ISPIN AG ZURICH
swiss made security.
Member of CymbiQ Group

Cloud Security Services

Sicherheit ohne Schattenseiten.

Cloud Security Risk Assessement

Wie viele Cloud-Anwendungen und -Dienste werden in Ihrem Unternehmen genutzt? Entsprechen diese Apps Ihren Security- und Compliance-Richtlinien? Wissen Sie im Detail, in welche Bereiche der Cloud Ihre Daten fliessen? Können Sie diese Fragen verlässlich beantworten oder gibt es da einen Graubereich, den Sie nicht überblicken und nicht kontrollieren? Sehr vielen Unternehmen fehlt die vollständige Transparenz und Kontrolle über die Cloud, womit ein enorm hohes Risiko für Compliance-Verstösse und Datenabflüsse einhergeht. Höchste Zeit, sich Klarheit zu verschaffen und den Steuerknüppel für die Cloud-Security und -Compliance wieder in die Hand zu nehmen.

Denn nur, wenn Sie die Schatten-IT in Ihrem Unternehmen ins Licht rücken, schaffen Sie die Grundvoraussetzung für die Erhöhung Ihrer Sicherheit. Oder wissen Sie, wo überall Ihre Mitarbeitenden Unternehmensdaten speichern? Durch die zunehmende Zahl an Home-Office- und Remote-Workern hat sich auch hier eine riskante Entwicklung aufgetan: Sehr häufig werden sensible Daten in privaten Cloud-Apps abgelegt, ohne dass das Unternehmen davon Kenntnis hat. Das ist mehr als bedenklich - zumal nicht nur Unternehmen, sondern verstärkt auch Cyberkriminelle auf die Cloud setzen und diese vermehrt als Tor zur Verteilung von Malware nutzen.

Ihre Vorteile auf einen Blick

- Umfassender Überblick über alle genutzten Cloud-Dienste.
- Qualifizierung der identifizierten Cloud-Dienste nach dem Cloud Confidence Level.
- Analyse des Datenverkehrs in Richtung Cloud, aufgeschlüsselt nach Anwendungen.
- Aufschlüsselung der wichtigsten Risiken, z. B. Data Loss, Compliance und Cloud Threats mit zugehörigen Metriken.
- Konkrete Handlungsempfehlungen für die Risikominimierung.

Kein Unternehmen kommt mehr ohne Cloud-Anwendungen aus. Im Gegenteil: Die Anzahl der in Organisationen eingesetzten Cloud-Dienste steigt kontinuierlich. Durchschnittlich 1300 Cloud-Anwendungen werden in grossen Unternehmen genutzt, mehr als 500 in mittelgrossen. Die Cloud überzeugt schlichtweg durch ihre Vorteile. Die vielen kleinen Helfer-Apps stehen sofort bei Bedarf zur Verfügung, sind einfach in der Bedienung, erfordern nur geringen Verwaltungsaufwand und erhöhen die Agilität und Produktivität im Unternehmen. Aber: Nur 2 % der eingesetzten Cloud-Services liegen in der Verantwortung der IT-Abteilung und werden von dieser kontrolliert. Der Rest bildet ein riesiges Schattenreich, das eine ganze Reihe von vielfach unerkannten und unterschätzten Gefahren mit sich bringt:

