das gibt ihm die Möglichkeit, eigene Snapshots seiner Virtuellen Maschinen (VMs) zu erstellen, um mögliche forensische Spuren zu sichern.

DIE HAUPTVERANTWORTUNG LIEGT BEIM CLOUD SERVICE PROVIDER

Die Verantwortung einer schlüssigen Cloud Forensik liegt daher hauptsächlich beim Cloud-Anbieter. Generell sind Angriffe auf die Infrastrukturebene, zum Beispiel die Abstraktionsschicht, ohnehin nur schwer erkennbar. Kompromittierte VMs müssen zudem lokalisiert werden. CSPs besitzen meist mehrere Rechenzentren mit Tausenden von Servern, sodass eine Ortung einen erheblichen Zeitaufwand bedeutet. Ohne Migrationsverzeichnis ist das sogar unmöglich. Beim Herunterfahren der VMs geht das jeweilige Image verloren – und damit auch die Möglichkeit zur Bestimmung der zugrunde liegenden Hardware. Ein Angreifer mit Zugriff auf eine VM kann so seine Spuren verwischen. Liegt die forensische Untersuchung nicht beim CSP, muss die ermittelnde Stelle (Behörde, Unternehmen etc.) ebenfalls erst Zugang zu den Beweismitteln erhalten. Das Einholen einer richterlichen Anordnung braucht Zeit. Aufgrund der verteilten Aufbewahrung der Spureninformationen über Ländergrenzen hinweg ist eine Sicherstellung von Beweisen daher ungewiss.



Wichtige forensische Schritte in der Cloud. (Quelle: ifis)

PROBLEME BEI DER DATENSAMMLUNG UND BEWAHRUNG

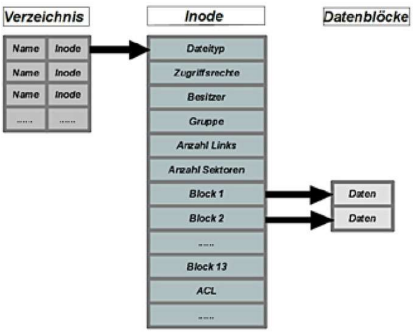
Ist eine virtuelle Festplatte gelöscht, steht ihre Kapazität wegen der cloudtypischen Speicherkonsolidierung sofort wieder anderen Anwendungen zur Verfügung. Daher erfolgt in der Regel eine sehr schnelle Überschreibung ihrer Daten. Durch Ressourcenpooling geschieht dies nicht nur bei Neustart der eigenen Ressourcen, sondern durch alle neu aufgesetzten Komponenten aller Kunden innerhalb der Cloud. Die virtuelle Festplatte besteht aus zwei Dateien, dem Base-Image und der Root-Disk.[3] Letztere speichert die Änderungen am Base-Image, wenn die Dateigröße wächst. Dieses Wachstum der Root-Disk hat eine starke Fragmentierung zur Folge. Werden Blöcke der virtuellen Festplatte größer zusammengestellt, als sie auf der physischen Festplatte vorhanden sind, kann es zu einer weiteren Fragmentierung kommen. Diese Art der Zerlegung von zusammenhängenden Dateien kann um den Faktor 1.000 ansteigen, im Gegensatz zu Festplatten im herkömmlichen Einsatz. Dies wiederum erschwert die Spurensuche anhand von Dateisignaturen (Carving), ebenso wie die Suche nach logischen Werten und Phrasen (Logische Dateisystemsuche) ungemein.

Einige Werkzeuge bieten eine logische Dateisuche an. Mithilfe von Metadaten ist es möglich, einzelne Speicherblöcke in die richtige Reihenfolge zu bringen. Dies ermöglich auch dann eine Stichwortsuche, wenn die Daten fragmentiert abgelegt sind. Die Phrase muss allerdings mindestens im Umbruch der Blöcke auftreten. Sind Blöcke in der virtuellen Umgebung kleiner als auf der physischen Festplatte angeordnet, sind meistens Blöcke miteinander verschmolzen. Dieser Umstand und bereits überschriebene Metadaten können auch dieses Unterfangen zunichtemachen.

Ein weiterer Aspekt ist die große Datenmenge, welche durch die Fähigkeit zur Skalierung des Speichers entstehen kann. Auch hier spielt der Faktor Zeit eine entscheidende Rolle. Die Daten müssen vor der Analyse nach ihrer Relevanz selektiert werden. Den Forensikern stehen keine Werkzeuge zur Verfügung, um eine forensische Extraktion der Daten durchzuführen. Durch die gemeinsame Nutzung von Storage Pools kann es zu einem Sammeln fremder Datenbestände kommen – oder von Details, welche den eigentlichen Straftatbestand nicht betreffen, jedoch den Datenschutz der jeweiligen Betreffenden verletzen würde.

