Broschüre

Datenhoheit: Digitale Sicherheit für Europa

W / T H
secure

Inhalt

Zusammenfassung

Diese Broschüre richtet sich an Experten für Cybersicherheit, die einen Managed Detection and Response (MDR)-Dienst für eine Sicherheitsstrategie suchen, mit der sie die in Europa – speziell in der Europäischen Union – geltenden Sicherheitsrichtlinien zuverlässig einhalten können. Die Informationen, die wir Ihnen hier kompakt liefern, werden Ihnen helfen, eine Lösung zu finden, die Ihren Anforderungen an eine solche „Europe-only"-Lösung entspricht.

Die Aufdeckung staatlicher Überwachungsmaßnahmen durch Edward Snowden hat die Besorgnisse in der Bevölkerung hinsichtlich des Datenschutzes deutlich verstärkt und über zehn Jahre hinweg zu einer Flut von Datenschutzvorschriften geführt.

Der internationale Datentransfer ist rechtlich unsicher und wird von den Verbrauchern misstrauisch beäugt. Daher suchen Unternehmen nach Cybersicherheitslösungen, die solche Datentransfers über Rechtsräume hinweg minimieren oder ganz vermeiden.

Inzwischen bieten viele Firmen MDR-Lösungen speziell für den europäischen Markt an. Aber herauszufinden, welche davon am besten geeignet sind, ist keine leichte Übung. Was sind die Vor- und Nachteile der einzelnen Lösungsvarianten? Und wie kann ich beurteilen, ob die Anbieter ihre Versprechen einhalten?

Antworten auf diese Fragen finden Sie auf den folgenden Seiten.

Mit einem Schlag wach!

Edward Snowdens Coup

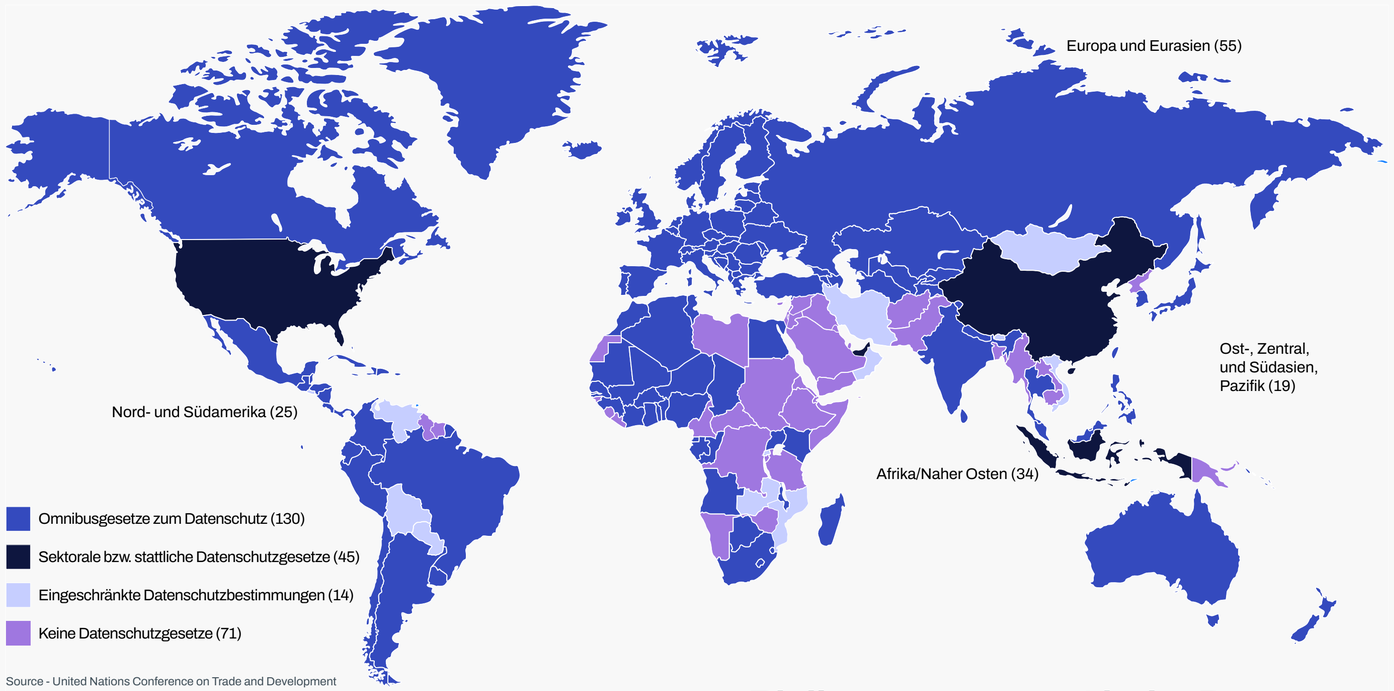
An jenem lauen Abend zog Edward Snowden den USB-Stick heraus, fuhr seinen Laptop herunter und machte sich auf den Weg. Die Aktion, die seine Karriere bei der National Security Agency (NSA) der USA beendete, entfachte eine weltweite Diskussion über Datenhoheit und Sicherheit. Snowden hatte als Angestellter der NSA direkten Zugang zu deren Servern am Hauptsitz in Ft. Meade, Maryland, etwa 5.000 Meilen entfernt.

