7 verborgene Wahrheiten der Cloud-Sicherheit

WITH secure

Inhalt

Vorwort

Seit nunmehr fast zwei Jahrzehnten lässt Cloud Computing etwas Wirklichkeit werden, was lange Zeit ein Zukunftstraum war: Unternehmen mit knappen Ressourcen können es mit Konkurrenten aufnehmen, die sehr viel größer, finanzstärker und besser ausgestattet sind. Diese Riesen wiederum genießen die Freiheit und Flexibilität, die ihnen die Cloud bietet.

Dieser Traum ist mittlerweile tägliche Wirklichkeit geworden. Nun ist es an der Zeit, sich einigen harten Wahrheiten zu stellen und zu klären, was Cloud Computing für die Sicherheit von Unternehmen bedeutet. Es fängt damit an, dass man versteht, wie sich die zugrunde liegenden Prinzipien von den vorherigen unterscheiden.

Natürlich kann „Cloud“ unterschiedliche Bedeutungen haben, von IaaS (Infrastructure as a Service) und PaaS (Platform as a Service), worauf wir uns alle verlassen, wovon die meisten Endanwender aber nichts mitbekommen, bis hin zu SaaS-Tools (Software as a Service) wie Microsoft 365 und Salesforce, mit denen viele Menschen täglich umgehen.

Was diese Cloud-Varianten gemeinsam haben, ist das Konzept der geteilten Verantwortung (Shared Responsibility) in Sachen Sicherheit: Als Kunde ist man für all das verantwortlich, was die Cloud-Provider mit ihren integrierten Sicherheitskontrollen nicht abdecken.

Nur eine winzige Minderheit von Unternehmen verfügt über die Ressourcen, die nötig wären, um sich vor den Bedrohungen zu schützen, die mit der Cloud einhergehen. Und daran lässt sich auch so leicht nichts ändern. Zu den wahren Kosten des Cloud-Betriebs bzw. der Cloud-Miete gehören auch Antworten auf die Sicherheitsherausforderungen der Cloud. Viele erkennen das erst, wenn sie plötzlich kompromittiert sind.

Hier verraten wir sieben verborgene Wahrheiten über die Cloud-Sicherheit im Jahr 2022. Und wir zeigen, wie es Unternehmen gelingt, die Regeln dafür so aufzustellen, dass sie die Vorteile des Cloud-Ansatzes wiedergewinnen und die Clouds ihren Zielen nicht im Weg stehen, sondern dienen.

Die Vorteile der Cloud sollten die Risiken überwiegen.[1] Der beste Weg dorthin ist ein ergebnisorientierter Ansatz.

„Mir fallen nicht mehr als ein oder zwei Unternehmen ein, an die ich mich wirklich wenden würde, wenn es um Angriffserkennung im Cloud-Bereich geht. So gut wie alle wichtigen Fähigkeiten, die wir bei Unternehmen sehen, sind rein intern entwickelt. Das ist o. k., wenn man eine Tier-1-Bank ist, aber gar nicht gut, wenn man zu den anderen 99,5 % gehört.“

Nick Jones,
Principal Security Consultant, WithSecure™

1 Nick Jones: Cloud security: striking the balance between risk, speed, and cost. WithSecure™ 2021.

Verborgene Wahrheit 1

Was Sie nicht sehen, können Sie auch nicht schützen

W / T H
secure

Verborgene Wahrheit 1

Was Sie nicht sehen, können Sie auch nicht schützen

Ishan Singh-Levett
Director, Product Management

Sichtbarkeit in der Cloud ist eine Herausforderung, mit der sich in ähnlicher Form alle IT-Abteilungen herumschlagen: Schatten-IT. Das Problem BYOD (Bring Your Own Device) wird nun durch BYOC (Bring Your Own Cloud) noch überboten.

Eine der Stärken der Cloud ist, dass sich jeder mit minimalem Aufwand Rechenleistung, Speicherplatz oder Anwendungen besorgen kann. Diese Flexibilität macht es IT-Abteilungen, Sicherheitsteams und ganzen Unternehmen aber schwer, zu verfolgen, welche Cloud-Ressourcen wo genutzt werden – selbst wenn man von SaaS-Anwendungen einmal absieht. Teams brauchen nichts als eine Kreditkarte, um Cloud-Instanzen mit sensiblen Daten und Systemen aufzusetzen.

Manche dieser Instanzen lassen sich nur schwer erkennen und nachverfolgen, und das kann aufgrund der Abhängigkeiten zwischen erkannten BYOC, genehmigten Clouds und unsichtbaren Auf-eigene-Faust-BYOC zu allerlei Komplikationen führen. Die Äquivalente on premises sind mit Agenten und Scans leichter zu finden.

Das Problem der Sichtbarkeit ist in Entwicklungsumgebungen besonders groß, weil dort schnell einmal Cloud-Instanzen gestartet, Produktionsdaten aufgespielt und Verknüpfungen zu internen Systemen gesetzt werden – und das mit allenfalls rudimentärer Übersicht und kaum Dokumentation oder Sicherheitsmaßnahmen. Abgesehen von Security und Datenschutz bezahlen Sie diese Cloud-Dienste wahrscheinlich viel zu teuer.

Der Moment der Wahrheit

Außer dem Problem mangelnder Sichtbarkeit bedeutet eine unstrukturierte Cloud-Einführung meist auch, dass die einzelnen Clouds nicht konsistent konfiguriert sind. Dies führt direkt zur zweiten und zum fünften Punkt: konsistente, sichere Konfiguration sowie konsistenter Schutz statt Sicherheitslücken.

Um die Zugriffe auf Cloud-Dienste nachzuvollziehen, ist ein CASB (Cloud Access Security Broker)[2] ein geeignetes Mittel. Unternehmen verwenden CASB als Abfang-Proxy. Wir werden später noch sehen, wie wichtig das sein kann. CASB ist jedoch ein Universalwerkzeug. Im Vergleich dazu bieten Single-Cloud-Lösungen wie Cloud Protection for Salesforce von F-Secure den nötigen Schutz mit weniger Komplexität. CASB verlangt außerdem Zugang zu Endpunkten, weil dort Agenten installiert werden, ähnlich wie bei EDR (Endpoint Detection and Response) bzw. MDR (Managed Detection and Response).