- Fast die Hälfte (47 %) des Internetverkehrs in die Cloud verläuft unverschlüsselt – und das, obwohl 37 % der Daten, die in Cloud-Apps genutzt werden, vertrauliche Informationen (personenbezogene Daten, Passwörter, Credentials oder Kreditkarteninformationen) sind.
- Pro Mitarbeiter und Monat werden durchschnittlich 20 sensitive Dateien auf Public Cloud Storage Services geladen, wo sie oft unverschlüsselt liegen.
- Viele Cloud-Services garantieren in ihren Nutzungsbedingungen nicht, dass die Daten ausschliesslich dem Kunden gehören.
- Unsichere und nicht autorisierte Cloud-Services können Kanäle für Angreifer öffnen. Diese nutzen die Situation: 60 % der Malware wird über Cloud-Storage verteilt; 36 % aller Phishing-Kampagnen zielen auf Cloud-Identitäten ab; 90 % aller Attacken starten mit Phishing. Viele Phishing-Webseiten sind vermeintlich korrekte Cloud-Services.
- Nur 22 % der Cloud-Services sind vertrauenswürdig, also für den Enterprise-Einsatz geeignet.
- Viele der genutzten Anwendungen sind nicht rechts- bzw. DSGVO-konform.

Keine blinden Flecken mehr

Mit den herkömmlichen Perimeter-zentrierten Sicherheitsmodellen ist das Problem nicht in den Griff zu kriegen. Diese Legacy-Lösungen bieten nur eine binäre Richtlinienauswahl: blockieren oder erlauben. Blockieren ist weder für die IT noch für die User eine wählbare Option. Denn die Anwender möchten uneingeschränkten und schnellen Zugriff auf die Apps und erwarten, dass dies möglich ist, ohne dabei die Sicherheit der Organisation zu beeinträchtigen. Notwendig sind also andere Sicherheitslösungen. Bevor Sie aber über eine neue Lösung nachdenken, sollten Sie sich zunächst einen Überblick darüber verschaffen, welche Cloud-Anwendungen in Ihrer Organisation bereits genutzt werden und wie diese im Hinblick auf Sicherheitsrisiken, Datennutzung und Rechtskonformität zu bewerten sind.

Risiken erkennen und verstehen

Transparenz die neugierig macht

Das Cloud Security Risk Assessment von ISPIN richtet den Blick durch die Lupe auf den Cloud-Einsatz in Ihrem Unternehmen. Sie erhalten einen bislang nie dagewesenen Ein- und Überblick in die Cloud- und Webnutzung sowie in managed und unmanaged Apps in Ihrem Unternehmen. Zudem unterstützt Sie ein detaillierter Bericht inklusive konkreter Handlungsempfehlungen bei der Risikoanalyse und bei der Steuerung.

Mit dem Cloud Security Risk Assessment sind Sie in der Lage:

- alle in Ihrem Unternehmen bereits genutzten Apps und Dienste nach Kategorie aufzuspüren,
- für die geschäftliche Nutzung qualifizierte Apps (enterprise readiness level) zu ermitteln,
- die Nutzung und die Datenbewegungen in sanktionierten und nicht erlaubten Apps zu erkennen,
- DLP-Verstösse und Datenexpositionen ausfindig zu machen,
- mögliche weitere Sicherheitsrisiken und Datenschutzverletzungen zu erkennen.

Verschaffen Sie sich ein vollständiges Bild über die Cloudrisiken Ihrer Organisation

Das Assessment startet mit einem Kick-Off-Workshop. Für die Analyse ziehen wir anonymisierte Logfiles von Proxy-Servern heran. Sobald wir also das Sample Log File von Ihnen erhalten haben, starten wir mit der Analyse und dem Parsing (pro Logfeed). Die Ergebnisse stellen wir in einem detaillierten Bericht zusammen, den wir Ihnen im Rahmen einer Remote- oder Vor-ort-Präsentation präsentieren und übergeben.

Was beinhaltet der Report?

