ÜBERWINDUNG DER SICHERHEITSBEDENKEN: KUNDEN WECHSELN ZU SAAS

Eine Umfrage zu Cloud-Sicherheit

Mai 2016

INFO~TECH
RESEARCH GROUP

INHALT

SICHER BLEIBEN MIT SAAS

Die Cloud ist seit fast zehn Jahren das dominierende Thema in der IT-Branche. Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) sowie die neue Welle des Anything-as-a-Service (XaaS) befördern die Einführung des Konzepts der Cloud-Services. Die Einführung dieser Services hat in den letzten Jahren exponentiell zugenommen, und eine neue Umfrage der Info-Tech Research Group zeigt, dass ganze 94 Prozent der Unternehmen im privaten Sektor mindestens eine Technologie einsetzen, die per Software-as-a-Service bereitgestellt wird (*Info-Tech Research Group SaaS Security Survey, 2016, n=305*). Für Info-Tech ist dies ein wichtiger Wendepunkt bei der Überwindung des größten Hindernisses für die Implementierung von SaaS-Lösungen: Sicherheitsbedenken.

Das Abgeben der Kontrolle über eine Produktionsumgebung birgt ernsthafte potenzielle Sicherheitsprobleme. Wenn eine Software-Umgebung personenbezogene Daten, geistiges Eigentum oder andere vertrauliche Informationen generiert, speichert oder auf sie zugreift, kann sie als potenzielle Quelle für ein schwerwiegendes Datenleck eingestuft werden. Diese Sorge führte zu einem hartnäckigen Widerstand gegen den Einsatz von SaaS oder anderen Cloud-Lösungen. Neue Daten zeigen jedoch eindeutig, dass diese Befürchtungen inzwischen zerstreut werden können. Die Zweifel waren durch drei Annahmen begründet:

- Die IT-Abteilung kann die Sicherheit von Systemen und Daten besser gewährleisten, wenn sie die volle Kontrolle hat.
- Es ist sehr schwierig, die Sicherheits-kontrollen und -protokolle eines SaaS-Anbieters zu prüfen.
- Aufgrund der unmittelbaren räumlichen Nähe zu den Daten anderer SaaS-Kunden können die Mehrmandanten-Umgebungen der SaaS-Anbieter zahlreiche neue Angriffsvektoren auf die eigenen Unternehmensdaten eröffnen.

MEHR ALS

94 %

der Unternehmen verwenden **Software-as-a-Service** bereits in irgendeiner Form im Geschäftsbetrieb.

Cloud-Vordenker könnten versucht sein, diese Aussagen als Gerüchte abzutun. Dennoch ist es wichtig, diese Befürchtungen nicht als Unsinn abzutun, denn dahinter stehen einige sehr reale Fakten. Doch selbst die größten Gegner von Cloud-Services, die sich am scheinbaren Fehlen ausreichender Sicherheitsfunktionen stören, sollten sich von den ebenso realen Daten überzeugen lassen.

Die Umfrageteilnehmer nannten Sicherheit, Leistung und Benutzerfreundlichkeit als die drei wichtigsten Faktoren für den Einsatz von SaaS (*n=305)*. Das Unternehmen muss jedoch auf die Sicherheit des Anbieters vertrauen können und akzeptieren, dass dessen Sicherheitsmaßnahmen häufig zuverlässiger sind als die des Unternehmens selbst.

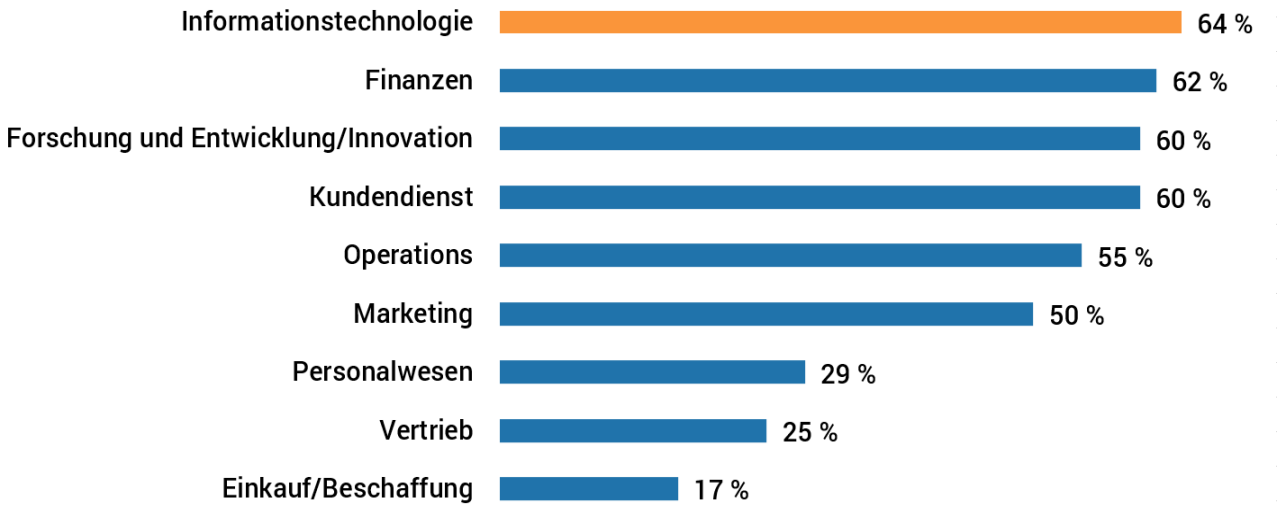
LOKAL	CLOUD
Sicherheit	Sicherheit
Benutzer-freundlichkeit	Leistung
Integration	Benutzer-freundlichkeit

SAAS-SICHERHEIT IST BESSER

Es mag manchen schwer fallen zu glauben, doch die meisten Unternehmen besitzen weder die Mittel oder Tools, noch die Erfahrung oder die Mitarbeiter, um ausreichende Sicherheitskontrollen zu implementieren. Sicherheit ist eine teure Angelegenheit, und der Schutz vor allen möglichen bekannten und unbekannten Angriffsvektoren (z. B. Zero-Day-Schwachstellen) erfordert enorme Investitionen, die nicht jedes Unternehmen stemmen kann. SaaS-Anbieter profitieren wiederum von den erheblichen Skalen-effekten durch Mehrmandanten-Modelle, da diese die Verteilung der Investitionen auf dutzende, hunderte oder gar tausende verschiedene Kunden ermöglichen.