2 Choosing the right tools: F-Secure Cloud Protection for Salesforce vs CASB solutions. WithSecure™ 2021.

Verborgene Wahrheit 2

Fehler in der Cloud-Konfiguration können überall sein

WITH secure

Verborgene Wahrheit 2

Fehler in der Cloud-Konfigurationen können überall sein

Nick Jones
Principal Security Consultant

Die Kombination aus Flexibilität und allgemeinem Zugang bedeutet, dass eine sichere Cloud-Konfiguration ebenso wichtig wie schwierig ist. Angreifer brauchen keine großen Fähigkeiten oder besondere Tools, wenn schon eine einzige Fehlkonfiguration das Unternehmen angreifbar macht.

Cloud-Anbieter sehen zur Sicherung einzelner Umgebungen einfache Abläufe vor; das ist ein Grundprinzip ihrer Produkte. Für ein einzelnes Konto und eine bestimmte Workload die ideale Konfiguration einzurichten, ist für jede IT-Abteilung absolut machbar. Die großen Provider haben alle hervorragende Dokumentationen sowie Tools, die auf jahrelanger Erfahrung aufbauen und grundlegende Probleme erkennen können.

Die Schwierigkeit besteht darin, mehrere Konten und Hunderte von Workloads bei diversen Cloud-Anbietern skalierbar zu schützen. Weil Unternehmen heute in der Regel drei bis fünf Cloud-Provider[3] nutzen, ist das ein gängiges Problem.

Es gibt Tools und Dienste, mit denen sich verteilte Umgebungen schützen lassen. Aber sie müssen auch so konfiguriert werden, dass sie die gewünschte Sicherheitsstrategie widerspiegeln, und sie müssen immer wieder angepasst werden, wenn sich die Workloads ändern.

Außerdem müssen diese Werkzeuge auch für diejenigen anwendbar sein, deren Auftrag die Erkennung von Sicherheitsverletzungen ist. Damit stößt man auf ein Problem, das F-Secure wohlvertraut ist, sowohl von der Beratung her als auch aus Managed-Service-Perspektive: Den Unternehmen ist durchaus klar, wie diese Schwierigkeiten zu bewältigen wären, nur mangelt es meist an den nötigen Ressourcen.[4]

Gleichwohl gibt es viele Teams, die es schaffen können und es auch tatsächlich schaffen – entweder indem sie bei einer überschaubaren Anzahl von Providern Standard-Sicherheitsrichtlinien durchsetzen oder indem sie die mit der Flexibilität eingekaufte Komplexität durch sehr viel Geduld und Ausdauer in den Griff bekommen.[5] In jedem Fall sind skalierbare und sichere Cloud-Konfigurationen nichts für schwache Nerven. Dazu braucht es außerdem eine enge Zusammenarbeit zwischen den Sicherheits- und den Technikteams, die die Workloads erstellen und warten.

3 Marc Wilczek: IT governance critical as cloud adoption soars to 96 percent in 2018. CIO 2018.
4 Mehmet Surmeli et al.: Der Moment der Wahrheit. Geschichten aus dem Auge des Cybersturms. F-Secure o. J.
5 Webinar replay: CISOs step up on Cloud and Cyber priorities for 2022. WithSecure™ 2021.

Einige Unternehmen – man denke etwa an die Top-Tier-Finanzhäuser – verfügen über die Ressourcen und das Fachwissen, um umfangreiche eigene Kapazitäten aufzubauen. Das ist aber nur eine verschwindend geringe Anzahl der Unternehmen, die insgesamt die Cloud nutzen.

Das Problem liegt zum Teil in der Unmenge der Cloud-Anwender. Die Cloud-Provider sind, wie gesagt, sehr geschickt darin, Tools und Anleitungen bereitzustellen, aber die Kunden sind – wenn überhaupt – nur für die allgemeinsten Sicherheitsanleitungen zu gewinnen. Und wenn dann noch mehrere Clouds und mehrere Konfigurationen hinzukommen, wird klar, warum dieses Problem ein Problem ist.

Die kreative Freiheit, die Cloud-Anbieter ihren Nutzern einräumen, ist einerseits beträchtlich und macht einen Großteil der Cloud-Attraktivität aus, andererseits stellt sie die Sicherheitsbranche vor eine enorme Herausforderung. Ein einzelnes Diagnose-Tool, das sämtliche Sicherheitslücken einer Umgebung beheben könnte, gibt es nicht.

Zur Komplexität trägt auch die Tatsache bei, dass eine Fehlkonfiguration in der einen Umgebung in einer anderen völlig korrekt ist, was bedeutet, dass Fehlkonfigurationen mit automatisierten Tools kaum zu erkennen sind. Die Antwort liegt in einem Ansatz, der mehr mit Menschen zu tun hat: Eine Auswahl qualifizierter, lernfähiger Fachleute ist effektiver als eine wohl gefüllte Werkzeugkiste mit starren Diagnosetools.

Der Moment der Wahrheit

Wenn Ihnen diese Lösung bekannt vorkommt, dann wahrscheinlich deshalb, weil derartige Probleme in der On-premises-IT schon seit geraumer Zeit durch spezialisierte Beratungsunternehmen, Incident-Response-Anbieter und MDR-Provider gelöst werden.

Cloud-Sicherheit bringt ihre eigenen Komplikationen mit sich, aber es ist ebenso richtig, dass man vorhandene Techniken aufgreifen und anpassen kann (und zum Teil bereits angepasst hat), um diese Herausforderung zu meistern.