Die Bewahrung der Daten beruht zumeist auf einer Konfiszierung der physischen Hardware. Dies ist durch die genannten Charakteristika kaum denkbar. Also müsste der forensische Prozess direkt vom CSP eingeleitet werden. Hierzu gehört die Isolierung der Festplatten, der Einsatz von Write-Blockern, die Sicherung der VM-Images und das Erstellen von Eins-zu-eins-Kopien der gesicherten Komponenten. Sind die Daten während einer Live-Response-Analyse gesammelt, stellt sich die Frage, ob Teile der flüchtigen Daten nicht gesichert wurden. Wird Speicher zu klein allokiert, können beispielsweise Teile von Images verloren gehen.

Auch die gesicherten Protokolldateien müssen nicht zwingend vollständig sein. Daher stellt sich für die Ermittler immer die Frage nach der Integrität und Authentizität der gesicherten Informationen. Straftaten, die zum Beispiel nur der Provider entdeckt, könnten von ihm nicht verfolgt und veröffentlicht werden. Jedes Unternehmen würde bei erfolgreichen Angriffen und den damit verbundenen Konsequenzen (Datenklau) erheblich an Reputation verlieren. Der Provider könnte bei Bekanntwerden von Vorfällen weniger Spuren liefern, um die Konsequenzen kleinzureden.



Ext-Dateisystem für Linux Betriebssysteme: Darstellung der Dateinamensdaten und der Metadaten in Inode-Tabellen und der Daten in Clustern

UNTERSUCHUNG UND ANALYSE

Die Datenanalyse gestaltet sich durch die bereits genannten Probleme sehr schwierig. Meistens sind die fraglichen Daten bereits ganz oder teilweise überschrieben.[2][3] Eine Rekonstruktion ist daher oft nicht mehr möglich. Die Werkzeuge, die zur Verfügung stehen, sind zudem der klassischen Forensik zuzuordnen. Das bedeutet, der physische Zugang zur Hardware muss gegeben sein. Cloudspezifische Tools gibt es zurzeit noch nicht. Einheitliche Schnittstellen, die eine Live-Analyse oder ein Sichern von Hardwarekomponenten aus der Ferne ermöglichen, gibt es ebenfalls noch nicht. Unterschiedliche Ereignis- und Protokollierungssysteme der Cloud Provider erschweren es zudem, einheitliche Analyse- und Diagnose-Werkzeuge zu entwickeln.

Ein weiterer wichtiger Aspekt der forensischen Untersuchung ist die Beweismittelkette (Chain of Custody). Die Abhängigkeiten von Anbieter und Kunde können sehr dynamisch sein. So nutzen CSPs Auftragnehmer, um Ressourcen auszulagern. Zusätzlich zur verteilten Aufbewahrung erschwert dies außerdem die Rekonstruktion der Chain of Custody. Über geografische Grenzen hinweg kann eine fehlende Synchronisation von Zeitstempeln die Beweismittelkette verändern. Jede Unterbrechung, Korruption oder Veränderung in der Verwahrungskette oder ein Mangel an Koordination der Verantwortlichkeiten zwischen allen beteiligten Parteien kann eine zielführende Dokumentation zunichtemachen. Unregelmäßigkeiten könnten daher vor Gericht angefochten werden.

PRÄSENTATION

Die Dokumentation muss im letzten Schritt als gerichtsverwertbare Präsentation aufbereitet werden. Die genannte Verwahrungskette muss sequenziell und fehlerfrei angefertigt sein. Durch die Komplexität des Cloud Computing, seiner Vielzahl an Diensten und der weltweiten Verteilung auf Tausenden Servern ist die Herausforderung, ein Gesamtbild nachvollziehbar zu dokumentieren, erheblich erschwert. Nicht ausgebildete Forensiker dürften dazu kaum in der Lage sein, und ausgebildete Forensiker stehen eher selten auf der Gehaltsliste von Cloud Providern. Die komplexe Technologie mit all ihren Facetten muss außerdem vor Gericht für Nicht-Informatiker auf ein verständliches Niveau heruntergebrochen und dargestellt werden. Gerade die typischen Charakteristika des Cloud Computings, wie schnelle Elastizität und Ressourcenpooling, erschweren die Durchführung des forensischen Prozesses in der Cloud.

