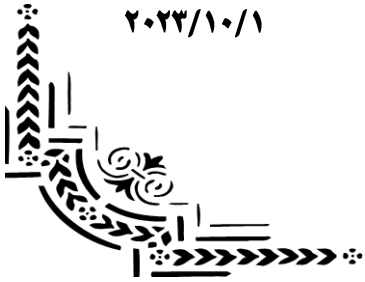
القرصنة الإلكترونية على مواقع الإنترنت: دراسة تطبيقية على عينة من مواقع مرافق المعلومات المصرية

Electronic piracy on websites: an applied study on a sample of Egyptian information facilities websites

د. هبة صلاح الدين النموري

مدرس بقسم المكتبات والمعلومات كلية الآداب جامعة طنطا

تاريخ الإرسال	تاريخ القبول	تاريخ النشر
٢٠٢١/٤/١٩	٢٠٢٢/٦/١٩	٢٠٢٣/١٠/١



المستخلص:

تناولت الدراسة القرصنة الإلكترونية على مو اقع عينة من مر افق المعلومات المصرية على شبكة الإنترنت، حيث استهدفت التعرف على حوادث القرصنة التي استهدفت مو اقع مر افق المعلومات المصرية على شبكة الإنترنت، ودو افعها، والخسائر الناجمة عنه، والإجراءات التي تم اتخاذها، ثم درست السياسات والإجراءات الأمنية المتبعة بعينة من مو اقع مر افق المعلومات المصرية على شبكة الإنترنت، ثم التحديات التى تعوق تأمين مو اقع مر افق المعلومات من مخاطر القرصنة وتقديم التوصيات التي من شأنها رفع مستوى الحماية المتو افر بها.استخدمت الباحثة المنهج الوصفى التحليلى و انتهت إلى عدة نتائج من أهمها: تعرضت بالفعل(٥) مو اقع من مو اقع الدراسة بنسبة ٦,٥٥٪ لهجمات القرصنة الإلكترونية، تفتقر جميع مر افق الدراسة لوجود سياسات لأمن المعلومات حيث توجد أجزاء مكتوبة تغطى فقط إجراءات الاستجابة للحوادث بمكتبة الإسكندرية ومركز معلومات مجلس الوزراء، تتعدد الأساليب والضو ابط الأمنية المتبعة بمر افق الدراسة وتأتى مكتبة الإسكندرية، ومركز معلومات مجلس الوزراء فى مقدمة مجتمع الدراسة من حيث تو افرهذه الأساليب، تأتى التحديات البشرية فى مقدمة التحديات التى تواجه تأمين مو اقع مر افق الدراسة بنسبة(٧٧,٧٨٪)، يليها التحديات المالية بنسبة(٤٤,٤٤٪) يليها التحديات التقنية بنسبة(١١,١١٪).

الكلمات المفتاحية: القرصنة الإلكترونية، الأمن السيبر انى، الهجمات الإلكترونية، الجر ائم السيبر انية، اختراق مو اقع الانترنت حماية البيانات، مر افق المعلومات، تأمين مو اقع الإنترنت.

Abstract

The study dealt with electronic piracy on the websites of a sample of Egyptian information facilities on the Internet. It aimed to identify the incidents of piracy that targeted the websites of Egyptian information facilities on the Internet, their motives, the resulting losses, and the measures that were taken. Then, it studied the security policies and procedures followed by a sample of Egyptian information facilities websites on the Internet, then the challenges that hinder securing information facilities websites from the risks of piracy and providing recommendations that would raise the level of protection

available in them. The researcher used the descriptive analytical approach and concluded with several results, the most important of which are: (5) of the websites were actually exposed. The study rate was 55.6% for electronic piracy attacks. All study facilities lack information security policies, as there are written sections that only cover incident response procedures at the Library of Alexandria and the Cabinet Information Center. There are many security methods and controls used at study facilities, and the Library of Alexandria and the Cabinet Information Center come in... Introduction to the study population: In terms of the availability of these methods, human challenges come at the forefront of the challenges facing securing the sites of study facilities at a rate of (77.78%), followed by financial challenges at a rate of (44.44%), followed by technical challenges at a rate of (11.11%).

