الأمن السيبراني والوعي الجماهيري

يعد موضوع الحماية والأمان الرقمي أحد أبرز الموضوعات التي تهم المستخدمين العاديين للإنترنت قبل المتخصصين في مجالات تكنولوجيا المعلومات والإعلام الإلكتروني ودراسة الشبكات الاجتماعية، بالإضافة للناشطين الإلكترونيين والفاعلين الاجتماعيين الذين يتخذون من الإنترنت فضاء للحرية وملتقى للآراء المختلفة يتجاوز الحدود والأماكن الثابتة.

ويجب عمل الاحتياطات الضرورية للأمان الرقمي ضد الاختراق والتدمير التجسس والاحتيال الإلكتروني، ويجب أن يتم ذلك وفق منطق مهم وهو ما لا يدرك جله لا يترك كله، فإن وجود بعض الشوائب والأفكار غير الصالحة الموجودة على بعض المنصات الإلكترونية لا يمكن اعتباره دليلاً ضد المجال كله ولكن الفيصل في ذلك هو المستخدم الواعي أولاً.

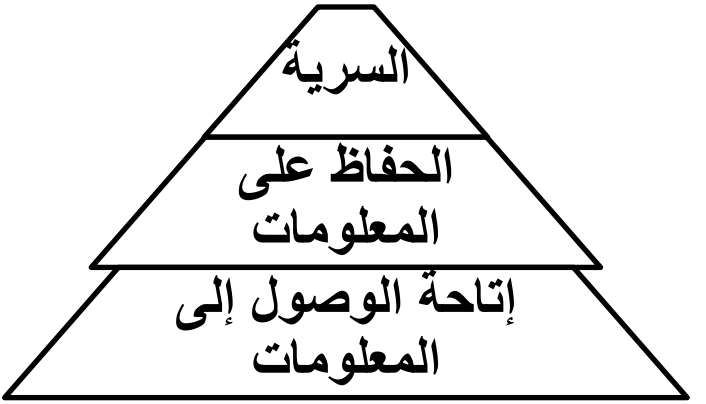
تعريف الأمن السيبراني

على الرغم من تعدد التعريفات والمفاهيم لمصطلح الأمن السيبراني إلا أنني سأركز على تعريفات الهيئات الوطنية للأمن السيبراني، وأبرز تلك التعريفات يذكر أنه عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها.

كما يشير تعريف آخر إلى أنه يشمل أمن المعلومات على أجهزة وشبكات الحاسب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث.

ويضيف أحد تلك التعريفات إلى أن من أهم مهام الأمن السيبراني احتواء أي ضرر محتمل قد ينشأ نتيجة الحوادث السيبرانية، وذلك بغرض مساعدة الجهات والأفراد على الاستجابة الملائمة للحوادث من خلال الإبلاغ عنها في الوقت المناسب، وتوفير التحليل والاستراتيجيات الفعالة للحد من وقوع الحوادث.

مكونات التعريف (الهرم السيبراني)



من خلال التعريفات السابقة نجد أن الأمن السيبراني له درجات ومكونات مهمة حسب الاستخدام، وقد أطلقت على ذلك اسم هرم الأمن السيبراني ويمر بعدة مراحل أو مستويات كالتالي:-

- **المستوى الأول (إتاحة الوصول إلى المعلومات) ويعني ذلك من منظور أمن المعلومات منع أو فلترة عرض المعلومات الملوثة والضارة على الشبكة من المنبع أي قبل نشرها من البداية، وهذا يستحيل تطبيقه عمليا نظرا لأن الإنترنت عالم ليس له حواجز وقانون يحكمه فكل شيء مباح وجائر نشره وعرضه على الشبكة.**

- **المستوى الثاني (الحفاظ على المعلومات) ويتم ذلك بواسطة أمن المعلومات من خلال عمل الاحتياطات الضرورية لحماية المعلومات المهمة والقيمة والخدمات الأساسية من الهجمات الإلكترونية.**
- **المستوى الثالث (السرية) ويكون ذلك في مجال أمن المعلومات بالنسبة للمعلومات المهمة جدًا كالحسابات البنكية والمستندات الخاصة بالجهات السيادية يقصد بها اتخاذ إجراءات وتدابير لمحاولة السيطرة عليها وفق أنظمة مشددة وقوية وهذا ما تنشده العديد من الدول وتسعى إلى تحقيقه في الوقت الحالي.**

أمن المعلومات (المصادر- الهجمات – الدفاع – الوقاية)

يعتبر موضوع أمن المعلومات من القضايا المهمة التي تشغل الجميع حتى الشخص الجالس وحيدًا مع جهاز الكمبيوتر أو الجوال الخاص به، فالموضوع لايمكن تركه لرجال السياسة أو الأمن وحدهم أو متخصصي تكنولوجيا المعلومات فقط، لا بد من مشاركة ووعي كامل بالقضية.

- **مصادر الأخطار الإلكترونية:**

ويمكن تقسيمها إلى نوعين أساسين :

١- المصادر غير المادية: المتمثلة في البرامج والتطبيقات الضارة مثل الفيروسات وبرامج الاختراق وأدوات التصيد الإلكتروني.

٢- المصادر المادية: وتشمل الأجهزة التي تحتوي على رقائق إلكترونية أو كاميرات تجسس أو غير ذلك مما يعد شيئًا ملموسًا ومحسوسًا.

