تصميم نموذج ذكي لحماية وتأمين المعلومات ضد التهديدات الإلكترونية (دراسة تحليلية)

د. أحمد محمد نور عجيل
أستاذ مساعد - جامعة السودان التقانية

المستخلص:

هـذه الدراسـة تقـدم حلـولاً لمشـاكل أمـن البيانـات والمعلومـات وطـرق حمايتهـا مـن كافـة المهـددات والمخاطـر الداخليـة والخارجيـة، وتناولـت الدراسـة بشـكل لافـت مسـألة التهديـد مـن قبـل البرمجيـات الخبيثـة وتعـرض الأنظمـة لخطـر القرصنـة الالكترونيـة. هدفـت الدراسـة إلى بنـاء وتنفيـذ نظـام الأمـان والحمايـة الفعـال وتحديـد نقـاط الضعـف في منظومـة الحمايـة وطـرق تقويتهـا وتعزيزهـا بمـا يضمـن عـدم حـدوث الأضرار وفقـدان للبيانـات والمعلومـات وتوقـف الأنظمـة عـن تقديـم الخدمـات. إعتمـدت الدراسـة المنهـج الوصفـي والمنهـج الاسـتنباطي في إسـتنتاج الأسـباب التـي تـؤدي الي حـدوث تلـك المشـاكل، واسـتخدمت النـماذج والخوارزميـة في التصميـم لتبسـيط خطـوات الحمايـة الضروريـة. ومـن أهـم النتائـج التـي توصلـت لهـا الدراسـة: تصميـم نمـوذج حمايـة لـه القـدرة عـلى توفـير أقـصي درجـات الأمـان والحمايـة للأنظمـة مـن التهديـدات عـلي المسـتوي الداخـلي والخارجـي، والتحكـم في منافـذ ارسـال واسـتقبال البيانـات، ومـن النتائـج ايضـا تحقيـق الأمـن الوقـائي في إطـار سياسـة أمـن وتكنولوجيـا المعلومـات. وقـد أوصـت الدراسـة بـضرورة إسـتخدام هـذا النمـوذج القـوي ذات القـدرة عـلي تقديـم أفضـل طـرق الحمايـة اللازمـة لتكنولوجيـا المعلومـات والـزام المؤسسـات بـضروة تطبيقـه خصوصـا في مواقـع تشـغيل مراكـز البيانـات (Data Centers)،. ومـن التوصيـات أيضـا فحـص وسـائل نقـل البيانـات خصوصـا (الفـلاش USB والاقـراص الليزريـة)، وتشـديد الرقابـة عـلي أنظمـة المراقبـة وتفعيـل ميـزة توزيـع الصلاحيـات وتقييـد التعامـل مـع الملفـات وتعقيـد كلـمات المـرور(password) وتغييرهـا بصـورة مسـتمرة، وتحديـث انظمـة التشـغيل (Updating of operating system). مـن التوصيـات أيضـا تثبيـت أحـدث برمجيـات مكافحـة الفيروسـات(Antivirus) وتحديثهـا بصـورة دوريـة، وتفعيـل ميـزة النسـخ الاحتياطـي(Backup) بشـكل دوري، وإسـتخدام الجـدار النـاري(Firewall) وفصـل الشـبكة الداخليـة عـن شـبكة الانترنـت، وإسـتخدام أحـدث تقنيـات تشـفير البيانـات، وتفعيـل المصادقـة الثنائيـة(2FA) لحسـابات البريـد الالكـتروني.

الكلـمات المفتاحيـة: تكنولوجيـا المعلومـات، الخـوادم الرئيسـية، البريـد الالكـتروني، المهـددات الداخليـة والخارجيـة، مراكـز البيانـات، البرمجيـات الخبيثـة، مكافـح الفيروسـات، النسـخ الاحتياطـي، الجـدار النـاري، التشـفير. التهديـدات الالكترونيـة.

Design of an Intelligent Model for Information Protection Against Cyber Threats: (An Analytical Study)

Dr. Ahmed Mohammed Nor Ejail

Abstract:

This study presents solution for the problems of data, information and the ways to preserve it from all internal and external threats. The study took great care of the matter of direct threat from malware which exposes the system to dangerous cyber piracy. The study aimed to build safe protection and effected system, determine the weak points in protection system and the ways of reinforces it so as to secure it from the damage , losses of data, information and stopping of the systems from presenting services. The study depending on descriptive and elicitation methods in determine the causes which leads to these problems using the models and algorithm in design simple protection steps. The study has arrived to important results in designing a model has ability to provide safety degrees to protect the system from the threats in internal and external level , control the access which send and receive the data. Other results also achieve safety prevention in policy framework in secure information technology. The study recommended of the necessity in using this strong model which has ability in presenting the best ways of protection for information technology and force the institution to applicant it especially in (Data Centers), Other recommendations is to examine the means of data transfer especially the Flash and the Laser Disks, toughening up on observation devices , activate the dealing with Folders , complicate and change the Password in continuity and refresh the turn on systems , finally the Study recommended to installation of the Malware Fighter and Updating it periodically , activate the characteristic of (Backup) periodically , Using of (Firewall) , Using Modern Data Encryption , activate Countersign (2FA) for E-mail accounts.

Keywords: Information Technology, The internal & External Threats, The Malware, The Firewall, The Data Center. Cyber threats

المقدمة:

تعتبر عملية تأمين تكنولوجيا المعلومات أمرا في غاية الأهمية ، خصوصا إعتماد معظم المؤسسات والأفراد علي نظم المعلومات في إتخاذ كافة المهام الأساسية وتقديم الخدمات للمستخدمين. في العصر الحديث اصبحت تكنولوجيا المعلومات تستخدم في شتي المجالات وبالتالي تواجهها الكثير من التحديات والصعاب، ومجموعة من المهددات المتزايدة علي المستوي الداخلي

والخارجي. تهتم الدول المؤسسات الكبري حاليا علي وضع سياسات وتشريعات لأهمية ونشر ثقافة الأمن السيبراني وتوفير التدريب اللازم للتعامل مع سياسات الخصوصية لنظم المعلومات. تهتم حماية تكنولوجيا المعلومات بحماية وسرية وسلامة البيانات والمعلومات الخاصة بالمؤسسات ودقتها ومدي توفرها وذلك وفقا للسياسات والاجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة بنظم المعلومات. حاليا تهتم الدول بإنشاء جسم داخل هيئة الاتصالات يهتم بالأمن السيبراني ويختص بمسألة كتابة وين التشريعات والضوابط لضمان أمن المعلومات والدفاع عن الأنظمة الحكومية الالكترونية وكيفية تجنيبها لهذه المهددات والمخاطر.