Keywords: electronic piracy, cybersecurity, electronic attacks, cybercrimes, website hacking, data protection, information facilities, website security.

المقدمة

لقد أحدثت شبكة الإنترنت تطورًا هائلاً غيَّر ملامح الحضارة الإنسانية حيث قدمت البنية التكنولوجية اللازمة لإنجاز شتى مجالات الحياة اليومية، وأصبحت الركيزة الأساس للاقتصاد العالمى، إلا أنها فى الوقت ذاته كشفت عن وجه آخر قبيح مظلم يحمل فى طياته أدوات التدمير والجريمة عندما أصبحت ميداناً لصراعات من نوع جديد انتقل من الو اقع المادى إلى الفضاء الإلكترونى، و أفرزت فئة مستحدثة من جر ائم الإنترنت من أخطرها جر ائم القرصنة الإلكترونية واختراق المو اقع وظهرت عصابات منظمة من قراصنة الإنترنت التى طوَّرت نفسها واستغلت كافة تقنيات الحاسب الآلى والإنترنت ومستحدثاتهما فى تحقيق أهدافهم غير المشروعة والحصول على المعلومات واستخدامها لتهديد الأمن والسلامة البشرية والمنشآت الحيوية أو لتخريب المو اقع نفسها، ولهذا، تعد القرصنة الإلكترونية من أخطر التحديات التى تهدد الأمن القومي و اقتصاديات الدول بل هى سلاح العصر الرقمى الذى تفوق خسائره أسلحة الحروب التقليدية.

وقد تعرضت(٥٢٪) من المؤسسات الأسيوية بالفعل لجر ائم القرصنة، وقد عبر عن هذا الخطر(روبرت ميولير) Robert S. Mueller المدير السابق لدى مكتب التحقيق الفيدرالى

الأمريكى (FBi)، حين أشار إلى أن المؤسسات نوعان: مؤسسات قد تعرضت مو اقعها بالفعل للاختراق، أومؤسسات سيتم اختراق مو اقعها مستقبلاً، ومن ثَم تحولت المسألة من هل يمكن الإختراق إلى متى يتم الاختراق؟ مما دفع بعض خبراء الإنترنت لتلخيص ما يحدث بقولهم: إن التكنولوجيا صارت تأكل بعضها البعض (SMITH F. A., 2017, p. 14).

وعلى الرغم من صعوبة التصدى والسيطرة الكاملة على جر ائم القرصنة- خاصة مع تز ايد وتطور تقنيات الحاسبات والإتصالات– إلا أن التطوير المستمر لإجراءات التأمين سيساهم في تقليم أظافر القراصنة ويحد بدرجة كبيرة من هذه الجر ائم، ويخفف من الخسائر الناجمة عنها.

وقد أدركت المؤسسات عامة مخاطرا لقرصنة السابقة و اتخذت إجراءات لتأمين مو اقعها وحماية بيانات المنتسبين لها ومن بينها قطاع مر افق المعلومات بما تتضمنه من قواعد بيانات ومجموعات رقمية وبيانات شخصية للمستفيدين منها، ولهذا تعد من المؤسسات المستهدفة من قبل القراصنة، فإذا كان اختراق موقع البنتاجون ومؤسسة جوجل وحسابات بليون شخص عام ٢٠١٥ قد تم بالفعل، فإنه من الممكن اختراق مو اقع مر افق المعلومات بكل أنواعها.

أولاً :الإطار المنهجى.

١/١ مشكلة الدراسة:

فى ظل التوجه نحو التحول الرقمى بجانب تر ابط العالم إلكترونيًا، أصبح الوصول لأى موقع إنترنت واختر اقه أمرًا ممكنًا، خاصة مر افق المعلومات لما تتيحه من بيانات ومجموعات رقمية وحسابات للمستفيدين والتى تتطلب بالضرورة حمايتها وتأمينها. وقد استوقف الباحثة حوادث القرصنة التى اجتاحت مو اقع الإنترنت فى السنوات الأخيرة بشراسة، حيث أصبح اختراق مو اقع البنوك، والمؤسسات الحكومية، والشركات العالمية من قضايا الساعة التى تطالعنا بها وسائل الإعلام بشكل مستمر على المستوى المحلى والدولى، وتعكس الأرقام التالية مؤشرًا مرعبًا لخسائر القرصنة على الصعيد الدولى على النحو التالى:-

