إقامة البيانات

منظورات سياسة AWS

نوفمبر 2019

[منظورات السياسة]

الإشعارات

العملاء مسؤولون عن إجراء تقييم مستقل خاص بهم للمعلومات الواردة في هذه الوثيقة. هذه الوثيقة: (أ) هي لأغراض تقديم المعلومات فقط، (ب) وتمثل عروض وممارسات منتجات AWS الحالية، والتي تخضع للتغيير دون إشعار، (ج) ولا تنشئ أيّ التزامات أو ضمانات من AWS والشركات التابعة لها أو الموردين أو المرخصين الخاصين بها. تُقدَّم منتجات AWS وخدماتها "كما هي" دون ضمانات أو تعهدات أو شروط من أيّ نوع، سواء صريحة أو ضمنية. وتحكم اتفاقية AWS مسؤوليات AWS والتزاماتها نحو عملائها، وهذه الوثيقة لا تمثل جزءًا من أيّ اتفاقية مبرمة بين AWS وعملائها، كما لا تمثل تعديلاً لها.

المحتويات

مقدمة

لا تزال مؤسسات القطاع العام، في بيئة الحوسبة المعقدة في هذه الأيام، تراودها مخاوف مشروعة بشأنأمن بياناتهم. ونتيجة لذلك، حددت بعض الحكومات أن تكليف إقامة البيانات
– المتطلب بأن يبقى كامل محتوى العميل، المخزن والمعالج في نظام تكنولوجيا المعلومات، ضمن حدود دولة معينة - مما يقدم طبقة إضافية من الأمن. يعكس إقامة البيانات مجموعة من المسائل المرتبطة في المقام الأول بالمخاطر الأمنية المتصورة (والحقيقية، في بعض الحالات) حول استخدام طرف ثالث للبيانات، بما في ذلك هيئات إنفاذ القانون الأجنبية. ويرغب عملاء القطاع العام في التأكد من أن بياناتهم محمية من الاستخدام غير المرغوب فيه، ليس فقط من المهاجمين العدوانيين، ولكن أيضا من الحكومات الأخرى.

يحد موضع إقامة البيانات الصارم في بعض الأحيان من استخدام مقدمي الخدمات السحابية ذوي النطاق الواسع ومتعددي الجنسيات (CSP)، وغالبا ما يطلق عليهم مصطلح مزودي الخدمات السحابية "الفائقة". وقد أسهمت الشواغل العامة المتعلقة بالأمن السبراني، وكذلك الشواغل المتعلقة بالتجاوز المحتمل من الكيانات السيادية، في استمرار التصور بضرورة الإبقاء على فئات معينة من البيانات داخل البلاد. ومع ذلك، فإن مثل هذه التصورات تؤدي إلى نتائج عكسية بالنسبة لهدف التأمين الفعَّال لبيانات القطاع العام. وكما هو موضح أدناه، فإن مزود الخدمات السحابية ذات النطاق الفائق، الذي قد يمتلك أصول بنية تحتية موجودة في بلد مختلف عن المكان الذي يوجد فيه كيان تابع للقطاع العام، يقدم لقاعدة العملاء الخاصة به القدرة على تحقيق مستويات عالية من حماية البيانات من خلال حماية النظام الأساسي الخاص به وباستخدام الأدوات الجاهزة للتشغيل لعملائه. وبالتالي، فإن ممارسات الإدارة السحابية والهيكلية القويان تبددان المخاوف التي تدفع العملاء إلى النظر في قيود إقامة البيانات.

تمثل الخدمات السحابية الفائقة عائقًا تحوليًا في التكنولوجيا بسبب الدرجة العالية من الكفاءة والتحكم والابتكار لتوفير أمن عالمي المستوى لدعم عملائها. ويعمل مزودو الخدمات السحابية الفائقة على تصميم وتشغيل وصيانة المنتجات لتمكين العملاء عبر قطاعات متعددة (تجارية، عامة، منظمة) من معالجة بعض نقاط الضعف والمخاطر الأمنية الأكثر شيوعًا. ويعتمد العملاء على منتجات مزود الخدمات السحابية الفائقة لتطبيق الممارسات الأمنية الديناميكية وسريعة الاستجابة للتهديدات الفورية، مما يحسن بشكل كبير الوضع الأمني لكل عميل. يتمتع مزودو الخدمات السحابية، لا سيما مزودو الخدمات السحابية الذين يعملون على أساس الدفع أولاً بأول، بجميع الحوافز المناسبة للحفاظ على الأمن السبراني على مستوى عالمي، حيث إنهم سيواجهون عواقب كبيرة طويلة الأجل - بما في ذلك التأثيرات المرتبطة بتعرض النظام للمخاطر، وفقدان ثقة العملاء، والضرر بالعلامة التجارية. وبعبارة أخرى، فإن الأمن الأفضل هو شيء إلزامي لنجاح مزود الخدمات السحابية الفائقة، ويجب دمج الأمن بشكل كامل في تصميم الخدمات السحابية الفائقة وتطويرها وعملياتها.

تتناول هذه الوثيقة ما يلي:

- إزالة المخاطر الأمنية المتصورة التي تُعرب عنها الحكومات عندما تطلب إقامة البيانات داخل البلاد.
- الآثار السلبية على صناعات القطاعين التجاري والعام والصناعات التكنولوجية بشكل عام الناشئة عن سياسات إقامة البيانات داخل البلاد التي تسري على البيانات الحكومية.
- اعتبارات يتعين على الحكومات تقييمها قبل إنفاذ المتطلبات التي من الممكن أن تحد عن غير قصد من أهداف التحول الرقمي للقطاع العام، مما يؤدي إلى زيادة مخاطر الأمن السبراني.

لماذا لا تقدم إقامة البيانات أمنًا أفضل؟

أصبحت ملكية البيانات وموضعها الجغرافي موضوعًا رئيسيًا لمبادرات السياسات السحابية والأمن السبراني في جميع أنحاء العالم. ومن الناحية التاريخية، كانت السيطرة والتحكم في بيانات المؤسسة الحساسة تعني تخزين المعلومات محليًا في أماكن العمل أو في مرافق يُمكن الوصول إلى موقعها المادي فعليًا ويملكها المقاولون داخل البلاد. وجود ملكية كاملة "للمجموعة"، من أرضية المبنى والجدران إلى البرنامج على الخوادم، جعل الناس يشعرون بالارتياح لأن بياناتهم كانت آمنة قدر الإمكان. ولا يزال هذا الأساس المنطقي قائمًا بالنسبة للعديد من الحكومات.

ومع تطور التكنولوجيا، أدت ثلاثة حقائق أساسية إلى تعطيل النموذج التقليدي "للتحكم الكامل في الحزم":

> بغض النظر عن الموقع المادي، إذا كانت أنظمة تكنولوجيا المعلومات متصلة بأيّ شكل من الأشكال بالإنترنت (أو غيرها من الشبكات متعددة الأطراف)، حتى بشكل غير مباشر، فإنها معرضة لخطر كبير.

1. **معظم نقاط الضعف الأمنية يتم استغلالها عن بعد.**
فالموقع المادي للبيانات ليس له تأثير يذكر على التهديدات التي تنتشر عبر الإنترنت.
الأنظمة المتصلة عبر الإنترنت تُعرّض المنظمة إلى حجم كبير من التهديدات، وكلها تنتشر من أيّ مكان. فعلى سبيل المثال، أثرت برامج فدية Petya الأخيرة على خدمات الرعاية الصحية، مما أضعف عملياتها وقدرتها على تنفيذ رعاية المرضى. وكان ذلك نتيجة البرامج الخبيثة التي تؤثر على مراكز البيانات المحلية الخاصة بهم المنتشرة عبر الإنترنت. وعلى الرغم من الجهد الهائل الذي بُذل لتأمين النظم المترابطة عبر الجدران النارية و غيرها من الأجهزة المضادة للتدخل، فقد أظهرت التجربة أن الأمن المحيطي يمثل جزءًا صغيرًا جدًا من نظام محمي.
وبغض النظر عن الموقع المادي إذا كانت أنظمة تكنولوجيا المعلومات متصلة بأيّ شكل من الأشكال بالإنترنت (أو غيرها من الشبكات متعددة الأطراف)، حتى بشكل غير مباشر، فإنها معرضة للخطر وعرضة لمجموعة كبيرة من تهديدات الاستخدام المنطقي.

2. **المعالجات اليدوية تشكل خطر حدوث الخطأ البشري.** يلعب فشل العملية البشرية دورًا في السبب الأساسي للفشل (إن لم يكن هو السبب بأكمله) لمعظم أحداث الأمن السبراني. ومثال شائع لذلك هو الفشل في تصحيح الأنظمة الضعيفة مع تحديثات البرامج المنشورة لعدة أشهر قبل الاستغلال.
المعالجات اليدوية
لتحديث الأنظمة مع أحدث التصحيحات هي أمر صعب وليس من الممكن القيام بها بانتظام دون أتمتة.

3. **التهديدات الداخلية تسود باعتبارها خطر كبير.** لقد حدثت الغالبية العظمى من تعرضات البيانات للمخاطر الكبيرة إما من خلال أخطاء غير مقصودة أو سلوك ضار متعمد من قبل أفراد يستخدمون حسابات مصرح بها جعلت من الممكن استغلال البيانات. وتعزى الانتهاكات رفيعة المستوى التي شهدتها السنوات القليلة الماضية إلى سوء ممارسات الصحة السبرانية. تشمل سيناريوهات التهديدات الأكثر شيوعًا من الحساب المصرح به ما يلي:

- غير متعمد: فقدان بيانات الاعتماد أو سوء إدارتها بحيث يمكن للمهاجم العمل داخل النظام كمستخدم صالح.
- الهندسة الاجتماعية: هجمات التصيد الاحتيالي وهجمات الهندسة الاجتماعية التي تخدع المستخدمين أو المسؤولين في الكشف عن بيانات الاعتماد للمهاجمين.
- خبيثة: التهديد المطلع التقليدي — الجهات أصحاب الفعل السيء من داخل المنظمة مع نية عدوانية.

الموقع المادي للبيانات لا يؤثر على أيٍّ من الحقائق المذكورة أعلاه.

وفي هذه الأيام، تُعتبر إدارة المخاطر مهمة أكثر صعوبة عند النظر في التكنولوجيا المحمولة والعلاقات المتبادلة بين الكيانات الخارجية والداخلية. وأيّ هيكلية للنظام تفتقر إلى أوجه الحماية الأمنية المناسبة تمثل ناقلاً موثوقاً لمسار الهجوم، بغض النظر عن الموقع المادي للبنية التحتية أو النظام. ومع استمرار تطور التكنولوجيا وتغيير نقاط الضعف التي تهدد العملاء وناقلاتها، يجب على الحكومات أن تعيد تقييم الكيفية التي تصمم بها استراتيجياتها وتحملها للمخاطر. أظهرت الأمثلة الواقعية
أن تخزين البيانات على الخوادم الخاصة بك أو في مركز البيانات الخاص بك في بلدك، لا يُمثل بأيّ حال من الأحوال أساسًا كافيًا لتأمين البيانات.