Der Report liefert Ihnen die nötige Transparenz, um gezielte Security-Verbesserungen durchführen zu können. Er enthält einerseits die Ergebnisse unserer Analyse:

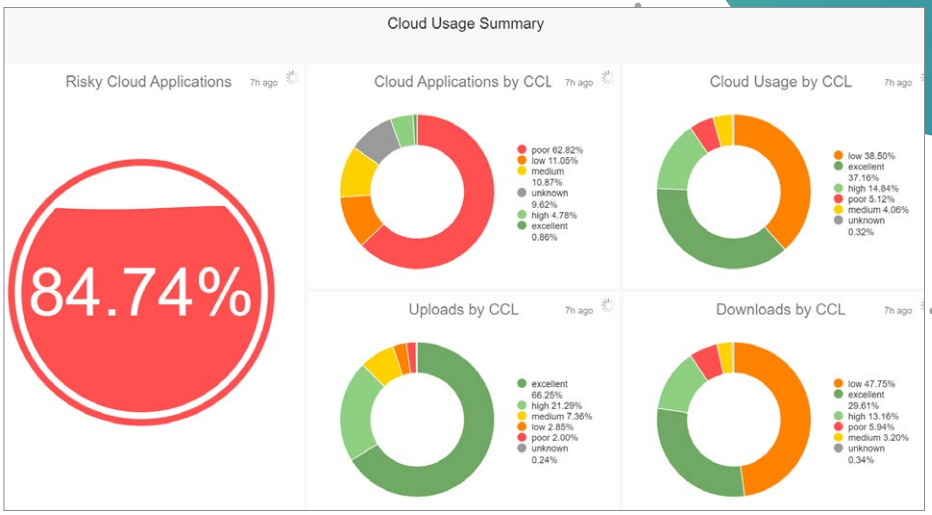
- Kontrollierte bzw. bekannte / unkontrollierte bzw unbekannte Cloud Services
- Risikolevel der Cloud Services basierend auf dem Cloud Confidence Index
- Instance Awareness (z.B. Erkennung von Firmen und privaten M365 Instanzen)
- Analyse von Datenschutzverletzungen

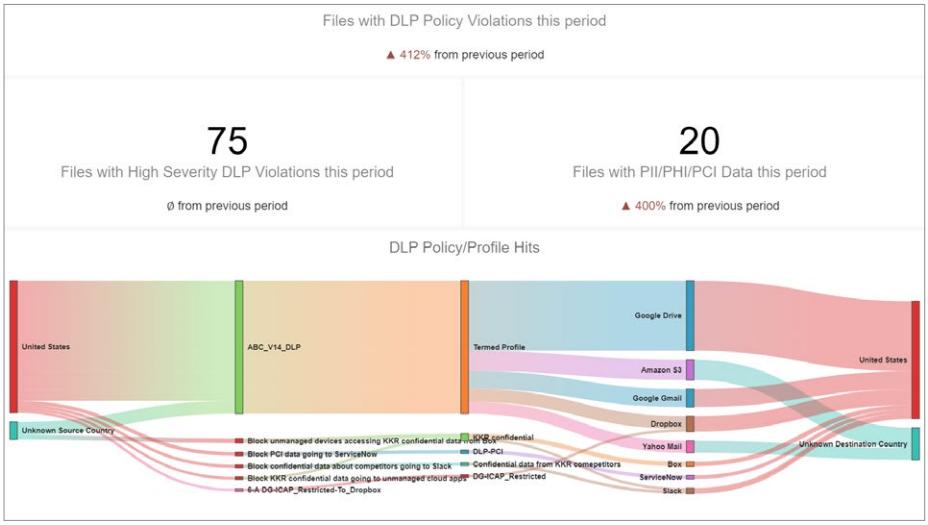
Andererseits zeigen wir Ihnen eine mögliche Roadmap auf und geben Ihnen taktische Empfehlungen für Massnahmen zur Risikominimierung in Ihrer IT-Infrastruktur wie z. B.:

- sofort, z. B. Sperren von nicht kategorisierten Webseiten
- mittelfristig, z. B. Aufbau einer reinen Monitoring-Umgebung für Cloud Services
- langfristig, z. B. Erweiterung mit Kontrolle der Cloud Services

Anwendungsanalyse

Die in Ihrem Unternehmen eingesetzten Cloud-Anwendungen ändern sich schnell - je nach Bedarf der Mitarbeitende kommen neue hinzu oder fallen vorhandene weg. Für Sie ist es daher unverzichtbar, die Anwendungsnutzung kontinuierlich zu überwachen und das Risikopotential zu identifizieren. Darauf aufbauend können Sie geeignete Massnahmen setzen, die die Einhaltung Ihrer Sicherheitsrichtlinien gewährleisten.