Snowden, zunehmend besorgt, wie die Überwachungstätigkeit westlicher Geheimdienste die Privatsphäre der Menschen beeinträchtig, wurde 2013 zum weltweit bekanntesten Whistleblower, als er hunderttausende von der NSA und anderen westlichen Geheimdiensten gesammelte Dateien an Journalisten weitergab.

Die Reaktionen der Staatenwelt

Datenschutz ist global und national ein immer zentraleres politisches Thema. Per Datenschutzgesetze kontrollieren inwischen einige Regierungen Datenverarbeitung und -speicherung.

Die chinesische Cyberspace-Verwaltung CAC etwa – und nicht nur sie – hält Daten für "wertvoller als Öl"[1].



Source - United Nations Conference on Trade and Development

Datenschutzvorschriften schießen wie Pilze aus dem Boden, da die Staaten versuchen, die Verarbeitung von Daten ihrer Bürger zu kontrollieren. Die UNO zählt 242 Datenschutzgesetze in der ganzen Welt[2]. 80 % der Länder haben Datenschutzgesetze formuliert oder beschlossen (siehe Karte).

In Europa wurde die Datenschutzgrundverordnung (DSGVO) im Jahr 2016 von den EU-Mitgliedstaaten verabschiedet. Die DSGVO enthält Sicherheitspflichten für Organisationen, die personenbezogene Daten verarbeiten.

Risikomanagement beim Datentransfer

Die meisten Datenschutzbeauftragten bezeichnen die Einhaltung der Bestimmungen zum grenzüberschreitenden Datentransfer als schwierigste Aufgabe[3]. Die Gesetze sind kompliziert, teils unklar und ändern sich mitunter.

Für große Unternehmen ist auch die Risikobewertung von Datentransfer-Vereinbarungen mit Partnern mühsam, weshalb einige in der EU bereits internationale Datentransfers ausschließen. Die Zentralbanken mancher EU-Staaten verbieten z. B. die Übermittlung ihrer Daten außerhalb der EU und verpflichten ihre wichtigsten Zulieferer (Geschäftsbanken und Anwaltskanzleien) ebenfalls dazu.

An wen richtet sich diese Broschüre?

Die folgenden Informationen richten sich an Experten für Cybersicherheit, die einen Managed Detection and Response (MDR)-Dienst suchen, der mit einer Europe-only-Sicherheitspolitik zu vereinbaren ist. Käufer von MSS-Diensten erhalten eine Orientierungshilfe im Dickicht der Datenschutzvorschriften, so dass sie besser verstehen, worum es geht:

- Was bedeutet Datenhoheit?
- Warum ist Datenschutz so wichtig?
- Wodurch wird die Entwicklung im Bereich der Datenschutz bestimmt?
- Was bedeutet das zukünftig für den internationalen Datentransfer?
- Wie lassen sich Lösungen für eine Europe-only-Cyber-sicherheit entwickeln?
- Wie reagiert WithSecure™ auf diese Herausforderungen?
- Welche Fragen sollten Sie Anbietern stellen, um die Einschränkungen speziell auf Europa zugeschnittener MSS-Lösungen besser zu erkennen?