فعلى سبيل المثال، حدث خرق رفيع المستوى لوكالة حكومية في الولايات المتحدة يؤثر على أكثر من 20 مليون موظف اتحادي في بيئة عمل محليّة نتيجة لاختراق بيانات اعتماد المستخدمين. وتم اختراق بيانات الاعتماد هذه واستخدامها عبر الإنترنت من مواقع مختلفة - تجاوز جميع أشكال الحماية التي تقدمها بيئة العمل المحلية. فخرق الوكالة الحكومية في الولايات المتحدة مثال جيد على التهديدات التي تنبعث عبر الإنترنت بغض النظر عن موقع البيانات أو الحدود الجغرافية.

تنطبق هذه المسألة على أكثر من مجرد أنظمة على واجهة الإنترنت. توفر الأنظمة التي لا تحتوي على اتصال مباشر بالإنترنت للمستخدمين إمكانية الوصول عبر اتصالات الشبكة الخاصة الظاهرية (VPN) من أجهزة الكمبيوتر المحمولة أو أجهزة الكمبيوتر المنزلية أو أجهزة الهاتف المحمولة. ولا تتطلب الخروقات الوصول المادي إلى خادم، ولكن بدلاً من ذلك استغلال
عدم فعَّالية ضوابط الأمن المنطقية المنفذة. وهذا يدل على أن متطلبات أماكن إقامة البيانات ليس لها أهمية تذكر
لحماية المعلومات من التهديدات الأكثر انتشارًا في هذه الأيام. وبالتالي، فإن متطلبات الموقع الجغرافي ليس لها أهمية تذكر لحماية المعلومات من التهديدات في هذه الأيام. وبدلاً من ذلك، فإن أفضل آليات الحماية والكشف والاستجابة والاسترداد هي استخدام الأمن التحويلي الذي يقدمه مزود الخدمات السحابية الفائقة من خلال التحديث والأتمتة.
يستثمر مزودو الخدمات السحابية الفائقة، مثل AWS، في أفضل الممارسات الأمنية التقنية والتشغيلية، ويطبقون هذه الممارسات، لأنها أساسية لعملياتهم ومنتجاتهم. ويستفيد العملاء عندما يستخدمون مزود خدمات سحابية، مثل الخدمات السحابية والبنية التحتية لـ AWS.

توصل كل من جارتنر[1] وIDC[2]، وهما منظمات أبحاث رائدة في مجال تقنية المعلومات، إلى أن الوضع الأمني لمقدّمي الخدمات السحابية الرائدين مساوٍ لأفضل مراكز بيانات المؤسسات أو أفضل منها، وأنه لا ينبغي اعتبار الأمن بعد الآن المانع الأساسي لاعتماد الخدمات السحابية. وفي الواقع، فإن الشركات تستفيد بشكل حقيقي من الأمن المتأصل في السحابة.

---

1 http://www.gartner.com/smarterwithgartner/is-the-cloud-secure

2 بيت لينداستروم: «تقدير الخطر: نعم قد تكون السحابة أكثر أمنا من محيط الموقع المحلي» شركة البيانات الدولية (يوليو 2015).

لماذا لا تؤثر السحابة على خطر الاستخدام القسري؟

بالنسبة لبعض الحكومات، تهدف متطلبات أماكن إقامة البيانات إلى التخفيف من المخاطر المتعلقة بإمكانية وصول كيان آخر إلى بياناتها. ويهدف هذا القسم إلى تناول الخطر المتصور المتمثل في قدرة الكيان على "قسر استخدام" بيانات الكيان السيادي عندما يتم تخزين تلك البيانات في بيئة مزود الخدمات السحابية الفائقة. ويشير مفهوم "الإفصاح القسري" أو "الاستخدام القسري" إلى حقوق استخدام البيانات من جانب الحكومات أو وكلائها بموجب القوانين واللوائح على المستوى الوطني ومستوى الأقاليم ومستوى القطاعات في أيّ بلد معين. ويتمثل القلق المتصور في أن الإفصاح القسري قد يترك مالك البيانات غير قادر على منع استخدام بياناته من قبل كيان سيادي يزعم تنفيذ القانون المعمول به. ومع ذلك، فإن الاستخدام القانوني للبيانات بدولة ذات سيادة ليس مسألة خاصة بالسحابة.

فامتلاك النظام المادي، إما مباشرة أو من خلال عقد استعانة بمصادر خارجية، لا يقلل من خطر الوصول القسري، لأن هناك بالفعل آليات قانونية أخرى توفر للحكومات في ولاية قضائية الوسائل اللازمة لطلب استخدام البيانات المخزنة في ولاية قضائية أخرى. فعلى سبيل المثال، وُضعت معاهدة المساعدة القانونية المتبادلة (MLATs)[3] والإنابة القضائية[4] لتنظيم طلبات دولة ذات سيادة للحصول على البيانات قبل ظهور تكنولوجيا السحابة بوقت طويل.

وبالمقارنة مع البيئة المحلية التقليدية، يجب أن يتغلب إنفاذ القانون عمومًا على المزيد من الحواجز عند محاولة إجبار مزود الخدمات السحابية على الكشف عن بيانات عميل آخر. ولا يمكن لإنفاذ القانون البحث في البيانات المخزنة في خوادم مزود الخدمات السحابية، أو الاستيلاء عليها، دون الامتثال للأطر القانونية التي تدعم مجموعة مستهدفة ضيقة النطاق من
أغراض إنفاذ القانون. وعلاوة على ذلك، يمكن أن يطعن مقدمو الخدمات السحابية في الطلبات التي تكون واسعة النطاق أكثر من المطلوب، أو تتجاوز سلطة الجهة الطالبة، أولا تمتثل تمامًا للقانون المعمول به.

والأهم من ذلك، فإن مزود الخدمات السحابية، مثل AWS ملتزم بالكامل بتقديم إشعار طلبات البيانات للعملاء ذوي الصلة، مما يتيح للعميل التعامل مع السلطات و/أو اتخاذ المزيد من الإجراءات المناسبة لمنع الكشف غير السليم عن بياناته. ومن المهم الاعتراف بأن هذا التحدي المعقد لا يقتصر على حكومة الولايات المتحدة أو الشركات التي يوجد مقرها في الولايات المتحدة، لأن أيّ شركة متعددة الجنسيات تخضع للقوانين واللوائح المعمول بها على المستوى الوطني والإقليمي والقطاعي في أيّ بلد، بغض النظر عن موقع البيانات.

---

3 معاهدة المساعدة القانونية المتبادلة عمومًا بتبادل الأدلة والمعلومات في المسائل الجنائية وما يتصل بها من مسائل.
https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm

4 الإنابة القضائية هي طلبات مقدمة من المحاكم في بلد ما إلى محاكم بلد آخر تطلب فيها تنفيذ قانون يمكن أن يشكل انتهاكًا لسيادة ذلك البلد إذا ما تم دون موافقة محكمة البلد الأخرى. و يجوز استخدام الإنابة القضائية للتبليغ بصحيفة الدعوى أو للحصول على الأدلة إذا سمحت قوانين البلد الأجنبي بذلك.
https://travel.state.gov/ content/ travel/en/legal/travel- legal-considerations/internl-judicial-asst/obtaining-evidence/Preparation-Letters-Rogatory.html

الحد من الاستخدام القسري

منذ القرن العشرين، كان لدى العديد من البلدان آليات قانونية تتيح الوصول إلى المعلومات المخزنة في الخارج استجابةً لطلبات قانونية كافية للحصول على معلومات تتعلق بالتحقيقات والدعاوى الجنائية. فعلى سبيل المثال، يمكن أن تخضع الشركة التي تقوم بأعمال تجارية في البلد "س" لطلب قانوني للحصول على معلومات، حتى إذا كان المحتوى مخزنًا في البلد "ص" بموجب الأطر القانونية القائمة ثنائية ومتعددة الأطراف. وفي معظم الحالات، تكون الآلية القانونية المعترف بها هي معاهدة المساعدة القانونية المتبادلة.

بالإضافة إلى اتفاقيات المساعدة القانونية المتبادلة ثنائية الأطراف للبلاد، توجد أيضا اتفاقيات مساعدة قانونية متبادلة إقليمية، مثل اتفاقية المساعدة القانونية المتبادلة للبلدان الأمريكية، واتفاقية المساعدة القانونية المتبادلة بين الاتحاد الأوروبي والولايات المتحدة الأمريكية، واتفاقية المساعدة القانونية المتبادلة الآسيوية. وفي حالة عدم و جود اتفاقية مساعدة قانونية متبادلة، يمكن للبلدان الحصول على إنابة قضائية لطلب المساعدة من الحكومات الأجنبية. وسيتضمن قانون كل ولاية قضائية معاييرًا لا بد من استيفائها لكي تقدم هيئة إنفاذ القانون ذات الصلة طلبًا صحيحًا.على سبيل المثال، قد تحتاج الهيئة الحكومية الطالبة للاستخدام إلى الحصول على مذكرة أو أمر محكمة يُبيّن سببًا صحيحًا لطلب استخدام المحتوى. وعلى الرغم من الآليات المشروعة، فإن هذه النصوص القانونية لم يكن القصد منها تناول مسألة استخدام أجهزة إنفاذ القانون للبيانات في عالم رقمي.

القوانين التي تحكم استخدام البيانات التي تخزنها وكالات إنفاذ القانون في الخارج دعمًا للتحقيق في الجرائم الخطيرة، مثل الإرهاب، لم تكن مكتوبة مع وضع مراعاة التكنولوجيا الحديثة في الاعتبار. وأدى ذلك إلى حالات حيث تواجه فيها شركات التكنولوجيا، التي تمتثل لأمر قضائي بموجب قوانين أحد البلدان، خطر انتهاك قوانين بلد آخر التي تحظر الكشف عن المعلومات. يوفر قانون توضيح الاستخدام الخارجي القانوني للبيانات (CLOUD) إطارًا جديدًا للطعن في طلبات إنفاذ القانون عندمايكون هناك اتفاقات تنفيذية بينالولايات المتحدة وبلد آخر، ويؤكد أيضًا،بموجب مبادئ المجاملة القضائية بين الدول، حق مزودي الخدمات في منع الكشف عن أيّ بياناتإذا كان ذلك يتعارض مع قوانين بلد آخر، حتى في حالة عدم وجود اتفاق تنفيذي. كما أنه يُمكن مزودي الخدمات السحابية من الكشف عن البيانات للحكومات التي تصدر أوامر أو مذكرات للحصول على معلومات استنادًا إلى حقائق كافية تثبت سببًا محتملاً لحدوث جريمة خطيرة وأن المعلومات المطلوبة تتصل مباشرة بتلك الجريمة.

في محاولة لمواءمة القوانين غير المتزامنة مع التكنولوجيا الحديثة، أصدرت الولايات المتحدة قانون توضيح الاستخدام الخارجي القانوني للبيانات في مارس 2018. قانون CLOUD يقدم آلية دولية قانونية أخرى للحصول على البيانات المخزنة في الخارج من خلال الطلبات المباشرة الموجهة إلى مزود الخدمة.[5] فقانون CLOUD يحدد إجراءات تدخل الولايات المتحدة في الاتفاقات التنفيذية مع البلدان الأخرى. وتسعى هذه الاتفاقات التنفيذية إلى إزالة القيود القانونية المفروضة على قدرة بعض الدول الأجنبية على الحصول على البيانات مباشرة من مزودي الخدمات في الولايات المتحدة، شريطة أن تكون الولايات المتحدة قد قررت أن قوانين الدولة الأجنبية تحمي بشكل كافٍ الخصوصية والحريات المدنية. وبموجب قانون CLOUD، يحق لمزودي الخدمات السحابية منع الكشف عن المعلومات إذا كان ذلك يتعارض مع قوانين بلد آخر. اتفاقيات المساعدة القانونية المتبادلة والإنابة القضائية والاتفاقات التنفيذية بموجب قانون الاستخدام الخارجي القانوني للبيانات، جميعها يقدم آليات قانونية دولية متبادلة من أجل استخدام أجهزة إنفاذ القانون للبيانات المخزنة في الخارج.