مشكلة الدراسة:

1. عدم إتباع سياسة الخصوصية الآمنة والحماية اللازمة للمحافظة علي الأنظم الالكترونية والتي تشغل كم هائل من البيانات والمعلومات الهامة، وإزدياد المخاطر في مراكز البيانات(ataD retneC) في المؤسسات .
2. التوقف المفاجئ لأنظمة الحاسب الآلي نتيجة لحدوث أضرار في المكونات البرمجية، وإزدياد خطر القرصنة الالكترونية ، وفقدان الاتصال بالتطبيقات نتيجة للإستيلاء ليها من قبل الهكر Hacker ،خصوصا تلك الانظمة التي تتصل بالانترنت وارتفاع تكاليف الصيانة.
3. عدم التشديد علي المراقبة لأماكن تشغيل الحاسبات مما يجعلها عرضة للسرقة
4. الخطر المتزايد من قبل البرمجيات الخبيثة علي الأنظمة والتطبيقات وسلامة البيانات والمعلومات.
5. إرتفاع حجم المهددات والمخاطر الداخلية والخارجية لنظم المعلومات الحديثة.

أهداف الدراسة:

تنبيه المؤسسات والأفراد بالمخاطر والمهددات التي تحيط بأنظمة الحاسب الآلي وضرورة توفير الميزاتيات اللازمة لبناء وتنفيذ نظام الأمان والحماية الفعال، وإسداء النصح بضرورة تغعيل وتطبيق سياسة الخصوصية الآمنة للوصول الي نظم المعلومات وتشديد القيود علي عملية التعامل مع البيانات.

توعية وتقيف المستخدمين بضرورة الحفاظ علي سرية البيانات وضمان سلامتها، وحماية الأنظمة والتطبيقات من الهجمات الالكترونية والبرمجيات الخبيثة .

تقديم افضل السبل لتأمين تكنولوجيا المعلومات والمحافظة عليها من كل التهديدات المتوقعة.

التقليل من المهددات الداخلية والخارجية، وضرورة توفير أعلي معايير الدخول المصرح به للأماكن الحساسة في المؤسسات مثل: (مراكز البيانات، أماكن معالجة البيانات الحساسة، مراكز المراقبة الأمنية ، غرف إتصالات الشبكة و سجلات الدخول والمراقبة لنظام الكاميرات الرقمية الحديثة (CCTV))

تبني مبدأ الوقاية من البرمجات الضارة وأهمية إقتناء البرمجيات الاصلية للدفاع وصد هجمات الفيروسات والإختراق والحد من برامج التجسس والتصيد الاحتيالي.

أهمية الدراسة:

تكمن أهمية الدراسة في تقديم طريقة أمثل في تأمين نظم المعلومات بوسائل حماية ذات درجات حماية أعلي من حيث مبدأ العمل ونظرية التشغيل. تشكل جملة التهديدات خطرا يهدد من استمرارية العمل علي الانظمة خصوصا خطر البرمجيات الخبيثة والاختراق والتطفل علي الانظمة. تسليط الضوء علي أهمية وضرورة أمن وحماية تكنولوجيا المعلومات خصوصا في ظل التسارع الكبير في إستخدامها من قبل المؤسسات والهيئات والأفراد في شتي المجالات(اوليفا،2011). تزداد أهمية الورقة في تناولها لأبرز المهددات الخارجية(التهديدات السيبرانية) مثل الفيروسات، وبرامج التجسس، والقرصنة الالكترونية. تتضمن الورقة الحلول الممكنة من أجل توفير الحماية اللازمة للبيانات ، والتطبيقات، والأنظمة مثل التشفير، واستخدام الجدار الناري، وبرامج مكافحة الفيروسات والتجسس والحد ومن برامج الخداع والتصيد الإحتيالي.

منهجية الدراسة:

استخدمت الدراسة المنهج الوصفي التحليلي للوصف الدقيق للمشكلة وتحليلها ، والمنهج الاستنباطي لفهم طبيعة المشاكل والمهددات والمخاطر التي تهدد تكنولوجيا المعلومات، وتم استنتاج واستخلاص جملة من المعايير القياسية الموصي بها لضمان سلامة البيانات والمعلومات بما يضمن من استمرارية العمل وضمان تقديم الخدمات للمستخدمين وطرق تأمين وحماية ووضع الخطوات الضرورية تلك في صورة نموذج يضمن التشغيل الآمن والمحمي للبيانات والمعلومات وتم استخدام الخوارزميات في التصميم ووضع الحلول اللازمة لحل تلك المشاكل والمهددات وتطبيقها مجموعة المعايير الضرورية لضمان الأمن والحماية القصوي لذلك. استخدمت فالدراسة المراجع والأوراق العلمية والشبكة العنكبوتية كمصادر للبيانات والمعلومات.