Was bedeutet Datenhoheit?

"Unternehmen entwerfen, produzieren, verkaufen und unterhalten das digitale Ökosystem, und die Staaten sind von diesen Firmen abhängig. Aber Staaten haben die Macht, den digitalen Sektor zu regulieren". [4]

Datenhoheit ist die rechtliche Verfügungsbefugnis über Daten – insbesondere personenbezogene Daten – derjenigen, die „Inhaber“ der jeweiligen Informationen sind. Die Speicherung und Verarbeitung der Daten bedarf grundsätzlich der Zustimmung der natürlichen oder juristischen Person, die über die Datenhoheit verfügt. Datenhoheit hängt eng mit der Datenresidenz (Speicherort) und der Datenlokalisierung (wo die Daten verbleiben müssen) zusammen.

Der Datenschutz wird definiert durch die Datenschutzvorschriften, die für die personenbezogenen Daten im Besitz einer Organisation und ihrer Lieferanten gelten, einschließlich der Bedingungen, unter denen Dritte auf die Daten zugreifen dürfen.

10 Jahre europäisches Datenschutz-Drama

Das EuGH-Urteil Schrems I

Snowden war quasi der Sputnik, der weltweit eine Art Apollo-Mission für Datenhoheit auslöste: Überall begannen Regierungen zu diesem Zweck mit neuen Regulierungen.

Im Zuge der Snowden-Affäre klagte der Datenschutzaktivist Max Schrems gegen den irischen Data Protection Comissioner. Kern der Auseinandersetzung war die Frage, ob das Safe-Harbor-Abkommen zwischen den USA und der EU seine Datenschutzrechte ausreichend schützt. Der Europäische Gerichtshof (EuGH) erklärte 2015 in der "Schrems I"-Entscheidung das Abkommenr für ungültig und rechtswidrig.

Das EuGH-Urteil Schrems II

Safe Harbor wurde durch "Privacy Shield“ ersetzt, das aber 2020 wiederum vom EuGH verworfen wurde ("Schrems II").

Seitdem rätseln Organisationen, wie sie denn nun ohne rechtliche Risiken personenbezogene Daten in Länder außerhalb der EU transferieren sollen. Wenn sie z. B. Cloud-Services nutzen, müssen sie jetzt die Datenschutzgesetze des Landes, das die Cloud-Services bereitstellt, bewerten, Datenschutzrisiken dokumentieren und diese ihren Kunden mitteilen.

Der aktuelle Umgang mit der Rechtsunsicherheit

Über ein Drittel der befragten Datenschutzbeauftragten gab in einer Umfrage von 2021 an, dass ihre Unternehmen die Vorschriften der DSGVO zur Datenübertragung nicht einhalten. 10 % sagten, dass ihr Unternehmen nach "Schrems II" beschlossen hat, Daten zu lokalisieren, den Transfer zu stoppen oder damit verbundene Dienste auszusetzen.[5]

Privacy Shield 2.0

Jüngste Äußerungen von EU- und US-Verantwortlichen Ende 2021 haben Hoffnungen geweckt, dass die Verabschiedung eines neuen Abkommens (Privacy Shield 2.0) unmittelbar bevorsteht, aber die Fortschritte bei diesem Prozess vollziehen sich eher in geologischen Zeiträumen.

Obwohl die Kommmission überarbeitete Standardvertragsklauseln (SCC) herausgegeben hat, die mehr Klarheit über ausreichende Sicherheiten beim Transfer personenbezogener Daten schaffen, bleibt ohne den Ersatz für Privacy Shield eine erhebliche Rechtsunsicherheit.

Die Forderungen in der Bevölkerung nach mehr Datenschutz werden lauter

Die Kunden nehmen den Umgang mit ihren persönlichen Daten zunehmend ernst. Studien zeigen ein wachsendes Gefühl des Kontrollverlusts bezüglich der eigenen Daten und der Möglichkeiten, Unternehmen am Horten dieser Informatione zu hindern[6].

