الأمن السيبراني في الأردن

تقرير بيان حقائق

ما هو الأمن السيبراني؟

الأمن السيبراني هو مجموعة من الأدوات ،السياسات والمفاهيم الأمنية ،الضمانات والمبادئ التوجيهية ،نهج إدارة المخاطر ،الإجراءات والتدريب وأفضل الممارسات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدم (الاتحاد الدولي للاتصالات) .

فوائد الأمن السيبراني

تقليل وقت تعطل الأنظمة وفقدان البيانات؛

يحسن الإنتاجية؛

يمنع الخسارة المالية الناجمة عن الهجمات السيبرانية.

ضمان مشاركة أكثر أمنا للتجار في سلاسل القيمة العالمية؛

يحمي الملكية الفكرية.

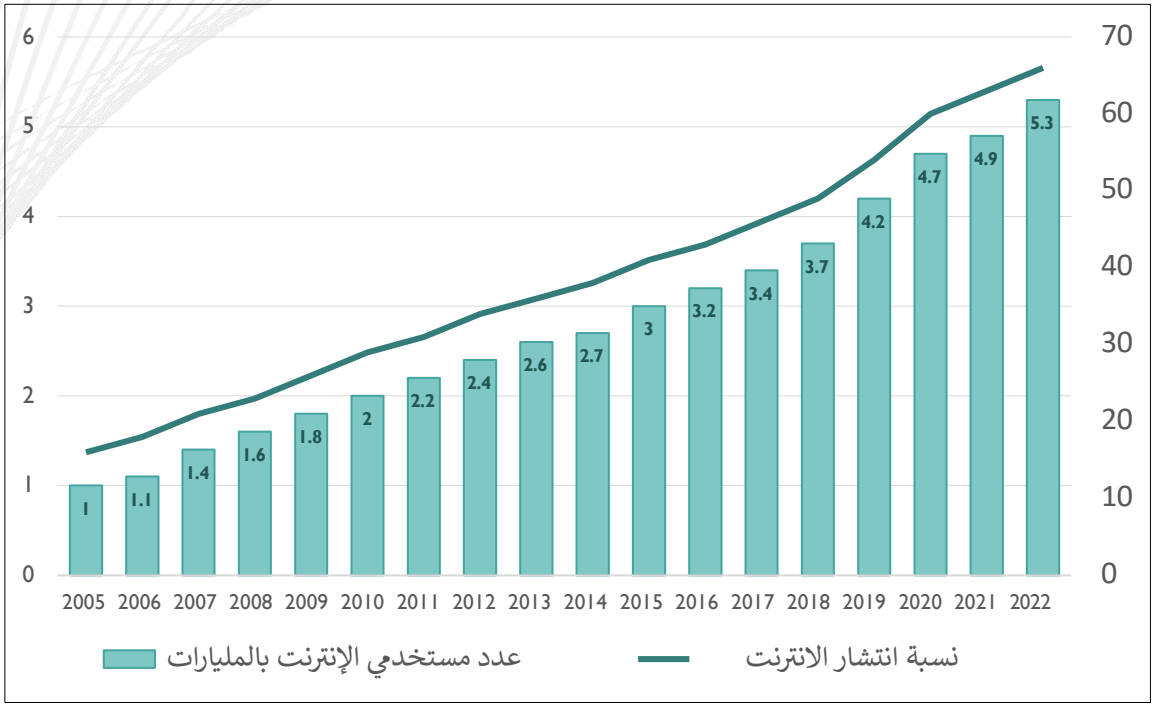
وظائف الأمن السيبراني

السرية - ضمان الوصول إلى البيانات فقط للمستلمين المقصودين؛

النزاهة - التأكد من أن البيانات أصلية ودقيقة وموثوقة؛

الجاهزية – ضمان عمل الأنظمة والشبكات والتطبيقات كما ينبغي.