الدراسات السابقة (مقارنة وتعقيب):

هنالك عدد من الدراسات في هذا المجال وتضمنت دراسة(عالية،2025)، والتي ركزت علي علي حماية البيانات وتأمين الشبكات من الهجمات السيبرانية، كما سلطت الضوء على استراتيجيات الحماية مثل التشفير والجدران النارية وإدارة الهوية. أيضا دراسة (فيلالي وآخرون،2019)، حيث تناولت الدراسة مشكلة التهديدات الالكترونية التي تتعرض لها المعلومات في المؤسسات وماهي سبل التصدي لها، وناقشت سبل الحماية اللازمة وجملة السياسات الضرورية التي تضمن الحماية لها.هنالك أيضا دراسة(حسنين،2012) ، والتي إهتمت بشكل عام بمسألة أمن شبكات المعلومات وما هي المخاطر التي تهددها؟ وكيفية مناهضة هذه المخاطر والحماية منها، وتوصلت الي جملة من سياسات الخصوصية التي يجب إتباعها لحماية وأمن الشبكات الالكترونية. إتفقت الدراسة الحالية مع الدراسات السابقة بضرورة تأمين البيانات والمعلومات وتطبيق أعلي معايير الحماية لها ، بينما تفردت الدراسة الحالية بالتركيز علي التوقف المفاجئ لأنظمة الحاسب الآلي نتيجة لحدوث أضرار في المكونات البرمجية، وإزدياد خطر القرصنة الالكترونية، خصوصا تلك الانظمة التي تتصل بالانترنت ، والخطر المتزايد من قبل البرمجيات الخبيثة علي الأنظمة والتطبيقات وسلامة البيانات والمعلومات ، وتصميم نموذج فعال لحماية وتأمين المعلومات ضد التهديدات الإلكترونية ، والتقليل من حجم المهددات والمخاطر الداخلية والخارجية لنظم المعلومات الحديثة.

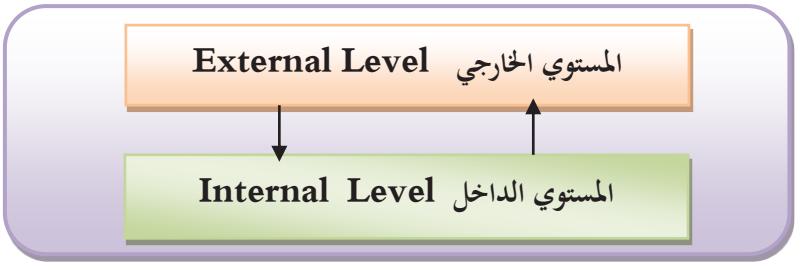
طرق حماية البيانات:

1. **التشفير (noitpyrcnE):** هو عبارة عن ترميز للبيانات والمعلومات وتحويلها الي صيغة غير مفهومة باستخدام المفاتيح العامة والخاصة في تشفير الرسالة، وتستخدم فيها خوارزميات معقدة جدا تمنع من عملية اعتراض الرسالة والاستفادة منها. في الجانب الآخر يتم عملية تحويل البيانات الي صيغتها الاصلية وذلك باستخدام المفتاح المستخدم لفك التشفير، وتعتبر خوارزمية ASR من أكثر خوارزميات تشفير المفتاح العام استخداما (شريف،8002).
2. **كلمات المرور (Password):** عبارة عن استخدام سلسلة طويلة من خليط من الحروف والارقام والرموز الخاصة تسمح بالتحقق من الهوية وصلاحية الدخول لمستخدمي الحواسيب والانظمة والدخول علي الشبكات السلكية واللاسلكية، ويجب أن تتمتع بالقوة والامتناع عن استخدام الكلمات والعبارات المفهومة او تاريخ الميلاد واقام الهواتف وذلك نسبة لسهولة تخمينها واستخدامها بصورة غير قانونية.

المعايير الدولية لإدارة أمن المعلومات:

وضعت المنظمة العالمية للمقاييس والمعايير مجموعة من الضوابط والشروط اللازمة لحماية البيانات والمعلومات وطرق التعامل معها، وتتكون معايير الأيزو(ISO) من مجموعة من الاصدارات المختلفة التي تم اصدارها بواسطة المنظمة الدولية ، حيث وضعت المنظمة المعياران (ISO/IEC-27001 & ISO/IEC-27002) وهما أكثر شيوعا وإستخداما في عملية أمن المعلومات علي نطاق واسع، وهذه المعايير توضح كيفية حماية البيانات والمعلومات من جملة التهديدات المختلفة، ومن خلالها يمكن ان نصل الي مثلث أمن المعلومات (CIA)(Confidentiality , Integrity , Availability) ، وتعني سرية المعلومات ، والتكامل ، وسلامة وصحة المحتوي ، وتوفر واستمرارية المعلومات بالتوافق مع المعيار الدولي لأمن المعلومات. (طلعت،2023).

مستويات الحماية في تكنولوجيا المعلومات:



شكل (1): مستويات الحماية في تكنولوجيا المعلومات– المصدر: تصميم الباحث 2025م

(1)خطورة المهددات على المستوي الخارجي:

يحدث على مستوي الربط الشبكي ومستوي الاتصالات والتواصل مع العالم الخارجي عن طريق الربط بالشبكات ذات المناطق الواسعة (WAN)، أو الشبكات العالمية ذات الانتشار الاوسع (Internet)، وتكمن الخطورة في حدوث الاختراق والقرصنة الالكترونية والتطفل والتصيد الاحتيالي،

وتعطيل الانظمة والتطبيقات عن الاستمرار في تقديم الخدمات. ايضا من ضمن المخاطر دخول البرمجيات الخبيثة مثل الفيروسات بأنواعها المختلفة وتعريض البيانات والمعلومات لخطر كبير يتمثل في التلاعب او السرقة أو التخريب أو إتلافها. تأمين هذا المستوي يتطلب جهدا كبيرا من معدات وبرمجيات خاصة تساعد في الحماية خصوصا إذا كانت الانظمة والتطبيقات تعمل على شبكة الانترنت. تعمل علي هذا المستوي معدات مثل الجدار الناري (Firewall)، والموجهات (Routers) واستخدام نظام (VLANs) لتطبيق معايير وسياسات الخصوصية والتحقق من الهوية(Michael,2017).

(2)خطورة المهددات علي المستوي الداخلي:

يحدث على مستوي الاستخدام من قبل المستخدمين في واجهة التطبيقات والخدمات، حيث يشكل المستخدم في حد ذاته في بعض الأحيان خطرا اشد من المهددات الخارجية، وذلك ما لم يتم السيطرة والتحكم وتشديد معايير المراقبة وتوزيع الصلاحيات بصورة دقيقة، (Autonomous,2021). يمكن ان يتم التحكم في المهددات والمخاطر علي هذا المستوي بأن يتم تفعيل مستوي الصلاحيات علي النظام وتقييد عملية الدخول علي الانظمة بواسطة اسم المستخدم وكلمة المرور(Activation of Permissions and using Password)، وتقييد عملية الوصول للإنترنت وحصر المواقع ذات الارتباط الوثيق بطبيعة العمل وحجب ما سواها والتحكم في تحميل وتنزيل الملفات والمرفقات(Upload/Download). وتسجيل بيانات المستخدمين ووحداتهم وتحديد طبيعة العمل على النظام (قراءة الملفات / التعديل / الحذف / تحميل الملفات / ادخال الملفات)، وتتيح هذه الخاصية بتتبع الخطر وتحميل المسؤوليات وإمكانية المسائلة القانونية في حال خرق أو تجاوز للصلاحيات من قبل أحد المستخدمين للنظام.