TECHNISCHER STAND DER CLOUD FORENSIK

Im Bereich der Identifikation, Datensammlung und der Bewahrung haben sich die CSP bisher kaum bewegt. Nachvollziehbare Wege von Daten in der zugrunde liegenden Hardware sind nicht zu ermitteln, und damit ist auch eine Datensammlung innerhalb der Organisation nicht durchführbar. Schnittstellen, um diese Aufgaben von extern wahrzunehmen, sind zurzeit nicht vorhanden, ja noch nicht einmal in Planung. Techniken zur Bewahrung der Daten, wie automatisches Isolieren der Images und die Erstellung eines Hashwertes zur Sicherung der Integrität, ein automatisch einsetzender Schreibschutz oder ein Migrationsverzeichnis, sind weder intern noch extern durchführbar. Der Zugriff auf die Protokolldateien verschiedener Komponenten ist mittlerweile möglich und wird von den Cloud Providern als Service angeboten. Dadurch steigen die Betriebskosten der Unternehmung durch zusätzlich reservierte Speicher. Der Service steht für alle drei Cloud-Service-Modelle zu Verfügung, jedoch nur als kostenpflichtige Option.

	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Benutzer	Kunde	Kunde	Kunde
Daten	Kunde	Kunde	Kunde
Applikationen	Kunde	Kunde	CSP
Operatives System	Kunde	CSP	CSP
Virtuelles Netzwerk	Kunde	CSP	CSP
Hypervisoren	CSP	CSP	CSP
Server und Speicherung	CSP	CSP	CSP
Physikalisches Netzwerk	CSP	CSP	CSP

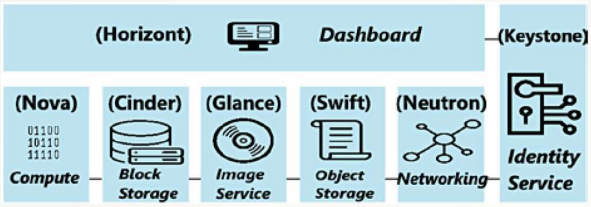
Verantwortung in den verschiedenen Servicemodellen (Quelle: ifis)

Im IaaS-Modell verwaltet der Cloud-Kunde ohnehin die meisten Komponenten selbst und hat damit Zugriff auf forensisch wichtige Daten. Spart der Dienstnehmer jedoch aus Kostengründen an diesem Service im PaaS- und SaaS-Modell, gehen alle diese Spuren verloren. Die Möglichkeiten zum Monitoring und zum Sichern der Daten bestehen dann nicht.

Eine weitere Komponente ist die automatische Ereigniskennung. Dieses Werkzeug scannt das System auf Fehlkonfigurationen, Schwachstellen und Sicherheitsvorfälle. Programmierschnittstellen (APIs) zur eigentlichen Hardware-Infrastruktur sind ebenfalls nicht vorhanden. Werkzeuge zum Testen der Hypervisor-Software auf Verletzungen sind lediglich von intern einsetzbar. Die großen Hyperscaler bieten den Kunden ein umfangreiches Monitoring an, um zusätzlich forensisch verwertbare Spuren zu sammeln. Messwerte, Ereignisse und Metadaten vieler Komponenten werden mit Diagrammen und Ereignisbenachrichtigungen informativ aufbereitet. Das Dashboard liefert mithilfe interner Tools extern dargestellte Anomalieberichte und eine Mustererkennung. Entsprechende Log-Daten zu den einzelnen Ereignissen werden dazu mitgeliefert. Um eindeutige Spuren zu sammeln, werden zusätzlich Honeypots angeboten. Sie imitieren unter anderem Server, Softwareanwendungen und APIs. Durch bewusst offen gehaltene Schwachstellen und attraktive Scheinanwendungen sollen die Angreifer anlockt werden. Da die Ähnlichkeit zu realen Infrastrukturen schwer unterscheidbar ist, können risikolos wichtige Spuren an Angriffen ermittelt werden.

MÖGLICHE LÖSUNGEN DES MOMENTANEN DILEMMAS IM FORENSISCHEN PROZESS IN DER CLOUD

Ein sehr vielversprechendes Projekt ist OpenStack,[3][4] mit dem Cloud-Architekturen auf Standard-Hardware realisiert werden können. Obwohl das viele Vorteile bietet, auch hinsichtlich forensischer Untersuchungen, wird es bislang noch sehr verhalten eingesetzt. Zudem gibt es keine Schnittstellen, um OpenStack beispielsweise mit Amazon- oder Google-Cloud zu kombinieren. Noch zieren sich die Hyperscaler, frei verfügbare OpenStack-Architekturen im großen Stil bei sich einzuführen.