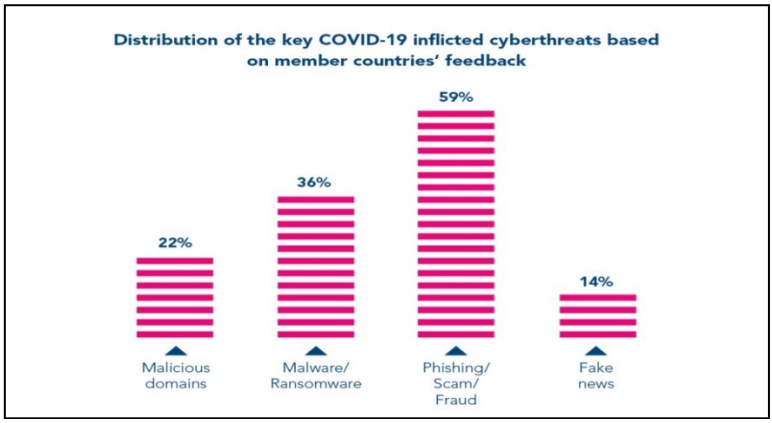
- بلغ إجمالى الخسائر الاقتصادية الناجمة عن الهجمات الإلكترونية خلال عام ٢٠١٨(١,٧٤٥) تريلون دولار.

- قُدِّرت الخسائر الاقتصادية الناجمة عن الجر ائم الإلكترونية لعام٢٠٢١ بحوالي (٦) تريليون دولاربو اقع (٥٠٠) بليون دولار شهريًا، و(١١٥,٤) بليون دولار أسبوعيًا، و(١٦,٤)

بليون دولار يوميًا ويشكل هذا الرقم ثالث اقتصاد في العالم بعد الولايات المتحدة والصين، ويتوقع الخبراء ارتفاعها الى(١٠) تريليون دولار بحلول عام ٢٠٢٥.

- بلغت تكلفة الإنفاق العالمي على منتجات وخدمات الأمن السيبر اني (واحد) تريلون دولار سنويًا للأعوام من ٢١٠٧ إلى ٢٠٢١ (Steve, 2020).

- كان لجائحة كورونا COVID-19 أيضًا تأثيرًا سلبيًا على الأمن السيبر انى حيث ارتفعت بشكل ملحوظ أعداد الهجمات الإلكترونية بكافة أساليبها وفق تقرير الإنتربول ومنظمة الصحة العالمية لعام ٢٠٢٠ (INTERPOL report shows alarming rate of cyberattacks during COVID-19, 2020)- كما يوضح الشكل رقم (١)



شكل رقم (١) ارتفاع معدلات الهجمات الإلكترونية بأساليبها المختلفة خلال فترة انتشار COVID- 19

(INTERPOL report shows alarming rate of cyberattacks during COVID-19, 2020)

ولهذا سعت الباحثة لإعداد هذه الدراسة؛ لاستكشاف و اقع جر ائم القرصنة الإلكترونية على مو اقع الإنترنت لمر افق المعلومات المصرية، والتعرف على إجراءات الحماية التى تتبعها ومدى استعدادها للتصدى لهذه الجر ائم، والوقوف على التحديات التى تواجهها فى سبيل تحقيق منظومة دفاع إلكترونى متكاملة.

١/٢أهمية الد راسة:-

ترجع أهمية الدراسة إلى استكشاف و اقع منظومة التأمين والحماية المتو افرة لمو اقع الإنترنت لمر افق المعلومات المصرية وبالتالى تصبح نتائجها أداة لمساعدة القائمين على إدارة هذه المر افق فى الاستعداد الأمثل لمواجهة مخاطر القرصنة من خلال تقييم و اقعهم،

والتعرف على جو انب القوة لتدعيمها والحفاظ عليها، وأوجه القصورلمعالجتها، والارتقاء بمستوى الحماية، فضلاً عن تعميم الاستفادة لكافة مر افق المعلومات الأخرى خارج العينة، والتوعية بالممارسات التى يمكن أن تؤثرعلى أمن مو اقعهم و أيضاً سبل الحماية.