الميزات الاساسية لأمن المعلومات:

أمن المعلومات وحمايتها توفر خصوصية عالية من أي دخول غير مصرح به وتجاوز سياسات وعايير الخصوصية المتبعة في المحافظة على البيانات والمعلومات بصورة أفضل، وتتلخص في:

1.الخصوصية والسرية (Confidentiality):

يقصد به حماية المعلومات من الوصول غير المصرح به أو افشائها لطرف آخر. ويشمل أيضا التدابير اللازمة لمنع إطلاع غير المصرح لهم بالمعلومات الحساسة أو السرية، خصوصا المعلومات الشخصية والموقف المالي لشركة ما، أو المعلومات العسكرية(الغبثر،2009).

2.الكمال(integrity):

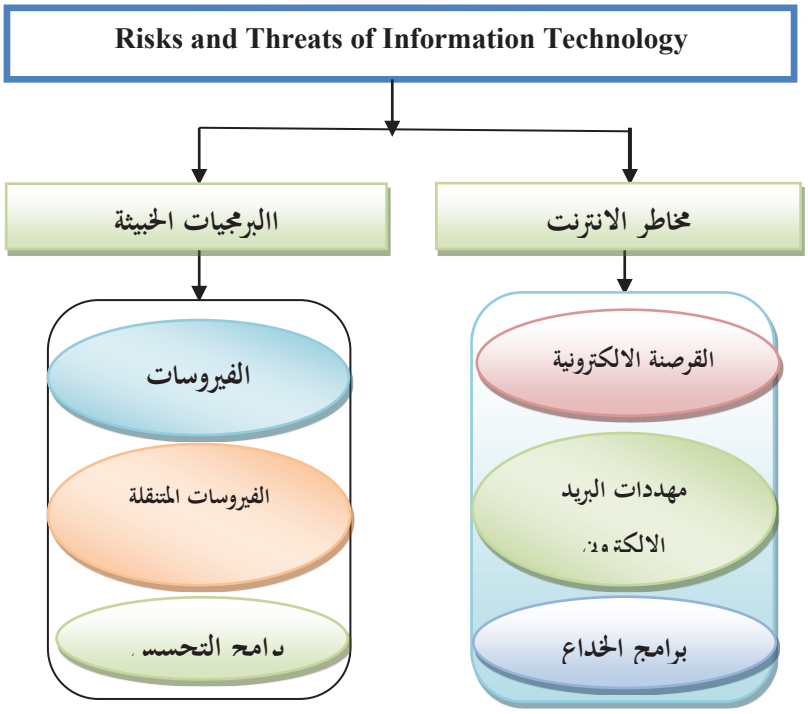
يشير الي توفر الثقة في مصادر المعلومات واتها معلومات صحيحة وكاملة ولم يتم تعديلها من قبل طرف ثالث، وإتخاذ كافة التدابير اللازمة لحماية المعلومات من التغيير وإستغلالها بصورة سيئة .

3.التوفر(Availability):

يقصد به توفر مصادر المعلومات وأنه يمكن الوصول والحصول علي المعلومات والبيانات عندما يتم طلبها من الاشخاص المخول لهم بالاستفادة منها. يشمل هذا الامر ضمان عدم تعطل الانظمة المعلومات بسبب الصيانة او التحديث أو بسبب وجود برامج خبيثة(القياس،2010).

مخاطر ومهددات تكنولوجيا المعلومات

هنالك مجموعة من المخاطر :المهددات علي المستوي الخارجي والداخلي، والتي تعمل علي الحاق أضرار كبيرة بنظم المعلومات، أخطرها البرمجيات الضارة (Male ware)، والقرصنة الالكترونية والتطفل علي الأنظمة(Hackers) والتي تعمل علي الحاق الضرر الكبير بأنظمة الحاسب الآلي والتلاعب بالبيانات والمعلومات والتحكم في تشغيل الانظمة وتطبيقاتها، تلك المهددات والمخاطر تعمل لعدة أسباب منها اسباب اقتصادية ومالية أو سياسية وأخري بغرض التخريب فقط.



شكل (٢): مهددات تكنولوجيا المعلومات- المصدر: تصميم الباحث ٢٠٢٥م

البرمجيات الخبيثة(Malware):

البرامج الضارة: عبارة عن برامج تصمم بغرض الحاق الضرر او القيام باجراءات غير مرغوب فيها في انظمة الحاسب الآلي وتطبيقاته وتتكون من الفيروسات والفيروسات المتنقلة واحصنة طروادة وبرامج التجسس وبرامج الامان الخادعة والديدان. هنالك مسميات كل نوع منها وتختلف في طريقة العمل:

(1)- الفايروسات والفيروسات المتنقلة:

الفيروسات والفيروسات المتنقلة واحصنة طروادة عبارة عن برامج يتم انشائها بواسطة المخربين من المبرمجين بغرض التخريب وتعطيل الانظمة والتطبيقات عن العمل، ويمكن للفيروسات

والديدان ان تنسخ نفسها بنفسها من جهاز الي آخر بينما تدخل احصنة طروادة عن طريق الاختباء داخل أحد البرامج والتطبيقات المفيدة. لذا يجب تفعيل خاصية Microsoft Security Essentials للحماية من الفيروسات، وتفعيل خاصية التحديث التلقائي لبرامج مكافحة الفيروسات للبحث عن الفيروسات الجديدة والحد من نشاطها.

