الأمن السيبراني السحابي

حجر الأساس للنمو الاقتصادي الشامل في العصر الرقمي

القمة العالمية للحكومات 2024

بالتعاون مع

Deloitte.

المحتويات :

ملخص

بعدما أصبحت الخدمات الرقمية عنصراً محورياً في التنمية الاقتصادية، بدأ الأمن السيبراني للحوسبة السحابية يكتسب أهمية أكبر، أكثر من أي وقت مضى.
يستكشف التقرير كيف يدعم الأمن السيبراني للحوسبة السحابية النمو الاقتصادي الشامل من خلال حماية البنى التحتية، والبيانات، والخدمات الضرورية لمبادرات الحكومة الرقمية. تهدف هذه الدراسة إلى تسليط الضوء على التحديات والفرص ضمن أطر الأمن السيبراني السحابي التي تعزز العدالة في حصول الجميع على الخدمات الحكومية؛ وفي الوقت نفسه، تُحفّز النشاط الاقتصادي من خلال اعتماد الخدمات السحابية بشكلٍ آمن. تُقدّم هذه الدراسة، من خلال إجراء تحليل شامل لإجراءات الأمن السيبراني الحالية، رؤى فعالة حول كيفية تطوير العمل الحكومي، لتتمكن الجهات الحكومية من تطبيق بروتوكولات قوية للأمن السحابي تضمن استفادة أفراد المجتمع من الخدمات الرقمية الآمنة بغض النظر عن وضعهم الاجتماعي والاقتصادي. لن يقتصر هذا البحث على تحديد الاستراتيجيات التي تمنع وقوع تحديات سيبرانية في الخدمات السحابية فقط، بل سيبحث في دور الأمن السيبراني في تعزيز الاقتصاد الرقمي القوي حيث تعمل الثقة والتكامل على تعزيز المشاركة والابتكار. يُقدّم هذا التقرير في خلاصته خارطة طريق لصنّاع السياسات وقادة تقنية المعلومات تساعدهم في وضع سياسات أمن سيبراني ترتكز على الخدمات السحابية بحيث تتوافق مع الهدف المزدوج المتمثل في تعزيز النمو الاقتصادي وضمان مجتمع رقمي شامل.
تُلخص الأقسام التالية الهدف الرئيسي من هذا التقرير، وهو تسليط الضوء على أهمية الأمن السيبراني السحابي في التحوّل الرقمي في سياق عملية التحوّل الرقمي التي تشهدها المملكة العربية السعودية، بالإضافة إلى قدرة الأمن السيبراني السحابي على دفع النمو الاقتصادي الشامل للمملكة.

بعدما أصبحت الخدمات الرقمية عنصراً محورياً في التنمية الاقتصادية، بدأ الأمن السيبراني للحوسبة السحابية يكتسب أهمية كبرى، أكثر من أي وقت مضى.

التحوّل الرقمي على المستوى العالمي

التحوّل الرقمي على المستوى العالمي

يشير ظهور العصر الرقمي إلى بداية التحوّل في تاريخ الاقتصاد العالمي.
يتناول هذا القسم من التقرير عملية الرقمنة السريعة للاقتصادات حول العالم وظهور التقنيات السحابية، ما يؤكد تأثيرها العميق على الشركات والحكومات والمجتمعات.

على الصعيد العالمي، أدى ظهور التقنيات الرقمية إلى إعادة تشكيل الاقتصادات، حيث أوجدت أسواقاً جديدة، وأحدثت اضطرابات في الأسواق القائمة. على سبيل المثال، سمح ظهور الإنترنت عالي السرعة وتقنيات الهاتف المحمول والحوسبة المتقدمة برقمنة الخدمات والمنتجات، ما أدى إلى وجود إجراءات عمل أكثر كفاءة، وتوسيع قنوات الوصول إلى الأسواق العالمية. نتج عن ذلك تحوّل كبير من الاقتصادات التقليدية القائمة على الصناعة إلى اقتصادات أخرى تعتمد بشكل متزايد على التكنولوجيا والمعلومات الرقمية. بدا هذا التحوّل جليّاً في ظهور التجارة الإلكترونية، والخدمات الحكومية، والخدمات المصرفية الرقمية، والتعليم عبر الإنترنت، والتطبيب عن بُعد، والتي أصبحت جميعها جزءاً لا يتجزأ من الحياة اليومية.