In einer demnächst erscheinenden WithSecure™-Studie, an der 2.000 europäische Unternehmen und 1.000 aus Nordamerika und Japan teilnahmen, fordern 40 %, dass die Daten aus ihrem Unternehmen im Herkunftsland verarbeitet werden. 13 % der leitenden Angestellten der befragten Unternehmen wünschen sich zudem einen europäischen Anbieter.

Regulierungsbehörden in der ganzen Welt haben erkannt, dass der E-Commerce sein volles Potenzial nicht ausschöpfen kann, wenn die wachsenden Bedenken der Verbraucher hinsichtlich des Online-Datenschutzes nicht beachtet werden[7].

Der Datenschutz im europäischen Recht

Die Datenschutzgrundverordnung (DSGVO) regelt den Datenschutz und den Schutz der Privatsphäre in der EU und im Europäischen Wirtschaftsraum (EWR). Erklärtes Ziel der DSGVO sind die Stärkung der Kontrolle und der Rechte des Einzelnen über seine personenbezogenen Daten sowie die Vereinfachung des regulatorischen Umfelds für internationale Unternehmen. Sie befasst sich auch mit dem Transfer personenbezogener Daten in Gebiete außerhalb der EU und des EWR.

Die DSGVO verpflichtet Unternehmen, sich bei der Verarbeitung personenbezogener Daten von Individuen in der EU an die Verordnung zu halten – unabhängig vom Standort des Unternehmens. Die DSGVO gilt als weltweit strengste Datenschutzregelung. Viele hoffen, dass sie auch für andere Rechtsordnungen "Goldstandard" wird.

Die EU attestiert nur 14 anderen Ländern, darunter dem Vereinigten Königreich, Argentinien, Kanada, Israel, Neuseeland, der Schweiz und Uruguay, vergleichbare Datenschutzgesetze und damit die Erfüllung ihrer Anforderungen an die Konformität.

MDR-Optionen speziell für Europa

Ein Europe-only- und DSGVO-konformer MDR-Service lässt sich in abgestufter Weise von außereuropäischen Infrastrukturen und Diensten trennen:

- Trennung von Speichern
- Operative Trennung auf Basis der getrennten Speicherung
- Vollständige Trennung auf Basis der Trennung von Betrieb und Speicherung

Trennung von Speichern (Option 1)

Grundbedingung für Europa-only-Services ist die Verwaltung der vom MSSP erfassten Daten in einem Rechenzentrum in Europa.

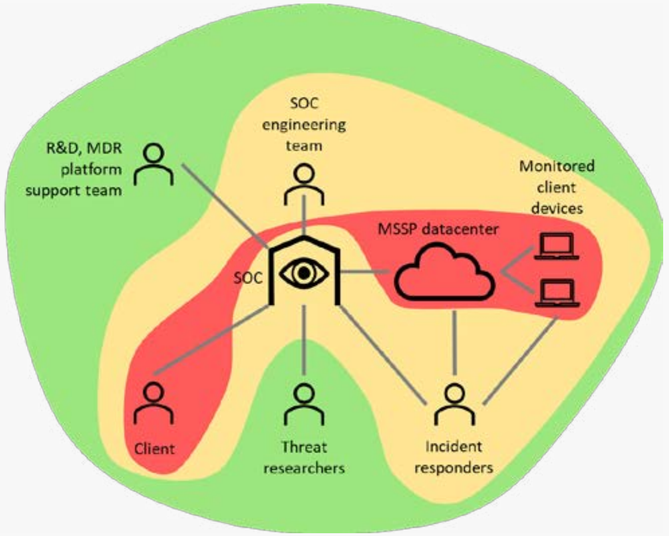
Operative Trennung (Option 2)

Security Operations Centres (SOC) sind der Kern eines Managed Detection and Response (MDR)-Dienstes. MSSPs bieten meist einen permanenten Service mit SOCs in verschiedenen Teilen der Welt, die ein Follow-the-Sun-Modell ermöglichen. MSSPs mit Europe-only-Services betreiben rund um die Uhr regionale SOCs mit SOC-Engineering-Teams und Incident Respondern in Europa. Operative Trennung verringert das Risiko, dass sensible Daten an Stellen außerhalb Europas gelangen, die eventuell nicht unter Kontrolle des MSSP stehen.

