

الإستهلال

الحمْدُ لله بجلال وجهه وعظيم سلطانه،
الحمْدُ لله الذي هداني لنعمة الإسلام،
وماكنت لأهتدي لولا أن هداني الله،
الحمْدُ لله الذي أعطاني نعمة التفكير،
ونعمة البصر ونعمة الحركة،
وهداني إلى زيادة العلم والمعرفة،
ووفقني لإكمال هذا البحث،
وأتمنى من الله الأجر والإستفادة لكل من يقرأه،،،،

آية

﴿ قَالَ رَبِّ اشْرَحْ لِي صَدْرِي ﴿٥٠﴾ وَيسِّرْ لِي أَمْرِي ﴿٥١﴾ وَأَحِلِّ عُنُقَدَةً
مِّنْ لِّسَانِي ﴿٥٢﴾ يَقْفَهُوا قَوْلِي ﴾

سورة طه (الآية 25-28)

شكر و عرفان

أشكر الله أولاً وأصلي وأسلم علي نبيه الأمي المصطفى الأمين صلى الله عليه وسلم،
أشكر كل من ساعدني في هذا البحث سواء بالصبر والتشجيع من قبل زوجي
وأسررتي أو بالمعلومة أو النصحية من قبل زملاء الدراسة وأساتذتي الأجلاء،
وأخص بالشكر مشرفي د.محمد عوض الشيخ.

الإهداء

أهدي هذا البحث إلى أمي العزيزة التي كانت مُرشدة لي وشجعتني على
الإستمرار بنهل العلم والدراسات العليا،
وإلى أبي الذي تعلمت منه الكثير الرجل الوقور العظيم بدينه وعلمه وحنانه.
وأهدي هذا العمل إلى رفيق دربي ومن كان معي في كل صغيرة وكبيرة إلى زوجي العزيز .
وأهدي هذا البحث إلى أساتذتي جميعهم وكل من ساعدني من الزملاء وإلى مشرفي.
وأخيراً أهدي هذا العمل إلى روح عمي الفقيد الذي وافته المنية وأنا في خواتيم عملي
بهذا البحث وكان يدعو لي، أدعوا له بالرحمة والمغفرة،،،،،

المُستخلص

في هذا البحث تم توضيح واحد من المواضيع التي تخص أمن المعلومات وهو استخدام مقاييس أمن المعلومات، حيث أن مجال أمن المعلومات واحد من المجالات التي حظيت باهتمام في السنين الأخيرة في السودان، ومع ذلك نجد أغلب المؤسسات السودانية تعاني من عدم المعرفة بكيفية قياس أمن المعلومات وإختيار المقاييس المناسبة لها.

ومن هنا كان الهدف الأساسي من هذا البحث هو إيجاد طريقة تساعد على معرفة مقاييس أمن المعلومات المناسبة للأنظمة الموجودة في مؤسسة معينة، وذلك بإتباع محددات تساعد على إختيار هذه المقاييس وهي تحديد أهداف المؤسسة، تحديد بنية أنظمة التحكم بالمؤسسة، تحديد درجة حساسية المعلومات، وكذلك معرفة المسؤولين بنظام التحكم بالمؤسسة، تحديد مكونات تطبيق الويب، تحديد أنواع الهجمات المحتملة، تحديد أنواع الثغرات وإصلاحها، بالإضافة إلى تقنيات الإكتشاف المتوفرة، وتقنيات الحماية المتوفرة، وأدوات القياس المتوفرة.

في هذا البحث تم عمل دراسة لمقاييس أمن المعلومات وتصنيفاتها والإستعانة بدراسات سابقة. من خلال هذه الدراسات تم توضيح عشرة من مقاييس أمن تطبيق الويب وعشرة من مقاييس أمن السايبر. هذه المقاييس أستخدمت لإثبات صحة محددات مقاييس أمن المعلومات وذلك عن طريق توزيع إستبيانات على ثلاثة أنواع من البيئات هي البيئات الحكومية والتعليمية والصناعية لأهمية هذه البيئات في الجوانب الإقتصادية والسياسية والإجتماعية والتقنية والأمنية.

لقد أثبتت النتائج صحة ومرونة محددات مقاييس أمن المعلومات، حيث تم إختيار المقاييس التي تناسب كل مؤسسة، وكانت النتائج تختلف بإختلاف طبيعة كل مؤسسة في بيئة معينة. ومن ثم تم توضيح بعض القرارات التي يمكن أن يتخذها المسؤول للتعديل أو التغيير للأفضل، وذلك لضمان سرية وأمن المعلومات حتى تصل المؤسسة إلى القيمة المثالية لمقاييس أمن المعلومات.

