المحاضرة الرابعة– الأمن السيبراني في ظل التهديدات التكنولوجية الحديثة:

في عالم اليوم أصبحت التكنولوجيا الرقمية قلب الحياة الإنسانية والتنظيمية، لم تعد المؤسسات تكتفي بالوسائل التقليدية في إدارة اتصالاتها وأنظمتها، بل انتقلت إلى اتصالات رقمية مترابطة تخزن كما هائل من البيانات والمعلومات الشخصية.

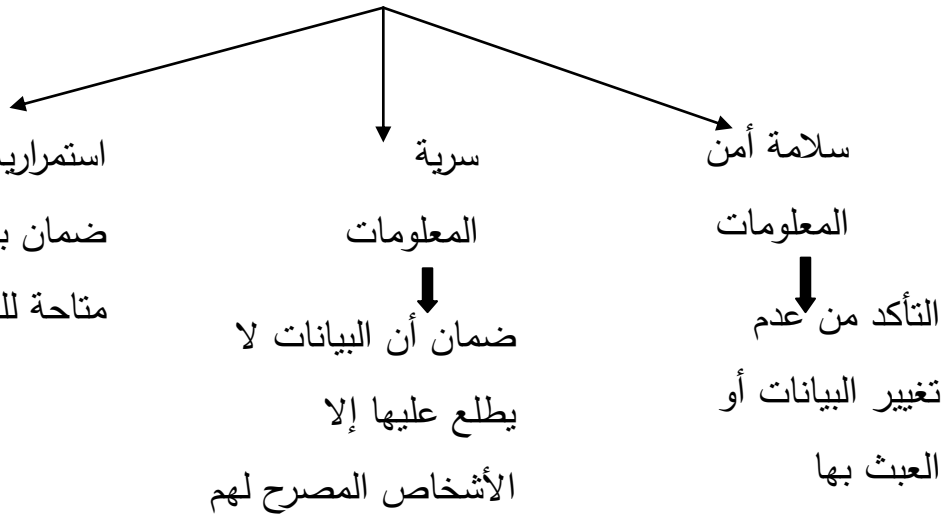
غير أن هذا التحول الرقمي، رغم ما يقدمه من سرعة وفعالية جلب معه تحديات غير مسبوقة، أهمها مخاطر القضاء السيبراني.

فالأمن السيبراني اليوم لم يعد قضية نسبة نحسب، بل أصبح قضية تنظيمية واستراتيجية تمس بناء المؤسسات، سمعتها، وثقة جمهورها.

أولا–

مع الثورة الصناعية الرابعة، دور أصبح الأمن السيبراني أحد ركائز الحوكمة الرقمية في المؤسسات والمتطلبات.

1–اهداف الامن السيبراني



2–العلاقة بين الأمن السيبراني والاتصال التنظيمي:

في المؤسسات الحديثة، يعتمد الاتصال الداخلي والخارجي على شبكات رقمية، بريد إلكتروني، أنظمة إدارة المعرفة، منصات سحابية، أي اختراق أو تسريب يمكن أن يعطل هذه الاتصالات ، أو يشوه صورة المؤسسة أمام جمهورها. لذلك أصبح الأمن السيبراني جزءا من استراتيجية الاتصال المؤسسي.

ثانيا- التحولات التكنولوجية وتأثيرها على الأمن السيبراني:

1- الثورة الرقمية والتحول الرقمي: اصبحت المؤسسات تعتمد على:

- الذكاء الاصطناعي AI .
- انترنيت الأشياء(LOT) .
- البيانات الضخمة (BIG DATA).
- الحوسبة السحابية (CLOUD COMPUTING).
- شبكات الجيل الخامس 5G.

هذه التطورات سهلت العمل وسرعت التواصل لكنها وسعت مساحة المخاطر أيضا.

2-أبرز التهديدات في البيئة الرقمية الحديثة.

- ✓ **الهجومات الإلكترونية:** محاولات اختراق أنظمة المعلومات.
- ✓ **التضليل الالكتروني:** رسائل خادعة تستهدف سرقة بيانات المستخدمين.
- ✓ **البرمجيات الخبيثة:** فيروسات أو برامج تجسس.
- ✓ **الابتزاز الإلكتروني:** تشفير البيانات، وطلب فدية مقابل فكها.
- ✓ **تسريب البيانات:** اختراق قواعد بيانات حساسة للمؤسسة.

3-أثر هذه التهديدات على الاتصال التنظيمي:

- ➢ تعطيل قنوات الإتصال الداخلي بين الموظفين.
- ➢ فقدان الثقة في الرسائل الرسمية للمؤسسة.
- ➢ تشويه صورة المؤسسة أمام الرأي العام.
- ➢ فقدان معلومات استراتيجية أو تسريب بيانات العملاء.

ثالثا–السياسات الداخلية للأمن المعلوماتي:

- ✓ استعمال كلمات مرور قوية.
- ✓ إدارة الصلاحيات والوصول إلى المعلومات.
- ✓ بروتوكولات التعامل مع البريد الإلكتروني المشبوه.
- ✓ خطط الطوارئ في حال الهجوم السيبراني.
- ✓ لا يكفي بناء برمجيات، بل يجب بناء ثقافة تنظيمية للأمن.

رابعا–كيف يمكن استخدام التكنولوجيا الحديثة، مثل الذكاء الاصطناعي، لتحسين الأمن السيبراني؟

يمكن استخدام التكنولوجيا الحديثة، مثل الذكاء الاصطناعي (AI)، لتحسين الأمن السيبراني بعدة طرق، منها:

1- **الكشف عن التهديدات:** يمكن للذكاء الاصطناعي تحليل كميات ضخمة من البيانات في الوقت الفعلي للكشف عن الأنماط السلوكية الغير طبيعية التي قد تشير إلى هجمات سيبرانية.

2- **استجابة تلقائية:** يمكن أن يتفاعل الذكاء الاصطناعي مع التهديدات بشكل سريع من خلال اتخاذ إجراءات تلقائية مثل عزل الأنظمة المصابة أو حظر العناوين IP المشبوهة.

3- **تحليل البيانات:** يساعد الذكاء الاصطناعي في تحليل البيانات المتعلقة بالهجمات السابقة لتحديد الثغرات ونقاط الضعف في الأنظمة، مما يمكن المؤسسات من تعزيز أمانها.

4- **تحسين المصادقة:** يمكن استخدام تقنيات الذكاء الاصطناعي في التعرف على الوجه، أو تحليل أنماط سلوك المستخدمين لتحسين أنظمة المصادقة الثنائية.

5- **توقع الهجمات:** من خلال التعلم الآلي، يمكن للذكاء الاصطناعي التنبؤ بالتهديدات المحتملة بناءً على الأنماط السابقة، مما يسمح للمؤسسات باتخاذ تدابير وقائية.

6- **تحليل السلوك:** يمكن للأنظمة الذكية مراقبة سلوك المستخدمين داخل الشبكة وتحديد الأنشطة غير المعتادة، مما يساعد في اكتشاف الهجمات الداخلية.

7- **التدريب والتوعية:** يمكن استخدام الذكاء الاصطناعي لتطوير برامج تدريب مخصصة للموظفين، تعتمد على تحليل سلوكهم لتحديد المجالات التي تحتاج إلى تحسين.

8- **إدارة المخاطر:** يساعد الذكاء الاصطناعي في تقييم المخاطر بفعالية من خلال تحليل البيانات التاريخية ومقارنة التهديدات الحالية، مما يمكن المؤسسات من اتخاذ قرارات مستنيرة.