Ihr Geschäft ist abhängig von ihrer guten Reputation, insbesondere in Bezug auf die Sicherheitslage, sodass die Investition in Sicherheit für die meisten Anbieter höchste Priorität hat. Jüngste Datenkompromittierungen bei privaten Unternehmen fügten ihrer Marke enormen Schaden zu, doch wenn diese Datenlecks einen großen Hosting-Anbieter betroffen hätten (und nicht ein Unternehmen aus dem Einzelhandel oder der Unterhaltungsbranche), wäre der Schaden irreparabel gewesen.

Doch woher kommen die Bedenken in Bezug auf die Sicherheit von SaaS-Anbietern? Seltsamerweise sind es noch nicht einmal die Sicherheitsteams oder IT-Abteilungen, die die Kompetenz der SaaS-Anbieter in Zweifel ziehen. Es sind vor allem die geschäftlichen Benutzer, die das geringste Vertrauen haben, dass der SaaS-Anbieter die Daten ihres Unternehmens sichern kann. Während 64 Prozent der an der Umfrage teilnehmenden IT-Experten (*n=241*) ihr Vertrauen in SaaS-Anbieter als hoch oder sehr hoch angaben, zeigten nur 44 Prozent der Teilnehmer aus allen anderen Abteilungen (*n=64*) das gleiche Vertrauen.



Vertrauen in SaaS-Sicherheit: Anteil der Umfrageteilnehmer, die ihr Vertrauen in SaaS-Sicherheit als hoch oder sehr hoch einschätzen

Könnte es sein, dass die verbesserte Übersicht der IT-Abteilung über die internen Sicherheitskontrollen sie motiviert, diese Komponente auszulagern – wohl wissend, dass sie nicht das gleiche Schutzniveau bieten können?

Wie sich gezeigt hat, ist das nicht der Fall. Die Umfrageteilnehmer, die ihr Vertrauen in die Cloud-Sicherheit als hoch oder sehr hoch einschätzen, haben tatsächlich mit einer Wahrscheinlichkeit von 19 Prozent höheres Vertrauen in ihre eigene interne Sicherheit und setzen im Schnitt 13 Prozent mehr Sicherheitstools in ihren Umgebungen ein (n=141). Das deutet darauf hin, dass umfangreiche Kenntnisse der internen Sicherheitsmaßnahmen nicht zu fehlendem Vertrauen führen, sondern stattdessen ein tieferes Verständnis für die Kompetenzen des SaaS-Anbieters ermöglichen.
Mit anderen Worten: Sicherheitsexperten wissen, dass sie den SaaS-Anbietern mindestens so sehr – wenn nicht noch mehr – vertrauen können wie ihren eigenen Schutzmaßnahmen.

Wann ist dieses Vertrauen in SaaS-Anbieter entstanden?

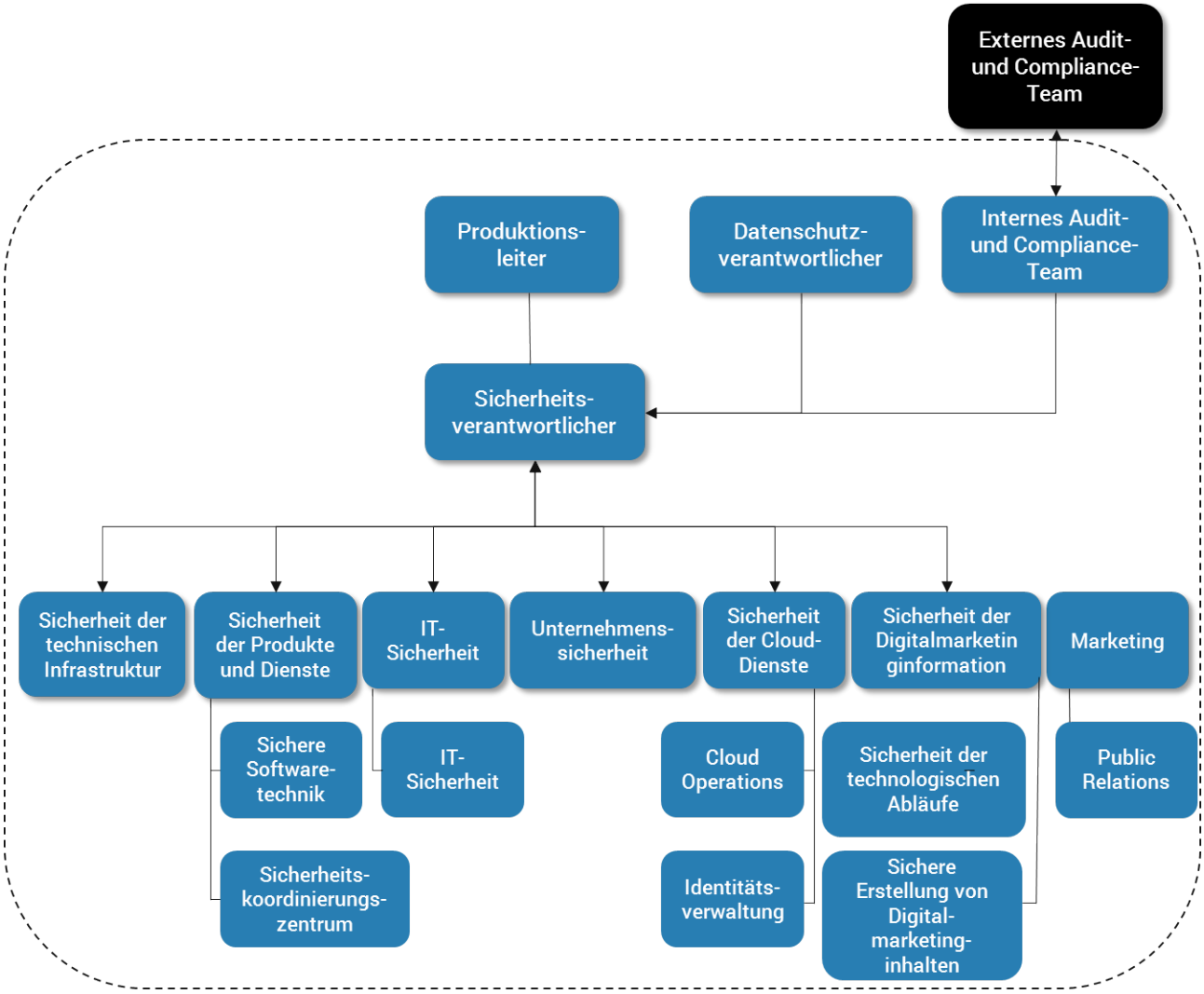
Auch wenn es nicht über Nacht gekommen ist, ist das Vertrauen in die Sicherheit von SaaS-Anbietern in den letzten Jahren so weit gestiegen, dass es kein Hindernis für den Einsatz mehr darstellt. Laut 81 Prozent der befragten Teilnehmer ist dieses Vertrauen mittlerweile ein Hauptargument. Die Cloud-Sicherheit hat sich erheblich schneller entwickelt als die Sicherheit der internen Teams. Laut dem Cloud-Sicherheitsbericht von Alert Logic für das Frühjahr 2014 („Cloud Security Report–Spring 2014", Alert Logic) zeigten Cloud-Anbieter in den Jahren 2012–2013 einen größeren Anstieg bei aus eigener Initiative gestarteten Schwachstellenscans ihrer vernetzten Ressourcen als vor Ort implementierte Lösungen. Die Umfrage zeigte auch, dass lokale Lösungen erheblich anfälliger für bestimmte Angriffe wie Malware und Botnets als ihre SaaS-Gegenstücke waren.