Datenschutzanalyse

Verschaffen Sie sich einen detaillierten Überblick darüber, wo bzw. in welchen Anwendungen sich Ihre Daten befinden. Stellen Sie fest, welche Risiken mit den jeweiligen Anwendungen für Ihr Unternehmen einhergehen.

Vertraulichkeitsanalyse

Im Jahr 2020 stieg die Anzahl der genutzten Cloud-Applikationen pro Unternehmen um 20 Prozent. Unternehmen mit 500 bis 2.000 Mitarbeitern nutzen im Durchschnitt 664 verschiedene Cloud-Apps pro Monat. Fast die Hälfte der in Unternehmen genutzten Anwendungen schneidet bei Analysen mit einem «mangelhaften» Cloud-Confidence-Index (CCI) ab. Der Cloud Confidence Index überwacht und bewertet mehr als 34'000 Applikationen kontinuierlich. Die Plattform erkennt dabei, ob die Dienste mit geschäftlichen oder privaten Konten genutzt werden und ob der Services für die geschäftliche Nutzung geeignet ist.

	Application	CCL	Compliance Certification	Sum - Total Bytes
1	Vagrant Cloud	poor	PCIDSS,Privacy Shield	748,450,694
2	Infomaniak	poor	No published support	499,580,977
3	Udemy	poor	No published support	177,095,663
4	LEGO	poor	PCIDSS,TrustArc	82,057,276
5	9GAG	poor	No published support	61,628,697
6	DeepL Translator	poor	Privacy Shield	59,811,481
7	urlscan.io	poor	No published support	48,110,413
8	Meetup	poor	No published support	45,925,001
9	Unsplash	poor	No published support	30,884,682
10	Hostpoint	poor	No published support	27,573,591

Das A und O für eine sichere Cloud: Umfassende Sichtbarkeit.

Treffen Sie datengesteuerte Sicherheitsentscheidungen auf der Grundlage eines kristallklaren Verständnisses dessen, was wichtig ist. Mit dem ISPIN Cloud Security Risk Assessment erkennen Sie Ihre vorhandenen Risiken und können genau bestimmen, wo Ihr Team seine Zeit und Energie einsetzen sollte.

Inhaltselemente des Cloud Security Risk Assessments
Entdeckte Applikationen zusammengefasst nach Kategorie
Vertrauens- und Risikobewertung der gefundenen Applikationen
Analyse der Datenbewegung inklusive detaillierte Zusammenfassung der Datenbewegungen, auch nach Benutzern (z.B. Up- und Downloads)
Applikations- und Nutzungsanalyse von riskanten Aktivitäten (z. B. Teilen, etc.) in sanktionierten Applikationen
Risikoanalyse, welche auf die geschäftlichen Anforderungen Ihres Unternehmens abgestimmt ist
Analyse der Offenlegung sensibler Daten (DLP-Verletzungen in gespeicherten Inhalten)
Analyse von Datenschutzverletzungen (DLP-Verletzungen im Netzwerkverkehr)
Handlungsempfehlungen mit Roadmap zur Risikominimierung

Rücken Sie die Schatten-IT in Ihrem Unternehmen ins Licht und fordern Sie Ihr persönliches Cloud Security Risk Assessment an.

Wir beraten Sie gerne.
Senden Sie uns Ihre Anfrage: cloudsecurity@ispin.ch

ISPIN AG
Grindelstrasse 6
CH-8303 Bassersdorf
Tel.: +41 44 838 31 11
www.ispin.ch