---

5 ينطبق قانون CLOUD على الشركات الأمريكية والشركات الأجنبية العاملة في الولايات المتحدة والتي تقدم "خدمات الاتصالات الإلكترونية" و/أو "خدمات الحوسبة عن بُعد"، مثل الشركات التي تقدم خدمات البريد الإلكتروني أو الرسائل الإلكترونية أو التخزين السحابي للعامة.

وتنطبق القوانين الوطنية لبلد ما عموما على جميع الشركات التي لها عمليات في ذلك البلد، بصرف النظر عن مكان تأسيس الشركة أو ما إذا كانت المعلومات مخزنة في السحابة، أو مركز بيانات في الموقع،

قصر مزودي الخدمات السحابية على اختصاص قضائي واحد لا يعزل بشكل أفضل البيانات عن الاستخدام الحكومي لها

قام تحليل قانوني مستقل على أوائل الحكومات التي تبنت السحابة بتقييم القوانين الخاصة بالدولة التي تحكم وصول أجهزة إنفاذ القانون إلى البيانات الموجودة على السحابة المخزنة في الخارج. قيمت هذه الدراسة عشر اختصاصات قضائية دولية - أستراليا وألمانيا وأيرلندا والدنمارك وفرنسا وكندا واليابان وإسبانيا المملكة المتحدة والولايات المتحدة الأمريكية - ووجدت أن قصر مزودي الخدمات السحابية على اختصاص قضائي واحد لا يعزل بشكل أفضل البيانات عن الاستخدام الحكومي لها.

أو في سجلات مادية. وفي الوقت الذي تواصل فيه الدول التحول الرقمي للمجتمعات الحديثة القائمة على المعلومات والمضي قدمًا نحو تحقيقها، تتطور أيضًا النظم القانونية للوصول القسري إلى المعلومات دعمًا للتحقيقات في الجرائم الجسيمة التي تؤثر على الأمن القومي، مثل الإرهاب. ويشكل سن قانون CLOUD إطارًا آخر يهدف إلى تعزيز الإجراءات القانونية الواجبة لطلب إنفاذ القانون في هذا السياق الحديث.

والحقيقة هي أن هذا الاستخدام القسري يحدث في عدد محدود جدًا من الحالات، وبشكل عام فقط عندما تكون هناك حاجة ماسة إلى المعلومات (على سبيل المثال، لمنع الأحداث المتعلقة بالإرهاب). وللتخفيف حتى من هذه المخاطر المنخفضة، يمكن للمؤسسات ممارسة العناية الواجبة وصياغة وسائل الحماية الخاصة بها من خلال الخدمات السحابية المتاحة. وفي AWS، يمكن استخدام العوامل المخففة، مثل تشفير البيانات العابرة والمنتقلة، وتقسيم البيانات وتوزيعها، واستراتيجيات الرموز، لجزء صغير من عبء الموارد مقابل حل محلي.

وخدمة AWS يقظة حول حماية محتوى عملائنا، بغض النظر عن المكان الذي يأتي منه الطلب أو من هو العميل. ولن تكشف AWS عن محتوى العميل إلا أن يطلب منها ذلك للامتثال لأمر ساري المفعول وملزم قانونًا، مثل مذكرة إحضار أو أمر قضائي. كما تدرس AWS بعناية كل طلب للمصادقة على دقته والتحقق من أنه يمتثل للقانون المعمول به. وستطعن AWS على الطلبات التي تكون واسعة النطاق أكثر من المطلوب أو تتجاوز سلطة الجهة الطالبة أو لا تمتثل تمامًا للقانون المعمول به. تحاول AWS أيضًا إعادة توجيه الطلب مباشرة إلى العميل، باستثناء ما يحظره القانون، مما يوفر للعميل فرصة لاتخاذ إجراء ضد الطلب. يمكن العثور على معلومات إضافية في أحدث تقرير شفافية لدينا والمبادئ التوجيهية لإنفاذ القانون لأمازون.[6]

---

6 http://d0.awsstatic.com/certifications/Amazon_LawEnforcement_Guidelines.pdf

لماذا ينخفض خطر الاستخدام غير المصرح به في السحابة؟

بالنسبة لبعض الحكومات، تهدف متطلبات أماكن إقامة البيانات إلى التخفيف من المخاطر المتعلقة بإمكانية وصول كيان آخر إلى بياناتها. يهدف هذا القسم إلى معالجة الزيادة الملحوظة في مخاطر الاستخدام غير المصرح به عند استخدام مزود خدمات سحابية فائقة. الاستخدام غير المصرح به هو التهديد الأكثر شيوعًا الذي يجربه الخصوم للوصول إلى بيانات العملاء باستخدام وسائل مختلفة. ويمكن أن يشمل الاستخدام غير المصرح به مخاوف وصول طرف خارجي، بما في ذلك احتمال وجود تهديدات مطلعة أو جهات خارجية سيئة.

تفشل متطلبات إقامة البيانات في معالجة الطرق الشائعة التي يستخدمها المهاجمون للحصول على وصول إلى البيانات. ويؤدي استغلال هذه الموجهات في جميع الحالات تقريبًا إلى فشل في ضوابط النظافة السيبرانية الأساسية، مثل إدارة مخزون النظام، وإدارة التكوين، وتشفير البيانات، وإدارة الوصول المميز.

تقليل الاستخدام غير المصرح به

منع الوصول غير المصرح به يتطلب ممارسة العادات الأمنية المناسبة وتنفيذ قدرات كشف وقدرات وقائية قوية. فعلى سبيل المثال، ينبغي تصميم النظم للحد من "نصف قطر الانفجار" لأي تسلل بحيث يكون للعقدة التي تعرضت للخطر تأثير ضئيل على أيّ عقدة أخرى في المؤسسة. يوفر مزودو الخدمات السحابية الفائقة، مثل AWS، بيئة أدوات أمن كاملة لتمكين العملاء من الحفاظ على الاتصالات المشفرة وتنفيذ وسائل الحماية من العبث للتخفيف من مخاطر الوصول غير المصرح به. ليس لدى AWS رؤية أو معرفة بمحتويات حساب العميل، بما في ذلك ما إذا كان هذا المحتوى يتضمن
أي معلومات شخصية من عدمه. يتم تمكين عملاء AWS لاستخدام تقنيات مختلفة مثل التشفير،[7] الرموز، وتقسيم البيانات، والخداع السبراني، لجعل المحتوى غير مفهومة لـ AWS أو للأطراف الأخرى التي تسعى إلى الوصول إلى محتواها.

- التشفير - يمكن أن يؤدي تشفير البيانات بشكل مناسب إلى جعل البيانات غير قابلة للقراءة. وهذا يعني أن تخزين البيانات المشفرة في السحابة، بغض النظر عن الموقع، يمكن أن يوفر حماية كافية ضد الغالبية العظمى من تهديدات تسرب البيانات. ومن الأهمية بمكان أن تتم إدارة مفاتيح التشفير الخاصة بالبيانات بعناية لضمان الحفاظ على الحماية القوية ضد أيّ طرف يحاول التسلل. توفر AWS الخدمات التي يمكن أن تقدم هذه القدرات على مستوى المؤسسة مع CloudHSM AWS أو KMS AWS (Key Management Service).[8] فمقدار التحكم الذي يرغب العملاء في الحصول عليه عن طريق التشفير، وتخزين مفاتيح التشفير، وإدارة مفاتيح التشفير المستخدمة مع بياناتهم، هو أمر متروك للعميل.[9]

---

7 يسمح AWS للعملاء باستخدام آليات التشفير الخاصة بهم لجميع خدمات AWS تقريبًا، بما في ذلك Amazon S3 وAmazon EBS و Amazon DynamoDB وAmazon EC2. كما يتم تشفير أنفاق IPSec إلى VPC. كما تقدم Amazon S3 تشفير من جانب الخادم كخيار للعملاء. ويمكن للعملاء أيضًا استخدام تقنيات تشفير لجهة خارجية.

8 تتيح لك خدمة AWS CloudHSM (وحدة أمن الأجهزة) حماية مفاتيح التشفير الخاصة بك داخل وحدات أمان الأجهزة المصممة والمعتمدة وفقًا للمعايير الحكومية (FIPS 140-2 المستوى 3) لإدارة المفاتيح الآمنة بما في ذلك وسائل الحماية القوية من العبث. توفر KMS AWS، المعتمدة وفقًا لمعيار FIPS 140-2 المستوى 2، خدمة مماثلة، ولكنها أكثر قابلية للتطوير وأكثر تكاملاً مع مجموعة كبيرة من خدمات AWS بحيث يتم توفير الحماية تلقائيًا استنادًا إلى تغييرات بسيطة في تكوين الخدمة. وباستخدام أيٍّ من الخدمتين، يمكنك إنشاء وتخزين وإدارة مفاتيح التشفير المستخدمة لتشفير البيانات بشكل آمن بحيث لا يمكن الوصول إليها إلا من قبلك فقط. لمزيدٍ من التفاصيل، انظر https://aws.amazon.com/cloudhsm and https://aws.amazon.com/kms.

9 يتم تفصيل خيارات التشفير لدى AWS عبر الروابط التالية: 1) Securing Data at Rest with Encryption، 2) Protecting Data Using Encryption in Amazon S3 3) AWS Key Management Service Cryptographic Details، 4) Overview of AWS Security Processes.

- الرموز - إنشاء الرموز هي عملية تسمح لك بتحديد تسلسل من البيانات لتمثيل قطعة حساسة بشكل آخر من المعلومات (على سبيل المثال، رمز لتمثيل رقم بطاقة الائتمان للعميل). الرمز لا معنى له في حد ذاته ولا يمكن تعيينه مرة أخرى إلى البيانات التي يمثلها دون استخدام نظام إنشاء الرموز. يمكن إنشاء خزائن الرموز في سحابات VPC لتخزين المعلومات الحساسة في شكل مشفر أثناء مشاركة الرموز إلى الخدمات المعتمدة لنقل البيانات الغامضة. -بالإضافة إلى ذلك، لدى AWS عدد من الشركاء المتخصصين في توفير خدمات إنشاء الرموز التي تتكامل مع قواعد البيانات الشائعة وخدمات التخزين الأخرى.

- تقسيم البيانات — هذه عملية تعمل على تقليل مجموعات البيانات إلى عناصر لا يمكن التعرف عليها والتي ليس لها أهمية بمفردها.[10] وبعد ذلك يتم تخزين هذه العناصر أو الأجزاء بطريقة موزعة بحيث لا يُسفر أيّ اختراق في عقدة واحدة إلا عن جزء غير هام من البيانات. وتتجسد ميزة خاصة لهذه التقنية في أنها تتطلب من فاعل التهديد إلى اختراق جميع العقد، والحصول على جميع الأجزاء، ومعرفة الخوارزمية (أو مخطط التجزئة) لتجميع البيانات بطريقة مترابطة.

