المقالات العلمية

المعايير العالمية لأمن المعلومات

الكاتب : فهد فايز المدرع

المقدمة

مما لاشك فيه أن أمن المعلومات تلعب دوراً مهما في حماية أصول الشركة أو المؤسسة . و كثيراً ما نسمع في الاخبار عن الحوادث الأمنية لأمن المعلومات ، مثل تشويه المواقع ، وقرصنة الخادم ، وتسرب البيانات. و لذلك المنظمات بحاجة ماسة إلى أن تدرك الحاجة إلى تكريس المزيد من الموارد لحماية أصول المعلومات . وأمن المعلومات يجب أن يصبح مصدر قلق كبير في كل من الحكومة وقطاع الأعمال.

و بما أنه لا يمكن أن نضمن حماية للمؤسسة أو الشركة بنسبة 100 ٪ . لذلك ، نحن بحاجة لوضع مجموعة من المقاييس أو المعايير التي يمكن من خلالها تحقيق مستوى ملائم من الأمن.

ومن خلال هذه المقدمة فإننا سنذكر أهم المعايير العالمية التي تساعد على تحقيق الحد الأدنى لأمن المعلومات مثل الآيزو ISO و الكوبيت COBIT و ITIL وكذلك بعض القوانين المرتبطة بأمن المعلومات مثل SOX, COSO HIPAA, FISMA.

معاييرالايزو

المنظمة الدولية للتوحيد القياسي (آيزو)(ISO) ، الذي أنشئ في عام 1947 ، هو هيئة غير حكومية تتعاون مع اللجنة الدولية الكهرتقنية (IEC) والاتحاد الدولي للاتصالات (ITU) على تكنولوجيا المعلومات والاتصالات (ICT) .

وهنا أشهر المعايير التابعة لها :

1 -. آيزو 27002 :

هذا المعيار يتضمن بعض السياسات والتوجيهات، منها :

أ - السياسة الأمنية Security policy

ب - تنظيم أمن المعلومات Organization of information security

ت - وإدارة الأصول Asset management

ث - أمن الموارد البشرية Human resources security

ج - الأمن البيئي والمادي Physical and environmental security

ح - الاتصالات وإدارة العمليات Communications and operations management

خ - التحكم في الوصول access control

د - اقتناء نظم المعلومات وتطويرها وصيانتها Information systems acquisition development and maintenance

ذ - إدارة الحوادث الأمنية للمعلومات Information security incident management

ر - إدارة استمرارية الأعمال Business continuity management

ز - إدارة الامتثال أو التوافق Compliance management

2 آيزو 27001 :

هذا المعيار يقدم نموذج دوري يعرف بـ(PDCA) وهو اختصار لـ (Plan-DO-Check-Act) وهو يهدف إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل ورصد واستعراض وصيانة وتحسين وتوثيق نظام إدارة أمن المعلومات داخل المنظمة. وعادة ما ينطبق على جميع أنواع المنظمات ، بما في ذلك المؤسسات التجارية والوكالات الحكومية ، وغيرها.

وكما ذكرنا فإن هذا النموذج يتم في أربع مراحل متتابعة:

أ - الخطة (Plan) : تأسيس نظام لإدارة أمن المعلومات.

ب - التنفيذ (Do) : البدء في تنفيذ الخطط وتشغيلها.

ت - التحقق (Check) : مراجعة النظام بعد تنفيذه.

ث - العمل (Act) : صيانة وتحسين النظام.

3 آيزو 15408 :

يساعد هذا المعيار على التقييم ، والتحقق ، والتصديق على الضمانات الأمنية للمنتجات التكنولوجية.

وكذلك يمكن تقييم الأجهزة والبرمجيات لمكافحة تغير المناخ في مختبرات معتمدة للتصديق.

4 آيزو 13335 :

يتكون من سلسلة من المبادئ والتوجيهات وهي

أ – آيزو 13335–1 :

عبارة عن توثيق للمفاهيم والنماذج لإدارة أمن تكنولوجيا المعلومات والاتصالات.

ب – آيزو 13335–3 :

عبارة عن توثيق للتقنيات لإدارة أمن تكنولوجيا المعلومات.

ت – آيزو 13335–4 :

يشمل أختيار الضمانات ، كالضوابط الأمنية التقنية .

ث – آيزو 13335–5 :

يشمل على التوجيه الإداري لأمن الشبكات.

معيار الكوبيت COBIT:(The Control Objectives for Information and related Technology) :

هو عبارة عن إطار للسيطرة أو التحكم تربط تقنية المعلومات بمتطلبات العمل ، وتنظيم لأنشطة تكنولوجيا المعلومات في نموذج العملية المقبولة ، وتحديد الموارد الرئيسية لتكنولوجيا المعلومات ، و أهداف الرقابة الإدارية التي سينظر فيها"

وقد تم بناء هذا المعيار من قبل معهد حوكمة تقنية المعلومات IT Governance Institute (ITIG) في عام 1995م .