معدل انتشار الإنترنت 2005 – 2022، نسبة مئوية



Source: ITU

لا يمكن القضاء على المخاطر السيبرانية بشكل كامل، ولكن يمكن تخفيف هذه المخاطر وإدارتها.

تأثير الهجمات السيبرانية

التأثير المادي: عطل في أنظمة التحكم؛

التأثير الاجتماعي: سرقة الهوية، والاحتيال في التجارة الإلكترونية، وقرصنة الويب (تشويه مواقع الويب الحكومية أو الشركات)؛

التأثير الاقتصادي: الخسارة المالية، وخسارة الإيرادات من التجارة الدولية، وفقدان الملكية الفكرية؛

تأثير المكانة و السمعة: فقدان الثقة في المنظمة/الجهة الحكومية المتضررة.

نقاط الضعف في الأنظمة الحكومية/الشركات:

التقنية: ميزات الأمان مفقودة أو غير كافية؛

البشرية: أخطاء غير مقصودة، أو تخريب متعمد؛

التنظيمية: الأخطاء التنظيمية، مثل عدم فعالية إسناد الأدوار والمسؤوليات.

كيفية تجنب الهجمات السيبرانية؟

الإطار القانوني: المؤسسات القانونية واللوائح التنظيمية في مجال الأمن السيبراني.

التدابير التقنية: الإجراءات التقنية لمنع الهجمات السيبرانية؛

التدابير التنظيمية: مؤسسات تنسيق السياسات واستراتيجيات تطوير الأمن السيبراني.

بناء القدرات: الوعي بنوع الهجمات السيبرانية واستراتيجيات للتخفيف منها؛

التعاون: الشراكة وتبادل المعلومات لأفضل الممارسات في مجال الأمن السيبراني.

مبادئ هيكل الأمن السيبراني

حماية أنظمة معالجة البيانات ضد مخاطر محددة

التعاون بين جميع أصحاب المصلحة؛

إنشاء وكالة للأمن السيبراني؛

استحداث آليات إصدار الشهادات تديرها وكالة الأمن السيبراني ؛

الاخطار بالحوادث الأمنية التي تؤثر على البيانات والبنية التحتية الحيوية؛

تنفيذ العقوبات؛

التعديل على قوانين مختلفة (مثل القانون الجنائي)؛

إدخال لوائح محايدة من الناحية التكنولوجية.

الأمن السيبراني في الأردن

- يعد قطاع تكنولوجيا المعلومات والاتصالات في الأردن من أسرع القطاعات نموا، حيث يمثل حوالي 3.8% من الناتج المحلي الإجمالي، وبإيرادات سنوية إجمالية تتجاوز 2.3 مليار دولار.
- حدد الأردن الاقتصاد الرقمي كأولوية عالية للتنمية الاجتماعية والاقتصادية للبلاد.

المركز بالنسبة الى مؤشر الأمن العالمي 2020 (GCI)

71st من بين 182 دولة

10th من 22 دولة عربية.

المصدر: مؤشر الأمن السيبراني العالمي 2020

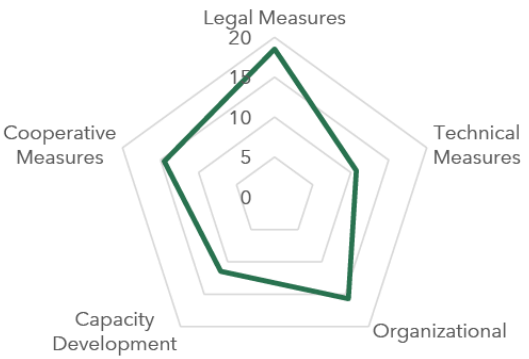
قانون الأمن السيبراني

- ينص على إجراءات تعيين السلطات المختصة ويحدد واجباتها ومسؤولياتها.
- يحدد السلطات الرئيسية المعنية بالأمن السيبراني وهي المجلس الوطني للأمن السيبراني والمركز الوطني للأمن السيبراني.