(2)- برامج التجسس:

تصمم وتبرمج بغرض الاعلان عن منتج ما، او جمع معلومات عن الضحية أو تغيير الاعدادات الموجودة علي الجهاز بدون الحصول علي الموافقة، وتجمع بيانات في غاية الأهمية والسرية خصوصا اذا كان الحاسوب مرتبطا بالانترنت. هنالك برنامج الحماية Windows Defender يساعد المستخدم في الدفاع والحماية إذا حاول برنامج تجسس تثبيت نفسه علي الحاسوب والقيام بعمليتي الفحص والازالة (Scan & Delete).

مخاطر ومهددات الإنترنت:

القرصنة الالكترونية:

يقصد بها الاستيلاء أو السيطرة علي معلومات الآخرين بدون وجه حق ، ويكون الاختراق بدافع البطالة والعطالة أو التخريب وفي الغالب تكون لأسباب مالية وامنية أ تجسسية والتنافس التجاري بين الشركات ، وتكمن **خطورة القرصنة الالكترونية في الآتي:**

1. الدخول علي اجهزة الحاسبات المملوكة للآخرين والمتصلة عبر الانترنت مباشرة او عن طريق خادم شركة وتدمير ما يمكن ان يصلو اليه.
2. اختراق انظمة حماية الشبكات الكبري وتعطيل خدماتها وايقافها لفترات من تقديم الخدمات للمستخدمين.
3. اختراق البريد الالكتروني والاطلاع علي رسائل الخاصة بدون إذن وربما منع صاحب البريد من الوصول الي رسائله.
4. الدخول الي شبكة الانترنت المحلية مجانا من غير اشتراك واختراق المواقع علي الشبكة العنكبوتية وسرقة او تدمير الملفات او الاستيلاء علي الصفحة الرئيسية وتغييرها بما يخدم اهداف المخترق.
5. تجميد بعض المواقع المشهورة على الانترنت بحيث يصعب تصفحها من قبل الزائرين.

الحماية من القرصنة الالكترونية:

1. عدم الابقاء على الحاسوب متصلا بشبكة الانترنت بشكل دائم الا عند الالحاجة.
2. استخدام الجدار النار(Firewall) لحماية الانظمة من المهددات والمخاطر الخارجية.
3. تحميل احدث اصدارات برامج الحماية من البرمجيات الخبيثة(Antivirus) وتثبيتها علي الحاسبات والخوادم الرئيسية، والعمل علي تحديثها بصورة دورية.
4. استخدام ميزة تشفير البيانات باستخدام احدث الادوات المناسبة لذلك، ومواراة البيانات واخفائها(Hiding) خصوصا ملفات الصورة والصوت والملفات ذات الأهمية العليا.
5. استخدام برنامج Microsoft Defender : يعتبر من اداة مكافحة البرامج الضارة والتي تساعد في إكتشاف الفايروسات وازالتها.

برامج الخداع وإنتحال الشخصية:

إحدي المهددات علي شبكة الانترنت وذات أثر خطير علي أمن المعلومات التي تتعلق بالأنظمة التي تتطلب العمل علي الشبكة العنكبوتية. تتطلب عملية الاعتداء علي الامن المعلوماتي أحيانا اللجوء الي أسلوب الخداع بتقديم بعض الاشخاص لانفسهم الي الأخرين علي انهم ممثلين لشركات وواضعين مواقع وهمية علي الويب يستطيعون من خلالها جمع معلومات سرية ، مما يؤدي الي تضليل الشخص المستقبل للمعلومات حيث تبدو كأنها مرسلة من جهه معينه وتكون في واقع الأمر مرسلة من جهه أخري(لرقط،2021).

الإجراءات الضرورية لحماية المعلومات ضد التهديدات الالكترونية:

- تفعيل كافة خصائص الجدران النارية واستخدام أحدث برامج مكافحة البرمجيات الخبيثة.
- فحص جميع رسائل البريد إللكتروني الواردة والصادرة الخاصة من المحتوى الضار والمشبوه.
- تطبيق آليات التحق من الهوية متعّدد العناصر (Multi-Factor Authentication MFA))) على إمكانية وصول المستخدمين للبريد من خارج الشبكة.
- إستعمال لآليات أخري للتحقق من الهوية عند الدخول من خارج الشبكة ، مثل الخصائص الحيوية(Biometric) ، أو جهاز توليد الارقام العشوائية(Hardware keys) ، أو الرسائل القصيرة المؤقتة لتسجيل الدخول(One – Time - Password).
- تطبيق تقنيات التشفير، مثل: (أمن مستوى النقل)(Security Layer Transport) ، والشبكات الخاصة الإفتراضية (Virtual Private Networks) ، لحماية آليات التحق من الهوية خلال إرسالها. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Such as Cipher Suit B) الموصي بها وفقا لمعايير التشفير المعتمدة.
- حجب إمكانية الوصول (Restrict Access) إلى مجلدات الشبكة (Network File Shares) والملفات الغير ضرورية.
- إستخدام أحدث بروتوكولات الأمن وخصوصية المعلومات (((Wired Equivalent Access WPA3) عند التراسل عن طريق الشبكات اللاسلكية خصوصا شبكات (Wi-Fi)، وهو معيار أمان جديد لاتحاد الشبكات الشخصية والشبكات المخصّصة للمؤسسات. ويهدف إلى تحسين أمان شبكة Wi-Fi بشكل عام باستخدام اتّباع خوارزميات أمان حديثة ومجموعات رموز تشفير أكثر أمانًا.(عجيل وآخرون،2025).
- إستخدام الشهادات الرقمية المعتمدة لمواقع الإنترنت لتأمين الاتصال بين المستخدم والخادم (الموقع) من خلال التشفير والتحقق من الهوية. **ومن أبرز أنواع الشهادات الرقمية المعتمدة:**

1. VD (noitadilaVniamoD): تتحقق فقط من ملكية النطاق ، وتُستخدم للمواقع الشخصية والمدونات.
2. (OV (Organization Validation): تتحقق من ملكية النطاق وبيانات المؤسسة. تُستخدم للمواقع التجارية والمؤسسات. تمنح ثقة أعلى من DV.