Abstract

This research demonstrates one of the topics that related to information security metrics. The field of information security importance has recently been evolved in the Sudan. Most of the Sudanese organizations suffer from lack of knowledge of how to deal with security information and how to select the appropriate metrics.

Hence, the primary objective of this research is to help these organizations to overstep these difficulties through giving serious consideration for goals, structure of control systems, degree of sensitivity of information, security group knowledge, web application components, possible attack types, detecting vulnerabilities and patch them, detecting and protecting mechanisms, and measurement tools - determination.

In this research intensive studies have been made through information security metrics and its taxonomies. From these previous studies we got ten clarifications of security metrics for web application and ten of the security metrics for cyber. These metrics were used for validity of information security metrics determinants, through distributing questionnaires to the three types of governmental, educational and industrial environment. The resultant shows the importance of such economical, political, social, technical and security aspects.

The validity and flexibility of information security metrics determinants proved that these metrics differ from one environment to another and from one organization to another in the same environment.

The samples of decisions were clarified in the thesis to give the administrator choices for amending or changing to fulfill a better information security support. Information security metrics will therefore continue in gradual advancing until it reaches its optimal security metrics.

فهرس محتويات البحث

| رقم الصفحة | الموضوع |
|--|---|
| | الإستهلال..... |
| | الشكر والعرفان..... |
| | الإهداء..... |
| | المستخلص..... |
| | Abstract..... |
| | قائمة الأشكال..... |
| | قائمة الجداول..... |
| الباب الأول - مقدمة | |
| 1 | 1.1 تمهيد..... |
| 2 | 2.1 مشكلة البحث..... |
| 2 | 3.1 الأهداف..... |
| 2 | 4.1 أهمية البحث..... |
| 2 | 5.1 منهجية البحث..... |
| 3 | 6.1 حدود البحث..... |
| 3 | 7.1 هيكلية البحث..... |
| الباب الثاني - الخلفية | |
| 4 | 1.2 مقدمة..... |
| 5 | 2.2 الثغرات والمهددات والضوابط..... |
| 5 | 3.2 المهاجم..... |
| 5 | 4.2 السابير..... |
| 5 | 5.2 أهداف الأمن..... |
| 6 | 6.2 أمن المعلومات..... |
| 6 | 7.2 المقاييس..... |
| 7 | 8.2 فوائد ومميزات مقاييس الأمن..... |
| 8 | 9.2 أنواع مقاييس أمن المعلومات..... |
| الباب الثالث - إستعراض الدراسات السابقة | |
| 10 | 1.3 مقدمة..... |
| 11 | 2.3 إطار المقاييس لتحسين التطبيق الأمني (A Metrics Framework to Drive Application Security Improvement)..... |
| 12 | 1.2.3 مقاييس دورة الحياة..... |
| 13 | 2.2.3 أبعاد المشروع..... |
| 13 | 1.2.2.3 المدخلات الغير صحيحة (Unvalidated input)..... |
| 13 | 2.2.2.3 التحكم في كسر الوصول (Broken Access control)..... |
| 14 | 3.2.2.3 كسر الموثوقية وإدارة الجلسات (Broken authentication and session management)..... |
| 14 | 4.2.2.3 ثغرات البرمجة عبر الموقع ((cross site scripting(XSS)..... |
| 15 | 5.2.2.3 فيضان الذاكرة المؤقتة (Buffer overflow)..... |
| 15 | 6.2.2.3 أخطاء الإدخال (Injection flows)..... |