المصدر: قانون الأمن السيبراني لسنة 2019

أبرز الجهات المستهدفة للهجمات السيبرانية:

- الجيش
- المؤسسات الأمنية
- القطاع المالي
- شركات الاتصالات
- قطاع الطاقة/ شركات الكهرباء
- المؤسسات الحكومية
- سفارات الأردن في الخارج



Development Level:
Developing Country

Area(s) of Relative Strength
Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
70.96	18.53	10.74	15.70	11.47	14.51

المصدر: مؤشر الأمن السيبراني العالمي 2020

الاستراتيجية الوطنية للأمن السيبراني

- هو عمل غير ملزم ويشكل خارطة طريق للأمن السيبراني؛
- يقدم ملخصًا للتقدم المحرز في تحقيق الأهداف المنصوص عليها في الاستراتيجية الوطنية لتأمين المعلومات والأمن السيبراني لعام 2012؛
- يشير إلى تحديات الأمن السيبراني الأردني وأهدافه وأولوياته الاستراتيجية ويضع خطة التنفيذ الخاصة بها.

المصدر: الاستراتيجية الوطنية للأمن السيبراني 2018-2023

التعاون الدولي

- الأردن جزء في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
- يشارك الأردن في مشروع الجنوب السيبراني، وهو مشروع مشترك بين الاتحاد الأوروبي ومجلس أوروبا؛
- أبرم الأردن اتفاقية شراكة بينه وبين الاتحاد الأوروبي، للفترة 2021-2027 وتتضمن التزام الأطراف بتعزيز الحوار والتعاون في مجال الأمن، بما في ذلك مكافحة التطرف والإرهاب والأمن السيبراني؛
- وقع الأردن والمملكة المتحدة مذكرة تفاهم لتعزيز التعاون في مجال الأمن السيبراني.

الشركات الصغيرة والمتوسطة في الأردن والأمن السيبراني

تحديات الشركات الصغيرة والمتوسطة للأمن السيبراني :

- زيادة تهديدات الأمن السيبراني؛
- زيادة العمل عن بعد، مما يؤدي إلى بيئة عمل أقل أمانًا؛
- ارتفاع تكلفة تنفيذ تدابير الأمن السيبراني؛
- الموارد والتدريب على إجراءات ولوائح الأمن السيبراني؛
- انخفاض ميزانية الأمن السيبراني؛
- انخفاض مستوى الوعي بتأثير الهجمات السيبرانية على الأعمال.

تمثل الشركات الصغيرة والمتوسطة 98% من القطاع الخاص في الأردن

تساهم الشركات الصغيرة والمتوسطة بأكثر من 50% من الناتج المحلي الإجمالي للبلاد

توظف الشركات الصغيرة والمتوسطة 60% من القوى العاملة الأردنية

تمثل الشركات الصغيرة والمتوسطة 45% من الصادرات

من أسباب الاستثمار في الأمن السيبراني؟

يمكن أن تؤثر الهجمات السيبرانية على القدرة التنافسية للشركات الصغيرة والمتوسطة وقدرتها على التجارة، وتؤثر على مشاركتها في سلاسل القيمة الإقليمية والعالمية.

