المحاضرة الثامنة: تدقيق أمن نظم المعلومات المحوسب

تعد عملية تدقيق أمن نظم المعلومات المحوسبة من المهام الأساسية التي تهدف إلى حماية بيانات المنظمة وأنظمتها من التهديدات والمخاطر المحتملة. يغطي التدقيق الجوانب المختلفة من الأمن، بما في ذلك تدقيق سياسات الأمن، الأمن المادي، الأمن المنطقي، والعمليات. سنناقش بالتفصيل كل جانب من هذه الجوانب، مع التركيز على أهدافها، وخطواتها، والتحديات التي قد تواجهها.

أولا: تدقيق سياسات الأمن

1. تعريف سياسات الأمن

سياسات الأمن هي مجموعة من القواعد والمبادئ التي تحدد كيفية التعامل مع البيانات والأصول المادية والرقمية لحمايتها من الوصول غير المصرح به، أو التعديل، أو التلف. تتضمن هذه السياسات تعليمات للموظفين والمستخدمين تحدد ما يجب فعله وما يجب تجنبه عند التعامل مع الأنظمة.

2. أهداف تدقيق سياسات الأمن

- التأكد من أن سياسات الأمن شاملة وتغطي جميع الجوانب المطلوبة لحماية المعلومات.
- التحقق من مدى توافق سياسات الأمن مع المتطلبات القانونية والمعايير الدولية.
- تقييم مدى الالتزام بهذه السياسات داخل المؤسسة.

3. خطوات تدقيق سياسات الأمن

- مراجعة وثائق السياسات: دراسة الوثائق التي تحدد السياسات الأمنية للمؤسسة وتقييم مدى شموليتها.
- التحقق من الامتثال: فحص التزام الموظفين بسياسات الأمن من خلال مقابلات واختبارات عشوائية.
- مقارنة السياسات مع المعايير الدولية: التحقق من أن السياسات تلتزم بمعايير الأمن المعترف بها مثل ISO 27001.
- تحديد الثغرات والتوصيات: اكتشاف أي قصور في السياسات وتقديم توصيات لتحديثها وتطويرها.

4. التحديات في تدقيق سياسات الأمن

- عدم وضوح بعض السياسات أو عدم تحديثها بانتظام.
- صعوبة التحقق من الالتزام الكامل من جميع العاملين في المؤسسة.
- مقاومة بعض الموظفين للتغيرات أو الإجراءات الأمنية المشددة.

ثانيا: تدقيق الأمن المادي

1. تعريف الأمن المادي

الأمن المادي هو حماية البنية التحتية المادية للأنظمة، مثل الخوادم وأجهزة الحاسوب والشبكات المادية، من الأضرار الناجمة عن الكوارث الطبيعية، أو الحوادث، أو الوصول غير المصرح به.

2. أهداف تدقيق الأمن المادي

- ضمان حماية المعدات والأجهزة من السرقة أو التخريب أو الكوارث.
- التأكد من وجود تدابير وقائية كافية لمنع الوصول غير المصرح به إلى الأماكن الحساسة.
- التحقق من سلامة وتوفر أنظمة النسخ الاحتياطي والاسترداد.

3. خطوات تدقيق الأمن المادي

- فحص إجراءات الوصول المادي: التحقق من نظام الأمن الخاص بالمداخل والمخارج، مثل بطاقات الهوية، وكاميرات المراقبة.
- التأكد من التدابير الوقائية: فحص الإجراءات الوقائية للكوارث الطبيعية مثل الحرائق أو الفيضانات.
- التدقيق على أنظمة النسخ الاحتياطي: التأكد من وجود أنظمة نسخ احتياطي في موقع خارجي يمكن الاعتماد عليه.
- التأكد من الحماية ضد السرقة والتخريب: فحص فعالية أنظمة الحماية مثل الأقفال الذكية وأجهزة الإنذار.