٣/١ أهد اف الد راسة:

تسعي الدراسة إلي تحقيق الأهداف التالية:-

١-التعرف على حوادث القرصنة التي استهدفت مو اقع مر افق المعلومات المصرية على الإنترنت، ودو افعها، والخسائر الناجمة عنها.

٢- دراســة الإجراءات المتبعة لحماية مو اقع مر افق المعلومات المصــرية على الإنترنت، من حيث مدى تو افر السياسات والخطط الموثقة، وتحديد أساليب تأمين هذه المو اقع، فضًلا عن نوع الاستضافة المتبعة ولغة البرمجة المستخدمة و أثرهما على أمن هذه المو اقع .

٣-دراسة الكوادر البشرية المسئولة عن تأمين وإدارة مو اقع مر افق المعلومات المصرية على الإنترنت من حيث أعدادهم ومؤهلاتهم وتطويرهم المهنى.

٤- الوقوف على التحديات التى تواجه تأمين وحماية مو اقع مر افق المعلومات موضوع الدراسة على الإنترنت.

٥- اقتراح التوصيات التى تُساهم في رفع كفاءة وفعالية تأمين مو اقع مر افق المعلومات موضوع الدراسة.

٤/١ تساؤلات الد راسة:-

تسعى الدراسة للإجابة على التساؤلات التالية :

١- ما حوادث القرصنة التى استهدفت مو اقع مر افق المعلومات المصرية على الإنترنت؟ وما الدو افع ورائها ؟ وهل اختلفت باختلاف طبيعة نشاط المرفق نفسه؟ وما الخسائر الناجمة عنها؟ وكيف تم التعامل معها ؟

٢- هل تتو افر سياسات وخطط موثقة وفعَّالة لأمن المعلومات، وللاستجابة للحوادث، ولاستعادة النظام بعد الكارثة بمر افق الدراسة؟ وما الإجراءات المتبعة لتأمين مو اقع مر افق المعلومات المصرية على شبكة الإنترنت؟ وإلى أى مدى تُمثل نقاط قوة أو ضعف فى تأمين المو اقع المدروسة؟

٣-ما نوع الاستضافة لمو اقع مر افق المعلومات المصرية على شبكة الإنترنت موضوع الدراسة، وما لغات البرمجة المستخدمة لبناء هذه المو اقع؟ وإلى أي مدى تُمثل نقاط قوة أو ضعف في تأمين المو اقع المدروسة؟

٤-ما أعداد ومؤهلات الكودار البشرية المسئولة عن أمن مو اقع مر افق المعلومات المصرية على الإنترنت؟ وهل يتم تدريبهم وتنمية مهاراتهم بالشكل الملائم ؟ وإلى أي مدى تُمثل نقاط قوة أو ضعف لتحقيق أمن هذه المو اقع؟

٥-ما التحديات التى تواجه تأمين مو اقع مر افق المعلومات المصرية على شبكة الإنترنت من مخاطر القرصنة؟

٦-ماالتوصيات التي يمكن أن تساعد فى رفع كفاءة وفغالية تأمين مو اقع مر افق المعلومات المصرية على الإنترنت؟

١/٥ حدود الدراسة.

تضمنت الدراسة الحدود التالية:-

- الحدود الموضوعية: تناولت الدراسة أمن المعلومات كموضوع عام، ومنها الموضوع الأدق وهو القرصنة الإلكترونية على عينة من مو اقع مر افق المعلومات المصرية على الإنترنت، من حيث سياسات وإجراءات التأمين المتبعة والتحديات التى تواجه تأمين هذه المو اقع.
- الحدود النوعية:تضمنت الدراسة عينة من مو اقع مر افق المعلومات المصرية على شبكة الإنترنت والتى شملت المكتبات بأنواعها المختلفة، ومراكز المعلومات، والبو ابات الإلكترونية.
- الحدود المكانية:استهدفت الدراسة مو اقع مر افق المعلومات المصرية على الإنترنت.
- الحدود الزمنية: غطت الدراسة حتى نهاية أكتوبر ٢٠٢١.