Der zweite Grund dafür, dass Cloud-Sicherheit so effektiv ist, sind die Skaleneffekte. Laut einer Untersuchung von Goldman Sachs soll der Cloud-Markt in den Jahren 2013–2018 eine jährliche Wachstumsrate von 30 Prozent erreichen („Roundup of Cloud Computing Forecasts and Market Estimates", 2015, Louis Columbus, Forbes). Es wird erwartet, dass die Unternehmensausgaben für IT im gleichen Zeitraum eine jährliche Wachstumsrate von 5 Prozent erreichen. Da das Cloud-Geschäft weiterhin boomt, können SaaS-Anbieter mit stabilen Einnahmen rechnen und Skaleneffekte nutzen, um stärkere, einheitlichere sowie umfassendere Sicherheitsfunktionen zu entwickeln. Durch den Druck auf die IT, das Geschäft dank technologischer Innovationen und nicht durch Commodity Services voranzubringen, verfügen die wenigsten IT-Abteilungen über die Budgets, Ressourcen oder Zeit, um die Daten ebenso zuverlässig abzusichern wie ein SaaS-Anbieter.

Ein Blick in die Sicherheitsumgebung eines SaaS-Anbieters

Die Sicherheitsmaßnahmen von SaaS-Anbietern sind umfassend und gründlich. Die meisten bekannten Anbieter verfügen über ein großes und umfassend geschultes Sicherheitsteam, sorgfältig ausgewählte Sicherheitsprodukte sowie effektive Richtlinien. Ein Blick auf die weltweit größten Cloud-Service-Anbieter zeigt, wie ernst ihnen die Sicherheit ihrer Angebote ist.

Diese Anbieter koordinieren ihre gesamten Sicherheitsmaßnahmen unter einem CSO (Chief Security Officer) oder CISO (Chief Information Security Officer). Das Büro dieses Sicherheitsverantwortlichen koordiniert alle Initiativen für Produkt- und Service-Sicherheit. Einer dieser Anbieter verfügt über unglaubliche 500 Experten für Informations-, Anwendungs- und Netzwerksicherheit.



Bei diesen Anbietern besteht ein sicherer Produkt- und Service-Lebenszyklus aus den folgenden Verfahren, damit sichergestellt ist, dass die angebotenen Anwendungen sicher und die gespeicherten Daten geschützt sind:

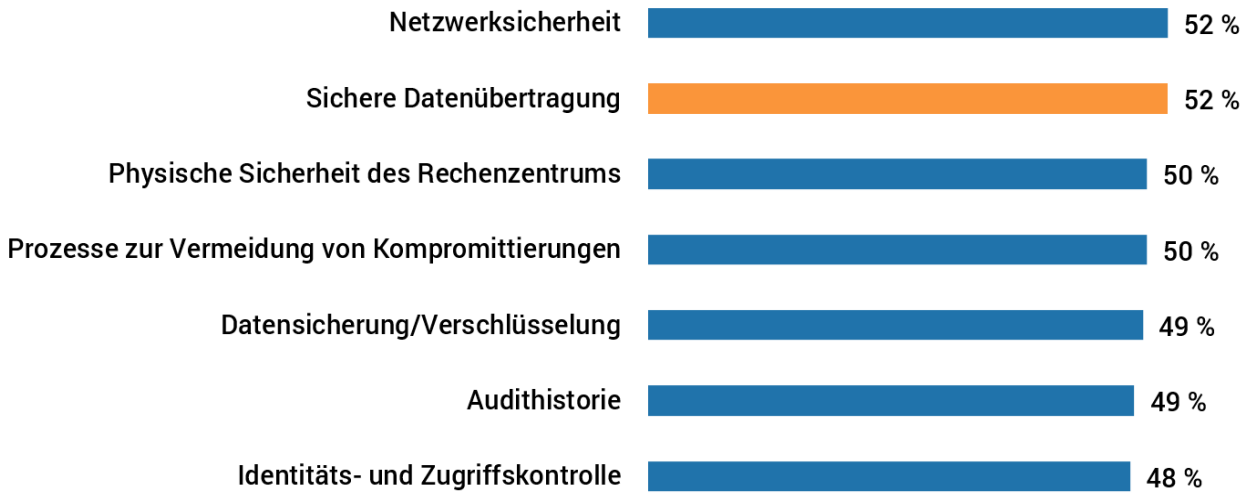
- Genaue Einhaltung der ISO 27034-Anforderungen
- Durchführung von Sicherheitsschulungen und Zertifizierungen für die Produktteams
- Durchführung von Analysen zu Produktstatus, Risiken und Bedrohungssituation
- Durchführung vorgeschriebener statischer Analysen
- Entwicklung von Richtlinien, Regeln und Analysen für sicheren Code
- Evaluierung aller Elemente der Sicherheitsumgebung
- Nutzung von Big Data zur Erkennung hochentwickelter Bedrohungen
- Entwicklung von Service-Roadmaps, Sicherheitstools sowie Testmethoden, die dem Sicherheitsteam dabei helfen, die zehn laut OWASP (Open Web Application Security Project) schwerwiegendsten Sicherheitsprobleme von Webanwendungen sowie die 25 laut CWE/SANS gefährlichsten Softwarefehler zu beheben
- Evaluierung der Sicherheitsarchitektur, Verschlüsselung und Penetrationstests
- Durchführung von Quellcode-Überprüfungen
- Einhaltung der gesetzlichen Vorschriften

