Jordan Economic Forum | JEF
المنتدى الإقتصادي الأردني

الأردن في مؤشر
الأمن السيبراني العالمي (GCI)

ورقة حقائق صادرة عن المنتدى الاقتصادي الأردني

المقدمة

يشهد العالم تحولًا غير مسبوق في الاعتماد على التكنولوجيا الرقمية الحديثة، حيث أصبحت التقنيات الرقمية عنصراً أساسيًا في عمليات الحكومات والشركات والأفراد، ومع تزايد هذا الاعتماد واتساع قاعدة مستخدمي الانترنت وبأكثر من 5.4 مليار شخص، ظهرت التهديدات السيبرانية كأحد التحديات الرئيسية التي تؤثر على سلامة وأمن المعلومات والبنية التحتية الرقمية.

يعد الأمن السيبراني أمرًا بالغ الأهمية للمؤسسات المالية، حيث يساهم في حماية البيانات المالية، ومنها الاستثمارات وغيرها، وبالتالي تعزيز الثقة لدى المستثمرين والشركات، وفي عصر التقدم التكنولوجي السريع، تكون المؤسسات المالية عرضة بشكل خاص للتهديدات السيبرانية، حيث يمكن للهجمات أن تزعزع استقرار الأسواق، وتعطل الخدمات، وتقوض الثقة بين العملاء وأصحاب المصالح. تعتبر التدابير القوية للأمن السيبراني ضرورية لضمان حماية معلومات العملاء، والحفاظ على سلامة البيانات، ومنع الوصول غير المصرح به إلى الأصول المالية، ومن جانب المستثمرين، توفر البروتوكولات الصارمة للأمن السيبراني حماية لمحافظهم من الاحتيال المحتمل وتضمن إجراء المعاملات المالية بأمان. أما الشركات، فتكتسب الثقة في شركائها الماليين عندما ترى إجراءات قوية للأمن السيبراني، مما يعزز الثقة ويدعم العلاقات التجارية طويلة الأمد، من خلال إعطاء الأولوية للأمن السيبراني، ولا تقتصر المؤسسات المالية على حماية عملياتها فقط، بل تساهم أيضًا في إنشاء نظام مالي مستقر وآمن يدعم النمو والابتكار.

وقد أشار صندوق النقد الدولي في تقريره عن الإستقرار المالي العالمي الصادر في أبريل 2024، إلى أن القطاع المالي قد تعرض لأكثر من (20,000) هجوم سيبراني خلال العقدين الماضيين، مما أدى إلى خسائر مباشرة تجاوزت (12 مليار دولار). ومن الجدير بالذكر أن الخسائر الكبيرة الناتجة عن الحوادث السيبرانية قد تضاعفت أربع مرات منذ عام 2017، مع وصول الأنشطة السيبرانية الخبيثة إلى أعلى مستوياتها على الإطلاق في عام 2023، ومن الأمثلة العالمية الشهيرة، كانت شركة الشحن العملاقة مايرسك واحدة من العديد من الضحايا لهجوم برمجيات الفدية "نوت بيتيا"، الذي عطل شبكة اللوجستيات العالمية الخاصة بها، حيث تسبب الهجوم السيبراني في اضطرابات تشغيلية كبيرة، مما أجبر مايرسك على إعادة تثبيت آلاف الخوادم والأجهزة المتأثرة عبر أنظمتها، وقد أسفر ذلك عن خسارة تجاوزت (300 مليون دولار)، مما يبرز كيف أن الثغرات السيبرانية في صناعة حيوية مثل الشحن يمكن أن تعطل سلاسل التوريد العالمية وتسبب أضرارًا اقتصادية كبيرة.