| | |
|--|--|
| 16 | 7.2.2.3 معالجة الأخطاء (Improper error handling)..... |
| 16 | 8.2.2.3 التخزين الغير أمن (Insecure storage)..... |
| 16 | 9.2.2.3 رفض خدمة التطبيق (Application denial of service)..... |
| 16 | 10.2.2.3 إدارة البنية الغير آمنة (Insecure configuration management)..... |
| 18 | 3.2.3 نتائج مشروع تأمين تطبيقات الويب..... |
| 19 | 3.3 إطار أمني لأنظمة التحكم من السايبر والمقاييس التقنية (Primer Control Systems Cyber Security Framework And Technical Metrics) |
| 20 | 1.3.3 إطار أمني لأنظمة التحكم من السايبر..... |
| 20 | 1.1.3.3 معرفة الفريق المسؤول..... |
| 20 | 2.1.3.3 معرفة مجموعة الهجمات..... |
| 21 | 3.1.3.3 الدخول..... |
| 21 | 4.1.3.3 الثغرات..... |
| 21 | 5.1.3.3 الأعطال المحتملة..... |
| 22 | 6.1.3.3 الإكتشاف..... |
| 22 | 7.1.3.3 الإستعادة..... |
| 23 | 2.3.3 المقاييس التقنية..... |
| 23 | 1.2.3.3 عدد أيام التعديل..... |
| 24 | 2.2.3.3 عداد نقص التقييم..... |
| 25 | 3.2.3.3 كشف نقل البيانات..... |
| 27 | 4.2.3.3 عداد الوصول..... |
| 28 | 5.2.3.3 عمق الهجوم..... |
| 29 | 6.2.3.3 عداد الثغرات..... |
| 30 | 7.2.3.3 زمن كشف كلمة المرور..... |
| 32 | 8.2.3.3 تكلفة أسوأ حالة..... |
| 33 | 9.2.3.3 نقص تقنية الإكتشاف..... |
| 34 | 10.2.3.3 زمن الإستعادة..... |
| 36 | 3.3.3 دراسات حالة..... |
| 36 | 1.3.3.3 الدراسة الأولى: نظام تحكم موزع (DCS Distributed Control System) لمصنع لمعالجة الكيماويات..... |
| 38 | 2.3.3.3 الدراسة الثانية: المراقبة الأشرافية لتوزيع الطاقة ونظام إكتساب البيانات (SCADA)..... |
| الباب الرابع - تصنيفات ومحددات مقاييس أمن المعلومات | |
| 40 | 1.4 مقدمة..... |
| 41 | 2.4 تصنيفات مقاييس أمن المعلومات..... |
| 41 | 1.2.4 التصنيف الأول..... |
| 41 | 2.2.4 التصنيف الثاني..... |
| 45 | 3.2.4 التصنيف الثالث..... |
| 49 | 4.2.4 التصنيف الرابع..... |
| 55 | 5.2.4 التصنيف الخامس..... |
| 57 | 3.4 بيئة المؤسسة أو بيئة القرار..... |

| | |
|--|---|
| 57 | البيئة التعليمية 1.3.4 |
| 58 | البيئة الحكومية 2.3.4 |
| 59 | البيئة الصناعية 3.3.4 |
| 60 | 4.4 محددات مقاييس أمن المعلومات Information Security Metrics Determinants |
| 60 | 1.4.4 تحديد أهداف المؤسسة |
| 60 | 2.4.4 تحديد بنية نظام التحكم بالمؤسسة |
| 61 | 3.4.4 تحديد درجة حساسية المعلومات |
| 62 | 4.4.4 معرفة المسؤولين بنظام التحكم بالمؤسسة |
| 62 | 5.4.4 تحديد مكونات تطبيق الويب |
| 62 | 6.4.4 تحديد أنواع الهجمات المحتملة |
| 63 | 7.4.4 تحديد أنواع الثغرات وإصلاحها |
| 63 | 8.4.4 تقنيات الإكتشاف المتوفرة |
| 64 | 9.4.4 تقنيات الحماية المتوفرة |
| 64 | 10.4.4 أدوات القياس المتوفرة |
| 65 | 5.4 أهداف المحددات |
| 65 | 6.4 أمثلة للقرارات التي يمكن أن يتخذها المسؤول من نظام التأمين بالمؤسسة |
| الباب الخامس – النتائج والتحليل | |
| 67 | 1.5 مقدمة |
| 68 | 2.5 أساليب القياس |
| 69 | 3.5 أسماء المقاييس والمحددات |
| 71 | 4.5 نتائج إستبيان أمن تطبيق الويب |
| 71 | 1.4.5 البيانات الحكومية |
| 72 | 1.1.4.5 البيئة الحكومية الأولى |
| 74 | 2.1.4.5 البيئة الحكومية الثانية |
| 76 | 3.1.4.5 البيئة الحكومية الثالثة |
| 78 | 4.1.4.5 البيئة الحكومية الرابعة |
| 80 | 5.1.4.5 البيئة الحكومية الخامسة |
| 82 | 2.4.5 البيانات التعليمية |
| 82 | 1.2.4.5 البيئة التعليمية الأولى |
| 84 | 2.2.4.5 البيئة التعليمية الثانية |
| 86 | 3.2.4.5 البيئة التعليمية الثالثة |
| 88 | 3.4.5 البيانات الصناعية |
| 88 | 1.3.4.5 البيئة الصناعية الأولى |
| 90 | 5.5 نتائج إستبيان أمن السايبر |
| 90 | 1.5.5 نتائج البيانات الحكومية |
| 91 | 1.1.5.5 البيئة الحكومية الأولى |
| 93 | 2.1.5.5 البيئة الحكومية الثانية |
| 95 | 3.1.5.5 البيئة الحكومية الثالثة |
| 97 | 4.1.5.5 البيئة الحكومية الرابعة |
| 99 | 5.1.5.5 البيئة الحكومية الخامسة |
| 101 | 2.5.5 البيانات التعليمية |

| | |
|---|--|
| 101 | البيئة التعليمية الأولى 1.2.5.5 |
| 103 | البيئة التعليمية الثانية 2.2.5.5 |
| 105 | البيئة التعليمية الثالثة 3.2.5.5 |
| 107 | البيئات الصناعية 3.5.5 |
| 107 | البيئة الصناعية الأولى 1.3.5.5 |
| الباب السادس - الخلاصة والتوصيات | |
| 109 | 1.6 الخلاصة |
| 110 | 2.6 التوصيات |
| | المراجع |
| | الملاحق |