Mit externer Unterstützung, z. B. durch die Cloud-Sicherheitsberater von F-Secure, sowie durch MDR-Services mit strategischen Cloud-Security-Managementfunktionen wie F-Secure Countercept lässt sich die Lücke zwischen den Sicherheitsvorkehrungen der Cloud-Provider und denen der meisten Anwenderunternehmen schließen.

Verborgene Wahrheit 3

Die Cloud hat die Regeln für alle verändert

W / T H
secure

Verborgene Wahrheit 3

Die Cloud hat die Regeln für alle verändert

Jennifer Howarth
Product Manager - Cloud

Identitätsbasierte Angriffe sind auf dem Vormarsch. Das liegt daran, dass immer mehr Unternehmen auf die Cloud umsteigen und ihre Anwendungen als Services (XaaS) beziehen. Was ändert sich damit? Vor allem unterscheidet sich die Angriffsfläche grundlegend von der, die wir aus der klassischen On-premises-IT-Umgebung gewöhnt sind. Dort sind offensichtlich die Endpunkte[6] das erste Ziel für Angreifer und daher auch die Stellen, auf die sich die Verteidiger konzentrieren.

Außer bei IaaS, wo die Cloud im Prinzip ein externes Rechenzentrum zum Hosten von VMs ist, exponieren Cloud-Workloads einfach kein Betriebssystem mehr. Exploits, Codeausführung durch Angreifer und ähnliche Konzepte sind also nicht mehr relevant, ebenso wenig wie die Schutzmaßnahmen, die man im Laufe der Jahre zu deren Bekämpfung entwickelt hat. Stattdessen erreichen Angreifer ihr Ziel, indem sie die Cloud-API mit gültigen Anmeldedaten aufrufen. Aus Defensivsicht ist zwar jeder einzelne API-Aufruf für sich genommen keineswegs bedrohlich, aber eine Reihe von Aufrufen, die vom normalen Anwenderverhalten abweicht oder in Bezug auf einen bestimmten Workload ungewöhnlich ist, lässt Verdacht schöpfen. Genau an dieser Stelle kommt UEBA (User Entity Behavior Analytics) ins Spiel.

UEBA entwirft ein Bild dessen, was in einer bestimmten Workload, in einer bestimmten Umgebung normalerweise abläuft, und zwar möglichst mit Bezug auf eine User-Identität. Die Vorstellung davon, was normal und was anormal ist, war schon in der On-premises-Welt eine nützliche Erkennungshilfe – in der Cloud ist sie die Grundlage jedes effektiven Überwachungsansatzes. Zu beachten ist dabei, dass die identitätsbasierte UEBA-Erkennung nicht nur menschliche Entitäten kennt. Die Endanwender sind zwar ein guter Ausgangspunkt für das SaaS-Monitoring, aber bei reinen Cloud-Services sind System-zu-System-Identitäten nicht weniger bedeutsam. Jüngste Vorfälle, mit denen sich das Incident Response Team von F-Secure befasst hat, zeigen, dass die Angreifer statt auf Log-ins von Endanwendern eher auf Maschinen-Anmeldedaten aus sind, wenn sie wirklich Schaden anrichten wollen.

Die Cloud bringt neue Technologien und Arbeitsweisen mit sich, und die klassische Security musste diese erst verstehen und lernen, damit umzugehen.[7] Manche Angriffe finden auf

6 Nick Jones: Detecting attacks in the cloud. WithSecure™ 2021.

7 Jorge Lamarca, Joani Green: How The Cloud Has Changed Digital Forensics And Incident Response. F-Secure 2021.

Cloud-Management-Ebene statt und erfordern keinerlei Interaktion mit einer herkömmlichen On-premises-Infrastruktur oder etwas Vergleichbarem. Darum ist es wichtig, dass die Unternehmen spezielle Cloud-Erkennungs- und Reaktionsfähigkeiten aufbauen. Das Incident Response Team von F-Secure befasst sich zunehmend mit Untersuchungen, die ausschließlich in der Cloud spielen, und wir gehen davon aus, dass dies in Zukunft noch zunehmen wird.

Der Moment der Wahrheit

Cloud Security ist derzeit eine Herausforderung. Es gibt wenig bis gar keine Erkenntnisse über die Bedrohungen, Daten sind oft schwer zu bekommen, das Volumen und das Ausmaß von Angriffen, soweit bekannt, sind noch gering, und die Unternehmen, die es hart getroffen hat, sprechen nicht gern darüber. Es gibt jedoch gute Gründe, positiv zu denken.

Die Bedrohungserkennung sortiert sich neu. Mit der richtigen strategischen Vorbereitung und der Anpassung bestehender Cloud-Plattform-Funktionen können DFIR-Fachleute (Digital Forensics and Incident Response) ihre Aufgaben auch bei Cloud-basierten Vorfällen erfüllen.

Ein weiterer Lichtblick ist MITRE, wo man sich aktiv darum bemüht hat, in das ATT&CK-Framework[8] mehr Bedrohungsdaten einzubeziehen. Dennoch bleibt es dabei, dass Anbieter und Anwender von Cybersicherheitslösungen, zumindest fürs Erste, noch im Forschungs- und Experimentiermodus sind.