في الأردن، أبدى جلالة الملك عبدالله الثاني اهتمامًا متزايدًا بتعزيز الأمن السيبراني، وهو ما تجلى في توجيهاته المستمرة للإرتقاء بالقدرات الرقمية للمملكة، وكان آخرها في كتاب التكليف السامي لحكومة الدكتور جعفر حسان، حيث شدد على ضرورة الالتزام بالجدول الزمني للتحول الرقمي في المؤسسات الحكومية ودعم جهود المركز الوطني للأمن السيبراني (NCSC) من خلال المساندة في إعداد البرنامج التنفيذي للاستراتيجية الوطنية للأمن السيبراني 2024-2028، لإرساء منظومة وطنية متطورة ومستدامة لإدارة العمليات السيبرانية تضمن الكشف المبكر والاستجابة الفاعلة للتهديدات السيبرانية، التي قد تتعرض لها المملكة.

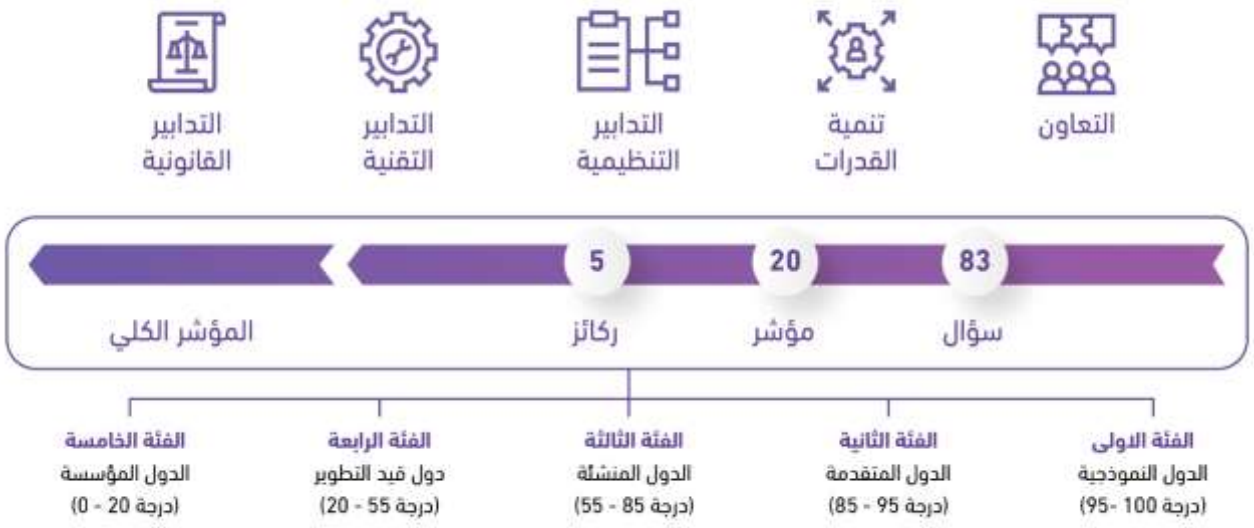
يعد إنشاء المركز الوطني للأمن السيبراني، بموجب المادة (5) من قانون الأمن السيبراني الأردني، خطوة محورية نحو بناء قدرات وطنية قادرة على التصدي للهجمات السيبرانية. ففي عام 2023، تعامل المركز مع 2455 حادثة سيبرانية، بزيادة قدرها 80% مقارنة بعام 2022.

مؤشر الأمن السيبراني العالمي

تجدر الإشارة الى أن **مؤشر الأمن السيبراني العالمي " Global Cyber Security Index"** ويُشار له (GCI) هو الإصدار الخامس الصادر عن منظمة الاتحاد الدولي للاتصالات (ITU)، المختصة بقضايا تكنولوجيا المعلومات والاتصالات، يقيس التزام 194 دولة حول العالم بمتطلبات ومعايير الأمن السيبراني استناداً الى 5 ركائز ذات العلاقة بإدارة الأمن السيبراني والممثلة بـ: **التدابير القانونية، التدابير التقنية، التدابير التنظيمية، تنمية القدرات، والتعاون**، ويتم تقييمها استناداً الى مجموعة المؤشرات الفرعية والمتمثلة بـ 20 مؤشراً يتم قياسها من خلال 83 سؤال ضمن استبيان يقدم للدول الأعضاء.