- دفاع الخداع السيبراني — يمكن أن تكون هيكليات وحلول الخداع السبراني عنصرًا أساسيًا للحد من الأعداء المتقدمين. يمكن لحلول الخداع استخدام الشراك والفخاخ المتطورة للغاية لتقديم للمهاجم تصور أنه قد تسلل إلى النظام بينما يكون في الواقع تم تحويله إلى بيئة تخضع لسيطرة عالية. يتم جمع المعلومات الاستخباراتية حول المهاجم من أجل الحد من التهديدات المستقبلية، ويتم تحييد الهجوم.

أحد الشواغل المتصلة بالاستخدام غير المصرح به يتمثل في وصول أطراف خارجية إلى محتوى العميل ومدى كفاية تدابير مراقبة الوصول لمنع الاستخدام غير المصرح به من موظفي مزود الخدمات السحابية. يتم تخصيص وصول الأطراف الخارجية إلى أنظمة AWS استنادًا إلى أقل امتيازات، والموافقة عليه من قبل فرد مخول قبل توفير الوصول، وإشراف من قبل موظف لدى AWS. يجب فصل الواجبات ومجالات المسؤولية (على سبيل المثال، طلب الاستخدام والموافقة على الاستخدام، وطلب إدارة التغيير والموافقة عليه، وما إلى ذلك) بين أفراد مختلفين للحد من فرص التعديل أو إساءة الاستخدام لأنظمة AWS بشكل غير مصرح به أو غير مقصود. ويُطلب أولاً من موظفي AWS، الذين لديهم حاجة تجارية للوصول إلى مستوى الإدارة، استخدام مصادقة متعددة العوامل، والتي تكون مختلفة عن بيانات اعتماد Amazon العادية للشركات، للوصول إلى المضيفين الإداريين لهذا الغرض. وهؤلاء المضيفون الإداريون هم أنظمة مصممة خصيصًا ومبنية ومكونة ومعززة لحماية مستوى الإدارة. يتم تسجيل كل هذا الاستخدام ومراجعته. عندما لا يكون لدى الموظف حاجة عملية للوصول إلى مستوى الإدارة، يتم إلغاء الامتيازات والوصول إلى هؤلاء المضيفين والأنظمة ذات الصلة. نفذت AWS سياسة قفل الجلسة والتي يتم تنفيذها بشكل منهجي. كما يتم الاحتفاظ بقفل الجلسة حتى يتم تنفيذ إجراءات تحديد الهوية والمصادقة المعمول بها.

وتراقب أيضًا AWS الإدارة عن بعد غير المصرح بها، وتقوم بسرعة بفصل أو تعطيل الوصول عن بعد غير المصرح به بمجرد اكتشافه. يتم تسجيل جميع محاولات الوصول الإداري عن بعد، ويتم مراجعة السجلات، ليس فقط من قبل أشخاص للنشاط المشبوه، ولكن أيضًا من خلال أنظمة التعلم الآلي التلقائية التي صممها فريق أمن AWS للكشف عن أنماط الوصول غير العادية التي قد تشير إلى محاولات غير مصرح بها للوصول إلى البيانات. وفي حالة اكتشاف نشاط مشبوه، تبدأ إجراءات الاستجابة للحوادث. وعلاوة على ذلك، أنشأت AWS

10 مجموعة من البحوث المتاحة بشأن تقنيات تقسيم البيانات. أحد هذه التقارير التي تم مراجعتها لهذه الوثيقة هو حماية البيانات عن طريق التجزئة في مختلف أنظمة التخزين الموزعة - دراسة استقصائية، كابوستا وميمي، 20 يونيو 2017.

الإجراءات السياسات الرسمية لتحديد معايير الوصول المنطقي إلى البنية التحتية لـ AWS والمضيفين. وتحدد السياسات أيضًا المسؤوليات الوظيفية لإدارة الوصول المنطقي والأمن. يشترط القانون أن يخضع جميع الموظفين لفحص الخلفية الجنائية، باستثناء ما يحظره القانون، بما يتناسب مع و ضعهم ومستوى الوصول المقدم لهم.

وأخيرًا، لا يتم التحكم في المثيلات الافتراضية للعميل إلا من قبل العميل الذي لديه الوصول الكامل للنظام أو السيطرة الإدارية على الحسابات والخدمات والتطبيقات. ولا يملك موظفو AWS القدرة على تسجيل الدخول إلى مثيلات العملاء.

سحابة ذات نطاق فائق: منهجية التحويل للأمن

توفر الشركات الرائدة في تقديم الخدمات السحابية الفائقة، مثل AWS، الفرصة للعملاء لبناء أمن متكيف ومرن للغاية لحجم أعمالهم.
ومن شأن قصر العمليات على متطلبات محددة داخل البلاد أن يحول دون ابتكار الخدمات ويعوق القدرة على مواجهة التهديدات، مثل التي تستهدف توافر الهدف. وثمة ناتج ثانوي ضار آخر للقيود الجغرافية داخل البلاد، ويتمثل في أن الجهات الفاعلة للتهديد يمكن أن تكتسب دقة الاستهداف بمعرفة أن البيانات يجب أن تكون ضمن مناطق محددة. تتوفر لدى مزودي الخدمات السحابية الفائقة منتجات وهيكليات داعمة لتقديم كل من قدرات الدفاع بشكل معمّق[11] والدفاع على نطاق واسع[12]. ويرجع ذلك إلى أن آليات الأمن متأصلة في تصميم منتجات مزودي الخدمات السحابية الفائقة وتشغيلها.

ومن النواتج الثانوية غير المقصودة لمتطلبات إقامة البيانات داخل البلاد أن الجهات الفاعلة للتهديد يُمكن أن تكتسب دقة أفضل في استهداف النظم بمعرفة أن البيانات موجودة في مواقع محددة.

تعكس العناصر الستة التالية سمات الأمن الأساسية التي تشكل جزءًا لا يتجزأ من مزود خدمات سحابية فائقة، مثل AWS:

1. التكامل العميق للأمن والامتثال (نادرًا ما يتحقق في الأنظمة التقليدية) يعني أن الأمن يستفيد مباشرة من الامتثال، لأن الضوابط الأمنية يتم رصدها وتحديثها باستمرار.
2. لا ينطبق مقياس اقتصادي من خلال زيادة مستوى الإنتاج على التكنولوجيا فحسب، بل ينطبق أيضًا على موظفي الأمن والعمليات الأمنية، مما يؤدي إلى عائد استثماري غير مسبوق مقارنة بالنظم التقليدية.
3. يتولى مزود الخدمات السحابية جزء كبير من "المساحة السطحية" الأمنية، حيث ينفذ مهامه بالتركيز المهني والمهارة التي تتجاوز تقريبًا أيّ عميل على وجه الأرض. ونتيجة لذلك، يمكن للعملاء إعادة تركيز المتخصصين في الأمن والموارد الأمنية لديهم على جزء أصغر بكثير من التحدي، مثل أمن التطبيقات.
4. توفر السحابة الرؤية والتجانس والأتمتة التي لم يسبق لها مثيل في الأنظمة التقليدية، وجميعها تستفيد بشكل كبير من الأمن. ويشمل ذلك إمكانات التدقيق والتسجيل العميقة بشكل كبير، والتي، على سبيل المثال، يمكنها تسجيل مكالمات API التي تقوم بتسجيل الإجراءات التي يتخذها مزود الخدمات السحابية والتي قد تؤثر على حساب العميل.

11 الدفاع بشكل معمّق هو ممارسة تنفيذ طبقات متعددة من الضوابط الأمنية لتوفير الاستقلالية والتكرار. فإذا فشلت طبقة واحدة من عناصر التحكم، تكون الطبقة اللاحقة متاحة للحد من مزيدٍ من الهجوم ضد الأصل.

12 الدفاع واسع النطاق هو نهج استخدام الأنشطة متعددة التخصصات لتوفير العديد من آليات الحماية في كل طبقة من طبقات الدفاع المحددة. وبشكل عام، يعني ذلك المزيد من الأتمتة والمزيد من الضوابط الأمنية في كل طبقة.

5. يعمل مزودو الخدمات السحابية بمثابة نوع من "حاوية النظام" التي توفر رؤية أكبر على سلوك النظام وأعماله، بما في ذلك العمليات الأمنية، مما يقدم للعملاء طبقة جديدة من "الدفاع بشكل معمّق".

6. مع الوصول السهل والرخيص إلى كميات هائلة من سعة التخزين والمعالجة، فإن عملاء AWS "يستخدمون السحابة لتأمين السحابة"، أيّ أنهم يقومون بإجراء تحليلات البيانات الضخمة على بيانات الأمن وبيانات السجلات، مما يوفر المزيد من الرؤى لوضعها الأمني ويسفر عن علاج أسرع بكثير للمشكلات.

مع سرعة الابتكار وزيادة النطاق، فإن قصة أمن السحابة تتجه نحو التحسُّن فقط. على سبيل المثال، أضافت AWS، في العام الماضي فقط، قدرات أمنية قوية مثل Amazon GuardDuty[13]، وهو منتج للكشف عن التهديدات المدارة التي ترصد باستمرار السلوك الخبيث أو غير المصرح به؛ و Amazon Macie[14]، وهو منتج يستخدم تعلم الآلة لحماية البيانات الحساسة؛ و AWS CloudHSM 2.0[15]، وهو منتج مدار بالكامل يستخدم أجهزة معتمدة وفقًا لـ FIPS 140-2 المستوى 3[16] التي تم توزيعها تلقائيًا في مجموعة مناطق توافر متعددة شديدة التوافر وزائدة والتي تُمكِّن العملاء من إنشاء وإدارة واستخدام مفاتيح التشفير الخاصة بهم في سحابة AWS بسهولة، مع عدم توفير امكانية وصول AWS إلى عمليات التشفير الأساسية أو المفاتيح الرئيسية.

يجب اعتبار التشفير خدمة أساسية نظرًا إلى إمكانية استخدامه كوسيلة لحماية البيانات في حالة فشل الإمكانات الأخرى. وهو يضيف طبقة إضافية من الأمن والتأمين لسرية البيانات وسلامتها في أثناء التنقل والاستقرار. تعد المجموعة المكونة من AWS Key Management Service (AWS KMS) وAWS CloudHSMبمنزلة أساس حل التشفير الصارم.[17] يوفر مزودو الخدمات السحابية الفائقة مثل AWS تشفيرًا واسع الانتشار يمكن أن يكون بعيدًا عن متناول العمليات المحلية. على سبيل المثال، توفر AWS Key Management Service (AWS KMS) تحقق FIPS 140-2 من المستوى 2، والذي يتيح بدوره خيار جلب المفاتيح الخاصة بك (BYOK)الذي يتيح للعملاء استخدام المواد الرئيسية الخاصة بهم التي تم إنشاؤها وتخزينها محليًا باستخدام خدمات AWS. يمكن للعملاء استيفاء متطلبات الأمن والامتثال المحددة فيما يتعلق بأعباء العمل شديدة الحساسية باستخدام هذه الإمكانية حيث يمكنهم الاحتفاظ بالمواد الرئيسية الخاصة بهم وإدارتها خارج AWS.

