**ما هو الأمن السيبراني**

«مجموعة من الأدوات التنظيمية والتقنية والإجرائية، والممارسات الهادفة إلى حماية الحواسيب والشبكات وما بداخلها من بيانات من الاختراقات أو التلف أو التغيير أو تعطل الوصول للمعلومات أو الخدمات، ويعد توجها عالميا سواء على مستوى الدول أو حتى المنظمات الحكومية أو الشركات».

أكد خبراء علوم الحاسب الآلي وأمن المعلومات في المملكة أن الأمر الملكي القاضي بإنشاء (الهيئة الوطنية للأمن السيبراني) وارتباطها بخادم الحرمين الشريفين الملك سلمان بن عبدالعزيز خطوة رائدة للمحافظة على أمن المجتمع السعودي واستقراره، وتأمين سلامة عمل قطاعات الدولة المختلفة من خلال تحقيق الأمن لها من أي اختراقات قد تحدث.

**انهيار الثقة**

وشدّد المتخصص في هندسة الحاسب العميد السابق لكلية الحاسب في جامعة الملك سعود البروفيسور سامي الوكيل على أن أمن الحاسب وتقنية المعلومات يعد مطلبا حيويا للمحافظة على خصوصية وسلامة تصرفات الأفراد والهيئات، ودونه ستنهار الثقة في التعامل مع القطاعات التي تقدم خدماتها بالاعتماد على معالجة البيانات والمعلومات.

**مكانة واستقلالية**

وأكد أستاذ أمن المعلومات في كلية علوم الحاسب والمعلومات بجامعة الملك سعود الدكتور خالد الغثبر، أن ارتباط الهيئة بخادم الحرمين الشريفين له دلالة على مكانتها واستقلاليتها لتستطيع سن التنظيمات والإجراءات المتعلقة بالأمن السيبراني وتطبيقها على بقية الجهات الحكومية، ومن ثم متابعة تطبيقها للتأكد من تناغم عمل الجهات الحكومية في حماية معلومات وخدمات الوطن.

**تكامل الأجهزة**

وقال المشرف العام على مركز القيادة والسيطرة للدراسات المتقدمة في جامعة الملك سعود الدكتور عبدالله الغامدي، إن قرار إنشاء الهيئة أتى في الوقت المناسب للعمل على تحقيق التكامل بين أجهزة الدولة المعنية بذلك المجال مثل: الاتحاد السعودي للأمن الالكتروني والبرمجيات التابع للهيئة العامة للرياضة، والمركز الوطني للأمن الالكتروني في وزارة الداخلية، ومركز التميز في جامعة الملك سعود، ومركز الأمن السيبراني في مدينة الملك عبدالعزيز للعلوم والتقنية، إضافة إلى مراكز أخرى في وزارة الدفاع والشركات الوطنية الكبرى، وستعمل الهيئة على سن الأنظمة والتشريعات وتوحيد الممارسات في سبيل ضمان تطبيق الأنظمة الحرجة للاتصالات وتقنية المعلومات والحفاظ على سرية وخصوصية وجاهزية وتكامل المعلومات في السعودية.

**حرب غير معلنة**

وأشار رئيس لجنة الاتصالات وتقنية المعلومات بغرفة الشرقية إبراهيم آل الشيخ إلى أن الهجمات الالكترونية أصبحت بمثابة حرب غير معلنة ولا بد من التصدي لها بكل السبل.

**التحديات**

المحافظة على خصوصية وسرية المعلومات (Privacy ) من خلال منع التوصل إلى المعلومة إلا من صاحب الصلاحية في ذلك والتحقق من هوية المستخدم لها.

سلامة ووحدة وتجانس المعلومات (Integrity ) بمنع التغيير والعبث في البيانات.

جاهزية المعلومات والتجهيزات وتوفرها عند الطلب لصاحب الصلاحية بعد التحقق من هويته (PeerAuthentication).

**من أنواع الأخطار المعلوماتية**

**منع الخدمة**

* منع استخدام الموارد والبرمجيات والتجهيزات المعلوماتية ويؤدي إلى انهيار النظام ومنع الاستفادة منه.
* خطر التسلسل والاختراق: Intrusion Attack
* ينجم عنه دخول غير المصرح له إلى الأنظمة والموارد المعلوماتية والتحكم بها أو استغلالها للهجوم على موارد وأنظمة أخرى.
* سرقة المعلومات أو العبث بها
* يمكن حدوثه بسبب ثغرات في الأنظمة أو التجهيزات أو باستخدام برامج خاصة.
* كيف تحدث هذه المخاطر؟
* من خلال استخدام وسائل برمجية متنوعة كفيروسات الحاسب، أو من خلال استغلال الثغرات في النظم المعلوماتية من قبل المتعدين أو ما يطلق عليهم «الهاكر».