وجاء الإصدار الأخير بتغييرات رئيسية أهمها الانتقال من تصنيف الدول بناءً على ترتيب محدد الى توزيع أداء الدول المشاركة تبعاً لـ (5) مستويات (Tiers) لتقييم التزام الدول المتشابهة بناءً على نتائجها بالأمن السيبراني، مما يساعد الدول على فهم وتحديد الدول النموذجية التي يمكن الاقتداء بها لتحسين أدائها، ويُعد المستوى الأول (T1- Role-modelling) هو الأعلى والمستوى الخامس (T5- Building) هو الأدنى.

كما أن المقياس الخاص بالقيمة الكلية للمؤشر من 0% (الأضعف) الى 100% (الأفضل) وكل ركيزة من ركائز المؤشر الفرعية يكون مقياسها من 0 درجة (الأضعف) الى 20 درجة (الأفضل).

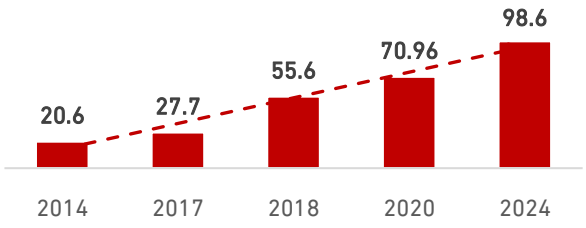


وحول أبرز نتائج مؤشر الأمن السيبراني لعام 2024، كان أداء البلدان بشكل عام أقوى في **الركيزة القانونية**، في حين جاء الأداء الأضعف في **الركيزتين تنمية القدرات والتدابير التقنية**، مما يشير على قدرة الدول على تبني أطرًا قانونية قوية، إلا أن هناك حاجة أكبر لتحسين القدرات التقنية والبشرية. وقد استطاعت 46 دولة النجاح في الانضمام إلى المستوى الأول (T1- Role-modelling) من المؤشر، من بينها 8 دول عربية (الامارات، السعودية، قطر، مصر، الأردن، البحرين، المغرب، عُمان).

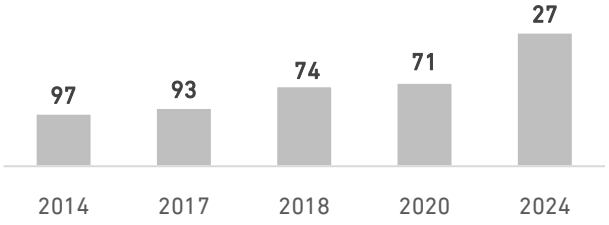
استطاعت المملكة الأردنية الهاشمية وللمرة الأولى أن تتصدر ضمن الفئة الأولى (T1- Role-modelling) والأعلى عالمياً (مجموع نقطي 95-100) في مؤشر الأمن السيبراني لعام 2024، حيث حققت قفزة نوعية بتقدمها 44 مركزاً لتحصل على المرتبة الـ (27) عالميًا بمجموع نقطي (98.6%) مقارنة مع المركز (71) عالمياً عام 2020 وبمجموع نقطي (71%)، ويعود هذا التقدم الملحوظ إلى صدور قانون الأمن السيبرانى رقم 16 لعام 2019، وإنشاء المركز الوطنى للأمن السيبراني، مما دفع العديد من المؤسسات إلى تعزيز تركيزها على الأمن السيبراني، وأسهم في تحقيق هذا التطور النوعي الكبير.