---

13 https://aws.amazon.com/guardduty

14 https://aws.amazon.com/macie

15 https://aws.amazon.com/cloudhsm

16 FIPS 140-2، متطلبات الأمن لوحدات التشفير تغطي 11 مجالاً ذا صلة بتصميم وحدة التشفير واستخدامها.

17 https://d1.awsstatic.com/whitepapers/compliance/AWS_Logical_Separation_Handbook.pdf

مسؤولية CSP: الأمن المتأصل في السحابة

تم تكوين بنية AWS التحتية خصيصًا للسحابة، حيث تم تصميم جميع العناصر للتواصل بشكل جيد وتوفير أقل قدر ممكن من الأجزاء المعرضة للهجمات. إضافة إلى ذلك، فقد تم تصميم ضوابط الأمن المادية الموجودة في مراكز البيانات لدينا لتكون من بين الأكثر صرامة في العالم. تمت مراجعة هيكلية AWS والتحقق من التزامها بعشرات من أطر عمل الامتثال الدولية.[18] نحن نستعين بخبراء مستقلين من جهة خارجية لتقييم وتدقيق مدى التزامنا بهذه الأنظمة وتوثيقه، وتزويد العملاء بإمكانية الوصول إلى التقارير الناتجة والأدلة الداعمة. لاستيفاء هذه المجموعة الكبيرة من متطلبات الأمن، تقوم AWS بإنشاء مراكز البيانات والهيكلية الخاصة بها لزيادة نطاق التقدم والابتكار وتعزيزه. وقد أدى هذا النهج إلى ثقة الحكومات والمؤسسات العسكرية والمصارف العالمية ومؤسسات الرعاية الصحية وغيرها من المؤسسات شديدة الحساسية في AWS.

في AWS، كانت بيئتنا الفريدة حافزًا لإنشاء العديد من أدوات الأمن الخاصة بنا. تعمل هذه الأدوات على الأتمتة لمجموعة ضخمة من المهام الروتينية، مما يتيح لخبراء الأمن لدينا التركيز على الجوانب الهامة
لحماية البيئة. أدى إنشاء الأدوات الخاصة بنا إلى ظهور متطلبات أمن يتم فرضها والالتزام بها خلال دورة حياة تطوير النظام. يتم علاج مخاوف الأمن الشائعة في المراحل الأولى لتطوير النظام، ما يتيح لخبراء الأمن لدينا التركيز على تخفيف حدة التهديدات المتقدمة والمعقدة على مستوى الإنتاج.

تقوم فرق الأمن التابعة لنا بمراقبة البنية التحتية طوال اليوم وكل يوم، وتتواصل بشكل جيد مع جميع مجموعات مراقبة نظام الأمن الرئيسية والموردين من أجل

تحديد التهديدات المحتملة على الفور. ويقومون بذلك على نطاق واسع، ما يعمل على تمييز مؤسسة أمن AWS. من خلال استخدام لوغاريتمات معقدة لفحص الملايين من حسابات العملاء النشطة التي تقوم بتشغيل أي نوع يمكن تصوره من أحمال العمل، يمكننا اكتشاف مشكلات قد تحدث مرة واحدة فقط كل مليار عملية عدة مرات في اليوم الواحد. عندما نقوم بحل المشكلة، نقوم بذلك للمنصة بالكامل. ومن الواضح أن هذا النوع من الرؤية والاستجابة

خيار محلي إضافي لاحتياجات التوطين

يعد التحول إلى الحوسبة السحابية رحلة متعددة المراحل تتمثل في الانتقال على مراحل، وغالبًا ما ينعكس هذا على شكل نهج سحابة هجينة (أي توزيع أعباء العمل بين بيئات السحابة المحلية والتجارية). لأسباب مختلفة، قد يجد العملاء أن بعض أحمال العمل من الأفضل أن تتم إدارتها محليًا سواء لضمان زمن انتقال أقل أو من أجل احتياجات المعالجة المحلية الأخرى.

تواصل AWS الابتكار لتزويد العملاء بمزيد من التحكم والمرونة في أثناء قيامهم بتنفيذ نهج الانتقال إلى الحوسبة السحابية. على سبيل المثال، توفر سحابة هجينة مثل AWS Outposts[1] خيارًا يتيح توفر خدمات AWS السحابية على مراكز بيانات العملاء، ما يعزز المرونة اللازمة لاختيار مكان نشر تطبيقات السحابة، بما في ذلك أعباء العمل الحساسة.

حتى قامت AWS بإطلاق Outposts، كان لزامًا على العملاء العمل في أقرب منطقة تتوفر فيها خدمات AWS للحفاظ على البيانات في منطقة قريبة. من خلال توسيع بنية AWS التحتية وخدماتها لتشمل بيئاتهم، يمكن للعملاء دعم أحمال العمل التي تحتاج إلى أن تظل خاضعة للإدارة محليًا مع الاستفادة من الأمن والإمكانات التشغيلية للخدمات السحابية التجارية.

يتم توصيل Outposts ببنية AWS التحتية في أي منطقة يختارها العميل لتبادل البيانات المستخدمة لتوفير الخدمة وتحسينها وتأمينها. يمكن للعملاء اختيار تخزين المحتوى محليًا في خدمات تخزين موجودة على Outpost، مثل EBS. كما يمكن للعملاء اختيار إرسال المحتوى مرة أخرى إلى المنطقة من أجل التوافر والاستمرارية، عادة بشكل مشفر، على سبيل المثال لقطات EBS ونسخ RDS احتياطية وما شابه.

تشجع AWS العملاء على تقييم نهج تصنيف البيانات المستخدم لديهم والتركيز على البيانات التي يجب الإبقاء عليها داخل بلدهم أو منطقتهم، وسبب ذلك. من خلال القيام بذلك، قد يجد العملاء أن بياناتهم، حتى البيانات الحساسة والمهمة، يمكن تخزينها و/أو نسخها في مكان آخر إذا لم تكن هناك متطلبات جغرافية محددة خاصة بالشؤون القانونية أو السياسة. قد يقلل ذلك من خطر فقدان تلك البيانات في حالة وقوع كارثة ويوفر إمكانية الوصول إلى التقنيات والإمكانات التي قد لا تكون متاحة في منطقتهم.

1. توفر AWS Outposts خدمات AWS للأمن المتأصل وبنية تحتية ونماذج تشغيل لأي مركز بيانات أو مساحة ذات مواقع مشتركة أو منشأة محلية. لمزيد من التفاصيل، يرجى زيارة https://aws.amazon.com/outposts

لا يمكن تحقيقه بالنسبة إلى الغالبية العظمى من المؤسسات التي تقوم بتشغيل مراكز بيانات محلية. توضح القيمة الناتجة عن الخبرة المركزة والنطاق الواسع لماذا قررت شركتا Gartner وIDC أن أحمال عمل البنية التحتية السحابية كخدمة (IaaS) العامة ستتعرض لحوادث أمن أقل مقارنة بتلك الموجودة في مراكز البيانات التقليدية. قدرت بحوث Gartner انخفاض حوادث الأمن بنسبة 60% على الأقل.[19]

مسئولية العميل: منهجية الهيكلية الآمنة

تعمل إمكانات الأمان المتأصل لدى مزودي الخدمات السحابية الفائقة مثل AWS على تمكين العملاء من إنشاء هيكليات فريدة لتقليل مخاطر الوصول. تفتقر المنشآت المحلية والمرافق المشابهة تفتقد إلى التجانس مقياس اقتصادي والرؤية والأتمتة التي من شأنها تحقيق تطورات أمن هائلة. هذه التطورات ضرورية لإنشاء أنظمة عالية الأمان يمكنها مواجهة التهديدات الناشئة التي تظهر خارجيًا
وداخليًا على حد سواء. تكافح المنشآت المحلية لاستخدام مفاهيم التشغيل الجديدة هذه بسبب متطلبات الموارد اللازمة لإعادة هيكلة الشبكات وتوفير أنظمة جديدة، فضلاً عن العمالة البشرية المطلوبة بسبب نقص البنى التحتية المستندة إلى البرامج. يقوم مزودو الخدمات السحابية الفائقة بإنشاء مستوى من السرعة والقدرة على التكيف في بنيتهم التحتية لتنفيذ تطورات الأمن هذه بشكل طبيعي. يعني هذا أن بإمكان العملاء استخدام التطورات الجديدة بسهولة أكبر نظرًا إلى أنها مدمجة في عروض مزود الخدمات السحابية، ما يتيح للعملاء إنشاء الأنظمة باستخدام هيكليات فريدة مثل التقسيم الدقيق والتصميمات متعددة الأشكال[20] وشبكات التضليل متعددة المستويات.

على سبيل المثال، بإلقاء نظرة أقرب على التصميم المستند إلى التقسيم الدقيق على AWS، يمكن للعميل استخدام مجموعة واسعة من التقنيات بما في ذلك Amazon Virtual Private Cloud (Amazon VPC) وAWS Identity and Access Management (IAM) ومجموعات الأمن وقوائم التحكم في الوصول إلى الشبكة والعديد من خدمات التشفير والتسجيل، علاوة على AWS Certificate Manager لتكوين أساس قوي لإنشاء شبكة مستندة إلى نموذج انعدام الثقة [21] (ZTM). نظريًا، قد يوفر نموذج انعدام الثقة ميزة مختلفة للحد من التهديدات ومراقبة الأداء. تحتاج المؤسسات بشكل واضح إلى تنفيذ نموذج انعدام الثقة أو تصميم مماثل للتقسيم بمعيار أمن لمواجهة التهديدات الحالية، لكن إنشاء هذا النوع من الهيكلية في بيئات المؤسسات التقليدية يعد أمرًا صعبًا ومكلفًا للغاية. الانتقال إلى مزود خدمات سحابية عام يمنح المؤسسات الفرصة لتنفيذ نموذج انعدام الثقة والمفاهيم المماثلة دون تكلفة كبيرة وعبء الموارد المقترن بتحديث/إنشاء الشبكة المادية.

18 انظر https://aws.amazon.com/compliance

19 https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

أدوار حماية البيانات

هناك خمسة مفاهيم أساسية مهمة تتعلق بملكية البيانات وإدارتها في نموذج المسؤولية المشتركة:

1. يستمر العملاء في امتلاك بياناتهم.
2. يختار العملاء الموقع (المواقع) الجغرافي الذي يتم تخزين بياناتهم فيه - ولا يتم نقلها إلا إذا قرر العميل نقلها.
3. بإمكان العملاء تنزيل بياناتهم أو حذفها عند الحاجة.
4. يمكن للعملاء "حذف تشفير" بياناتهم عن طريق حذف مفاتيح التشفير الرئيسية المطلوبة لفك تشفير مفاتيح البيانات، والمطلوبة بدورها لفك تشفير البيانات.
5. يجب على العملاء أخذ حساسية بياناتهم في الحسبان واتخاذ قرار بشأن ما إذا كان سيتم تشفير البيانات وكيفية تشفيرها في أثناء التنقل والاستقرار.