تميزت هذه الثورة الرقمية بشكل رئيسي بظهور التقنيات السحابية واعتمادها بسرعة. عملت الحوسبة السحابية على توفير إمكانية الحصول على موارد الحوسبة القوية للجميع، ما سمح للشركات من جميع الأحجام بالتوسع والابتكار والتنافس في السوق العالمية، كما قدمت الحوسبة السحابية حلاً مرناً وفعالاً من حيث التكلفة لتخزين كميات هائلة من البيانات ومعالجتها وإدارتها، وهو أمر بالغ الأهمية في عالم يعتمد على البيانات. تميّزت قابلية التوسع في الخدمات السحابية بأنها تحويلية بشكل خاص، ما مكّن الشركات الناشئة من نشر خدماتها بسرعة وإنشاء شركات تتكيف بشكل فعّال مع التحولات في السوق.

مما لا شك فيه أن التأثير الاقتصادي للرقمنة والتقنيات السحابية كان كبيراً وجوهرياً نظراً لأنها كانت بمثابة عوامل مُحفّزة لخلق وظائف جديدة في جميع القطاعات وتعزيز القدرة الإنتاجية في مختلف الصناعات. بالإضافة إلى ذلك، اضطلعت الرقمنة والتقنيات السحابية بدور حاسم في نمو اقتصاد الوظائف المؤقتة وقدمت فرص توظيف مرنة في جميع أنحاء العالم. كما أدت هذه الرقمنة إلى ظهور صناعات ونماذج أعمال جديدة كلياً, مثل خدمات البث الرقمي المتواصل، وحلول البرمجيات القائمة على الخدمات السحابية والشركات القائمة على المنصات.

كما يمكن رصد التأثيرات المهمة الأخرى للتقنيات الرقمية والحوسبة السحابية في تعزيز التواصل والتعاون على مستوى العالم، حيث تخطّت الحدود الجغرافية وسمحت بالتعاون والتواصل في الوقت الحقيقي بين القارات، الأمر الذي سهّل عمليات الشركات العالمية ومهّد الطريق إلى الابتكار وتبادل المعرفة بين الدول. باتت الخدمات السحابية الآن المنصة الافتراضية للعديد من ابتكارات الأعمال والتكنولوجيا – ما سمح بظهور كل شيء بدءاً من الذكاء الاصطناعي والتعلّم الآلي والأمن السيبراني المتقدم وإنترنت الأشياء والحوسبة الحدية.

دور الأمن السيبراني السحابي في النمو الاقتصادي

دور الأمن السيبراني السحابي في النمو الاقتصادي

في سياق العمليات الحكومية، يتعاظم دور الأمن السيبراني السحابي على خلفية زيادة مبادرات التحوّل الرقمي. تتبنى الحكومات في جميع دول العالم التقنيات الرقمية لتعزيز خدماتها الحكومية وتحسين كفاءتها وشفافيتها. يستكشف هذا القسم أهمية الأمن السيبراني السحابي من منظور حكومي، مع التركيز على دورها المحوري في حماية المصالح الوطنية وثقة الأفراد بالعصر الرقمي.

حماية البيانات الوطنية وبيانات أفراد المجتمع: بالنسبة للحكومات، يكمن الاهتمام بالأمن السيبراني السحابي بشكل رئيسي في حماية بيانات أفراد المجتمع والبيانات الوطنية الحساسة، والتي تتراوح بين تفاصيل الهوية الشخصية إلى أسرار الدولة، وبالتالي فهي تتطلب أعلى مستوى من الأمن. تمنع إجراءات الأمن السيبراني الفعالة الوصول غير المُصرّح به وانتهاكات البيانات، وهو أمر بالغ الأهمية في الحفاظ على الأمن الوطني وخصوصية الأفراد.