Vollständige Trennung (Option 3)

Vollständige Trennung beseitigt das Risiko, dass sensible Daten für Stellen außerhalb Europas zugänglich sind. Dies wird durch die Bereitstellung des MDR-Dienstes über eine eigene Plattform erreicht, die von MSSP-eigenen Ingenieuren entwickelt und gewartet wird, die innerhalb Europas arbeiten.

MSSPs, die Technologien von Drittanbietern für die Bereitstellung eines MDR-Dienstes nutzen, haben weniger Kontrolle über Support-Techniker, die eventuell von außerhalb Europas aus tätig sind.



Die 3 Optionen sind in der Abbildung und der dazugehörigen Tabelle unten dargestellt.

Option		Bezeichnung	Speicher	SOC D&R-Team	SOC Engineeringteam	Incident Responder	Threat Hunter	R&D, MDR-Plattform Supportteam
1		Speicher-Trennung	✓					
2		Operative Trennung	✓	✓	✓	✓		
3		Vollständige Trennung	✓	✓	✓	✓	✓	✓

Entscheidungskriterien für Ihre Option

Die Tabelle zeigt Vor- und Nachteile der drei Optionen:

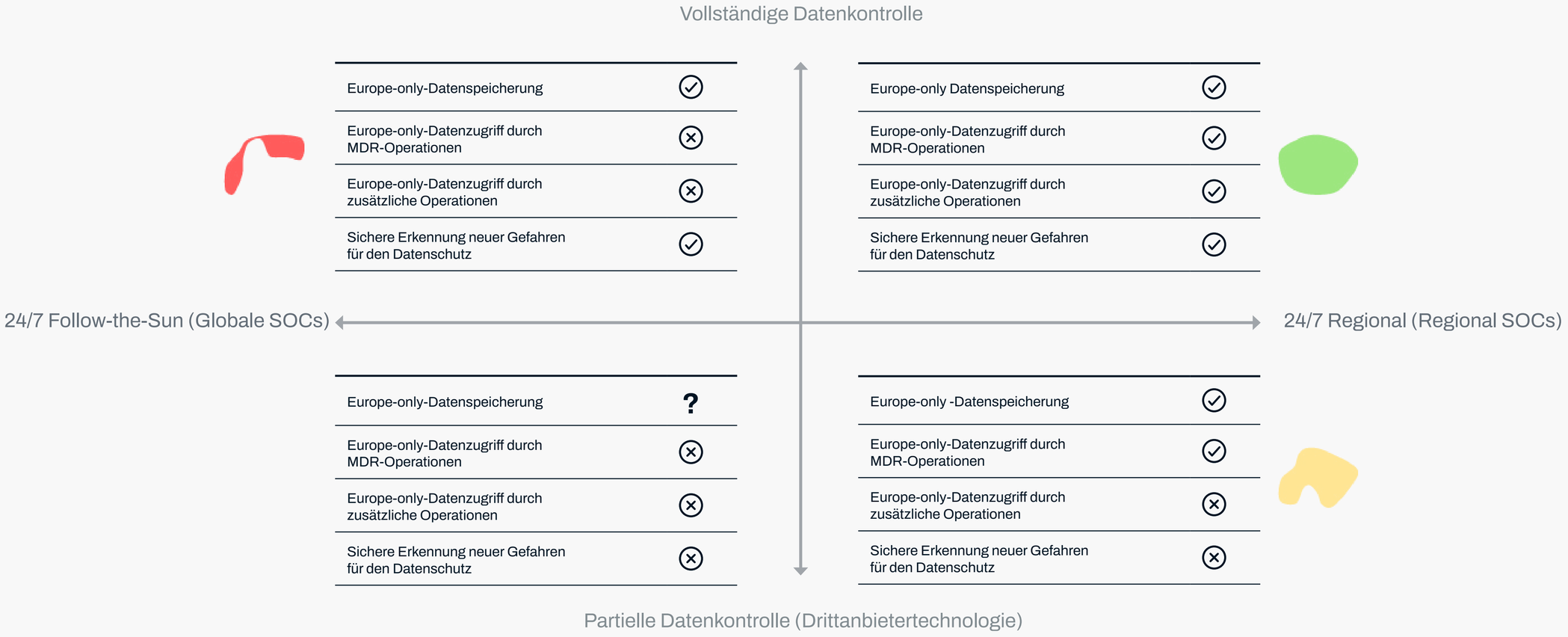
	Bezeichnung	Eigenschaften	Vorteile	Nachteile
1	Speicher-Trennung	Europe-only-Datenspeicher	• Gängige Marktlösung • Mögliche Flexibilität bei der Frage des Speicherorts in Europa	• Nicht geeignet für Kunden, die den Zugriff außerhalb Europas kontrollieren wollen
2	Operative Trennung	Europe-only-Speicherung und -Zugriff für MDR-Operationen	• Noch weniger Risiko eines Datenzugriffs für den Kunden durch Nutzung von MDR • Eventuell preiswerter als Option 3.	• Ausnahmen durch Einsatz von Technologien von Dritten durch den Anbieter können die Bedingungen für den Datenzugriff aushebeln.
3	Vollständige Trennung	Europe-only-Speicherung, Zugang für MDR- und zusätzliche Operationen	• Das Risiko eines Datenzugriffs wird für den Kunden bei der Verwendung von MDR vollständig reduziert.	• Eventuell teurer als die operative Trennung