3. EV (Extended Validation)): أعلى مستوى من التحقق ، تُعرض باللون الأخضر أو اسم المؤسسة في شريط العنوان (في بعض المتصفحات). تُستخدم للمواقع البنكية والمتاجر الكبرى.
4. Wildcard Certificate: تغطي النطاق الأساسي وجميع النطاقات الفرعية (مثل *.example.com).
5. Multi-Domain (SAN) Certificate: تغطي عدّة نطاقات مختلفة في شهادة واحدة.

بروتوكولات حماية المعلومات ضد التهديدات الإلكترونية:

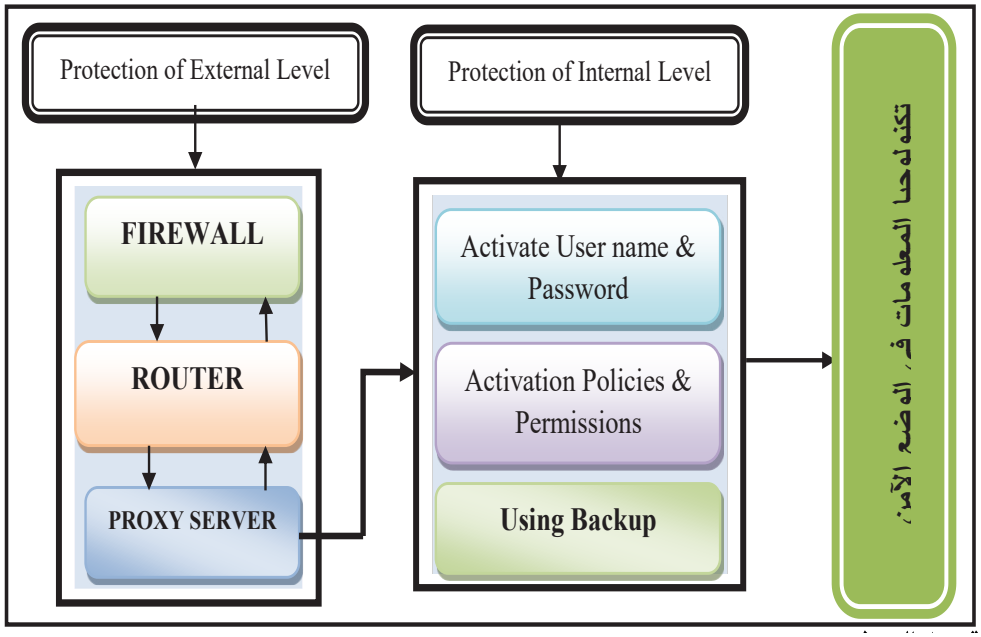
هي مجموعة من القواعد والمعايير التقنية المصممة لتأمين نقل البيانات وتخزينها من التهديدات الإلكترونية. ومن أبرز هذه البروتوكولات:

1. SPTTH (HyperText Transfer Protocol Secure): يوفّر اتصالاً مشفّراً بين المتصفح والخادم باستخدام SLT/LSS.
2. SSL/TLS (Secure Sockets Layer / Transport Layer Security): تُستخدم لتأمين الاتصالات عبر الإنترنت وتشفير البيانات المنقولة.
3. IPSec (Internet Protocol Security): يُستخدم لحماية البيانات على مستوى الشبكة، خاصة في الشبكات الافتراضية (VPNs).
4. Secure Shell(SSH): لتأمين الاتصال عن بُعد وإدارة الخوادم بشكل مشفّر.
5. S/MIME (Secure/Multipurpose Internet Mail Extensions):
لتأمين رسائل البريد الإلكتروني عبر التوقيع الرقمي والتشفير.
6. PGP (Pretty Good Privacy): لتشفير البريد الإلكتروني والملفات وتوفير الخصوصية والتوثيق.
7. Kerberos: نظام مصادقة قوي يُستخدم في الشبكات لتحديد هوية المستخدمين بأمان.
8. RADIUS و TACACS+: تُستخدم في إدارة الدخول إلى الشبكات وتأمين المصادقة المركزية.

محاذير الاتصال بالإنترنت:

1. تنشيط ميزة منع العناصر المنبثقة من خلال متصفح الانترنت(Internet Explorer).
2. تفعيل خاصية عامل التصفية ليساعد علي حماية جهاز الحاسوب من هجمات البرامج الضارة والتصيد الاحتيالي.
3. عدم تشغيل تطبيقات غير معروفة تم تحميلها من الانترنت قبل فحصها ونظافتها.
4. استخدام اعدادات الخصوصية لمستعرض الانترنت وفي الغالب بعض مواقع الويب تستخدم المعلومات الشخصية لإرسال اعلانات بغرض الاحتيال وسرقة الهوية.
5. مسح ذاكرة التخزين المؤقتة للإنترنت ومحفوظات الاستعراض، لأن معظم المتصفحات الانترنت تقوم بالحفظ المؤقت للمعلومات حول المواقع التي تمت زيارتها وجملة المعلومات التي تم تنزيلها.

النموذج المقترح للنظام(Model of System):

