المحاضرة السادسة–التهديدات والجرائم الناشئة في الفضاء السيبراني:

أنواع وأشكال الهجمات السيبرانية:

تتنوع أشكال الهجمات السيبرانية وتختلف باختلاف التقنيات الحديثة، وقدرات المهاجمين والمخترقين الذين يحرصون ويحاولون دائما الالتفاف على الأنظمة الأمنية السيبرانية واختراقها وابتداع وتطوير أساليب جديدة لتحقيق أهدافهم، وتنقسم لهجمات خارجية وداخلية.

وتنشأ الهجمات الداخلية من الأفراد ذوي النوايا السيئة داخل المؤسسة. ويمكن للموظفين الذين يمتلكون وصولا عاليا إلى أنظمة الكمبيوتر أن يسببوا عدم استقرار في أمن البنية التحتية من الداخل.ومن أبرز التقنيات المستعملة في الهجمات السيبرانية:

- **البرمجيات الخبيثة:**

برامج ضارة تنشأ بهدف توفير الوصول غير المصرح به لأطراف ثالثة، إلى معلومات حساسة أو تعطيل عمل البنية التحتية الحيوية وأنظمة العمل الأساسية. ومثالا عليها: أحصنة طروادة وبرامج التجسس والفيروسات.

- **برامج الفدية:**

أحد أشكال البرامج الخبيثة، وتستخدم تقنيات وأساليب بقصد الابتزاز للحصول على الأموال، عبر تقييد الوصول إلى أنظمة الحاسوب وبياناته، ومطالبة صاحبه بدفع فدية مالية لفك الحظر واستعادة البيانات.

- **الذكاء الاصطناعي:**

تقنية سريعة التطور تستخدم لإنشاء هجمات سيبرانية أكثر تعقيدا وقوة، مما يجعل من الصعب اكتشافها والتصدي لها، ويمكن استخدامها لإنشاء برامج ضارة أكثر ذكاء يمكنها التهرب من تقنيات الأمان التقليدية، كما يمكن أيضا استخدام الذكاء الاصطناعي لإنشاء هجمات تستهدف البنية التحتية الحيوية، مثل شبكات الطاقة أو نظم النقل.

- **إنترنت الأشياء (آي أو تي):**

وتُستخدم من أجل إنشاء هجمات حجب الخدمة الموزعة (دي دي أو إس) أو سرقة البيانات أو حتى السيطرة على الأجهزة، وقد يزداد التركيز على استهدافها للوصول إلى بيانات المستخدمين أو التحكم في الأنظمة المتصلة.

والهجوم الموزع لتعطيل الخدمة هو محاولة منسقة لإرباك الخادم عبر إرسال عدد كبير من الطلبات المزيفة، لمنع المستخدمين العاديين من الوصول إلى الخادم المستهدف أو الاتصال به.

- **هجوم الوسيط:**

يحاول عبره طرف خارجي الوصول إلى الاتصالات في الشبكة أثناء تبادل البيانات، بهدف الحصول على معلومات حساسة كالبيانات المالية.

- **الهجمات الهجينة:**

وتَستخدم الهجمات الهجينة مزيجا من الأساليب التقليدية وغير التقليدية، وتتميز بأنها أكثر تعقيدا وصعوبة في الاكتشاف والحماية منها مقارنة بالهجمات التقليدية.

- **هجمات الحواسيب الكمومية:**

قد تظهر هجمات تعتمد على الحوسبة الكمومية من أجل كسر أنظمة التشفير، إذ تتميز الحواسيب الكمومية بقدرتها على إجراء العمليات الحسابية بشكل أسرع بكثير من الحواسيب التقليدية، وهذا يجعلها قادرة على كسر أنظمة التشفير

- **التصيد الاحتيالي:**

تهديد سيبراني يستخدم تقنيات الهندسة الاجتماعية لخداع المستخدمين وكشف معلوماتهم الشخصية. فقد يرسل المهاجمون رسائل إلكترونية تزعم أنها من جهة موثوقة، وتدعو المستخدمين للنقر على روابط، أو إدخال بيانات بطاقة الائتمان على صفحات ويب وهمية. ويمكن عبرها أيضا تنزيل مرفقات ضارة تثبت برامج خبيثة على الأجهزة.

- **الهجمات على الذكاء الاصطناعي:**

تُستهدف نظم الذكاء الاصطناعي بشكل مباشر لتشويه البيانات أو النتائج، وقد تتسبب هذه الهجمات بتعطيل الأنظمة أو سرقة البيانات أو حتى تعديل البيانات أو إتلافها.

- **التهديدات السيبرانية للصحة الرقمية:**

قد تستهدف أجهزة الرعاية الصحية أو نظم السجلات الطبية، وذلك لأنها حساسة للغاية ويمكن استخدامها لأغراض ضارة، مثل الابتزاز أو التجسس أو حتى إلحاق الضرر الجسدي.

- **هجمات التحكم في الطائرات المسيرة:**

أصبح استهداف الطائرات المسيرة أو أنظمة التحكم فيها محط اهتمام متزايد، وقد تتسبب هذه الهجمات بأضرار جسيمة، بما في ذلك تعطيل الطائرات أو سرقة البيانات أو حتى إسقاطها.