يتم تطبيق تدابير حماية البيانات بأقصى قدر من الفعالية بعد تحديد أدوار معالجة البيانات لتحديد أدوار أصحاب المصالح ومسؤولياتهم. تعمل معظم مخططات حماية البيانات على التمييز بين المتحكم في البيانات (يُشار إليه أيضًا باسم "المستخدم") ومعالج البيانات وفرض الالتزامات وفقًا لتلك الأدوار المتميزة. على سبيل المثال، بموجب اللائحة العامة لحماية البيانات الصادرة عن الاتحاد الأوروبي، يكون المتحكم في البيانات مسؤولاً عن تنفيذ التدابير التقنية والتنظيمية المناسبة لحماية البيانات من الإتلاف غير المقصود أو غير القانوني أو الضياع عن طريق الخطأ أو تغييرها أو الكشف عنها أو الوصول إليها دون تصريح. عندما تتم المعالجة بواسطة معالج بيانات نيابة عن المتحكم في البيانات، يكون المتحكم في البيانات مسؤولاً أيضًا عن اختيار معالج يوفر التدابير التقنية والتنظيمية الكافية التي تحكم المعالجة المطلوب تنفيذها. تساعد عمليات التمييز هذه على تحديد المسؤوليات بين مزودي الخدمة الخارجيين وعملائهم.

---

20 بعبارات بسيطة، إنه تصميم متعدد الأشكال يتيح إنشاء أهداف متحركة، ما يجعل من الصعب على الخصوم تنفيذ هجمات ناجحة.

21 المفهوم الذي ابتكرته في الأصل شركة Forrester Research. يقترح هذا المفهوم أنه لا يمكن الوثوق بأي كيان على الشبكة. ويتمثل الهدف في فرض وصولٍ آمنٍ إلى جميع الموارد سواءً الداخلية أم الخارجية. يعني هذا أنه يجب على أي مؤسسة فهم بياناتها وتصنيفها وتحديد كيفية تدفق تلك البيانات، ولا سيما البيانات الحساسة، بين عمليات التخزين والمعالجة والنقل والعملاء. ثم بمجرد فهم البيانات يمكن للمؤسسة تنفيذ آليات نموذج انعدام الثقة التي تعمل على تطبيق أقل امتياز مطلق وتشفير شامل وفحص حركة مرور البيانات بالكامل وتشغيل هذه العمليات تلقائيًا.

بوصفها مزودًا للبنية التحتية للخدمة الذاتية التي تخضع بالكامل لتحكم العملاء - بما في ذلك ما يتعلق بكيفية معالجة البيانات وما إذا كانت تتم معالجتها - توفر AWS خدمات البنية التحتية للعملاء الذين يرغبون في تحميل المحتوى على AWS ومعالجته. لا تستطيع AWS رؤية أو معرفة ما يقوم العملاء بتحميله على شبكتها، بما في ذلك ما إذا كان ذلك المحتوى يتضمن أي بيانات شخصية أم لا. كما يتم تمكين عملاء AWS وتشجيعهم على استخدام التشفير ليصبح المحتوى غير واضح لـ AWS وأي جهة خارجية قد تسعى للوصول إلى البيانات.

تعد خدمات AWS غير محددة المحتوى نظرًا إلى أنها توفر مستوى الأمن المرتفع نفسه لكل العملاء، بغض النظر عن نوع المحتوى الذي تتم معالجته أو تخزينه أو المنطقة الجغرافية التي يتم فيها هذا. بعبارة أخرى، تستخدم AWS حد الأمن المرتفع نفسه عبر جميع خدماتنا. يعني هذا
أننا نستخدم أعلى مستوى تصنيف لنقل البيانات وتخزينها في السحابة التجارية الخاصة بنا ونطبق مستويات الحماية نفسها على جميع عروضنا ولجميع عملائنا. ومن ثم، يتم ترتيب هذه العروض للحصول على شهادة اعتماد وفقًا لأعلى حد من الأمن والامتثال، والتي تؤدي إلى استفادة العملاء من ارتفاع مستويات حماية بياناتهم التي تتم معالجتها وتخزينها في السحابة. وقد تم اعتماد سحابة AWS وفقًا للعديد من اعتمادات الصناعة المنظمة (الرعاية الصحية والشؤون المالية، وما إلى ذلك) والوطنية (على سبيل المثال
البرنامج الفيدرالي لإدارة المخاطر والتفويض (FedRAMP) في الولايات المتحدة ودليل ضوابط امتثال الحوسبة السحابية (C5) في ألمانيا وبرنامج المقيمين المسجلين لأمن البيانات (IRAP) في أستراليا) والاعتمادات العالمية (مثل شهادة منظمة المعايير الدولية ISO 27001[22] وISO 27018[23] ومعيار أمن بيانات صناعة بطاقات الدفع (PCI DSS)[24] وضوابط تنظيم الخدمة (SOC)[25])، التي تقوم باختبار أمان أنظمتنا والتحقق منه مقابل أشد المعايير صرامة.

<u>التدفق الحر للبيانات غير الشخصية مقترح كمعيار فعلي لمناطق الاتحاد الأوروبي وعبر المحيط الهادئ</u>

نشرت مفوضية الاتحاد الأوروبي مؤخرًا مشروع لائحة حول التدفق الحر للبيانات ***يحظر قواعد توطين البيانات الوطنية في الدول الأعضاء في الاتحاد الأوروبي*** والاعتراف بمبدأ حرية حركة البيانات غير الشخصية داخل
الاتحاد الأوروبي. يحدد هذا الاقتراح تدفق البيانات عبر الحدود بوصفه المعيار الفعلي، ما يضع على عاتق الدول الأعضاء مسؤولية تقديم تبرير السلامة العام لفرض متطلبات توطين البيانات. بينما كان هذا الاقتراح في المراحل الأولى من التشاور، كان يعترف بالمزايا الاقتصادية والأمنية لتدفقات البيانات عبر الحدود، التي تعد أكثر أهمية من الاعتبارات المتعلقة بتطبيق سياسات إقامة البيانات. علاوة على ذلك، في بداية العام 2018 ،
كانت **اتفاقية الشراكة الشاملة والمتقدمة عبر المحيط الهادئ** التي عقدت بين 11 دولة تدعم أيضًا ***تدفقات البيانات عبر الحدود*** ولا تُلزم الشركات بإقامة
منشآت حوسبة داخل الدولة كشرط لممارسة الأعمال التجارية في تلك الدولة.

---

22 ISO 27001/27002 هو معيار أمن عالمي يُستخدَم على نطاق واسع يحدد المتطلبات وأفضل الممارسات للوصول إلى نهج منظم لإدارة معلومات الشركة والعملاء يستند إلى تقييمات دورية للمخاطر تتناسب مع سيناريوهات التهديدات دائمة التغير.

23 ISO 27018 هو قانون ممارسات يركز على حماية البيانات الشخصية الموجودة في السحابة. وهو يستند إلى معيار أمن المعلومات ISO 27002، ويقدم توجيهات تنفيذ ضوابط معيار ISO 27002 المطبقة على معلومات التعريف الشخصية (PII) على السحابة العامة. كما يقدم مجموعة من الضوابط الإضافية والتوجيهات ذات الصلة التي تهدف إلى استيفاء متطلبات حماية بيانات التعريف الشخصية على السحابة العامة التي لا تفي بها مجموعة ضوابط ISO 27002 الحالية.

24 معيار أمن بيانات صناعة بطاقات الدفع (المعروف أيضًا بالاختصار PCI DSS) هو معيار أمن المعلومات الخاصة الذي تتم إدارته بواسطة مجلس معايير الأمن المعني بصناعة بطاقات الدفع (https://www.pcisecuritystandards.org)، والذي تم تأسيسه بواسطة شركات American Express و Discover Financial Services و JCB International و MasterCard Worldwide و Visa Inc. ينطبق معيار PCI DSS على جميع الكيانات التي تقوم بتخزين بيانات حامل البطاقة (CHD) و/أو بيانات التوثيق الحساسة (SAD) أو معالجتها أو نقلها بما في ذلك التجار ومسؤولو المعالجة والمشترون والمصدرون ومزودو الخدمات.

25 تهدف تقارير ضوابط تنظيم الخدمة (SOC 1، 2، 3) إلى استيفاء مجموعة كبيرة من متطلبات التدقيق المالي لهيئات التدقيق الأمريكية والدولية. يتم إجراء التدقيق لهذا التقرير وفقًا للمعايير الدولية لضمان الجودة رقم 3402 (ISAE 3402) والمعهد الأمريكي للمحاسبين القانونيين المعتمدين (AICPA): AT 801 (والمعروف سابقًا باسم SSAE 16).

مواءمة السياسة الأمنية والتحول الرقمي والنمو الاقتصادي

يجب تطوير السياسات لمواكبة الواقع المتغير للتكنولوجيا والعالم الذي تساعد على إنشائه. وإلا فقد تواصل الحكومات التخلف عن مواكبة التطورات فيما يتعلق بترقية عملياتها وتقديم الخدمات لمواطنيها واستخدام أحدث الحلول وأكثرها أمانًا. يصف هذا القسم كيفية قيام AWS بتحقيق أهداف الأمن الضمنية لمتطلبات إقامة البيانات لتقليل مخاوف صانعي السياسات. كما يستكشف التحديات الاقتصادية وتحديات تحديث تكنولوجيا المعلومات المرتبطة بإقامة البيانات واعتبارات السياسة لتطوير استخدام السحابة بشكل آمن في القطاع العام.

تحديات القطاعين التجاري والعام فيما يتعلق بإقامة البيانات

يجب على الحكومات النظر في كيفية مساهمة سياساتها الوطنية في النهوض بالنمو الاقتصادي وفرص تنمية القوى العاملة التي يتم تمكينها عبر الخدمات السحابية الفائقة أو إعاقة تلك الفرص. يمكن أن تكون هناك آثار سلبية ضخمة لتنفيذ متطلبات إقامة البيانات، مثل:

- **تأثير سلبي حاد على جهود التوسع التجاري متعدد الجنسيات في الأعمال التجارية المحلية** - نظرًا إلى نمو الأعمال التجارية وتوسعها خارج نطاق العمليات الإقليمية، فمن الضروري أن تتوفر لها إمكانية الوصول إلى الموارد ذات النطاق العالمي. ويحد تقييد الوصول إلى خدمات مزودي الخدمات السحابية الفائقة بشكل كبير من مستوى تجربة المستخدم التي يمكن أن توفرها أي شركة لقاعدة عملائها العالمية.

- **خيارات تكرار جغرافي محدودة مقارنة مناطق مزودي الخدمات السحابية العالمية**- بالنسبة إلى الحكومات والشركات التجارية، يكون ضمان التكرار في حالة فشل التشغيل بسبب حدوث كارثة أو ظروف أخرى أمرًا حيويًا لضمان الاستقرار. إن وجود عمليات مجمعة في دولة واحدة فقط يعرضالمؤسسة إلى مستوى من المخاطر قد يفوق المخاوف المرتبطة بالوصول إلى البيانات بشكل كبير.

- **البنى مرتفعة التكلفة اللازمة لاستيعاب المتطلبات الصارمة** - تتطلب بيئات "السحابة" المصممة لمستخدم واحد أو مجتمع مستوى من التسعير لضمان الاستدامة التشغيلية قد يقلل فعليًا من القدرة على توفير الإمكانات الإضافية اللازمة لضمان تحقيق الدفاع بشكل معمّق.