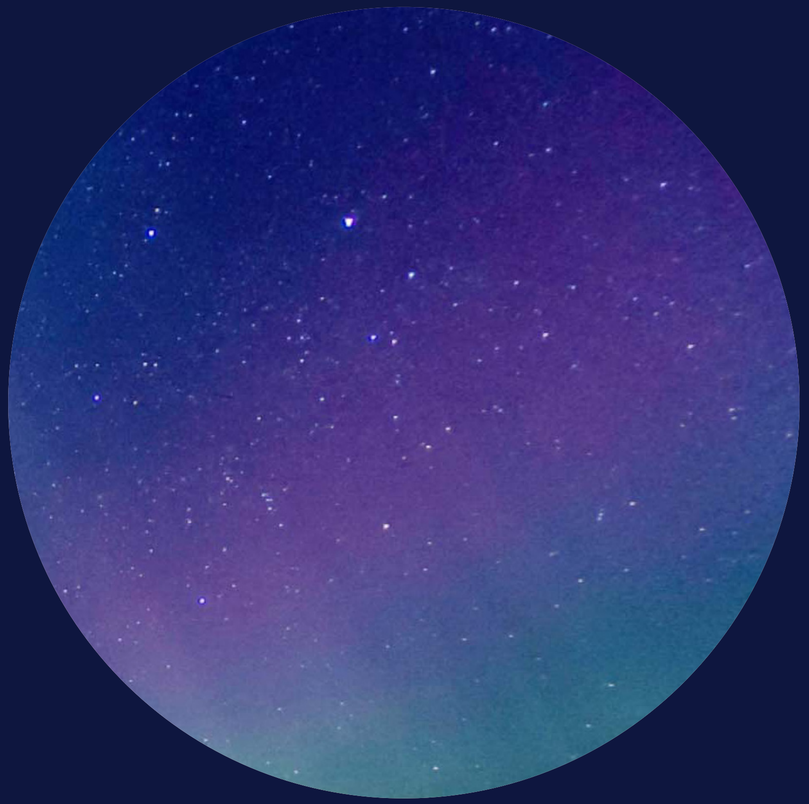
Wie das Incident Response Team von F-Secure bei der Arbeit in der Cloud vorgeht und wie die strategische Vorbereitung und Anpassung bestehender Cloud-Plattform-Funktionen aussehen kann, schildert ein separater Beitrag.[9]

8 F-Secure Overview. MITRE Engenuity ATT&CK Evaluation 2021.

9 Jorge Lamarca, Joani Green: How The Cloud Has Changed Digital Forensics And Incident Response. WithSecure™ 2021.

Verborgene Wahrheit 4

Die Endpunkte müssen weiterhin geschützt werden



W / T H
secure

Verborgene Wahrheit 4

Die Endpunkte müssen weiterhin geschützt werden

Harri Ruusinen
Director, Global Sales Engineering

Selbst mit aktiven UEBA sind die Endpunkte doch Einfallstore in die Cloud. Die Angriffsfläche ist größer geworden.

Auch wenn die Unternehmen im großen Stil zu Cloud-Services gewechselt sind, gilt immer noch, dass Sie die Rechner und die übrigen Geräte schützen müssen, die Sie zum Zugriff auf Ihre Dienste verwenden. In diesem Punkt ist EDR auch in Cloud-Sicherheitsszenarien immer noch hilfreich. Das ist aber nur der erste Ansatzpunkt, und die Wirksamkeit von EDR ist damit noch lange nicht erschöpft.

Cloud-Services werden normalerweise mit unterschiedlichen Sicherheitsleveln konzipiert. So verhindert z. B. die Multi-Faktor-Authentifizierung (MFA), dass Angreifer mit gestohlenen Anmeldedaten auf Systeme zugreifen. Falls nun aber das Gerät, das diesen Dienst nutzt, aus der Ferne kompromittiert oder direkt gestohlen wird, dann könnte die Sitzung noch aktiv sein, sodass der Angreifer diese zusätzliche Sicherheitskontrolle einfach umgehen kann.

Endgeräte ohne MFA oder Verschlüsselung stellen ein Problem dar: Wenn ein Angreifer an die richtigen Schlüssel gelangt, um sich Zugang zu verschaffen, liegt die Verantwortung beim Anwenderunternehmen – und nicht etwa beim Anbieter des Cloud-Dienstes. EDR bleibt daher unerlässlich für Geräte, über die auf die Cloud-Services des Unternehmens zugegriffen wird.

Der Moment der Wahrheit

Die gute Nachricht ist, dass viele Unternehmen bereits über Tools verfügen, die solche offenen Wunden heilen können. Endpunktschutz- und EDR-Lösungen sind heute wichtiger denn je, weil sie dazu beitragen, die Cyberresilienz eines Unternehmens insgesamt zu stärken.

Mithilfe von EDR können die Sicherheitsteams offenkundig böswillige Verhaltensmuster und Anomalien erkennen und alle Aktionen aufzeichnen, die auf den Endpunkten stattfinden. Aber EDR muss dazulernen und sich auf die besonderen Erfordernisse der Cloud-Sicherheit ausrichten, wenn es auch in dieser Welt eine Rolle spielen will. Dies ist eine Aufgabe, die wir bei F-Secure in allen Abteilungen angehen, denn die zeitgleiche Überwachung sämtlicher Umgebungen ist eine Herausforderung, die immer mehr an Bedeutung gewinnt.

Ein konkreter Bereich der EDR-Optimierung betrifft die Frage, ob eine EDR-Lösung erkennen kann, wenn an einem Endpunkt Cloud-Zugangsdaten gestohlen werden. Dann geht bei der ersten Anlaufstelle ein automatisch ausgelöster Alarm ein, der wiederum mit Cloud-UEBA-Anomalien korreliert werden kann, sodass deutlich wird, wann ein Angreifer einen Endpunkt kompromittiert hat, um in die Cloud zu gelangen.

WithSecure™ arbeitet auch daran, wie unser EDR zur Sicherheitslage des Kundenunternehmens berichtet, inklusive Hardware-Sicherheitsfunktionen, damit wir es Angreifern so schwer wie nur möglich machen, die Endpunkte unserer Kunden zu kompromittieren und sich in ihren Systemen auszubreiten.

EDR ist also alles andere als tot; EDR ist nach wie vor unverzichtbar, wenn es darum geht, Endgeräte zu schützen und auf diese Weise Angreifer von der Cloud fernzuhalten.

Wir bei F-Secure erwarten in Zukunft mehr Synergien zwischen Cloud-Sicherheit und EPP/EDR, damit unsere Kunden und Partner weiterhin resilient bleiben – auch dann, wenn sie neue Arbeitsformen einführen.