- **الهجمات:**

ويمكن تقسيمها إلى قسمين أساسيين:

١- هجمات مباشرة: من خلال تنفيذ هجوم على المدى القصير لإيقاف أو عرقلة نشاط إلكتروني أو تدميره.

٢- هجمات غير مباشرة: من خلال استنزاف المعلومات الخاصة بالضحية الإلكترونية لفترات طويلة، وعادة ما يكون الغرض الأساسي هو التجسس الإلكتروني أو الاحتيال الإلكتروني.

- **الدفاع:**

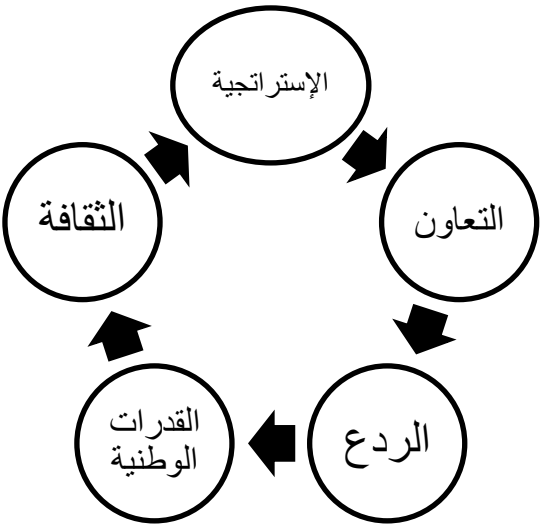
ويمكن ذلك عن طريق التحكم في مزود خدمة الإنترنت، أو إنشاء جدران الحماية، وتنزيل مضاد للفيروسات، أو استخدام برامج محددات المضمون من خلال برامج تقوم بوضع أكبر قدر من الكلمات المفتاحية لمنعها من إظهار النتائج للمستخدمين، وتوفير تطبيقات للسلامة الإلكترونية.

- **الوقاية:**

من خلال نشر الوعي العام بخطوة الهجمات الإلكترونية على الأمن القومي والخصوصية الشخصية.

الركائز الخمسة للأمن السيبراني

١. **الإستراتيجية الوطنية للأمن السيبراني**
٢. **التعاون بين الحكومة ومجتمع صناعة الاتصالات والمعلومات**
٣. **ردع الجريمة السيبرانية**
٤. **خلق كوادر وقدرات وطنية لمواجهة الأخطار السيبرية**
٥. **نشر ثقافة وطنية للأمن السيبراني**



الوعي العربى بالأمن السيبراني

من أهم المحاولات للتشريعات الإلكترونية الندوة الإقليمية حول (التشريعات الإعلامية في العالم العربي في ظل تطور وسائل الإعلام الجديدة) التي عقدتها المنظمة الإسلامية للتربية والعلوم والثقافة "الإيسيكو" بمقرها الدائم في الرباط في الفترة من ٤ إلى ٦ يونيو ٢٠١٢م

وفي ختام أعمالها دعا المتخصصون والمشاركون إلى تكوين لجنة علمية تحت إشراف الإيسيسكو لإعداد مشروع قانون للإعلام الجديد، تضم ممثلين من دول العالم الإسلامي كافة، وتبادل الخبرات الإعلامية والقانونية لسد النقص التشريعي في هذا المجال، وتوصلوا إلى مجموعة من التوصيات أهمها تفعيل التعاون بين الدول العربية لإصدار القوانين الرادعة في مجال جرائم الإنترنت، والتعاون بين الأجهزة القضائية وأجهزة الشرطة في هذا المجال. واعتبار الأمن والسلامة في الفضاء السيبراني من أولويات القطاع الإعلامي، لعلاقته بسلامة الأشخاص والوسائل والمستخدمين.

وفي مصر قام الجهاز القومي لتنظيم الاتصالات بتأسيس المركز المصري للاستجابة لطوارئ الحاسب الآلي (سيرت) في إبريل ٢٠٠٩، حيث يعمل به فريق من ستة عشر متخصصًا بدوام كامل. ويقدم الفريق المتخصص الدعم الفني على مدار ٢٤ ساعة لحماية البنية التحتية الحيوية للمعلومات.

كما صدر قرار بإنشاء المجلس الأعلى للأمن السيبراني في ١٦ ديسمبر ٢٠١٤، وهو يتبع مجلس الوزراء مباشرة، وهدفه الرسمي هو وضع استراتيجية لمواجهة التهديدات السيبرانية والإشراف على تنفيذها.

ونشرت الجريدة الرسمية قرارًا لرئيس مجلس الوزراء المصري بشأن الأمن السيبراني، وذلك في عددها رقم ١٧ مكرر (ب) بتاريخ ٢ مايو، حيث تنص المادة الأولى للقرار على التزام كافة الجهات الحكومية بكافة مستوياتها وشركات قطاع الأعمال العام بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني، فيما يتعلق بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات الخاصة بها، واتخاذ كافة الإجراءات الفنية والإدارية لمواجهة الأخطار والهجمات السيبرانية وتنفيذ الاستراتيجية الوطنية للأمن السيبراني.

وفي السعودية صدر أمر ملكي بإنشاء هيئة باسم (الهيئة الوطنية للأمن السيبراني) فى عام ٢٠١٧.

وعلى الرغم من كل ذلك لا زالت الأمور تحتاج لتكاتف مجتمعي أكثر منه قرارات حكومية.