وهو الآن في النسخة الرابعة ، وتتكون من سبعة أجزاء رئيسية :

1 –النظرة التنفيذية.Executive overview
2 –إطار الكوبيت.COBIT framework
3 –التخطيط والتنظيم.Plan and Organize
4 –الاكتساب والتنفيذ.Acquire and Implement
5 –التسليم والدعم.Deliver and Support
6 –الرصد والتقييم .Monitor and Evaluate
7 –الملاحق ، بما في ذلك المعجم أو المصطلحات Appendices

و الكوبيت هو مجموعة من المواد التوجيهية الدولية تستخدم لحوكمة تقنية المعلومات و كذلك تتيح للمديرين سد الفجوة بين متطلبات الرقابة والقضايا التقنية والمخاطر التجارية. واستناداً إلى أبرز النقاط في الكوبيت تبين أنه يركز على مخاطر محددة حول أمن تكنولوجيا المعلومات بطريقة بسيطة لمتابعة وتنفيذ المنظمات الصغيرة والكبيرة .

معيار ITIL :

هو اختصار لـ The Information Technology Infrastructure Library ويسمى أيضاً آيزو 20000 .

هو عبارة عن مجموعة من أفضل الممارسات في مجال إدارة خدمات تقنية المعلومات (ITSM) ، ويركز على خدمة عمليات تقنية المعلومات ويعتبر الدور الرئيسي للمستخدم.

وقد تم بناؤه بواسطة مكتب المملكة المتحدة لتجارة الحكومة (OGC)

وإدارة خدمة التقييم الذاتي يتم العمل بها عن طريق وضع استبيانات على الإنترنت

استبيان التقييم الذاتي يساعد على تقييم إدارة المناطق التالية :

أ – إدارة مستوى الخدمة Service Level Management

ب –الإدارة المالية Financial Management

ت –إدارة بناء القدرات Capacity Management

ث –إدارة استمرارية خدمة Service Continuity Management

ج –إدارة التوفر Availability Management

ح –مكتب الخدمات Service Desk

خ –إدارة الحوادث Incident Management

د – إدارة المشكلة Problem Management

ذ – إدارة التكوين Configuration Management

ر – إدارة التغيير Change Management

ز – إدارة الإصدار Release Management

اللوائح والقوانين المتعلقة بأمن المعلومات :

بما أن هناك بعض المعيير العالمية والمبادئ التوجيهية ، وضرورة الالتزام بها المبادئ والمعايير التي حددتها تلك المؤسسات أو الهيئات ، فإننا سنذكر بعض القوانين واللوئح للولايات المتحدة الأميريكية ومنها : SOX, COSO HIPAA, FISMA وسنطرق لها بالأسفل :

1 –قانون **SOX** :

هو اختصار لـ Sarbanes-Oxley Act.

بعد ارتفاع عدد الفضائح العالية في الولايات المتحدة ، بما في ذلك شركة انرون و وورلدكوم . صدر قانون ساربانيس أوكسلي Sarbanes-Oxley Act في عام 2002 والغرض من ذلك هو "لحماية المستثمرين عن طريق تحسين دقة وموثوقية نظام الإفصاح أو التعريف المقدمة عملاً لقوانين الأوراق المالية ، ولأغراض أخرى" و هذا النظام يؤثر على جميع الشركات المدرجة في أسواق الأوراق المالية في الولايات المتحدة . و قانون SOX يتطلب " كل تقرير سنوي ... يحتوي على تقرير للرقابة الداخلية .. وذلك يتضمن تقييماً لفاعلية هيكلة

وإجراءات المراقبة الداخلية من الجهة المصدرة لإعداد التقارير المالية". كما تكنولوجيا المعلومات تلعب دورا رئيسيا في عملية إعداد التقارير المالية والتي السيطرة عليها ستكون من الضروري لتقييم معرفة إذا كان قانون SOX تحقق أم لا ؟

2 -قانون COSO :

وهو اختصار لـ (Committee Of Sponsoring Organizations of the Tread way Commission)

هو إطار يبدأ من عملية الضوابط الداخلية ، كما أنها تساعد على تحسين وسائل السيطرة على الشركات من خلال تقييم فاعلية الضوابط الداخلية ، ويحتوي على خمسة مكونات رئيسية :

أ – مراقبة البيئة ، بما في ذلك عوامل مثل السلامة من الناس داخل المنظمة وإدارة السلطة والمسؤوليات.

ب –تقييم المخاطر ، وتهدف إلى تحديد وتقييم المخاطر التي يتعرض لها قطاع الأعمال .

ت –مراقبة الأنشطة ، بما في ذلك سياسات وإجراءات لتنظيم.

