المحاضرة التاسعة–الأمن السيبراني في بيئة العمل المؤسسي:

لقد أحدثت تكنولوجيا المعلومات والاتصالات ثورة شاملة في جميع نواحي الحياة، اذ تزداد المخاطر السيبرانية في غالب الاحيان كلما زادت هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة، فأصبحنا أمام جرائم حقيقية ومتكاملة الأركان تتم عن طريق شبكات الانترنت، أجهزة الحاسوب وشبكة الإنترنت بأشكال كثيرة، كسرقة الأموال، النصب والاحتيال، التخطيط لعمليات إرهابية،ح ترويج الأخبار الكاذبة، وكذلك القرصنة باعتبارها الجريمة الأكثر شيوعا في العالم الرقمي.

وفي هذا السياق، فإن البحث في قضايا التهديدات السيبرانية والتحديات الأمنية يقتض ي الغوص في حيثيات العصر الرقمي الجديد وتوصيف بيئة هذه التحديات، حيث إن شبكة الإنترنت تتوفر على 30 تريليون موقع إلكتروني.

أولا– التهديدات السيبرانية الشائعة التي تواجه المؤسسات اليوم:

تواجه المؤسسات اليوم عدة تهديدات سيبرانية شائعة، منها:

1. **هجمات الفدية (Ransomware):** تقوم هذه الهجمات بتشفير بيانات المؤسسة وطلب فدية لإعادة الوصول إليها، مما يمكن أن يتسبب في خسائر مالية كبيرة.
2. **البرمجيات الخبيثة (Malware):** تشمل الفيروسات والديدان وأحصنة طروادة، وتستهدف الأنظمة لتدميرها أو سرقة البيانات.
3. **الهجمات من خلال التصيد الاحتيالي (Phishing):** تستخدم هذه الهجمات رسائل إلكترونية مزيفة تخدع المستخدمين للكشف عن معلومات حساسة مثل كلمات المرور أو بيانات بطاقات الائتمان.
4. **الهجمات المتقدمة المستمرة (APT):** تستهدف هذه الهجمات المؤسسات الكبرى وتستمر لفترات طويلة، حيث يقوم المهاجمون بالتسلل إلى الشبكة بسرية لجمع المعلومات.
5. **اختراقات البيانات (Data Breaches):** تتضمن سرقة معلومات حساسة من قواعد البيانات أو الأنظمة، مما يؤثر على سمعة المؤسسة ويعرضها للمساءلة القانونية.
6. **هجمات حجب الخدمة (DDoS):** تستهدف هذه الهجمات إغراق موارد الشبكة بكمية هائلة من الطلبات، مما يؤدي إلى تعطيل الخدمات.

7. **الهجمات الداخلية:** تشمل الأفعال الضارة التي يقوم بها موظفون أو متعاقدون داخل المؤسسة، مثل سرقة البيانات أو التلاعب بالنظام.
8. **الإصابة بالأجهزة المحمولة:** تستهدف هذه التهديدات الهواتف الذكية والأجهزة اللوحية، مما يمكن أن يؤدي إلى تسرب البيانات الشخصية والمهنية.
9. **إتلاف المعلومات أو تعديلها:**

ويقصد به الوصول إلى معلومات الضحية عبر شبكة الانترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات الهامة دون أن يكتشف الضحية ذلك، فالبيانات تبقى موجودة لكنها مضللة قد تؤدي إلى نتائج كارثية خاصة إذا كانت خطط عسكرية أو مواعيد أو خرائط سرية.

10. **التجسس على الشبكات:**

ويقصد به الدخول غير المصرح به والتجسس على شبكات الخصم، دون تدمير أو تغيير في البيانات، والهدف منه الحصول معلومات قد تكون خطط عسكرية أو أسرار حربية، اقتصادية، مالية، أو سياسية، مما يؤثر سلبا على مهام الخصم.

11. **تدمير المعلومات:** ويتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، يصطلح عليه " تهديد لسلامة المحتوى" ويعني بها إحداث تغيير في البيانات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين.

وهناك من يميز بين عدة أنواع لمخاطر التهديدات السيبرانية نذكر منها:

- التعرض لسرية الاتصالات التي تطال البريد الالكتروني، والدخول إلى الأنظمة والملفات دون إذن، وهذا يعتبر اعتداء على الحريات والحقوق الشخصية.
- التلاعب بالمعلومات الموجودة في نظام معين، وتشويهها أو إتلافها، سواء عبر الاختراق أو نشر الفيروسات.
- الجرائم العادية التي تستخدم الانترنيت، للسرقة والغش وسرقة الهويات، والاعتداء على الملكية الفكرية وغيرها.
- الجرائم التي تندرج في إطار الجريمة المنظمة، والتي تهدد امن الأفراد والدول، كتبييض الأموال والإرهاب...إلخ، كالتهديدات الأمنية الخاصة بنظام الفدية، وهي أداة إجرامية انتشرت عبر الإنترنت لعدة سنوات، مستمرة في التطور وتشمل كً لا من الأفراد والاقتصادات. على المستوى الفردي، حيث لا تزال حملات القرصنة بنظام الفدية تحقق عائدات كبيرة للقراصنة

ففي الإمارات وحدها، تم خسارة حوالي 1.1 مليار دولار أمريكي من أفراد المجتمع لأنشطة الجريمة السيبرانية في عام 2017.

ثانيا–أدوات الحماية في الأمن السيبراني:

لحماية البيانات الحساسة من الاختراق، يمكن اتباع أفضل الممارسات التالية:

1. **تشفير البيانات:** استخدم تقنيات التشفير لحماية البيانات أثناء التخزين والنقل، مما يجعلها غير قابلة للقراءة إلا للأشخاص المصرح لهم.
2. **تحديث البرمجيات بانتظام:** تأكد من تحديث الأنظمة والبرامج بشكل دوري لتصحيح الثغرات الأمنية المعروفة.
3. **استخدام كلمات مرور قوية:** اختر كلمات مرور معقدة وصعبة التخمين، ويفضل استخدام مديري كلمات المرور لتجنب استخدام كلمات مرور متشابهة.
4. **تفعيل المصادقة الثنائية (FA2):** استخدم المصادقة الثنائية لتعزيز أمان الحسابات، حيث تتطلب خطوة إضافية لتأكيد الهوية.
5. **تقييد الوصول:** امنح الوصول إلى البيانات الحساسة فقط للأشخاص الذين يحتاجون إليها لأداء وظائفهم، وطبق مبدأ "أقل امتياز".
6. **التدريب والتوعية:** قم بتدريب الموظفين على أفضل ممارسات الأمن السيبراني وكيفية التعرف على التهديدات مثل التصيد الاحتيالي.
7. **مراقبة الأنظمة:** استخدم أدوات مراقبة لاكتشاف الأنشطة غير المعتادة أو المشتبه بها في الشبكة.
8. **إجراء نسخ احتياطية منتظمة:** احتفظ بنسخ احتياطية من البيانات الحساسة في مواقع آمنة لضمان استعادتها في حالة حدوث اختراق.
9. **إعداد خطط استجابة للحوادث:** ضع خططًا واضحة للاستجابة السريعة لأي خرق أمني محتمل، بما في ذلك كيفية إبلاغ العملاء والجهات المعنية.
10. **تقييم المخاطر بانتظام:** قم بإجراء تقييمات دورية للمخاطر لتحديد الثغرات المحتملة وتحديث استراتيجيات الأمان بناءً على التهديدات الجديدة.