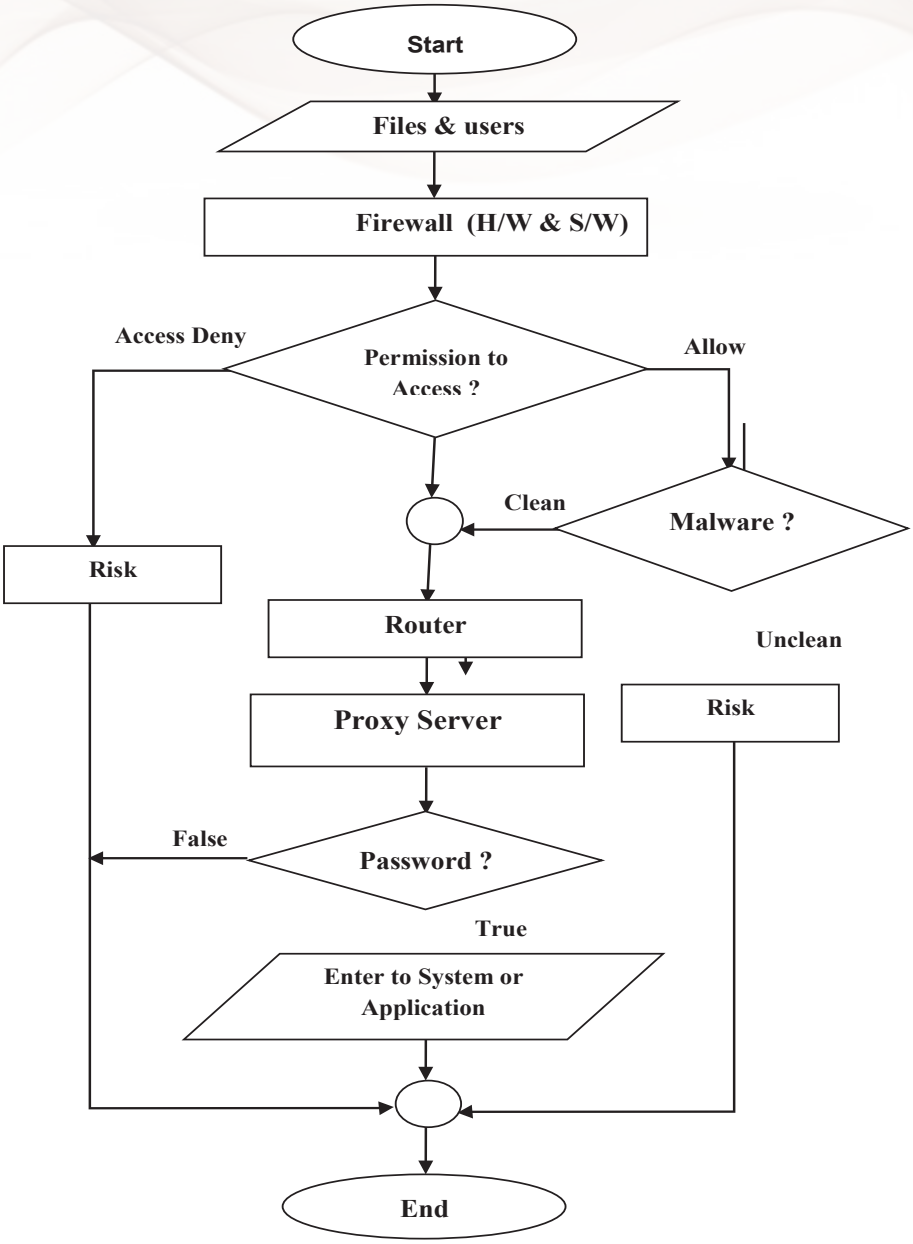


شكل(3): بنية النموذج المقترح للنظام- المصدر: تصميم الباحث 2025م

طريقة عمل النموذج:

علي المستوي الخارجي يجب ضبط اعدادات الجادار الناري(Configuration of Firewall) علي اساس الترشيح والتصفية ووضع سياسات الخصوصية بما يضمن من سلامة المرور من مستخدمين وبيانات وملفات، وفصل الشبكة الداخلية عن شبكة الانترنت ووضع الضوابط الصارمة للاتصال بالانترنت، وفلترة المواقع وحجب الغير ضروري منها. بعدها يتم تمرير حزم البيانات الي جهاز الموجه(Router) والذي بدوره يعمل تنظيم عملية مرور البيانات من والي الشبكة والانظمة الداخلية والتحكم في عملية الربط الشبكي. أخيرا ياتي دور الجهاز الرئيسي(Server) والذي يعتبر نقطة البداية لتنظيم عمل الشبكة المحلية(LAN) وتوزيع الخدمات والتطبيقات علي الاجهزة المضيفة وتشغيل الانظمة التي تخدم المستخدمين، وتطبق عليه كافة سياسات وضوابط التشغيل الضرورية للأنظمة والتطبيقات وتثبيت برمجيات الحماية. من ثم تبدأ عملية تفعيل استخدام ميزة الدخول علي الاجهزة الطرفية باستخدام اسماء المستخدمين وكلمات المرور وربطها بمجال ونطاق العمل(Domain) للتحكم الكامل في الصلاحيات وضبط عمليتي الدخول والخروج. ويجب الاهتمام بعمل نسخة احتياطية من البيانات والمعلومات (Backup) بصورة دورية اقصاها شهر وتحفظ في الاقراص في اماكن بعيدة وسرية ويمكن الرجوع اليها في حال حدوث مشكلة في النظام او تعرضها للسرقة او التخريب.

الخوارزمية العامة:



شكل(٤): الخوارزمية العامة – المصدر: تصميم الباحث ٢٠٢٥م

الخاتمة:

من خلال تتبع عمل تصميم النموذج فإن الإلتزام بتنفيذه وتطبيقه يمكن الوصول الي مجموعة النتائج التالية:

1. ضمان أقصي درجات الحماية لنظم تكنولوجيا المعلومات بما يضمن استمرارية التشغيل وعدم توقف الانظمة التي تعمل علي تشغيل التطبيقات التي تخدم المستخدمين.
2. التحكم في منافذ ادخال واخراج البيانات(serial & parallel port Specially USB port) .
3. توفير أفضل طريقة لإدارة المخاطر بصورة تضمن من تخفيض تكاليف الصيانه والسيطرة عليها وتوفير المال والجهد وضمان التشغيل المستمر للأنظمة والتطبيقات.
4. إمكانية التنبؤ بالمخاطر والسيطرة علي جملة المهددات الداخلية والخارجية وامكانية رصد كل عمليات الاختراق وصده وتتبع العمليات التخريبية علي الانظمة والقيام بالمسائلة القانونية.
5. حماية المعلومات الرسمية للأنظمة والتطبيقات التي تؤتمن عليها المؤسسات الحكومية، وتحقيق الأمن الوقائي في إطار سياسة أمن وتكنولوجيا المعلومات.