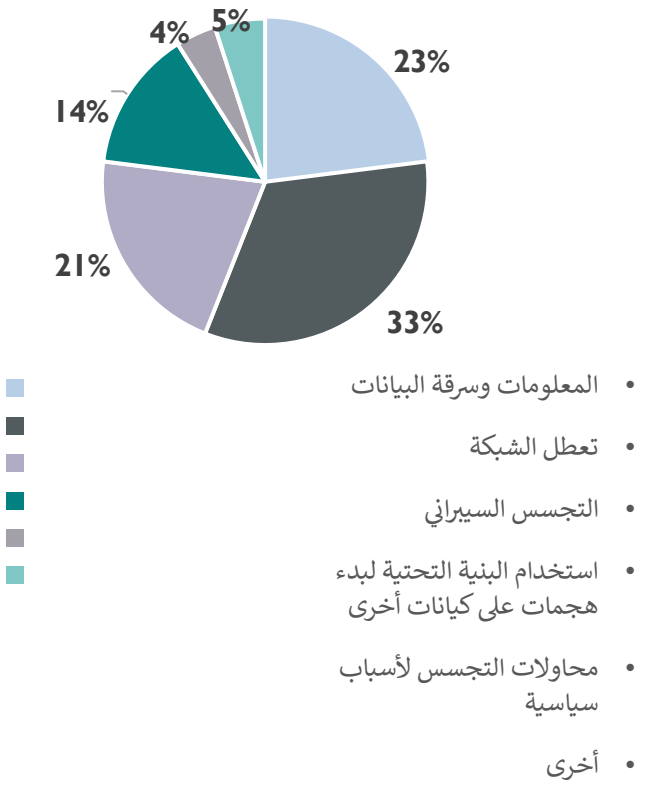
1. تؤدي متانة الحماية ضد الهجمات السيبرانية إلى زيادة ثقة العملاء في استخدام بيانات الشركة بشكل أمن.
2. يزيد الأمن السيبراني من جودة واستمرارية تقديم الخدمة / توصيل المنتج. وبالتالي المحافظة على سمعة الشركة وقدرتها التنافسية.

المصدر: دليل الأمن السيبراني للشركات الصغيرة والمتوسطة الحجم - 12 خطوة لتأمين عملك

طرق الحد من المخاطر السيبرانية

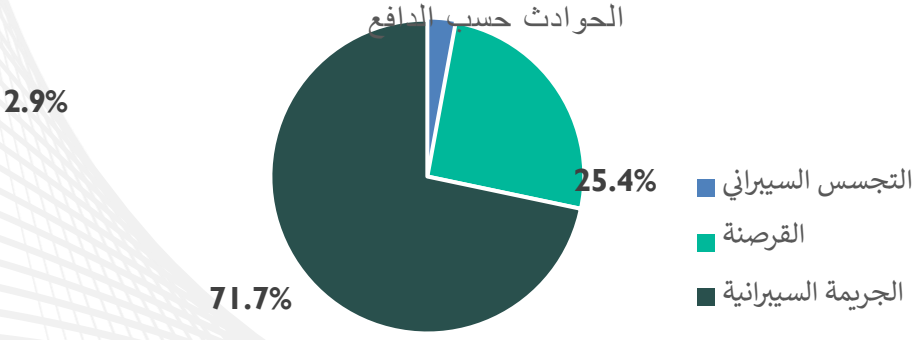
حوادث الأمن السيبراني في الأردن

في عام 2021، تعرض الأردن لـ 897 هجمة سيبرانية.



Source: The Jordan Times

في النصف الأول من عام 2022، تعامل المركز مع 544 حادثة تتعلق بالأمن السيبراني.



Source: Center's report

التعاون الدولي

- الأردن جزء في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.
- يشارك الأردن في مشروع الجنوب السيبراني، وهو مشروع مشترك بين الاتحاد الأوروبي ومجلس أوروبا؛
- أبرم الأردن اتفاقية شراكة بينه وبين الاتحاد الأوروبي، للفترة 2021-2027 وتتضمن التزام الأطراف بتعزيز الحوار والتعاون في مجال الأمن، بما في ذلك مكافحة التطرف والإرهاب والأمن السيبراني؛
- وقع الأردن والمملكة المتحدة مذكرة تفاهم لتعزيز التعاون في مجال الأمن السيبراني.

موارد إضافية

1. Global Cybersecurity Index 2020
2. Guide to developing a national cybersecurity strategy - Strategic engagement in cybersecurity
3. Cybersecurity for SMEs - Challenges and Recommendations
4. What Europe's SMEs need to do for a cyber-secure future


بيت التصدير
JORDAN EXPORTS


International
Trade
Centre


تنفيذ
giz
Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH


Kingdom of the Netherlands


التعاون
الألماني
DEUTSCHE ZUSAMMENARBEIT