فهرس الأشكال

| رقم الصفحة | عنوان الشكل | رقم الشكل |
|------------|--|-----------|
| 31 | شبكة نظام التحكم الموزع لمصنع الكيماويات..... | شكل 1.3 |
| 33 | المكونات الأساسية لنظام المراقبة وجمع البيانات (SCADA) وطريقة الإتصال بينها..... | شكل 2.3 |
| 37 | التصنيف الثاني لمقاييس أمن المعلومات..... | شكل 1.4 |
| 40 | التصنيف الثالث لمقاييس أمن المعلومات..... | شكل 2.4 |
| 43 | التصنيف الرابع لمقاييس أمن المعلومات..... | شكل 3.4 |
| 44 | تصنيف مقاييس أمن المعلومات التنظيمية..... | شكل 4.4 |
| 46 | تصنيف مقاييس أمن المعلومات التقنية..... | شكل 5.4 |
| 47 | تصنيف مقاييس أمن المعلومات التشغيلية..... | شكل 6.4 |
| 49 | تصنيف مقاييس أمن المعلومات لإدارة الأعمال..... | شكل 7.4 |
| 49 | تصنيف مقاييس الأمن لإدارة أمن المعلومات..... | شكل 8.4 |
| 50 | تصنيف مقاييس الأمن والإعتمادية والثقة للمنتجات والأنظمة والخدمات..... | شكل 9.4 |

فهرس الجداول

| رقم الصفحة | عنوان الجدول | رقم الجدول |
|------------|--|------------|
| 15 | ملخص مقاييس أمن تطبيق الويب..... | جدول 1.3 |
| 32 | نتائج المقاييس لنظام تحكم موزع لمصنع لمعالجة الكيماويات..... | جدول 2.3 |
| 34 | نتائج المقاييس من إختبار نظام إكتساب البيانات..... | جدول 3.3 |
| 61 | أساليب القياس..... | جدول 1.5 |
| 62 | المقاييس والمحددات التي تحدد تطبيقها أو عدم تطبيقها..... | جدول 2.5 |
| 64 | نتائج إستبيان أمن تطبيق الويب للبيئة الحكومية الأولى..... | جدول 3.5 |
| 66 | نتائج إستبيان أمن تطبيق الويب للبيئة الحكومية الثانية..... | جدول 4.5 |
| 68 | نتائج إستبيان أمن تطبيق الويب للبيئة الحكومية الثالثة..... | جدول 5.5 |
| 70 | نتائج إستبيان أمن تطبيق الويب للبيئة الحكومية الرابعة..... | جدول 6.5 |
| 71 | نتائج إستبيان أمن تطبيق الويب للبيئة الحكومية الخامسة..... | جدول 7.5 |
| 72 | نتائج إستبيان أمن تطبيق الويب للبيئة التعليمية الأولى..... | جدول 8.5 |
| 74 | نتائج إستبيان أمن تطبيق الويب للبيئة التعليمية الثانية..... | جدول 9.5 |
| 76 | نتائج إستبيان أمن تطبيق الويب للبيئة التعليمية الثالثة..... | جدول 10.5 |
| 78 | نتائج إستبيان أمن تطبيق الويب للبيئة الصناعية الأولى..... | جدول 11.5 |
| 81 | نتائج إستبيان أمن السايبر للبيئة الحكومية الأولى..... | جدول 12.5 |
| 83 | نتائج إستبيان أمن السايبر للبيئة الحكومية الثانية..... | جدول 13.5 |
| 85 | نتائج إستبيان أمن السايبر للبيئة الحكومية الثالثة..... | جدول 14.5 |
| 87 | نتائج إستبيان أمن السايبر للبيئة الحكومية الرابعة..... | جدول 15.5 |
| 89 | نتائج إستبيان أمن السايبر للبيئة الحكومية الخامسة..... | جدول 16.5 |
| 91 | نتائج إستبيان أمن السايبر للبيئة التعليمية الأولى..... | جدول 17.5 |
| 93 | نتائج إستبيان أمن السايبر للبيئة التعليمية الثانية..... | جدول 18.5 |
| 95 | نتائج إستبيان أمن السايبر للبيئة التعليمية الثالثة..... | جدول 19.5 |
| 97 | نتائج إستبيان أمن السايبر للبيئة الصناعية الأولى..... | جدول 20.5 |