التوصيات:

1. ضبط اعدادات الحاسوب بصورة تضمن التحكم في المنافذ(stroP) من شاشة الاعدادات(puteS)، وفحص وسائل نقل البيانات(الفلاش BSU والاقراص الليزرية) قبل فتحها.
2. إلزام المؤسسات والهيئات بضروة تطبيق هذا النموذج خصوصا في مواقع تشغيل الحاسبات المركزية(Servers) ومراكز البيانات (Data Center). ووضع الميزانيات المطلوبة لذلك.
3. الاحتفاظ بكلمات المرور بعيدا عن الحاسوب وعن الآخرين مع ضرورة تغييرها بصورة دورية.
4. استخدام أحدث التقنيات مع الرسائل مثل البصمة الالكترونية(Message Digits) أو التوقيع الالكتروني(Digital Signature).
5. تفعيل ميزة النسخ الاحتياطي(Backup) بشكل دوري والاحتفاظ بالملفات والمعلومات الهامة علي احد الاقراص الخارجية للرجوع اليها في حالة حدوث ضرر أو خطر.
6. إستخدام الجدار الناري(Firewall) وفصل الشبكة الداخلية عن شبكة الانترنت ووضع الضوابط الصارمة للاتصال بالانترنت، وفلترة المواقع وحجب الغير ضروري منها.
7. توعية المستخدمين علي الاستخدام الآمن للأنظمة والتطبيقات والتعامل معها وفقا للصلاحيات الممنوحة لهم وتوضيح مخاطر ومهددات الهندسة الاجتماعية والتي تتمثل في: التصيد الاحتيالي والموقع المزيفة، وبرامج الخداع.
8. تفعيل المصادقة الثنائية(2FA) لحسابات البريد الالكتروني، وعدم فتح الملفات المرسلة عبر البريد الالكتروني من اشخاص غير معروفين وغير موثوق بهم.
9. ضرورة تنصيب وتفعيل خدمة خادم البريد الالكتروني(Exchange Mail Server) الخاص بالمؤسسة للتراسل عبره.

10. تحديث انظمة التشغيل (Updating of operating system)، وتثبيت أحدث برمجيات مكافحة الفيروسات وبرامج التجسس الأصلية وتحديثها بصورة دورية. وضرورة تبني سياسة وطنية للأمن السيبراني وإنشاء وحدة مختصة لذلك وتدريب الموظفين علي الوعي الأمني وتوفير الميزانيات اللازمة لذلك.

المصادر والمراجع:

(1)عجيل أحمد محمدنور، غفاري حسن (2025) ، « حماية وأمن شبكات الواي فاي ضد الإختراق والتطفل - بالتطبيق علي كلية كسلا التقانية « ، مجلة النيل الابيض للدراسات والبحوث ، العدد (26) ، الصفحات: 61 – 73 .

(2)شركة القياس لمهارات الحاسوب(2010)، أمن تكنولوجيا المعلومات، سلسلة منشورات الرخصة الدولية لقيادة الحاسب الآلي(ICDL Approved Courseware 2010)، الاصدار السادس ، ص5.

(3)لرقط سمية، معليم سعاد(2021)، أثر التكنولوجيا علي الأمن المعلوماتي ، مجلة الابحاث الاقتصادية والادارية ، المجلد 15 ، العدد 03 ، 448 – 431 . ، ص 437.

(4)فيلالي أسماء ، شليل عبداللطيف (2019) ، « تهديدات أمن المعلومات وسبل التصدي لها « ، مجلة البشائر الاقتصادية ، المجلد (4) ، العدد (3) ، الصفحات : 163 – 177 .

(5)اوليفا لورنس م. / ترجمة: مراياتي محمد (2011)، أمن وتقنية المعلومات، سلسلة كتب التقنيات الاستراتيجية والمتقدمة – المنظمة العربية للترجمة – مدينة الملك عبدالعزيز للعلوم والتقنية ، ص51.

(6)طويلة جميل حسين (-)، البرمجيات الخبيثة(دليل عملي لاستخدام البرمجيات الخبيثة وبرمجيات التجسس وطرق الوقاية والحماية منها) ، Dolghin-syria@hotmail.com، ص10 .

(7)منشآت (2022)، الأمن السيبراني، سلسلة منشورات الهيئة العامة للمنشآت الصغيرة والمتوسطة – المملكة العربية السعودية ، ص4.

(8)عالية محمد أحمد (2025) ، « الأمن السيبراني: درع المعلومات الرقمية» ، جامعة الزيتونة ، عمان، المملكة الاردنية الهاشمية.

(9)حسنين رجب عبدالحميد (2012)، « أمن شبكات المعلومات الالكترونية : المخاطر والحلول» ، مجلة الأمن السيبراني ، العدد (30) ، الصفحات : 74 – 101 .

(10)لهيئة الوطنية للأمن السيبراني(2018) ، الضوابط الاساسية للأمن السيبراني Essential Cyber security Control (ECC-1: 2018) ، وزارة الاتصالات ، المملكة العربية السعودية ص22.

(11)سلسة اصدارات المركز الوطني للأمن السيبراني(2018) – الوثيقة الأساسية لاطار سياسة أمن المعلوماتية ، مركز الاتصالات السورية ، النسخة 1.3 ، ص 12.

(12)شريف سامي محمد(2008)، أمن الحواسيب ، سلسلة منشورات جامعة السودان المفتوحة(حسب 5046) ، الطبعة الأولي ، ص 160.

(13)الغثبر خالد بن سليمان، القحطاني محمدبن عبدالله(2009)، امن المعلومات بلغة ميسرة ، مكتبة الملك فهد للنشر ، الطبعة الأولي ، ص 21

(14)طلعت أماني محمد(2023)، حوكمة تكنولوجيا المعلومات كمدخل لحماية امن المعلومات الشركات وأثرها علي الأداء المالي وغير المالي: دليل الشركات المصريه ، المجلة العلمية للتجارة والتمويل 104 – 53, 41(4). ، ص13.

(15)الطائ محمدعبدحسين، الكيلاني محمود ينال(2015)، إدارة أمن المعلومات ، دار الثقافة للنشر والتوزيع ، ص 114.

المراجع الإنجليزية:

(1)Michael and Herbert(2017)- Principal of information security- sixth edition , Congage Learning – Kennesaw state University . USA. Page 325.

(2)Autonomous Institution UGC of India(20202021-) Digital notes on Cyber Security, Department of Information Technology Mallareddy College of Engineering & Technology. Page 22.

(3)He Yang(2022), " study on Hardware Security and its Defense Measures " , SHS web Conference 144,02011(2022) ,[STEHF 2022]. Page 3.