ضمان استمرارية الخدمات الحكومية: تعتمد الحكومات على المنصات الرقمية لتقديم الخدمات الحكومية الأساسية. يضمن الأمن السيبراني في الخدمات القائمة على السحابة صمود هذه المنصات ضد الهجمات السيبرانية، وبالتالي ضمان استمرارية تقديم الخدمات إلى أفراد المجتمع بلا انقطاع. يحظى هذا الأمر بأهمية كبيرة, لا سيما في بعض المجالات مثل الرعاية الصحية وخدمات الطوارئ والمرافق العامة حيث ينطوي انقطاع الخدمات على آثار خطيرة.

بناء الثقة في الحوكمة الرقمية: تُعتبر ثقة المجتمع أساس الحوكمة الفعالة. يجب على الحكومات، لدى تحوّلها إلى المنصات الرقمية، ضمان وجود أمن سيبراني قوي وبناء هذه الثقة والمحافظة عليها. يجب أن يطمئن أفراد المجتمع إلى أنه يتم التعامل مع بياناتهم بشكل آمن وأن الخدمات الحكومية الرقمية آمنة الاستخدام. تُعتبر هذه الثقة أمراً أساسياً في اعتماد الأفراد الخدمات الرقمية بنجاح.

الامتثال للمعايير | لقانونية والتنظيمية: تلتزم الحكومات بمعايير قانونية وتنظيمية صارمة لحماية البيانات وخصوصيتها. يضمن الأمن السيبراني السحابي الامتثال لهذه المعايير وتفادي العواقب القانونية واستخدام أفضل الممارسات في التعامل مع البيانات وحمايتها. كما يُعد هذا الامتثال بالغ الأهمية في التعاملات الدولية حيث تكون معايير أمن البيانات شرطاً رئيسياً.

تسهيل الابتكار الرقمي الآمن: تستفيد الحكومات بشكل متزايد من التقنيات الرقمية لتقديم الخدمات الحكومية المبتكرة وتحسين الكفاءة والفاعلية الداخلية. من الضروري وجود بيئات سحابية آمنة لتجريب تلك التقنيات وتنفيذها دون المساس بالأمان. يمكّن الأمان الحكومات من استكشاف مجالات عدة, مثل الذكاء الاصطناعي وتحليلات البيانات الضخمة وإنترنت الأشياء وتحسين قدراتها في الخدمات الحكومية.

التكيّف مع التحديات السيبرانية المعقدة: غالباً ما يكون القطاع الحكومي هدفاً رئيسياً للتحديات السيبرانية. ومع تطور هذه التحديات وزيادة تعقيدها، يصبح من الضروري وضع استراتيجيات الأمن السيبراني. يتعين على الحكومات اتخاذ موقف استباقي وتحديث إجراءات الأمن السيبراني وتعزيزها باستمرار في مواجهة التحديات المتطورة.

أصبح الأمن السيبراني السحابي واحداً من أهم جوانب التحوّل الرقمي للحكومات، حيث تشمل أهميته على عدة عوامل، هي: حماية البيانات الحساسة، وضمان استمرار تقديم الخدمات الحكومية، وبناء ثقة الأفراد، والامتثال للوائح والأنظمة المعمول بها، وتمكين الابتكار، ومواجهة التحديات السيبرانية المتطورة. ومع استمرار حكومات العالم في اعتماد التقنيات الرقمية، منح الأولوية للأمن السيبراني السحابي القوي لم يعد مجرد خيار فقط وإنما أصبح ضرورة لضمان تحقيق تلك الحكومات أجندتها الرقمية بشكل ناجح وآمن.