تعد تكنولوجيا السحابة العامل المساعد لتحقيق التطورات في القطاعين التجاري والعام، وسيؤثر مدى قيام الحكومات بدعم مبدأ تدفقات البيانات عبر الحدود أو معارضته في قوة اقتصادياتها المحلية وقدرتها على التنافس في الأسواق العالمية.

الأثر التجاري

إن تمكين التدفق الحر للبيانات عبر الحدود له أثر إيجابي نهائي كبير على الاقتصاد العالمي. تؤكد الدراسات الحديثة التي أجرتها مؤسسات الأبحاث المختلفة هذا الأثر، وتتجاوز الأمر لتسليط الضوء على تكلفة فرض حواجز على تدفقات البيانات. قدر تقرير أعده معهد ماكنزي العالمي في فبراير 2016 أن تدفقات البيانات عبر الحدود ساهمت بنحو 2.8 تريليون دولار في الاقتصاد العالمي في عام 2014 [26] عبر تمكين

---

26 http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

تدفق السلع والخدمات والموارد الأخرى. تقدر التقارير أن هذا الرقم قد يصل إلى 11 تريليون دولار بحلول عام 2025. وتدفع الحكومات التي تتطلب توطين البيانات والحد من التدفقات الاقتصادية عبر الحدود ثمنًا باهظًا. أصدر المركز الأوروبي للاقتصاد السياسي الدولي (ECIPE)، وهو مركز أبحاث سياسي مستقل، دراسة حول التأثير الاقتصادي لمتطلبات توطين البيانات التي تميز ضد الموردين الأجانب في سبع ولايات قضائية: البرازيل والصين والاتحاد الأوروبي والهند وإندونيسيا وكوريا الجنوبية وفيتنام.[27] خلص بحثهم إلى أن القيود من جانب واحد على تدفق البيانات عبر الحدود والوصول إلى الأسواق الأجنبية تؤثر سلبًا على النمو الاقتصادي والانتعاش لأنها تحد من الوصول إلى الأسعار التنافسية ونمو الوظائف في العديد من قطاعات الخدمات والسلع وفرص الاستثمار. وقد لاحظت الدراسة أن متطلبات إقامة البيانات لا تؤثر في تدفق البيانات فحسب، لكنها تؤثر أيضًا في مجموعة أكبر من فرص التوسع التجاري التي تعتمد على تدفقات البيانات عبر الحدود.

قامت دراسة مشابهة أجراها البنك الدولي بدراسة ست دول نامية والدول الأعضاء في الاتحاد الأوروبي وعددها 28 دولة، ووصلت إلى أن متطلبات توطين البيانات قد تقلل من الناتج المحلي الإجمالي بنسبة تصل إلى 1.7 بالمائة والاستثمارات بنسبة تصل إلى 4.2 بالمائة والصادرات بنسبة 1.7 بالمائة.[28] يظهر هذا الأثر أكثر وضوحًا على قطاعات الأعمال التجارية الصغيرة والشركات الناشئة. من خلال استخدام السحابة على سبيل المثال، يمكن للأفراد والشركات الصغيرة إلى متوسطة الحجم (SMEs) الوصول إلى موارد تكنولوجيا المعلومات بتكلفة وحجم لم يكونا متاحين سابقًا إلا للكيانات ذات رأس المال الضخم. تعد الشركات الصغيرة إلى متوسطة الحجم بمنزلة المحركات الرئيسية لتوفير فرص عمل جديدة. تقلل الحوسبة السحابية من الحواجز أمام إنشاء الشركات والوصول إلى الأسواق، ما يتيح تأسيس المزيد من الشركات الناشئة، والذي يؤدي بدوره في نهاية الأمر إلى توفير مزيدٍ من فرص العمل. ومع ذلك، فوفقًا للمفوضية الأوروبية يمكن لشركات التكنولوجيا مثل مزودي الخدمات السحابية أن تدفع تكاليف ضخمة للتكيف مع مختلف القوانين الوطنية، ما يجعل تكاليف البيع على الإنترنت تتجاوز الفوائد. ومؤخرًا، في مايو 2017، توصلت مؤسسة تكنولوجيا المعلومات والابتكار، وهي معهد أبحاث غير حزبي، بشكل مستقل إلى نتائج مماثلة.[29]

---

27 المركز الأوروبي للاقتصاد السياسي الدولي (ECIPE): "تكاليف توطين البيانات: نيران صديقة على الانتعاش الاقتصادي ". http://www2.itif.org/2015-cross-border-data-flows.pdf?_ga=1.8208626.1580578791.1473954628.

28 http://documents.worldbank.org/curated/en/961621467994698644/pdf/102724-WDR-WDR2016Overview-ENGLISH-394840B-OUO-9.pdf -WebResBox

29 نايجل كوري ، "تدفقات البيانات عبر الحدود: أين العوائق وما تكلفة ذلك؟ " مؤسسة تكنولوجيا المعلومات والابتكار (مايو 2017) http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.243762501.1722557619.1508762047- 1611916082.1508762047.

1

يتمثل الاستنتاج الرئيسي المتطابق عبر جميع هذه الدراسات في أن حظر تدفقات البيانات عبر الحدود في شكل متطلبات إقامة البيانات قد يؤثر في النمو الاقتصادي المحلي والإقليمي والقدرة على التنافس في الأسواق العالمية، علاوة على التأثير الأكبر الذي تتحمله الشركات الصغيرة إلى متوسطة الحجم. لا يعد النظام الآمن في الاتحاد الأوروبي أكثر أو أقل أمنًا من
نظام مصمم بشكل مماثل في أمريكا اللاتينية. تعتقد الحكومات بشكل خاطئ أن حماية البيانات لا تعتمد بشكل عام على مكان تخزين المعلومات، وإنما على التدابير المستخدمة لتأمين البيانات. عادة لا يكون الموقع الفعلي ذا صلة بشكل عام نظرًا إلى أن مراكز البيانات دائمًا ما تكون مرتبطة بشبكات يسهل الوصول إليها على نطاق واسع، ومن ثم يعتمد الأمن الفعلي على الممارسات والعمليات التقنية والتشغيلية والإدارية التي ينفذها مزودو الخدمات السحابية والعملاء.[30]

تكاليف تشغيل مراكز البيانات داخل الدولة حصريًا

قيّمت دراسة أجرتها شركة متخصصة في أمن المعلومات في عام 2015 كيف يكون نموذج مركز البيانات داخل الدولة أكثر تكلفة مقارنة بالاستفادة من مزودي الخدمات السحابية العالميين. ووجدت الدراسة أن تكلفة الخدمات السحابية قد تزيد بشكل ضخم بسبب توطين البيانات، وفقًا لمدى توافر الخدمات البديلة. اكتشفت الدراسة ما يأتي:

- إذا كانت البرازيل قد قامت بتشريع توطين البيانات كجزء من "قانون حقوق الإنترنت" الصادر عام 2014، لكان على الشركات دفع مبالغ أكثر بنسبة 54 بالمائة في المتوسط للاستفادة من خدمات السحابة (من جميع الفئات) من مزودي الخدمات السحابية المحليين مقارنة بالأسعار المنخفضة في جميع أنحاء العالم.
- إذا كان الاتحاد الأوروبي قد قام بتشريع توطين البيانات، لكانت الشركات ستظل مضطرة إلى دفع تكلفة أكبر بنسبة تصل إلى 36 بالمائة لاستخدام خدمات مماثلة يقدمها مزودو الخدمات السحابية الفائقة. وفي وقت إجراء الدراسة كانت بعض مراكز البيانات الأقل تكلفة موجودة في الاتحاد الأوروبي.[29]

تأثير القطاع العام

يمكن للدول التي تفرض حواجز على تدفقات البيانات أن تحد من قدرة مواطنيها على الاستفادة من الخدمات المبتكرة التي تساعد على تحسين جودة الحياة وتقديم الخدمات الحكومية. على سبيل المثال، تتطلب تطبيقات الذكاء الاصطناعي وتعلم الآلة (AI/ML) بنية تحتية مخصصة لتحقيق الأداء الأمثل، [32]وفي حين يواصل مزودو الخدمات السحابية العالميون توسيع نطاق مراكز البيانات الخاصة بهم، فمن غير الواقعي افتراض إنشاء مراكز البيانات في كل دولة. ومن ثم، فمع تزايد استخدام AI/ML لتحسين الخدمات، مثل توقعات الرعاية الصحية والتنبؤ بحالة الطقس من أجل الاستعداد لحالات الطوارئ، سيتأخر المواطنون في الدول التي تحدد متطلبات صارمة إقامة البيانات في الحصول على التطورات التكنولوجية الحديثة في الخدمات الموجهة للمواطنين.

30 المرجع نفسه الصفحة 4، تستخلص هذه الوثيقة استنتاجات مماثلة بصورة مستقلة.

31 http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.51021357.566718019.1510350061-1611916082.1508762047

32 على سبيل المثال، الأنظمة التي تتميز بإمكانات وحدة معالجة رسومات ذات أغراض عامة ومصفوفات بوابات قابلة للبرمجة الميدانية (FPGA).

هناك أيضًا تكاليف اجتماعية واقتصادية متعاقبة للحد من تدفقات البيانات، ولا سيما فيما يتعلق بالقدرة التنافسية التجارية وتطوير القوى العاملة. نظرًا إلى أن التكنولوجيا السحابية أصبحت أكثر انتشارًا وارتباطًا بالتقدم الاقتصادي، ستصبح التجارة الرقمية (والحد من الحواجز المفروضة عليها) أولوية قصوى للحكومات. وستصبح الدول التي تسمح بتدفقات البيانات الحرة في وضع أفضل نظرًا إلى وصولها إلى التكنولوجيا الرائدة، الأمر الذي سيؤثر بدوره في تحديث خدمات القطاعين التجاري والعام وتحسين إنتاجية العمال والتعجيل بزيادة الوظائف والمهارات المحلية عبر القطاعات. أما الدول التي تقيد تدفقات البيانات والتجارة الرقمية، فستجد نفسها غير قادرة على المنافسة بمرور الوقت. على سبيل المثال، سيكون من الصعب الحصول على المجموعة الكاملة من المزايا المرتبطة بإنترنت الأشياء لتمكين
الزراعة أو الصناعة أو إنشاء المدن "الذكية" بسبب سياسات التقييد التي تفرض حدودًا على تحليلات البيانات الضخمة أو تعلم الآلة أو غيرها من الميزات التي يتم توفيرها عبر حركة البيانات الحرة والآمنة في الوقت نفسه.

يوجد طلب متزايد ومستمر لمهارات الحوسبة السحابية في مجالات رئيسية مثل أمن التطبيقات وتطوير تطبيقات المؤسسات السحابية وتحول المؤسسات للحوسبة السحابية والبيانات الضخمة. -الولايات المتحدة تشير تقارير مكتب إحصاءات العمل الأمريكي إلى أنه من المتوقع زيادة حجم الطلب المقدر على الوظائف في قطاع أمن المعلومات بمعدل 37% في الفترة من 2012 إلى 2022. ولاستيفاء الحاجة إلى وظائف جديدة، سيتعين على الحكومات الاستثمار لتوفير فرص التعليم والتدريب للأفراد لاكتساب المهارات التكنولوجية.