Praktische Tipps, worauf Sie bei einer Cloud-fähigen EDR-Lösung achten sollten, finden Sie in unserem Themenratgeber, der zehn Punkte nennt, die beim EDR-Einkauf im Pflichtenheft stehen sollten.[10]

10 10 Punkte, die Sie bei der EDR-Auswahl beachten sollten. WithSecure™ 2021.

Verborgene Wahrheit 5

Getrennte Schutz-mechanismen machen verwundbar

W / T H
secure

Verborgene Wahrheit 5

Getrennte Schutzmechanismen machen verwundbar

Domenico Gargano
Director, Technical Operations

Es ist praktisch unmöglich, ausschließlich in der Cloud zu arbeiten. Jedes Unternehmen wird zumindest eine kleine physische IT-Endpunktpräsenz haben. Seit die Dienste und Anwendungen derart zwischen On-premises und Cloud verteilt sind, hat sich die Angriffsfläche vergößert, bei der Gegner ansetzen können. Sie haben mehr als eine einzige Cloud? Dann ist das Problem noch sehr viel größer.

Diese Sicherheitslücken zu schließen, ist natürlich von entscheidender Bedeutung. Vermutlich hat Ihr Unternehmen bereits aktiv Maßnahmen in die Wege geleitet, mit denen diese Herausforderung angegangen wird.

Der sogenannte Shift-Left-Ansatz, bei dem die Verantwortung für die Sicherheit im Lebenszyklus einer Anwendung weiter „nach links“ gerückt und in die Entwicklung integriert wird,[11] sowie der aktuelle Trend, dass sich die Chief Information Security Officers (CISOs) von der reinen IT-Verantwortung lösen und eine geschäftsübergreifende Führungsrolle übernehmen, haben dazu geführt, dass dem „Bindemittel“ zwischen den Cloud-Services und den Anwendungen mehr Aufmerksamkeit geschenkt wird.

Also, warum gibt es dieses Problem überhaupt? Aus demselben Grund, aus dem wir – also Software-Entwickler, Betriebssystemanbieter und eigentlich wir alle – uns mit genau demselben Problem in der klassischen On-pemises-IT herumschlagen, seit Desktop-Computer die Firmen-IT prägen. Die Cloud-Anbieter haben enorme Sicherheitsressourcen und die Mittel, ihre Kunden mit den nötigen Kenntnissen und einigen ganz erstaunlichen Tools zu versehen. Damit endet die Unterstützung dann aber auch. Es ist nicht so gedacht, dass die Cloud-Provider sich mit jedem einzelnen Kunden zusammensetzen und die Sicherheitsvorkehrungen auf dessen Bedürfnisse zuschneiden. Damit würden sie die Cloud-Kosten in unerschwingliche Höhen treiben.

Die Cloud-Anbieter operieren auf einer gigantischen Skalengröße, sowohl bei der Infrastruktur als auch in puncto Anwendungen, und sie müssen damit die Erwartungen der Benutzer erfüllen. Der Weg dorthin führt über Sicherheitstools und -konfiguratoren, die in der Tat beeindruckend sind. Aber sie sind doch nur Teile des gesamten Security-Puzzles, nämlich der umfassenden Aufgabe, ein Cloud-aktives Unternehmen zu schützen.

11 Neil Roebert: Style over substance: why tech not culture is key to DevSecOps security. WithSecure™ 2020.

Getrennte Verteidigung, getrennte Teams?

Bei WithSecure™sehen wir im Beratungseinsatz, dass viele Unternehmen eigene SOCs (Security Operations Centers) für ihre Cloud-Umgebungen betreiben. Dieses Vorgehen ist nicht immer von Erfolg gekrönt und scheint oft mit einem zweiten Phänomen einherzugehen: dem ewigen Kampf um Cloud-Sicherheitsfachleute, die es zu finden und zu halten gilt. Dieser Mangel ist nichts Neues, wenn man ihn vor dem Hintergrund der Kompetenzlücken betrachtet, die den gesamten IT-Sektor seit Jahrzehnten plagen.

Die Situation bei diesem speziellen Fachkräftemangel sieht jedoch etwas anders aus: Die Cloud-Teams bauen eigene Sicherheitskapazitäten auf und umgehen dabei manchmal die Security-Struktur völlig. Das geht so weit, dass die Cloud-Sicherheitsberater von WithSecure™ in manchen Fällen am Ende mehr mit der technischen Seite des Unternehmens zusammenarbeiten, weil man dort in der Regel besser als das Security-Team weiß, wie es um die Cloud-Sicherheit bestellt ist. Die typische Sicherheitsstruktur ist heute insgesamt stärker fragmentiert als früher.

Erkennen und korrelieren

Wenn Sie nicht mit den richtigen Datenquellen arbeiten, dann haben Sie nur einen unvollständigen Überblick über die Aktivitäten in Ihrer Umgebung. Dann wird es sehr schwer, bedeutsame Anomalien zu erkennen oder Beobachtungen aus verschiedenen Teilen der Umgebung in Verbindung zu setzen. So etwas freut die Hacker.

Es ist wichtig, dass man Datenpunkte aus der On-premises-Infrastruktur mit solchen in der Cloud bzw. den Clouds korrelieren kann, damit man ein vollständiges Bild davon bekommt, was ein Angreifer vorhaben könnte. Es ist Ihre beste Chance, eine Bedrohung zu erkennen und darauf zu reagieren.