كما اعتمدت خطط ومشاريع المركز الوطنى للأمن السيبرانى فى عامى 2022-2023 على مؤشر الأمن السيبرانى العالمى (GCI)، حيث ألزم قانون الأمن السيبراني المؤسسات الحكومية بتطبيق إجراءات رقابية، وتشكيل فرق متخصصة بالاستخبارات والعمليات السيبرانية، إضافة إلى تنفيذ برامج توعية وتدريب وبناء القدرات، وإجراء البحوث والتطوير بهدف رفع مستوى الأمن السيبراني عالميًا.

درجات الأردن في مؤشر الأمن السيبراني (100%)



ترتيب الأردن في مؤشر الأمن السيبراني



المصدر: Global Cyber Security Index, 2024

وعلى صعيد المحاور الفرعية، حقق الأردن نتائج كاملة في ثلاثة من هذه المعايير وبنسبة 100% (أي بمجموع 20 درجة) في أداء المؤشر العالمي للأمن السيبراني، وهم:

1- محور **التدابير القانونيّة؛** من خلال سن وتطبيق التشريعات والقوانين لمكافحة الجرائم الإلكترونية وإصدار قانون حماية البيانات الشخصية وقوانين التراخيص والسياسات الجديدة من المركز
2- محور **تنمية القدرات؛** من خلال القدرات والتوعية، وانشاء المركز الوطني للامن السيبراني مركز العمليات الأمنية (SOC) , الذي يتعاون مع الجهات المختلفة لرصد التهديدات.
3- محور **التعاون؛** من خلال تحقيق تعاوناً مُشتركاً بين كافة مؤسسات الدولة وقطاعاتها المُختلفة وتعزيز الحوار والتنسيق مع القطاعين الخاص والحكومي محليًا والدولي مع دول مثل عمان وقطر ومصر.

وفيما يتعلق بالمحاور الفرعية الأخرى؛ ارتفع **المحور التنظيمي** بمقدار 3.52 درجة عن عام 2020، حيث حقق (20/19.22) في عام 2024، ويعزى هذا الارتفاع إلى تطبيق الاستراتيجية التي فرضها المركز، والتي تتضمن تنفيذ المبادرات المخصصة لها. أما **المحور التقني**، فقد جاء بدرجة (20/19.38) في عام 2024، بزيادة 8.64 درجات عن 10.74 في 2020، وذلك بفضل قانون المركز والمهام المسندة إليه، بالإضافة إلى تشكيل فريق وطني بالتعاون مع حوالي 10 مؤسسات من القطاعين العسكري والخاص والأكاديمي وغيرها من القطاعات.

وبمقارنة المحاور الفرعية لمجموعة الدول العربية المصنفة ضمن المستوى الأول (T1- Role-modelling)، استطاعت كل من الامارات، السعودية، قطر، ومصر أن تحقق العلامة الكاملة في جميع المؤشرات الفرعية بمجموع (20 درجة)، ويظهر الشكل أدناه ترتيب مجموعة الدول العربية ذات تصنيف المستوى الأول (T1- Role-modelling) في المؤشرات الفرعية.

ترتيب الدول العربية ذات تصنيف المستوى الأول في المؤشرات الفرعية

وعليه، يرى المنتدى الاقتصادي الأردني أنه من الضروري تحسين التدابير التنظيمية والتقنية لتعزيز البنية التحتية السيبرانية وتطوير الأطر والسياسات التي تدعم حوكمة الأمن السيبراني بفعالية. بالإضافة إلى ذلك، يجب الاستثمار في التقنيات الحديثة لزيادة كفاءة البنية التحتية السيبرانية. كما يوصي المنتدى بضرورة الإسراع في إعداد الاستراتيجية الوطنية الشاملة للأمن السيبراني على أن تكون متوافقة مع المعايير الدولية، كخطوة حاسمة لرفع تصنيف الأردن في محور التدابير التنظيمية. هذا إلى جانب تعزيز التعاون بين مؤسسات الدولة والقطاعات المختلفة لتنسيق الجهود وتحقيق تقدم ملموس ومستدام في هذا المجال.