Welche Option für Sie am besten geeignet ist, hängt davon ab, wie hoch Sie das Risiko für die Vertraulichkeit Ihrer Daten einschätzen, da Sie selbst bestimmen können, wer auf Ihre Daten zugreifen darf.

Bei der Auswahl einer Lösung müssen Sie drei Fragen berücksichtigen:

1. **Wo soll der MSSP Ihre Daten speichern?** Müssen die an den MSSP gelieferten Daten vollständig in Europa gehostet werden? – Dann brauchen Sie einen Europe-only-Service.
2. **Wo soll die Sicherheitseinrichtung ansässig sein?** Ein "Follow-the-sun"-Modell erfordert 24/7-Zugriffs-möglichkeiten des Betriebspersonals auf Ihre Daten.
3. **Wer soll zusätzliche Operationen durchführen** – etwa Entwicklung und Wartung der Plattform, Patching und Bedrohungsforschung? MSS basieren häufig auf Drittanbietertechnologie , die von Zulieferern entwickelt und gewartet werden. MSSPs mit eigener Technologie haben deutlich mehr Kontrolle über:
   - die Techniker, die auf Ihre Daten zugreifen könnten;
   - die Roadmap für die MSS-Entwicklung.

Organisationen mit höchsten Sicherheitsanforderungen werden Dienste bevorzugen, die innerhalb eines einzigen Rechtsraums erbracht werden: regional angesiedelte Security Operations Centers (SOCs), die eigene, von ihnen kontrollierte Technologieplattformen betreiben, wie unten dargestellt.



Unsere Lösung

Der Europe-only MDR-Dienst von WithSecure bietet die vollständige Trennung von Speicherung, Betrieb und zusätzlichen Leistungen (Option 3).

Countercept arbeitet mit der Erfassung verschiedener Datentypen:

- **Endpoint Detection and Response (EDR) Daten** von Endgeräten der Kunden, d. h. von den Workstations und Servern, die zum Unternehmen gehören
- **Log-Ereignisse** von Sicherheitsvorrichtungen des Kunden, z. B. Proxys und VPN-Servern
- **Audit-Ereignisse** von Microsoft 365-Kunden (früher bekannt als Office 365)
- **Konfigurations-Details und Metadaten** von AWS-Kundenkonten und Azure-Abonnements

Alle Countercept MDR-Daten werden in der AWS-Region Irland (eu-west-1) gespeichert. Wir haben uns für AWS entschieden, weil deren vertragliche Zusagen über die Vorgaben des Schrems-II-Urteils hinausgehen. AWS wird Strafverfolgungsanfragen nach Kundendaten von Regierungsstellen innerhalb oder außerhalb des EWR widersprechen bzw. im Falle einer rechtskräftigen Aufforderung zur Offenlegung von Kundendaten nur das erforderliche Minimum offenlegen.[8]