التحديات والفرص ضمن أطر الأمن السيبراني السحابي

التحديات والفرص ضمن أطر الأمن السيبراني السحابي

تنطوي أطر الأمن السيبراني السحابي في الخدمات الحكومية على تحديات وفرص في الوقت ذاته، لا سيما في سياق ضمان الحصول العادل على الخدمات الحكومية، وتحفيز النشاط الاقتصادي من خلال الاعتماد الآمن للخدمات السحابية. فيما يلي بعضاً من تلك التحديات والفرص:

أمن المنظومة: يتعين على الحكومات تأمين شبكاتها ومنظومة أمنها السيبراني بأكملها, يشمل ذلك إدارة المخاطر المرتبطة بالهجمات على سلسلة التوريد، والاعتماد السريع للخدمات السحابية، والعمل عن بُعد. إن الطبيعة المترابطة والمتشابكة لتلك الأنظمة تعني أنه عند وجود نقاط ضعف في مجال ما قد تثر نقاط الضعف هذه على الشركاء والمتعاملين والقطاعات بأكملها. على سبيل المثال، أثبت عدد من الهجمات الأخيرة مدى سرعة انتشار الهجمات في الشبكات العالمية، ما يؤثر على الجهات الحكومية والخاصة على حد سواء.

تأمين البيئات السحابية: يُطوّر القراصنة الرقميون والمتسللون أساليب عملهم بالتوازي مع تطور التكنولوجيا والحلول السحابية. وبالتالي يجب على فرق الأمن تجاوز الأساليب التقليدية لإدارة وحماية الأصول الحيوية مثل بيانات الأفراد والسجلات الحكومية. يتطلب الاعتماد السريع للخدمات السحابية وجود رؤية استراتيجية وحوكمة مناسبة لتفادي خلق نقاط ضعف جديدة.

خصوصية البيانات والمخاوف الأمنية: على الرغم من الفوائد الكبيرة التي تقدمها الخدمات السحابية، إلا أنها لا تقضي تلقائياً على المخاوف المتعلقة بسرية البيانات وأمنها. إن ضمان قيام المختصين في تقنية المعلومات والمخاطر والأمن السيبراني بإدارة الخدمات السحابية الرئيسية ومراقبتها بشكل مناسب، يعتبر أمراً بالغ الأهمية في مشهد التحديات المتطور في عالم اليوم.

أصبح الأمن السيبراني السحابي واحداً من أهم جوانب التحوّل الرقمي للحكومات، حيث تشمل أهميته: حماية البيانات الحساسة، وضمان استمرار تقديم الخدمات الحكومية، وبناء ثقة الأفراد، والامتثال للوائح والأنظمة المعمول بها، وتمكين الابتكار، ومواجهة التحديات السيبرانية المتطورة.

توصيات لصنّاع السياسات ومسؤولي أمن وتقنية المعلومات

توصيات لصنّاع السياسات ومسؤولي أمن وتقنية المعلومات

يتضمن مراحل هادفة لمساعدة صناع السياسات ومسؤولي تقنية المعلومات وإرشادهم إلى كيفية مواجهة التحديات المذكورة آنفاً في هذا التقرير، وتطوير سياسات الأمن السيبراني المرتكزة على السحابة و التي تعزز النمو الاقتصادي وتضمن في الوقت نفسه مجتمعاً رقمياً شاملاً، بالإضافة إلى تطوير السياسات الحالية لصنّاع القرار ومسؤولي تقنية المعلومات وتوسيعها إلى السحابة لمعالجة انكشاف مؤسساتهم للمخاطر.

المرحلة 1: التقييم والتخطيط الاستراتيجي

. **تقييم خط الأساس:**
- تقييم الوضع الحالي للبنية التحتية للأمن السيبراني الوطني، ومستويات تبني الحوسبة السحابية، والتكامل الرقمي.
- تحديد الفجوات في السياسات، والموارد، والقدرات الحالية.

. **وضع الأهداف:**
- وضع أهداف واضحة وقابلة للقياس للأمن السيبراني في سياق النمو الاقتصادي والتكامل الرقمي.
- تحديد مؤشرات الأداء الرئيسية لقياس التقدم المحرز.