4. التحديات في تدقيق الأمن المادي

- صعوبة تأمين بعض المناطق الحساسة بالكامل.
- التكلفة العالية لبعض أنظمة الحماية المتقدمة.
- عدم الالتزام الدائم من قبل الموظفين بالإجراءات الأمنية المادية.

ثالثا: تدقيق الأمن المنطقي

1. تعريف الأمن المنطقي

الأمن المنطقي هو مجموعة من التدابير الأمنية التي تحمي المعلومات الرقمية من الوصول غير المصرح به، ويشمل ذلك إدارة كلمات المرور، والتحقق من الهوية، وتشفير البيانات، والتحكم في الوصول إلى النظام.

2. أهداف تدقيق الأمن المنطقي

- التأكد من حماية البيانات والمعلومات الحساسة من الوصول غير المشروع.
- التحقق من أن الأنظمة متوفرة فقط للمستخدمين المصرح لهم.
- التأكد من فعالية آليات التحقق والمصادقة وكفاءة إدارة كلمات المرور.

3. خطوات تدقيق الأمن المنطقي

مراجعة سياسات إدارة الوصول: فحص الآليات التي تحدد من يمكنه الوصول إلى النظام وكيف يتم هذا الوصول.

التدقيق على إجراءات التحقق: التحقق من فعالية إجراءات التحقق مثل المصادقة الثنائية (Two-Factor Authentication).

فحص إجراءات التشفير: التأكد من أن البيانات الحساسة يتم تشفيرها أثناء النقل وفي وضع التخزين.

مراجعة سجلات الدخول والخروج: التحقق من وجود سجلات دقيقة لتتبع من يدخل إلى النظام وما العمليات التي يقوم بها.

4. التحديات في تدقيق الأمن المنطقي

- مقاومة بعض الموظفين لتطبيق سياسات كلمات مرور قوية أو إجراءات التحقق الإضافية.
- تعقيد أنظمة الحماية بما قد يؤدي إلى حدوث أخطاء غير مقصودة.
- الحاجة الدائمة لتحديث آليات الحماية لمواكبة التطورات التقنية في مجال الهجمات السيبرانية.

رابعا: تدقيق العمليات

1. تعريف تدقيق العمليات

تدقيق العمليات هو مراجعة وفحص العمليات اليومية التي تتم داخل نظم المعلومات المحوسبة، ويشمل مراقبة إجراءات معالجة البيانات، وإدارة التحديثات، والتأكد من امتثال النظام للإجراءات التشغيلية المتبعة.

2. أهداف تدقيق العمليات

- التأكد من كفاءة وفعالية العمليات التشغيلية للنظام.
- التأكد من أن العمليات تتم بشكل متوافق مع السياسات والإجراءات المحددة.
- التحقق من سلامة البيانات خلال العمليات المختلفة داخل النظام.

3. خطوات تدقيق العمليات

مراجعة إجراءات معالجة البيانات: التأكد من أن البيانات تتم معالجتها بشكل دقيق وفعّال ووفقًا للإجراءات المحددة.

التدقيق على إدارة التحديثات: التحقق من أن النظام يتم تحديثه بانتظام وأن التحديثات لا تؤثر سلبًا على أمنه.

التأكد من امتثال العمليات للسياسات: التحقق من أن كل عملية تتم وفقًا للسياسات والإجراءات المتبعة.

تحليل تقارير الأداء: فحص تقارير الأداء لضمان كفاءة النظام في إتمام العمليات بشكل فعال ودون تعطيل.

-التحديات في تدقيق العمليات:

- تكرار العمليات بصورة خاطئة بسبب عدم الالتزام بالإجراءات المحددة.
- صعوبة متابعة كافة العمليات اليومية بالتفصيل لضمان الامتثال الكامل.
- عدم وضوح بعض الإجراءات التشغيلية أو عدم تحديثها بما يناسب التطورات الجديدة.