Die WithSecure™-Untersuchungen der Nobelium-Aktivitäten haben gezeigt, dass dieser Bedrohungsakteur in der Lage ist, über einen On-premises-Angriffsvektor einzudringen und von dort aus in die Cloud zu wechseln, wo er sich festsetzt und sich die Informationen aussuchen kann, die ihn interessieren. Microsoft-Forschungen haben außerdem gezeigt, wie Nobelium vorgeht, um Anmeldedaten zu stehlen, die der Gruppe letztlich Zugang zu den ADFS (Active Directory Federation Services) der Zielorganisation verschaffen. Von dort aus können die Angreifer auf die Cloud zugreifen und sich festsetzen.[12]

WithSecure™ hat diesen Ansatz in Red-Team-Trainings durchgespielt und dabei festgestellt, dass das Red Team bis zur Zielerreichung in den Cloud-Umgebungen des Kunden präsent bleiben kann, auch wenn die Verteidiger die On-premises-Implantate entfernt haben. Sygnia hat ferner beschrieben, wie Nobelium zuerst ADFS-Admin-Rechte erlangt und damit dann das SAML-Zertifikat (Security Assertion Markup Language) des Opfers kompromittiert.[13] Dieser „Golden SAML“-Angriff gewährt im Endeffekt unbestrittenen Zugang zu den Services, die von SAML ausgestellten Tokens vertrauen, sodass sich Nobelium sowohl in Cloud-Diensten als auch in XaaS einnisten kann. Die TTPs (Techniken, Taktiken und Prozesse) von Nobelium hat die CISA (Cybersecurity and Infrastructure Security Agency) in einer Warnmeldung näher beschrieben.[14]

Ohne die Möglichkeit, die ADFS-Authentifizierungslogs mit den Cloud-Aktivitätslogs zu korrelieren, konnten die Opfer gar nicht erkennen, ob jemand erfolgreich auf Cloud-Umgebungen zugegriffen hatte, ohne sich beim ADFS-Server des On-premises-Systems zu authentisieren, der eigentlich erst Zugang gewährt.

12 Ramin Nafisi: FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor. Microsoft 2021.

13 Detection And Hunting Of Golden SAML Attack. Sygnia 2021.

14 Alert (AA21-008A). Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments. CISA 2021.

Sicherheit in der Build-Pipeline

Hier kommt das Silo-Problem ins Spiel, das bereits beim Punkt Fehlkonfigurationen angesprochen wurde. Infrastruktur-Technikteams und Security-Teams überschauen nicht immer den Kontext der geloggten Aktivitäten, und das Fachwissen der Teams, die für die Pipelines und andere Entwicklungstools zuständig sind, ist ebenfalls erforderlich. Fehlkonfigurationen, die auf dezentralisierte DevOps zurückzuführen sind, waren laut Joani Green vom UK-Team der Hauptgrund der Cloud-Kompromittierungen, die das Incident Response Team von WithSecure™ in den letzten Jahren untersucht hat, wie im Fachbeitrag Nicholas Evans zu lesen ist.[15]

Evans rät dazu, die Vorteile von DevOps und DevSecOps zu nutzen und die Verantwortung für die Sicherheit an einen frühen Punkt im Entwicklungszyklus zu verschieben. Entwicklungs- und Sicherheitsteams arbeiten immer dann einvernehmlich zusammen, wenn sich die Business-Funktionen selbst und aktiv um Sicherheit bemühen müssen. Außerdem ist eine enge Kommunikation zwischen dem Sicherheitsteam und der Cloud-Entwicklung unerlässlich.

Auch hier beobachtet unser Incident Response Team, dass die CISOs unabhängig von der IT-Abteilung operieren und die Security Operations auf die einzelnen Geschäftsbereiche aufgetrennt werden. Hier geht es aber nicht um separate, schlecht vernetzte Silos, sondern um dezentralisierte, gut vernetzte Teams.

Der letzte Aspekt ist, dass die Dezentralisierung nicht dazu führen darf, dass sich die Risikobereitschaft im Unternehmen unterschiedlich ausbildet. Es ist also eine neue mittlere Ebene einzuziehen, die zwischen den verschiedenen Einheiten vermitteln kann.

Unerwartete Schwachstellen

Sowohl bei Beratungs- als auch bei Incident-Response-Aufträgen von F-Secure hat sich gezeigt, dass die Schwachstellen – abgesehen von simplen Fehlkonfigurationen – nur selten bei den Internet-seitigen Cloud-Assets zu finden sind. Als problematisch erweisen sich vielmehr die Dienste, Anwendungen und Tools, die das Unternehmen zur Einrichtung der Clouds verwendet. Bei diesen „Kronjuwelen“ handelt es sich häufig um Identitätsanbieter, Quellcode-Repositories, Infrastrukturcode und Werkzeuge zur Bereitstellung von Diensten in der Produktion.

CI/CD-Tools (Continuous Integration/Continuous Delivery) wie Jenkins können in Cloud-Umgebungen enorme Macht und weitreichende Privilegien anhäufen; falls sich dann ein Angreifer Zugang verschafft, ist der Kampf schon so gut wie verloren.

Der Moment der Wahrheit

Der Schlüssel zur Lösung dieser Problemlage lautet „kultureller Wandel“. In vielen Unternehmen ist er bereits im Gange, und es braucht oft nur noch kleinere Anpassungen, um diese Entwicklung in Richtung stärkerer Cloud-Sicherheit zu steuern.

Ein Unternehmen, das Verantwortlichkeiten und Finanzierung den Business-Funktionen aufgibt, während die Gesamtverantwortung beim CISO bleibt, der unabhängig vom IT-Team agiert, ist auf dem besten Wege dazu, einen sicheren Stand in der Cloud zu gewinnen.

15 Nicholas Evans: What will the security team of the future look like? WithSecure™ 2021.

Verborgene Wahrheit 6

Niemand weiß, wer für die Cloud-Daten verantwortlich ist

W / T H
secure

Verborgene Wahrheit 6

Niemand weiß, wer für die Cloud-Daten verantwortlich ist

Dmitriy Viktorov
Head of Product and
Technology, Cloud Solutions

Es ist eine gängige Weisheit, dass Daten „das neue Öl“ sind – ein äußerst wertvolles Gut für jedes Unternehmen. Darum ist gründliche Überlegung gefordert, wenn Sie Ihre Daten in die Cloud verlagern. Wenn Sie das richtige Maß an Kontrolle und Sichtbarkeit behalten wollen, gibt es vieles zu bedenken.