Diese Fragen sollten MSSPs Ihnen beantworten

Es gibt mehr MDR-Anbieter als Eissorten in einer gutsortierten italienischen Gelateria. Manche Anbieter behaupten zwar, einen Europe-only MDR-Dienst bereitzustellen, aber Gewissheit, welche Art von Dienst das tatsächlich ist, werden Sie erst mit diesen 12 Fragen erlangen:

1. **Wie kategorisieren Sie die Daten?**
2. **Wo werden sensible Daten generiert und gespeichert?**
3. **Wem gehören die Rechenzentren, in denen sensible Daten gespeichert sind?**
4. **Wie belegen Ihre Cloud-Partner die Erfüllung aller Ihrer lokalen und globalen Datenschutzanforderungen in ihren Rechenzentren?**
5. **Wie sehen Ihre Back-up-Verfahren aus? Wo werden Ihre Daten gesichert? Welche lokalen Vorschriften gibt es für die Sicherheit oder Verschlüsselung dieser Daten?**
6. **Wie bieten Sie einen 24/7-Service an? Führen Sie Sicherheitsoperationen nur innerhalb Europas durch?**
7. **Auf welchen Technologien basiert der MDR-Dienst?**
8. **Wer betreibt die MDR-Serviceplattform und wie kontrollieren Sie den Zugriff?**
9. **Wie werden Forschung und Entwicklung von Entdeckungen durchgeführt? Wo sind die Verantwortlichen angestellt? Sind sie in der EU ansässig?**
10. **Wo befindet sich Ihr Threat Intelligence Team? Wie kontrollieren Sie den Zugriff Ihres Threat Intelligence-Teams auf sensible Daten?**
11. **Wer stellt die Incident-Response-Services bereit und wo befinden sich diese Ressourcen?**
12. **Können Sie beschreiben, wie Sie versehentliche oder weitergehende Zugriffe auf sensible Informationen kontrollieren?**

Zur weiteren Information empfohlen

Für diese Broschüre wurden zahlreiche Forschungsarbeiten und Berichte gelesen. Die nachstehenden empfehlen wir besonders:

- The Snowden Files von Luke Harding, einem angesehenen Journalisten (https://www.goodreads.com/book/show/20661548-the-snowden-files).

- Die von der International Association of Privacy Professionals (IAPP) und EY gemeinsam durchgeführte Umfrage unter Datenschutzfachleuten für das Jahr 2021 bietet einen guten Einblick in die Herausforderungen bei der Einhaltung der sich weiterentwickelnden Vorschriften (https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf).

- Fieldfisher veröffentlichte im Januar 2022 einige wertvolle Einblicke in die Zukunft des Datentransfers (https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/what-future-for-the-transfers-of-personal-data).

- Die International Association of Privacy Professionals (IAPP) hat eine detaillierte Übersicht über die Datenschutzgesetze weltweit erstellt (https://iapp.org/media/pdf/resource_center/global_comprehensive_privacy_law_mapping.pdf).

- Das UK Information Commissioner's Office stellt eine Checkliste zur Verfügung, die Käufer von Managed Security Services zur Bewertung der Sicherheit eines MSP verwenden können (https://ico.org.uk/for-organizations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/).

Quellen

[1]https://www.controlrisks.com/campaigns/china-business/chinas-cyber-security-law

[2]https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[3]https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

[4]Luciano Floridi, Professor of Philosophy and Ethics of Information at the University of Oxford. (https://www.hinrichfoundation.com/research/article/digital/data-is-disruptive-how-data-sovereignty-is-challenging-data-governance/)

[5]https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

[6]https://dma.org.uk/uploads/misc/5a857c4fdf846-data-privacy---what-the-consumer-really-thinks-final_5a857c4fdf799.pdf

[7]https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

[8]https://d1.awsstatic.com/Supplementary_Addendum_to_the_AWS_GDPR_DPA.pdf

[9]https://www.withsecure.com/en/about-us/legal/privacy

Über WithSecure™

WithSecure™, ehemals F-Secure Business, 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™ Corporation wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd. gelistet.

WITH secure