. **تعزيز مشاركة الشركاء:**
- إشراك الشركاء المعنيين من القطاعين الحكومي والخاص ووالقطاع المجتمعي لجمع وجهات النظر المتنوعة.
- تشكيل لجنة استشارية متعددة التخصصات من أجل تقديم الاستشارات المستمرة.

المرحلة 2: تطوير السياسات

.**صياغة السياسات:**
- تطوير سياسات شاملة تركز على معايير أمن السحابة، وحماية البيانات، وقوانين الخصوصية.
- الحرص على أن تكون تلك السياسات مرنة كي تتأقلم مع التقدم التقني والتحديات المصاحبة له.

. **التوافق مع النمو الاقتصادي:**
- اعتماد الاستراتيجيات التي تشجع الابتكار والاستثمار في القطاع التقني.
- تصميم حوافز للشركات حتى تتبنى تقنيات السحابة الآمنة.

. **التركيز على التكامل الرقمي:**
- تضمين مقاييس تضمن الوصول العادل للخدمات الرقمية الآمنة. وخصوصاً للمجتمعات التي لا تحصل على الخدمات الكافية.
- تعزيز محو الأمية الرقمية والتوعية حول الأمن السيبراني.

المرحلة 3: التنفيذ وبناء القدرات

. **تخصيص الموارد:**
- تخصيص الموارد اللازمة لتنفيذ مبادرات الأمن السيبراني، بما في ذلك التمويل، والتقنية، ورأس المال البشري.

. **تطوير البنية التحتية:**
- الاستثمار في إنشاء بنية تحتية وطنية صلبة للأمن السيبراني.
- تشجيع تطوير خدمات الحوسبة السحابية المحلية الآمنة.

. **التدريب وتطوير القوى العاملة:**
- تنفيذ برامج تدريب وطنية لتطوير متخصصين مهرة في مجال الأمن السيبراني.
- تعزيز الشراكة مع المؤسسات التعليمية لضمان البدء في التطوير المقرر في الأمن السيبراني وتقنية السحابة.

المرحلة 4: المراقبة والتقييم

. **متابعة الأداء:**
- المراقبة المنتظمة للتَقدم في تنفيذ سياسات الأمن السيبراني مقارنة بمؤشرات الأداء الرئيسية.
- استخدام تحليلات البيانات لتقييم فعالية سياسات ومبادرات الأمن السيبراني.

. **آلية المراجعة / التغذية الراجعة:**
- تشكيل حلقة المراجعة مع الشركاء من أجل التحسين الدائم للسياسات.
- تعديل الاستراتيجيات وفقاً للتغييرات الاقتصادية والتكنولوجية والمجتمعية.

. **إعداد التقارير والشفافية:**
- نشر تقارير تقدم السياسات بانتظام لضمان الشفافية والمساءلة.
- مشاركة أفضل الممارسات المستفادة مع الشركاء الدوليين.

المرحلة 5: التحسين المستمر والتأقلم

. **تطور السياسة:**
- تحديث السياسات باستمرار لتعكس الرؤى الجديدة، والتقدم التكنولوجي والتحديات الناشئة.
- مواكبة اتجاهات الأمن السيبراني العالمية وتعديل السياسات المحلية وفقها.

. **التعاون الدولي:**
- المشاركة في معارض ومبادرات الأمن السيبراني العالمية لتبادل المعرفة والتعاون بشأن المعايير الدولية.
- تعزيز الشراكات العابرة للحدود من أجل اتباع نهج قوي للأمن السيبراني السحابي.

. **الوعي العام والمشاركة:**
- إطلاق حملات التوعية الوطنية لزيادة الوعي العام حول أهمية الأمن السيبراني
- تعزيز المشاركة المجتمعية في صياغة المستقبل الرقمي الآمن.