Wenn Sie Cloud-Services kaufen, schieben Sie einen Teil der Verantwortung für die Datensicherheit auf den Cloud-Anbieter, und das macht mit den Reiz dieser Lösung aus. Aber Ihnen sollte unbedingt bewusst sein, dass Sie immer noch für die Sicherheitshygiene verantwortlich sind. Dies ist das Modell der geteilten Verantwortung (Shared Responsibility).

Einmal mehr geht es um Sichtbarkeit, in diesem Fall um die Sichtbarkeit der Daten. Sie müssen wissen, welche Art von Daten Sie haben, wie sie sortiert sind, woher die Daten kommen, wer darauf zugreifen kann und wohin sie gehen. Wenn Daten aus externen, nicht vertrauenswürdigen Quellen stammen (z. B. aus E-Mails), müssen Sie schädliche und nicht zugelassene Inhalte blockieren, bevor sie an interne oder externe Benutzer gelangen. Mit Blick auf die Compliance-Anforderungen müssen Sie außerdem den Zugriff auf Ihre sensiblen Daten überwachen und einen Prüfpfad erstellen, damit Sie feststellen können, ob die Daten Gegenstand einer Compliance-Regel sind und wer darauf zugreifen darf.

Zu den Risiken, auf die Sie achten müssen, zählen übel gesinnte Insider und unbefugter Datenzugriff. SaaS-Cloud-Dienste können leicht sehr komplex geraten, was ebenso leicht zu Fehlkonfigurationen oder schwachen Zugangskontrollen führen kann (siehe die verborgene Wahrheit 2). Fehlkonfigurationen sind wiederum eine häufige Ursache von Datenlecks.

Ein weiteres Risiko besteht darin, dass andere Anwendungen und Dienste, die über APIs mit der SaaS-Cloud verbunden sind, auf die Daten zugreifen. Wenn diese APIs fehlerhaft konfiguriert sind oder mehr Rechte vergeben als nötig, so kann auch dies eine Kompromittierung zur Folge haben. Und selbst dann, wenn sie korrekt konfiguriert sind, muss man im Kopf behalten, dass auch die APIs selbst kompromittiert werden können, wie wir das bei den jüngsten Lieferkettenangriffen erlebt haben.

Der Moment der Wahrheit

Die zunehmende Nutzung von Salesforce, Microsoft 365, Google Workspace und anderen SaaS-Cloud-Diensten macht sie zu lukrativen Zielen für Angreifer. Wir glauben, dass künftige Attacken nicht immer darauf aus sein werden, wertvolle Daten zu stehlen, die in der Cloud gespeichert liegen. Die

Angreifer werden stattdessen versuchen, Cloud-Dienste als „Sprungbrett“ zu nutzen, um von dort in die Unternehmensnetzwerke einzudringen und andere interne oder externe Systeme anzugreifen. Wir haben bereits Fälle von derartigen Phishing- und Ransomware-Angriffen über Cloud-Dienste gesehen. Je mehr sich die Bedrohungslandschaft verändert, desto mehr werden wir bei F-Secure unsere Lösungen weiter verbessern und die Erkennungs- und Reaktionsmöglichkeiten bei Endgeräten ebenso wie für IaaS-, PaaS- und SaaS-Cloud-Plattformen erweitern.

Eine unserer bestehenden Lösungen, Cloud Protection for Salesforce,[16] bietet Echtzeitschutz vor Viren, Trojanern und Ransomware und scannt alle Inhalte, die über die Salesforce-Cloud geteilt werden. Diese einzigartige Lösung von WithSecure™ ergänzt die Sicherheitskontrollen der Cloud-Plattform von Salesforce und schließt eine Shared-Responsibility-Lücke bei Kundendaten in der Cloud. Damit können Kunden der Salesforce Sales Cloud, der Salesforce Service Cloud oder der Salesforce Experience Cloud Angriffe über Schaddateien oder Phishing-URLs verhindern bzw. ins Leere laufen lassen.[17] Außerdem bietet Cloud Protection for Salesforce vollständige Sichtbarkeit sowie Analysen der Inhalte, auf die interne und externe Benutzer zugreifen.

WithSecure™ Cloud Protection for Salesforce nutzt dabei die F-Secure Security Cloud, eine Cloud-Plattform zur Reputationsanalyse von Inhalten und zur Analyse von Bedrohungen. Unter der Haube arbeitet die Security Cloud auf mehreren Ebenen mit modernen Spitzentechnologien und einem fortlaufend erweiterten Repository von Cyber-Erkenntnissen und bedrohungsbezogenen Daten, die in Echtzeit aus Millionen von Sicherheitssensoren auf der ganzen Welt bezogen werden.

Die Security Cloud ist die tragende Säule unserer preisgekrönten Endpunktschutzprodukte und anderer Lösungen zum Schutz von Cloud Collaboration, etwa WithSecure™ Elements for Microsoft 365.

16 Salesforce Data Protection 101 – What is Salesforce security model? WithSecure™e 2021.

17 Die Kill Chain durchbrechen – mit F-Secure Cloud Protection for Salesforce. WithSecure™-Whitepaper 2021.

Verborgene Wahrheit 7

Collaboration über Cloud-Plattformen wird noch wichtiger

W / T H
secure

Verborgene Wahrheit 7

Collaboration über Cloud-Plattformen wird noch wichtiger

Juha Högmander
Director, Technical Offering

Nur wenige arbeiten derzeit im Büro der Firma, und wahrscheinlich werden wir das auch in Zukunft nicht mehr oft tun. Für viele ist Telearbeit seit zwei Jahren das neue Normal, und es ist gut möglich, dass einige von uns auf Dauer im Homeoffice arbeiten werden.

Zusammenarbeit ist unter diesen Bedingungen ausgesprochen wichtig geworden, und das bedeutet natürlich, dass auch der Schutz dieser Arbeitsweisen von ganz entscheidender Bedeutung ist. Ihre Materialien müssen Sie digital austauschen können, Workshops und Live-Meetings halten Sie digital und Präsentationen ebenso. Mit anderen Worten: Sie brauchen eine Möglichkeit, zu kommunizieren und zusammenzuarbeiten, eine Möglichkeit der Collaboration. Bei den Red-Team-Übungen von F-Secure, bei denen es darum geht, versuchsweise in die Umgebung eines Kunden einzudringen, hat sich allerdings gezeigt, dass Collaboration- bzw. Echtzeit-Kommunikationsplattformen wahre Goldgruben für Angreifer sind.