Die OpenStack-Plattform als Cloud-Infrastruktur-Lösung

Neun Basiskomponenten werden von OpenStack angeboten, wovon einige die Umsetzung von Cloud-Forensik vereinfachen. Die Komponente NOVA verwaltet die VMs und nutzt vorrangig die lizenzfreien Hypervisoren der im Linux-Kernel integrierten Kernel-VMs und das von der Universität Cambridge entwickelte XEN. Dadurch kann ein komplettes Hauptspeicherabbild in einer Datei gespeichert werden, ohne eine Veränderung herbeizuführen. GLANCE ist ein Image-Service, der die Lokalität der VMs aufspürt, sie sichert und wiederherstellen kann. Zudem besteht ein Zugriff auf alle möglichen Protokoll- und Nutzungsdateien. Die Schnittstellen von OpenStack sind offen und standardisiert. Möchte man trotzdem die herkömmlichen Anbieter nutzen, aber die Problematik der Cloud-Forensik in der öffentlichen Cloud umgehen, ist im Moment nur die Nutzung einer Hybrid Cloud möglich. Dies löst das Problem zwar nur teilweise, der forensische Prozess in der privaten Cloud ist jedoch gesichert.

AUSBLICK

Die Cloud-Anbieter werden wahrscheinlich auch in Zukunft keine externen Schnittstellen zu ihrer Hardware-Infrastruktur zulassen. Dies könnte zusätzliche Schwachstellen durch weitere Zugriffspunkte bedeuten und demnach auf die sensibelsten Komponenten in der IT-Infrastruktur. Denkbar wäre ein Forensik Servicemodell, das dem Kunden angeboten werden könnte. Dazu müssten die entsprechenden Werkzeuge noch entwickelt werden. In einer Datenbank müssten laufend und automatisch aktuelle Images gespeichert werden. Wie bei OpenStack sollten diese anhand von Knoten verfolgbar und wiederherstellbar sein. Die Datenmenge muss automatisiert die relevanten Spuren von den belanglosen Daten trennen. Dieser Service könnte dann auf Wunsch des Kunden ausgelöst und intern bearbeitet werden, was jedoch wieder zu den beschriebenen internen Problemen führt. Da ein solcher Service aufgrund der zusätzlichen Speicherkapazität und des benötigten Fachpersonals vermutlich nicht kostenlos wäre, ist es fraglich, ob dieser von den Kunden überhaupt angenommen würde. Wenn die Cloud-Anbieter nicht gesetzlich dazu verpflichtet werden, den forensischen Prozess in der Cloud umzusetzen, werden die beschriebenen Probleme auch in der Zukunft weiter bestehen.

ZUSAMMENFASSUNG

Das Sichern beziehungsweise Wiederherstellen und Aufbewahren der persistenten Spuren auf physischen und virtuellen Festplatten ist für eine Cloud-Forensik essenziell. Schnittstellen müssen geschaffen werden, um einen Fernzugriff zu ermöglichen. Hinzu kommt ein Monitoring und die Aufzeichnung der flüchtigen Daten sowie die Möglichkeit, über Kontaktpunkte eine Live-Analyse während eines Angriffs vorzunehmen, um dabei zusätzlich wichtige Informationen zu sammeln. Ein Remote-Zugriff auf die IT-Infrastruktur zum Hashen der Festplatten, damit Integrität und Authentizität gewahrt wird, ist weiterhin zwingend notwendig. Die Synchronisation der Zeitstempel sollte sobald wie möglich umgesetzt werden. Das Network Time Protocol steht dafür bereits zur Verfügung. Das Sammeln der Spuren, die Untersuchung und die Aufbewahrung der Beweise müssen Experten durchführen. Werkzeuge, die den forensischen Prozess in der Cloud ermöglichen und unterstützen und Sicherheitsvorfälle aufspüren, sollten schnellstmöglich entwickelt werden. Dabei stehen das Sammeln der enormen Datenmengen und das Selektieren der forensisch wichtigen Spuren im Vordergrund. Beim Bündeln der Informationen dürfen keine Verletzungen des Datenschutzes geschehen. Allein mit der Umsetzung dieser Kriterien baut sich eine lückenlose Beweismittelkette auf. ■

Literatur

[1] N. Pohlmann: „Cybersicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cybersicherheitssystemen in der Digitalisierung", Springer-Vieweg Verlag, Wiesbaden 2019

[2] Cloud Forensics: A Review of Challenges, Solutions and Open Problems https://ieeexplore.ieee.org/document/7149635

[3] Digitale Forensik in IaaS-Cloud-Umgebungen https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/ITSiKongress/13ter/Andreas_Kolb_14052013.pdf?__blob=publicationFile

[4] Einführung in OpenStack https://docs.openstack.org/de/security-guide/introduction/introduction-to-openstack.html

DETLEF SCHWARZKOPF
studiert im Master „Internet-Sicherheit" an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit der Digitalen Forensik in der Cloud-Umgebung.

NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.