Diese Anbieter schützen auch übertragene Kundendaten mittels Secure Socket Layer (SSL) und Secure Shell (SSH), um die Verbindung der Infrastruktur abzusichern. Die größeren Anbieter stellen außerdem verschiedene verwaltete Services bereit, bei denen sie die Verantwortung für das Gastbetriebssystem, die Anwendungssoftware und die Firewall der Infrastrukturverbindung übernehmen, um die Ende-zu-Ende-Verbindung abzusichern. Dadurch können Unternehmen nicht nur die Datenverarbeitung und -speicherung auslagern, sondern auch große Teile der Absicherung während der Übertragung. Erst dadurch lassen sich die Vorteile einer Cloud-Lösung wirklich nutzen.

Diese Maßnahmen bleiben heutigen IT-Experten, die in Bezug auf die Sicherheit gut geschult sind und gleichzeitig ihre eigenen Grenzen kennen, natürlich nicht verborgen.

Im direkten Vergleich ihrer Wahrnehmung der internen Sicherheitsfunktionen mit denen der SaaS-Anbieter waren 31 Prozent der Umfrageteilnehmer der Meinung, dass die SaaS-Anbieter die Datenübertragung besser absichern können als die Sicherheitsmaßnahmen des eigenen Unternehmens. Noch stärker verbreitet war das Vertrauen in die Verfahren der SaaS-Anbieter zur Behebung von Datenkompromittierungen.

Seriöse Cloud-Anbieter nutzen alle Tools zur Absicherung von Daten. Sie verfügen über die Größe, die Umgebung, das Budget sowie die Mitarbeiter, um auf dem allerneuesten Sicherheitsstand zu bleiben. Sie führen regelmäßig neue Funktionen ein, die den Vorsprung vor den internen IT-Sicherheitsteams weiter vergrößern.



SaaS-Anbieter sind kompetenter: Anteil der Teilnehmer aus dem IT-Bereich, die SaaS für kompetenter als die interne IT halten

VERTRAUEN SCHAFFEN

SaaS-Anbieter für Unternehmen betreiben unbestreitbar enormen Aufwand, um ihren Kunden die größtmögliche Sicherheit zu gewährleisten. Doch wie sieht es mit Second- und Third-Tier-Anbietern aus? Die meisten Anbieter nehmen die Sicherheit sehr ernst und treffen alle notwendigen Maßnahmen. Es ist jedoch wichtig, jeden Anbieter gründlich zu überprüfen, der mit den vertraulichen Informationen des Unternehmens in Berührung kommt. Insbesondere in Branchen, die Vorschriften wie PIPA, HIPAA, PCI oder Sarbanes-Oxley befolgen müssen, muss unbedingt analysiert werden, an welcher Stelle ein SaaS-Anbieter Zugriff auf Daten hat, die unter diese Vorschriften fallen.

Gleichzeitig muss sichergestellt werden, dass ausreichende Schutzmaßnahmen implementiert sind. Dies ist notwendig, da bei einer Datenkompromittierung andernfalls finanzielle Strafen verhängt werden und irreparable Schäden für die Reputation und Marke des Unternehmens entstehen können.