Zu dieser Diskussion gehört aber auch die Feststellung, dass E-Mails immer noch der stärkste Angriffsvektor sind. Mehr als die Hälfte (51 %)[18] der kleinen und mittleren Unternehmen wurden in den letzten beiden Jahren Opfer eines Angriffs, was auf einen Wandel in der Einstellung der Cyberkriminellen hinweist: Viele Angreifer suchen jetzt nach leichter Beute, unabhängig von Unternehmensgröße und Branche. Massenhaft automatisierte E-Mail-Angriffe sind billig in der Durchführung und versprechen den Kriminellen hohe Rendite.

Natürlich ist es wichtig, dass Sie die Belegschaft im Umgang mit Phishing schulen, damit die Leute wissen, worauf sie achten müssen, und nicht so oft suspekte Mails anklicken. Das ist aber nur ein Teil der Lösung, und wir wissen alle, dass das nicht immer klappt. Phishing hat in den Quarantänezeiten enorm zugenommen: Der Anteil der Kompromittierungen mit Phishing machte 2021 einen Sprung von 25 % im Vorjahr auf 36 %.[19] Links in E-Mails sind insgesamt der wichtigste Malware-Vektor bei Sicherheitsverletzungen – Malware wird zu etwa 46 % per E-Mail übertragen.[20]

Nun wollen wir nicht verhindern, dass die Leute auf Daten zugreifen, auch wenn das der einfachste Weg wäre, die Sicherheit zu gewährleisten. Aber wir wollen verhindern, dass

18 Cost of a Data Breach Report 2020. IBM 2020.
19 2021 Data Breach Investigations Report (DBIR). Verizon 2021.
20 2020 Data Breach Investigations Report (DBIR): Results and analysis. Verizon 2020

die Leute etwas tun, wozu sie nicht befugt sind, z. B. dass sie vertrauliche Daten an Orten weitergeben, an denen sie es nicht tun sollten. Und wir wollen die Möglichkeit haben, ungewöhnliche Aktivitäten sichtbar zu machen und nachzuverfolgen.

Der Moment der Wahrheit

Microsoft 365 ist die mit Abstand größte Austauschplattform dieser Art. Aus diesem Grund hat WithSecure™ der Entwicklung von Elements for Microsoft 365[21] Priorität eingeräumt, auch wenn daneben weitere Lösungen in Arbeit sind und auch WithSecure™ Cloud Protection for Salesforce die Zusammenarbeit schützt.

Wir haben außerdem an der Verbesserung unserer E-Mail-Schutzlösung für SharePoint und Teams gearbeitet, sodass wir umfassenden Plattformschutz bieten können. Und wir haben die Erkennung kompromittierter Konten integriert, was für die Sicherheit des gesamten Dienstes von Bedeutung ist.

Wenn man sich die Welt und ihren derzeitigen Zustand ansieht, dann wollen wir nicht die Security-Spielverderber sein, die sich gegen den Trend zur Offenheit sträuben. Der Wandel in den Technologieunternehmen, der sich in der gesamten Wirtschaft fortsetzt, geht dahin, dass die Menschen individuelle Entscheidungen treffen. Diese Freiheit funktioniert am besten ohne unnötige Risiken.

21 F-Secure: Added security for your email – F-Secure Elements for Microsoft 365. YouTube 2021.

Fazit

Die neuesten Tools und Verfahren reichen nur bis zu einem gewissen Punkt – das gilt für Cloud-Anbieter, Sicherheitsanbieter und Kunden gleichermaßen. Weitaus wirksamer ist ein kultureller Wandel – dann kann der richtige, ergebnisorientierte Sicherheitsansatz die Effektivität guter Tools und Techniken um das Tausendfache verstärken.

Die Wahrheit ist, dass Investitionen in einen starken, delegierenden Ansatz zur Cloud-Sicherheit wie zur Sicherheit des eigenen Unternehmens die potenziellen Mehrkosten, die in der Cloud verborgen sind, deutlich reduzieren kann.

Über WithSecure™

WithSecure™ ist der zuverlässige Partner für Cybersicherheit. IT-Dienstleister, Managed Security Services Provider und andere Unternehmen vertrauen WithSecure™ – wie auch große Finanzinstitute, Industrieunternehmen und führende Kommunikations- und Technologieanbieter. Mit seinem ergebnisorientierten Ansatz der Cybersicherheit hilft der finnische Sicherheitsanbieter Unternehmen dabei, die Sicherheit in Relation zu den Betriebsabläufen zu setzen und Prozesse zu sichern sowie Betriebsunterbrechungen vorzubeugen. WithSecure™ nennt diesen Ansatz „Outcome-based Cyber Security“. KI-gesteuerte Sicherheitsmaßnahmen sichern Endpoints und die Zusammenarbeit in der Cloud mit intelligenten Erkennungs- und Reaktionsmechanismen. Die Detection & Response-Experten von WithSecure™ identifizieren Geschäftsrisiken, indem sie proaktiv nach Bedrohungen suchen und bereits laufende Angriffe abwehren – dabei arbeiten sie eng mit Instituten, großen Unternehmen und innovativen Tech-Firmen zusammen. Sie haben mehr als 30 Jahre Erfahrung in der Entwicklung von Technologien, die sich an den Bedürfnissen der Unternehmen orientieren. Das Portfolio von WithSecure™ eröffnet durch flexible Vertriebsmodelle die Möglichkeit, gemeinsam mit Partnern zu wachsen.

WithSecure™ ist Teil der 1988 gegründeten F-Secure Corporation, die an der NASDAQ OMX Helsinki Ltd. gelistet ist.

WITH secure