المحاضرة الثامنة–تقنيات وأدوات الحماية في الأمن السيبراني:

التقنيات الأمنية السيبرانية:

تتنوع أساليب الحماية التقنية التي تستعملها مؤسسات الأمن السيبراني الحكومية والخاصة ومجالاتها، ومن أبرزها:

أمن البيانات عبر:

- تخزين بيانات النظام على جهاز وسيط خارجي، غير موصول بالنظام الحاسوبي، وتشفيرها بمفتاح تشفير فريد أثناء النقل والتخزين.
- تقنيات التشفير لتأمين البيانات عند نقلها عبر الشبكة، وحمايتها من التجسس والاستخدام غير المصرح به.
- تقنيات الوقاية من فقدان البيانات منعا لتسريب البيانات غير المصرح بها، عبر نسخها احتياطيا لاستعادتها في حال فقدانها.

أمن التطبيقات عبر:

- تحسين أمان التطبيقات من خلال رفع مستويات الحماية، عبر برمجية آمنة لمنع الأخطاء التي قد تزيد من مخاطر الأمان، لحماية التطبيقات من محاولات الاختراق.
- وعمل اختبارات الاختراق لتحديد الثغرات الأمنية، وتحديث الأمان لإصلاحها.

أمن الشبكة عبر:

- جدران الحماية، ومراقبة حركة المرور بين الشبكة الداخلية والشبكة الخارجية، مما يساعد في حماية الأنظمة من الاختراق.
- التحليل السلوكي عبر رصد التصرفات غير الطبيعية والاعتداءات السيبرانية باستخدام تحليل سلوك المستخدم والنظام عبر أنظمة الكشف.
- أمن "في بي إن" لتأمين الاتصالات عبر الإنترنت.

أمن النهايات الذي يهتم بحماية أجهزة الكمبيوتر والأجهزة المتصلة بالشبكة، عبر:

- برامج مكافحة البرمجيات الخبيثة، وتساعد في اكتشاف وإزالة البرامج الضارة والفيروسات من الأنظمة.
- تحديثات البرمجيات والأنظمة بانتظام لضمان سد الثغرات الأمنية وتعزيز الأمان.
- إدارة الهويات والوصول، من خلال ضبط وصول المستخدمين إلى الموارد بناء على صلاحياتهم، تقليلا من مخاطر الوصول غير المصرح به، وتتأكد من أن المستخدمين المتصلين بالأنظمة أو الشبكات هم الأشخاص المصرح لهم.
- معالجة المخاطر الأمنية التي تنشأ عند محاولة المستخدمين الوصول إلى شبكة المؤسسة عن بعد. وتقوم الآلية بفحص الملفات الموجودة على أجهزة الأفراد وتعمل على تقليل التهديدات فور اكتشافها.

إضافة إلى أنواع أخرى منها:

- الحرص على التعافي بعد الهجوم لضمان استمرارية العمل، عبر خطة طوارئ تسمح للمؤسسات بالاستجابة السريعة لحوادث الأمن السيبراني، للعمل دون انقطاع أو انقطاعات لمدة قصيرة.
- الرصد الأمني للأنشطة السيبرانية وتحليل الحوادث للاستجابة السريعة.
- الهندسة الأمنية عبر تصميم الأنظمة والشبكات بطريقة تجعلها أكثر مقاومة للهجمات.
- تدريب أفراد المؤسسة وتوعيتهم حول إستراتيجيات الأمن السيبراني، فهم الواجهة الأولى لتلقي الهجمات، مثل تنبيههم على حذف الرسائل الإلكترونية المشبوهة والامتناع عن أي سلوك يمكن أن يكون مدخلا للاختراق.