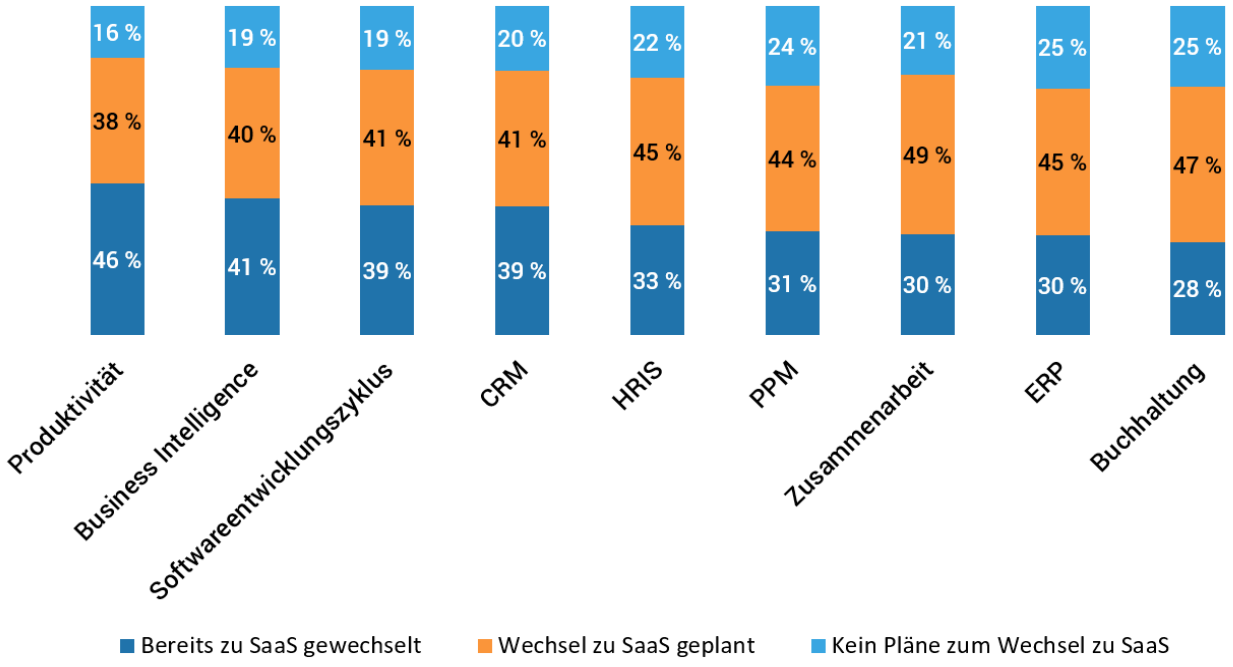
Die einzige Möglichkeit, um bei der Übertragung von Workloads in eine SaaS-Umgebung wirklich sicher zu sein, ist die Umsetzung eines strukturierten und prozessgesteuerten Ansatzes. Info-Tech empfiehlt diese dreistufige Vorgehensweise:

Analyse des Unternehmensrisikos

Die Daten, die ein Unternehmen in die Cloud auslagern kann, sind abhängig von geschäftlichen, Compliance- und Kundenanforderungen. Daher spielen die rechtlichen Vorschriften, die Wichtigkeit und Vertraulichkeit der Daten sowie die Art der zu implementierenden SaaS-Lösung eine wichtige Rolle bei der Bewertung der Risikostufe. Um das Risiko zuverlässig zu definieren, muss ein Unternehmen daher untersuchen, welche Auswirkungen die SaaS-Einführung auf die folgenden Elemente hat:

- Geschäftliche Aspekte
- Umsatz
- Kundenakquise oder Kundenbindung
- Benutzerzufriedenheit
- Markteinführungszeit
- Kosten durch Lastspitzen
- Einhaltung gesetzlicher Bestimmungen

Es überrascht nicht, dass für die Umfrageteilnehmer SaaS am wenigsten bei Software in Frage kam, die vertrauliche Finanzdaten enthält (z. B. Buchhaltung und Enterprise Resource Planning). Interessant ist jedoch, dass Lösungen zur Entwicklung oder Speicherung des eigenen geistigen Eigentums (z. B. Produktivitätstools oder Business Intelligence und Analysen) am häufigsten von den Teilnehmern in SaaS-Dienste ausgelagert werden. Sie nehmen die Kompromittierung von Finanzdaten als größeres Risiko wahr als der potenzielle Verlust von geistigem Eigentum.



SaaS-Implementierung nach Softwaretyp: Anteil der Umfrageteilnehmer, die den genannten Softwaretyp in SaaS ausgelagert haben

Anforderungen an die Zugriffssicherheitskontrollen

Ein Unternehmen kann nur dann die richtige Entscheidung über die Übertragung von Workloads in SaaS-Services treffen, wenn es seine internen Möglichkeiten realistisch einschätzt. Obwohl 67 Prozent der Umfrageteilnehmer ihr Vertrauen in die eigene interne Sicherheit als hoch oder sehr hoch einstufen, hat Info-Tech einen Überhang von etwa sechs Prozentpunkten in der Wahrnehmung der internen Sicherheit im Vergleich zu den tatsächlich getroffenen Maßnahmen registriert. Diese Unternehmen sind in der gefährlichsten Lage überhaupt, da im Sicherheitsbereich übermäßiges Selbstvertrauen zu großen Risiken führt. Wer seine Grenzen, Schwächen und Sicherheitslücken kennt, kann die allgemeine Sicherheitslage realistisch überblicken – übermäßiges Selbstvertrauen führt jedoch zu unnötigen Schwachstellen.

Die meisten Unternehmen geben zwar an, dass sie Datenschutz und -verschlüsselung, Identitäts- und Zugriffskontrollen sowie Netzwerksicherheitsmaßnahmen einsetzen, doch nur die Hälfte verfügt über physische

Rechenzentrumsicherheit in irgendeiner Form oder führt interne Sicherheits-Audits durch. Noch einmal weniger Umfrageteilnehmer (etwa ein Drittel) gab an, dass sie Pläne zur Behebung von Datenkompromittierungen ausgearbeitet haben. Ein starker SaaS-Anbieter setzt all diese Technologien ein, betreibt ein nach ISO 27001 zertifiziertes Rechenzentrum und führt regelmäßig Penetrations- und Schwachstellentests durch. Die Ergebnisse werden dokumentiert und können sicherheitsbewussten Kunden vorgelegt werden.

Bewertung von Anbietern im Hinblick auf Sicherheit

Info-Tech Research Group empfiehlt die Implementierung des CAGI-Modells (Completeness/Function, Auditability, Governability und Interoperability) zur Analyse der Sicherheitskompetenzen eines Anbieters.

Das Unternehmen muss die Gestaltung eines SaaS-Servicevertrags genau verstehen, um einen Anbieter auf die Vollständigkeit des Angebots zu analysieren. Im Kundenvertrag müssen Datenrichtlinien in Bezug auf Datensicherheit, Redundanz, Standort, Verifizierung eines neuen Datenstandorts und Beschlagnahme untersucht werden. Wenn ein SaaS-Anbieter die richtigen Datenrichtlinien implementiert hat, kann ein Unternehmen eher darauf vertrauen, dass dessen Sicherheitsmaßnahmen effektiv sind.