توفر خارطة الطريق هذه نهجاً منظماً لصنّاع السياسات ومسؤولي تقنية المعلومات لتطوير سياسات الأمن السيبراني المرتكزة على السحابة والتي لا تعمل على تغذية النمو الاقتصادي فقط، بل وتعزز التحول الرقمي الشامل من خلال نهج مبني على مراحل التقييم، وتطوير السياسات، والتنفيذ، والمراقبة، والتحسين المستمر، ويهدف إلى تأسيس بيئة رقمية آمنة ومرنة وعادلة.

دعوة للعمل

تأكيد الرؤية:

على ضوء الرؤية المتمثلة في "صياغة وتنفيذ سياسات الأمن السيبراني المرتكزة على السحابة والتي لا تدفع عجلة النمو الاقتصادي فحسب، بل تعزز المجتمع الرقمي الشامل"، تتجلى الضرورة المزدوجة، وهي: الأمن، وإمكانية الوصول في المشهد الرقمي سريع التطور.

لقد أكد هذا التقرير على الدور الحساس للأمن السيبراني السحابي في العمليات الحكومية، لا سيما في سياق التحول الرقمي. لقد بحثنا في التحديات والفرص التي يوفرها العصر الرقمي، مع التركيز على الحاجة إلى الأمن السيبراني القوي لحماية البيانات الحساسة، وضمان استمرار الخدمات لحكومية، وبناء ثقة المجتمعات في الحوكمة الرقمية.

توفر خارطة الطريق المذكورة أعلاه استراتيجية شاملة لصناع السياسات ومسؤولي أمن وتقنية المعلومات. وهي تحدد نهجاً على مراحل يشمل التقييم والتخطيط الاستراتيجي وتطوير السياسات، وتنفيذها، ومراقبتها، وتقييم التقدم في تنفيذها، و مواءمتها باستمرار مع مختلف التغييرات. لقد تم تصميم إطار العمل هذا ليس فقط لتلبية احتياجات الأمن السيبراني الحالية، ولكن أيضاً لمواجهة التحديات و مواكبة الابتكارات المستقبلية والتكيف معها.

دعوة للعمل:

تتطلب الرحلة نحو مستقبل رقمي آمن وشامل جهوداً متضافرة من مختلف الشركاء. إن صناع السياسات ومسؤولي أمن وتقنية المعلومات مدعوون إلى التعاون والابتكار والبقاء يقظين في سعيهم لتحقيق سياسات الأمن السيبراني القوية المرتكزة على السحابة.

إنها عملية مستمرة للتعلم والتكيف والتحسين. وبالنظر إلى المستقبل، فإن الطبيعة الديناميكية للتقنيات الرقمية ومشهد الأمن السيبراني تمثل فرصة وتحدياَ في الوقت نفسه. من خلال البقاء على دراية بالتحديات الناشئة، والاستفادة من التقنيات الجديدة، وتعزيز ثقافة الوعي بالأمن السيبراني. يمكن للحكومات تأمين حدودها الرقمية مع ضمان إتاحة فوائد التحول الرقمي لجميع شرائح المجتمع.

في الختام، لا يمكن اعتبار هذا التقرير مجرد مجموعة من الاستراتيجيات والتوصيات، بل هو مخطط للعمل ودعوة لاحتضان المستقبل الرقمي بثقة ومسؤولية. من خلال إعطاء الأولوية للأمن السيبراني السحابي والتكامل الرقمي، فإننا نمهد الطريق لمجتمع مرن ومزدهر ومنصف في العصر الرقمي.

إن صناع السياسات ومسؤولي أمن وتقنية المعلومات مدعوون إلى التعاون والابتكار والبقاء يقظين في سعيهم لتحقيق سياسات الأمن السيبراني القوية المرتكزة على السحابة. إنها عملية مستمرة للتعلم والتكيف والتحسين.

WORLD GOVERNMENTS SUMMIT

JOIN THE CONVERSATION

@WorldGovSummit

www.worldgovernmentssummit.org