ث –المعلومات والاتصالات ، بما في ذلك تحديد المعلومات المهمة لرجال الأعمال وقنوات الاتصال لتقديم قنوات الرقابة من جانب الإدارة للموظفين.

ج –الرصد ، بما في ذلك عملية استخدامها لرصد وتقييم جودة جميع نظم الرقابة الداخلية على مر الزمن.

3 -قانون HIPAA :

هو اختصار لـ The Health Insurance Portability And Accountability Act ويعني قابلية التأمين الصحي وقانون المحاسبة

هو قانون للولايات المتحدة تهدف إلى تحسين قابلية واستمرار تغطية التأمين الصحي في المجموعة على حد سواء والأسواق الفردية ، ومكافحة الهدر ، والاحتيال ، وسوء المعاملة في التأمين الصحي والرعاية الصحية . ويحدد القانون معايير الأمنية للحصول على معلومات الرعاية الصحية ، ويأخذ في الاعتبار عددا من العوامل بما في ذلك القدرات التقنية لنظم السجلات المستخدمة للحفاظ على المعلومات الصحية ، والتكاليف الأمنية ، والحاجة لتدريب الموظفين ، وقيمة مسارات مراجعة الحسابات في حوسبة نظم السجلات ، واحتياجات وقدرات مقدمي الرعاية الصحية الصغيرة ، و ينبغي حماية المعلومات بشكل صحيح من الأخطار التي تهدد أمن وسلامة هذه المعلومات ، والاستخدامات أو الكشف غير المصرح بها .

4 -قانون FISMA :

هو اختصار لـ Federal Information Security Management Act ويعني قانون إدارة أمن المعلومات الفيدرالي وهي تتطلب وكالات اتحادية أمريكية لتطوير وتوثيق وتنفيذ برنامج على نطاق الوكالة لتوفير أمن معلومات عن المعلومات (ونظم المعلومات) التي تدعم عمليات الأصول للوكالة. بعض الاحتياجات ما يلي :

أ – تقييم المخاطر الدوري للمعلومات ونظم المعلومات التي تدعم عمليات وأصول المنظمة .

ب – السياسات والإجراءات للمخاطر إلى تهدف إلى الحد من مخاطر أمن المعلومات إلى مستوى مقبول.

ت – التخطيط لتوفير الأمن الكافي لشبكات ونظم المعلومات.

ث – التدريب على الوعي الأمني لجميع الأفراد ، بمن في ذلك المتعاقدون.

ج – التقييم والاختبار الدوري لفعالية السياسات الأمنية والإجراءات والضوابط.

ح – خطة استمرارية العمل في مكان لدعم عمل المنظمة.

5 – قانون FIPS :

هو اختصار لـ The Federal Information Processing Standards ويعني قانون معايير معالجة المعلومات الفيدرالية .

عبارة عن سلسلة من المنشورات الرسمية المتعلقة المعايير والمبادئ التوجيهية المعتمدة والمتاحة.

والمجالات المتصلة به ما يلي :

أ – التحكم في الوصول access control

ب – التوعية والتدريب awareness and training

ت – التدقيق والمساءلة audit and accountability

ث – التصديق ، والاعتماد التقييمات الأمنية certification, accreditation, and security assessments

ج – إدارة التكوين ;configuration management

ح – التخطيط للطوارئ contingency planning

خ – تحديد الهوية والتوثيق identification and authentication

د – استجابة الحادث incident response

ذ – الصيانة maintenance

ر – حماية وسائل الاعلام media protection

ز – لتوفير الحماية المادية والبيئية physical and environmental protection

س – التخطيط planning

ش – أمن الأفراد personnel security

ص – تقييم المخاطر risk assessment

ض – اقتناء نظم الخدمات ;systems and services acquisition

ط – حماية نظام الاتصالات system and communications protection

ظ – النظام وسلامة المعلومات system and information integrity .

الخلاصة:

ورغم أن هناك عددا من معايير أمن المعلومات المتاحة ، وهي منظمة بحيث لا يمكن الإستفاد منها إلا إذا تم تنفيذ هذه المعايير بشكل صحيح. الأمن هو شيء ينبغي أن تشارك فيها جميع الأطراف سواءاً من الإدارة العليا والعاملين في أمن المعلومات ، والمحترفين في تكنولوجيا المعلومات والمستخدمين والكل منهم له دور يؤديه في تأمين أصول المؤسسة. نجاح أمن المعلومات يمكن تحقيقه من خلال التعاون الكامل على جميع مستويات المنظمة ، سواء في الداخل والخارج.

المراجع:

1 – http://www.iso27001security.com/index.html
2 – منشور على صيغة PDF
http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/ObtaiO_COBIT/CobiT4.1_Brochure.pdf
3 – http://csrc.nist.gov/groups/SMA/fisma/overview.html
4 – منشور على صيغة PDF
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
5 – بحث علمي : An overview of information security standards لحكومة منطقة هونغ كونغ الإدارية الخاصة .