Die Prüfbarkeit eines Anbieters kann danach analysiert werden, ob er bereit ist, unabhängige umfassende Audit-ergebnisse bereitzustellen. Diese Audit-daten müssen Forensik-Analysten die Möglichkeit geben, zu verstehen, wie es zu einem bestimmten Ereignis gekommen ist und welche Ressourcen kompromittiert wurden. Zudem sollten Analysten mithilfe dieser Informationen erkennen können, welche Richtlinien, Verfahren und Technologien geändert werden müssen, um ähnliche Zwischenfälle in Zukunft zu verhindern. Wenn ein SaaS-Anbieter diese Transparenz nicht bietet, sollten Sie sich von ihm fernhalten.

Die „Governability" (Überwachbarkeit) eines SaaS-Anbieters kann analysiert werden, indem überprüft wird, wie häufig und umfassend er seine Umgebung überwacht. An erster und wichtigster Stelle steht, dass der Anbieter die Protokolle und Leistung überwachen muss. Der Anbieter muss jedoch auch nach Anzeichen für böswilligen Missbrauch, Kompromittierung und Richtlinien-verstöße suchen. Um auf die Schnelle die Einhaltung von Überwachungsvorschriften zu bestätigen, sollte der Anbieter einen SOC 2 Type 2-Bericht, eine ISO 27001-Zertifizierung sowie eine CSA STAR-Zertifizierung, einen PCI DSS-Analysebericht und eine FedRAMP-Autorisierung vorlegen. Wenn der Anbieter all das bereitstellen kann, hat das Unternehmen die Sicherheit, dass die Daten in guten Händen sind.

Zu guter Letzt muss ein Unternehmen sicherstellen, dass seine Daten sicher geschützt zu einem neuen Anbieter oder – wenn es sich vom SaaS-Anbieter trennt – in seine eigenen Grenzen übertragen werden können. Die Interoperabilität betrifft dabei Daten, Prozessintegration sowie Verwaltungs- und Geschäftsfunktionen. Wenn die Daten nicht übertragen werden können, kann das Unternehmen gezwungen sein, die Daten manuell vom alten zum neuen Anbieter zu importieren, was mit erheblichem Zeit- und Kostenaufwand verbunden ist.

KAUF VON SAAS

„Sobald ein Unternehmen eine SaaS-Lösung angeschafft hat, muss es nichts mehr tun, um seine Daten zu sichern, da es alle Arbeit dem Anbieter überlassen kann." Diese Ansicht findet sich überraschend häufig, könnte jedoch nicht weiter entfernt von der Realität sein. Es gibt tatsächlich Schritte, die ein Unternehmen durchführen kann und sollte, um den Schutz seiner Daten, Kunden und des Geschäftsbetriebs zu sicherzustellen.

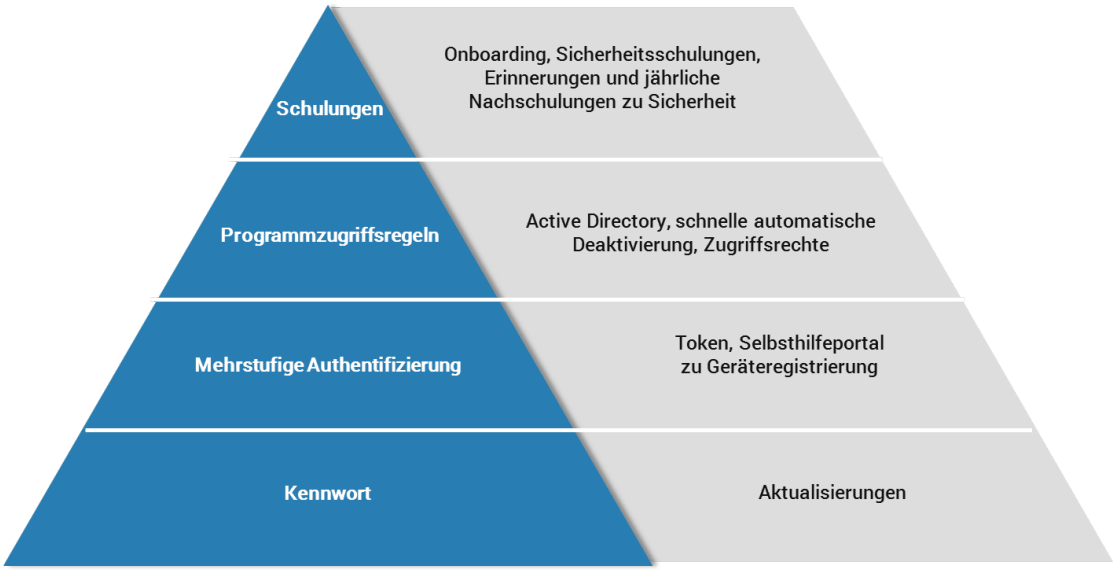
Ein Unternehmen kann verschiedenste Prozesse implementieren, die die Cloud ergänzen und sie weiter absichern. Zugriff, Überwachung und Partnerverwaltung sind Kernbereiche, die ein Unternehmen stets im Blick haben muss.

Analyse der Zugangsmöglichkeiten

Selbst wenn die notwendigen Sicherheitstechnologien vorhanden sind, verzichten viele Unternehmen auf die wichtigsten Schritte, um die Exfiltrierung dieser Daten mithilfe anderer Methoden zu unterbinden. 60 Prozent aller Sicherheitsvorfälle im Jahr 2014 wurden von Mitarbeitern verursacht, berichtet der 2016 Data Breach Industry Forecast von Experian („Cloud security: 10 things You Need To Know", Conner Forrest, Tech Republic).

Ein SaaS-Anbieter kann jede nur mögliche Kontrolle implementieren, doch eine einzige schwache bzw. gestohlene Benutzername/Kennwort-Kombination für das Unternehmen ist ausreichend, um all diese Kontrollen wertlos zu machen, da der unbefugte Zugriff durch die Vordertür geschieht.

Die folgenden vier Elemente verringern die Wahrscheinlichkeit einer Kompromittierung beim Zugriff:



An erster Stelle steht, dass das Kennwort der Benutzer mindestens zwölf Zeichen lang sein sollte (mit Groß-/Kleinbuchstaben, Sonderzeichen und Ziffern). Hinzu kommt, dass das Unternehmen eine Richtlinie implementieren sollte, wonach Benutzer ihr Kennwort regelmäßig – mindestens aller drei Monate – ändern sollten.