ستؤدي القيود المفروضة على الوصول إلى أنواع خدمات تكنولوجيا المعلومات المتطورة التي يقدمها مزودو الخدمات السحابية الفائقة أيضًا إلى وجود فجوة دائمة في تطوير قوى عاملة ذات مهارات عالية وذكاء تقني مرتفع والحفاظ عليها. ويرجع هذا إلى أن قدرة القوى العاملة ترتبط بالتطور التكنولوجي للمؤسسة، الذي يعتمد بدوره على قدرة تلك المؤسسة على الوصول إلى التكنولوجيا الحديثة. يتطلب الاستخدام الفعال للتكنولوجيا الحديثة قوى عاملة ذات مهارات متكافئة لاستخدام تلك التكنولوجيا. نظرًا إلى
زيادة الابتكار وسرعته فيما يتعلق بالخدمات السحابية، توجد فجوة معروفة ومتزايدة في المهارات. وقد تأخرت الحكومات، على وجه الخصوص،
بشكل ملحوظ في سباق الحصول على قاعدة من الخبراء الذين لا غنى عنهم لتحديث التطبيقات وفي الوقت نفسه حماية معلومات القطاع العام ونظمه من الخصوم شديدي التطور والانتهاكات التي يزداد معدل تكرارها وتأثيرها.

اعتبارات خاصة بوضع سياسات إقامة البيانات

كما تمت المناقشة أعلاه، لا يزال من الممكن تحقيق السيادة التنظيمية للدولة القومية على البيانات مع الاستفادة من مزايا التكلفة والأمن التي يقدمها مزودو الخدمات السحابية الفائقة مثل AWS. توفر تدابير الأمن المستخدمة بشكل واسع الانتشار في خدمات AWS، والتي تم التحقق منها عبر عمليات تدقيق من جهة خارجية، مستوى مرتفعًا من الضمان لمنع الحوادث الخطيرة للوصول غير القانوني إلى البيانات ومواجهتها.

نحن نشجع الحكومات على النظر في السياسات الآتية لتحقيق أهداف الأمن المقترنة بإقامة البيانات.

1. تطوير سياسات ومتطلبات تتيح استخدام منشآت معالجة البيانات خارج الدولة في حالة معالجة البيانات وتخزينها في بيئة سحابية فائقة حديثة وآمنة للغاية. كما يمكن للعملاء اختيار مواقع تتمتع بقوانين حماية بيانات تتوافق مع تلك الخاصة بهم وحيث توجد اتفاقيات نقل بيانات سارية بالفعل.
2. مواءمة السياسات الوطنية والمتطلبات التنظيمية مع مبدأ حرية حركة البيانات عبر الحدود لتحقيق التوازن الفعال بين أغراض الأمن والاقتصاد وتحديث تكنولوجيا المعلومات.

3. تقييم نماذج نقل البيانات، مثل درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة، والبنود التعاقدية القياسية، مثل بنود نموذج الاتحاد الأوروبي التي تم اعتمادها بواسطة سلطات حماية البيانات في الاتحاد الأوروبي ويمكن استخدامها في الاتفاقيات بين مزودي الخدمة وعملائهم لضمان أن أي بيانات شخصية تغادر المنطقة الاقتصادية الأوروبيةسيتم نقلها وفقًا للائحة العامة لحماية البيانات (GDPR).[33] توفر هذه الأنواع من اتفاقيات نقل البيانات ضمانات بقيام مزودي الخدمات السحابية الفائقة بحماية البيانات الشخصية بشكل مسؤول كما توفر وسائل معتمدة سابقًا لدعم تدفق وحماية البيانات دوليًا بطريقة آمنة ومتوافقة.

4. التأكد من قيام مزودي الخدمات السحابية والمتعاقدين من الجهات الخارجية بتطبيق ضوابط أمن قوية لمواجهة الوصول غير المصرح به بواسطة جهات خارجية إلى البيانات والأنظمة والأصول من خلال الحصول على اعتمادات جهات خارجية معترف بها دوليًا (مثل ISO 27001، ISO 27018، معيار ضوابط تنظيم الخدمة ومعيار أمان بيانات صناعة بطاقات الدفع، وما شابه ذلك).

5. تصنيف البيانات وتحديد أدوار معالجة البيانات والمسؤوليات المرتبطة بها لتحديد التزامات حماية البيانات المناسبة لكل طرف. يجب على الحكومات تحديد نموذج النشر السحابي المناسب وفقًا لاحتياجاتها الخاصة ونوع البيانات التي تعالجها وحجم المخاطر. وبالنسبة إلى مجموعة البيانات الأقل استهدافًا، المصنفة كبيانات شديدة الحساسية، قد تجد الحكومات أن الخيارات الهجينة أكثر ملاءمة.[1]

تهدف اللائحة العامة لحماية البيانات الصادرة عن الاتحاد الأوروبي، والتي أصبحت سارية في مايو 2018، إلى مواءمة قوانين حماية البيانات في جميع أنحاء الاتحاد الأوروبي (EU) من خلال تطبيق قانون واحد لحماية البيانات يكون ملزمًا في كل دولة من الدول الأعضاء. ولا تتطلب اللائحة العامة لحماية البيانات وجود قوانين لإقامة البيانات داخل الاتحاد الأوروبي، بل تدعم أطر العمل القانونية في شكل نماذج نقل البيانات والبنود التعاقدية القياسية (أي بنود نموذج الاتحاد الأوروبي) لتشجيع تدفقات البيانات عبر الأقاليم.

تنص المادة 45 من اللائحة العامة لحماية البيانات على المبدأ المتمثل في أنه يجوز إجراء عمليات نقل البيانات الشخصية إلى دولة ثالثة أو مؤسسة دولية إذا كانت الدولة الثالثة أو المنطقة أو قطاع معين واحد أو أكثر داخل تلك الدولة، أو المؤسسة الدولية المعنية تضمن مستوى كافيًا من الحماية. لتحقيق ذلك، يجوز للحكومات:

- تغيير قانون حماية البيانات الساري لديها والاشتراك في مناقشات حول الكفاية مع الدول الأخرى. على سبيل المثال، تعمل نيوزيلندا على التوصل إلى قرار كفاية من جانب مفوضية الاتحاد الأوروبي.
- إنشاء أطر عمل ثنائية مثل درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة .

يجب على الحكومات أيضًا النظر في الاستفادة من معيار ISO 27018 لتحديد أدوار المتحكم في البيانات ومعالج البيانات. يمكن للحكومات العمل مع مزودي الخدمات السحابية لفهم مسؤوليات حماية البيانات وتطبيقها بشكل وافٍ على كلٍ من المتحكم في البيانات ومعالج البيانات لكل نموذج من نماذج الخدمات السحابية.

6. ضمان فهم العملاء لخدمات الأمن الخاصة بتشفير البيانات وتنفيذها. وقد قامتAWS بتصميم خدمات تشفير رائدة توفر للعملاء القدرة على التحكم الكامل في مفاتيح التشفير- توفر AWS للعملاء خيارًا لتشفير البيانات باستخدام مفاتيحهم الخاصة التي يمكن تخزينها خارج AWS أو بشكل آمن داخل عروض المنتجات، مما يتيح لهم التحكم في مفاتيحهم واستخدام البيانات مع

[1] توفر AWS Outposts حلًا سحابيًا هجينا لأحمال العمل التي تتطلب إدارة البيانات محليًا.

استيفاء التزامات الأمن والامتثال الصارمة.

7. المشاركة في جهود ثنائية ومتعددة الأطراف لتحديثإجراء اتفاقية المساعدة القانونية المتبادلة (MLAT) للموازنة بين احتياجات الحكومات إلى الحصول بشكل عاجل على الأدلة اللازمة في التحقيقات والملاحقات الخاصة وبين حق أي فرد في التمتع بخصوصية المحتوى الإلكتروني الذي يملكه. نحن ندعم التشريعات التي من شأنها تحديث الخصوصية ووصول سلطات إنفاذ القانون إلى الاتصالات الإلكترونية -- محليًا ودوليًا على حد سواء. كما نشجع الحكومات على مراجعة قوانينها الوطنية وتحديثها لتحديد الأدوار والمسؤوليات والآليات التي تحكم الاستخدام القانوني للبيانات بشكل يتسق مع مبادئ إجراء اتفاقية المساعدة القانونية المتبادلة.

الخاتمة

بينما قد تشعر الحكومات بزيادة الأمان عند فرض متطلبات إقامة البيانات على البيانات التي تتم معالجتها وتخزينها في منشآت تكنولوجيا المعلومات المحلية لأنها تتيح إمكانية التواجد المادي بالقرب من تلك البيانات والتحكم فيها، إلا أن التقييم المتعمق أظهر أن تقييد خدمات تكنولوجيا المعلومات على الدائرة القضائية المحلية فقط لا يوفر مستوى إجماليًا أفضل لأمن البيانات. من منظور تجنب المخاطر والحصول على الفوائد، يمكن لمزودي الخدمات السحابية الفائقة، مثل AWS المساعدة بشكل أفضل في إدارة مخاطر الأمن على الإنترنت مع الحد من خطر استخدام الحكومات الأجنبية للبيانات. تحتاج الحكومات أيضًا إلى مراعاة المفاضلات المهمة المقترنة بمتطلبات إقامة البيانات. لن تتنازل الحكومات التي تفرض متطلبات مقيدة على إقامة البيانات عن إمكانية الوصول إلى عدد من أكبر بيئات الحوسبة الأكثر أمانًا على وجه الأرض فحسب، بل سيكون لزامًا عليها، بخلاف مسألة الأمن، أن تتعامل مع التأخر الدائم في الوصول إلى التكنولوجيا المتطورة ومنخفضة التكلفة اللازمة لتحقيق التحول الرقمي الذي تحتاجه. نحن نشجع الحكومات على إعادة تقييم أهداف الأمن التي تحققها بالفعل عبر فرض قيود على توطين البيانات فيما يتعلق بالتكاليف الهائلة لزيادة فرص تعزيز الاقتصاد
وتحديث تكنولوجيا المعلومات وتكلفة الفرصة البديلة للأمن ولا تقتصر إمكانات الأمن المقدمة من مزودي الخدمات السحابية الفائقة على التخلص من المخاوف البارزة فحسب، بل توفر مستوى أعلى من الأمن مقارنة بالمنشآت المحلية أو التي تم التعاقد معها محليًا. يمكن للحلول السياسية، مثل اتفاقيات نقل البيانات والاستفادة من اعتمادات الأمن من الكيانات الدولية الشهيرة، أن تمثل وسيلة كافية لتحقيق أهداف إقامة البيانات في أثناء دعم أهداف التحول الرقمي للقطاع العام.

---

33 أصبح ملحق معالجة البيانات الخاص باللائحة العامة لحماية البيانات لشركة AWS والذي يتضمن بنود نموذج الاتحاد الأوروبي الآن جزءًا من شروط الخدمة الخاصة بنا عبر الإنترنت. يعني هذا أن جميع عملاء AWS على مستوى العالم يمكنهم الاعتماد على شروط ملحق معالجة البيانات الخاص باللائحة العامة لحماية البيانات لشركة AWS متى استفادوا من خدمات AWSلمعالجة البيانات الشخصية بموجب اللائحة العامة لحماية البيانات. يتوفر مزيد من المعلومات حول نهج AWS للامتثال لمتطلبات اللائحة العامة لحماية البيانات هنا: https://aws.amazon.com/ compliance/gdpr-center/