Zweitens sollte die IT-Abteilung sicherstellen, dass alle Abteilungen eine mehrstufige Authentifizierung einsetzen.
Die Authentifizierung kann über ein RSA-Token, OTP per SMS oder Telefon, Smartcard, Public-Key-Infrastruktur und Biometrie erfolgen. Außerdem können Unternehmen risikobasierte Authentifizierung einsetzen, bei der die Validierungskriterien abhängig sind von der Art der Transaktion innerhalb der Anwendung sowie von der Geräteidentifikation, dem geografischen Standort, dem ISP und heuristischen Informationen. Diese Tools können als zweite Authentifizierungsebene verwendet werden, wenn eine Person eine VPN-Verbindung über ein unsicheres Netzwerk aufbaut.

Drittens muss ein Unternehmen gewährleisten, dass der Benutzerzugriff ausschließlich auf die Bereiche beschränkt ist, die für diese Rolle notwendig sind. Diese Zugriffsrechte müssen sich einfach ändern lassen, und wenn ein Mitarbeiter das Unternehmen verlässt, sollten sich alle Zugriffsrechte automatisch mithilfe einer Active Directory-Abfrage widerrufen lassen.

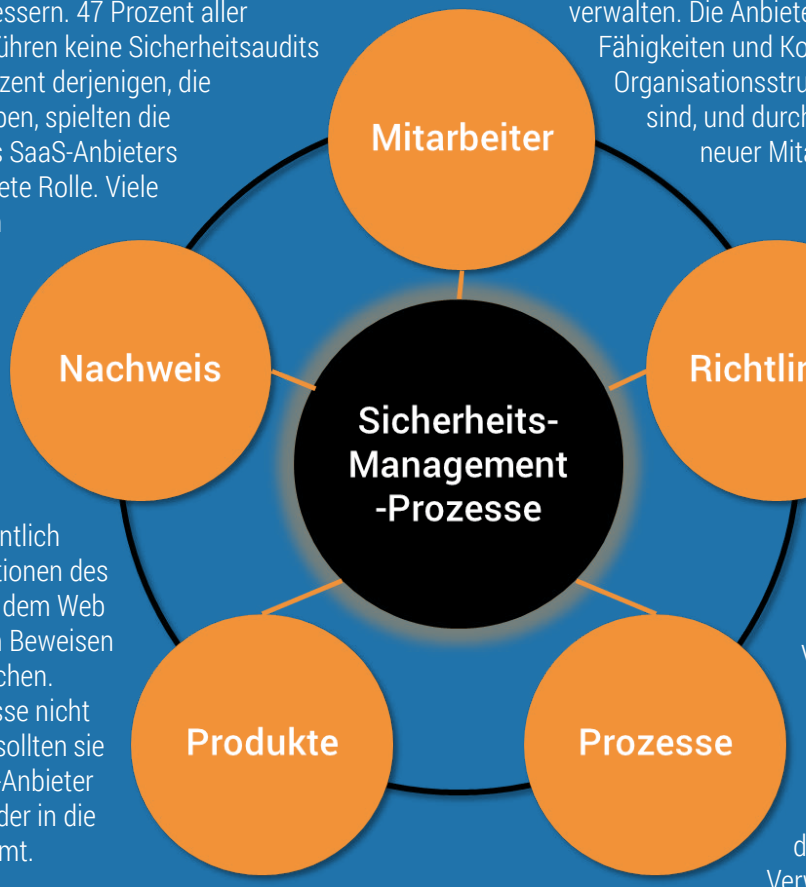
Und schließlich gilt: Sofern möglich, sollten Mitarbeiter die notwendigen Schulungen zu den richtigen Sicherheitsverfahren erhalten. Da viele Kompromittierungen aufgrund von Mitarbeiterfehlern geschehen, kann kein Unternehmen darauf verzichten, seine Angestellten zu schulen. Mithilfe dieser Schritte kann ein Unternehmen es seinen Mitarbeitern erleichtern, die richtige Vorgehensweise zu beachten und die Wahrscheinlichkeit einer Datenkompromittierung zu verringern.

Analyse der Überwachung

Selbst die besten Pläne können dank Zero-Day-Schwachstellen und anderen Angriffsvektoren, die sich kaum oder gar nicht verhindern lassen, innerhalb eines Augenblicks zu Makulatur werden. Unabhängig davon, ob diese Schwachstelle auf Kundenseite oder in der Umgebung des SaaS-Anbieters gefunden wird, gewährleistet die frühzeitige Implementierung ausreichender Überwachungsmaßnahmen, dass bei einem Zwischenfall alle Parteien einem festgelegten Plan folgen und möglichst wenige Überraschungen auftreten.
Wichtige Elemente eines ausreichenden Überwachungsplans für SaaS-Anbieter umfassen die Forderung nach sofortiger Benachrichtigung, Zeitpläne für Situations-Updates sowie die Verpflichtung zur Ursachenanalyse.

Es gibt fünf wichtige Bereiche, die ein Unternehmen im Blick haben sollte: Mitarbeiter, Richtlinien, Prozesse, Produkte und Nachweise.

Nachweis: Die Effektivität der Sicherheitskontrollen muss kontrolliert werden, um die Überwachung der Cloud weiter zu verbessern. 47 Prozent aller Umfrageteilnehmer führen keine Sicherheitsaudits durch, und für 63 Prozent derjenigen, die in SaaS investiert haben, spielten die Auditnachweise ihres SaaS-Anbieters nur eine untergeordnete Rolle. Viele SaaS-Anbieter führen regelmäßig Audits zur Einhaltung von ISO und SOC 2 durch oder nehmen andere Sicherheitstests vor (z. B. Penetrationstests). Info-Tech empfiehlt, in den öffentlich verfügbaren Informationen des Anbieters (sei es aus dem Web oder in Artikeln) nach Beweisen für diese Tests zu suchen. Sind die Testergebnisse nicht öffentlich verfügbar, sollten sie direkt von dem SaaS-Anbieter angefordert werden, der in die engere Auswahl kommt.



Mitarbeiter: Verlangen Sie nicht von einem Mainframe-Programmierer, die Beziehung zum SaaS-Anbieter zu verwalten. Die Anbieterverwaltung erfordert eigene Fähigkeiten und Kompetenzen, die nicht immer in der Organisationsstruktur des Unternehmens vorhanden sind, und durch Schulungen oder die Einstellung neuer Mitarbeiter erworben werden müssen.

Richtlinien: Ein Unternehmen muss die Sicherheitsrichtlinien und -verfahren dokumentieren, die abhängig von der Situation befolgt werden müssen. Dazu sollten unter anderem Anweisungen zur ordnungsgemäßen Nutzung, Kennworterstellung und Vertraulichkeit gehören.

Prozesse: Der sichere Betrieb von Cloud-Diensten und abgesicherte Datenübertragungen können durch die Implementierung effektiver Verwaltungsmodelle für Sicherheit und störungsfreien Geschäftsbetrieb gewährleistet werden. Dazu gehört beispielsweise, dass die Inbetriebnahme oder Außerbetriebnahme beliebiger SaaS-Lösungen einem vorgeschriebenen Prozess folgt und keine wichtigen Elemente übersehen werden.

Produkte: Auch wenn der SaaS-Anbieter für die Absicherung seiner Umgebung verantwortlich ist, bedeutet der Trend zu Hybrid-Umgebungen, in denen der Kunde einen Teil der Daten speichert, dass auch er alle erforderlichen Tools zur Absicherung der Daten einsetzen muss.

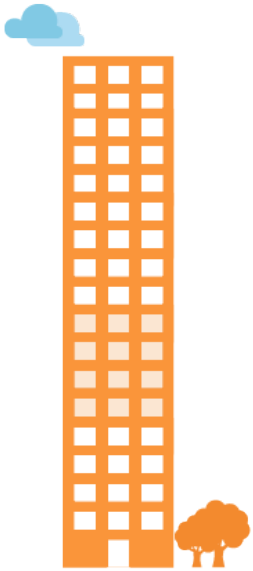
- Systemweite Endgerätesicherheit
- Firewall der nächsten Generation
- Eindringungsschutz
- Risiko und Compliance
- Sicherheitsinformations- und Ereignis-Management (SIEM)
- Hochentwickelte Malware
- Web- und E-Mail-Sicherheit
- Datenschutz
- Mobilgerätesicherheit
- Sicherheit des Rechenzentrums
- Identitäts- und Zugriffsverwaltung

Die Bedeutung der Partnerverwaltung

Durch die Einführung von SaaS-Technologien wechselt das IT-Bereitstellungsmodell von der Entwicklung, Wartung und Unterstützung von Lösungen zur Verwaltung von Verträgen und Beziehungen mit Anbietern. Es ist unumgänglich, offene Kommunikationskanäle aufrecht zu erhalten, um die Transparenz zu fördern. Wenn es zu Produkt-Update- und Versionszyklen, planmäßigen Ausfallzeiten sowie Änderungen bei Backend-Frameworks oder Entwicklungssprachen keine Unklarheiten gibt, entstehen keine Überraschungen, die zu neuen Schwachstellen führen können.

Bei der effektiven Verwaltung der Beziehung haben Unternehmen mehrere Möglichkeiten. Welche dieser Möglichkeiten für die Beziehungsverwaltung eine Rolle spielen, ist abhängig von der Größe und dem Umfang der angebotenen Leistung. Beispielsweise rechtfertigt der Kauf von Komponenten einer Technologie, die niemals mit vertraulichen Daten oder geistigem Eigentum in Berührung kommt, wahrscheinlich keine regelmäßigen Updates oder Überprüfungen. Info-Tech empfiehlt jedoch, in jedem Fall standardmäßig anhand dieser Liste vorzugehen und sie situationsabhängig anzupassen:

1. Definieren Sie alle wichtigen Kontakte beim Anbieter – von der Kontoverwaltung, dem Technik-Support sowie dem Notfall-Support nach Feierabend.
2. Legen Sie intern eine Person fest, die die Beziehung verwaltet und dafür verantwortlich ist.
3. Legen Sie einen klaren Eskalationspfad fest, der den SLAs und anderen gut dokumentierten Erwartungen entspricht.
4. Planen Sie regelmäßige Updates mit dem Anbieter.
5. Führen Sie aller drei Monate Überprüfungen durch, um die Einhaltung der Performance-Ziele zu gewährleisten.



ÜBERBLICK UND SORGFALTSPFLICHT

Es wird wahrscheinlich niemals absolute Sicherheit geben, dass jede der Cloud überantwortete Datenressource vor Kompromittierung geschützt ist. Wenn die in den vorherigen Kapiteln erläuterten Taktiken jedoch befolgt werden, kann das Unternehmen eine zuverlässige Sicherheit etablieren. Der wichtige erste Schritt ist das Kennenlernen der Sicherheitsmaßnahmen – sowohl der internen IT als auch der des SaaS-Anbieters, dem Sie Ihre Daten überantworten. Nur dann kann mit der ordnungsgemäßen Analyse, Validierung und Überprüfung des SaaS-Anbieters begonnen werden, um die Datenressourcen abzusichern. Vertrauen in Cloud-Sicherheit sollte nicht blindlings gewährt, sondern über einen strukturierten und gründlichen Ansatz aufgebaut werden, um zu analysieren, wie, wo und von wem die Daten gesichert werden.

Daten der Info-Tech Research Group-Umfrage zur Cloud-Sicherheit. Diese Online-Umfrage wurde vom 23. Februar bis 9. März 2016 mit 305 Teilnehmern aus den USA, Großbritannien, Frankreich, Deutschland, Indien, Australien und Neuseeland durchgeführt.

INFO-TECH RESEARCH GROUP

Sponsored by Adobe