١/٦ مصطلحات الدراسة

١/٦/١ القرصنة: Hacking

يُعرف قاموس(كامبريدج) مصطلح القرصنة بأنه:"الاستخدام غير المشروع لتقنيات الحاسبات الآلية للوصول إلى المعلومات المخزنة على أجهزة الحاسبات الأخرى، أو لنشر الفيروسات، والقرصانHacker: هو أى شخص يحاول اختراق أنظمة الحاسب والوصول دون حق مشروع " (Hacking, 2021).

ويُعرفها معاذ أحمد عبد الرازق أحمد بأنها: "استخدام نظم المعلومات والشبكات بطريقة غير مشروعة" وتصنف كأحد الجر ائم الإلكترونية وجر ائم الإنترنت (أحمد م.، ٢٠١٦).

وتجدر الإشارة إلى مصطلح أخر Piracy ويعنى النسخ أو البث أو إعادة إنتاج غير المصرح بهم للبرمجيات والمصنفات الفنية وحقوق التأليف بغرض بيعها (piracy, 2021)، ولكن هذا المصطلح خارج حدود الدراسة الحالية.

٢/٦/١ جر ائم الإنترنت: cybercrimes

تسمى أيضًا جريمة الحاسب الآلى computer crime وتعنى استخدام الحاسب الآلى كأداة لتحقيق غايات غيرقانونية أخرى مثل ارتكاب الاحتيال والاتجاربالأطفال والتجسس الأمنى والسرقة و التزويروالتصنت والقرصنة إلى غيرذلك من الأعمال الإجرامية المشابهة (cybercrime, 2021).

٣/٦/١ الهجمات الإلكترونية Attacks:

هى "محاولة للحصول على وصول غيرمصرح به إلى خدمات أو موارد أو معلومات النظام، أو محاولة المساومة على تكامل النظام وبمعنى موسع هو الفعل المتعمد لمحاولة تجاوز خدمة أمنية أو أكثر أو ضوابط نظام معلومات ويرتبط بهذا المصطح مصطلح أخر وهو الهجوم النشط active attack ويعنى اعتداءً فعليًا يرتكبه مصدرتهديد متعمد يحاول تغييرالنظام أو موارده، أو بياناته، أو عملياته. أما الهجوم السلبىpassive attack فهو اعتداء فعلى يرتكبه مصدر تهديد متعمد يحاول الاستفادة من معلومات النظام، لكنه لا يحاول تغيير النظام أو موارده أو بياناته أو عملياته " .(Attacks, 2021)

٤/٦/١الاختراقpenetration /التسلل intrusion :

هما مصطلحات مترادفان وفق ماورد بمعجم مصطلحات الأمن السيبر انى ويعرفان بأنهما:" فعل غيرمُصرح به؛ لتجاوزآليات الأمن لشبكة أو نظام معلومات" (penetration, 2021).

٥/٦/١ الأمن السيبر انى cybersecurity:

هو"النشاط أو العملية التي يتم بموجبها حماية وتأمين أنظمة المعلومات والاتصالات والدفاع عنها ضد الضرر أو الاستخدام غير المصرح به أو التعديل أو الاستغلال، يتطلب معرفة واسعة بالتهديدات المحتملة مثل الفيروسات أو الأشياء الخبيثة الأخرى. تُشكل إدارة الهوية وإدارة المخاطر وإدارة الحوادث جوهر استراتيجيات الأمن السيبراني للمؤسسة". (Cybersecurity، ٢٠٢١)

٦/٦/١ أمن المعلومات Information security

هو"حماية كافة أنواع المعلومات وأنظمتها سواء رقمية أو غير رقمية من الوصول أو الاستخدام أو الإفصاح أو الخلل أو التغيير أو التدمير غير المُصرَّح به بهدف توفير سرية تلك المعلومات وتكاملها واستمرارية توفرها"ويهدف أمن المعلومات الى تحقيق ثلاث مبادئ رئيسة تتمثل فيما يلى:

١- السرية Confidentiality : ويُقصد بها السرية في حماية البيانات من الاستخدام غير المرخص به .

٢- السلامة Integrity : وتعنى سلامة البيانات وحمايتها من العبث أو التدمير أو التغيير.

٣-الإتاحة Availability : أي استمرارية إتاحة المعلومات والسماح بالوصول إليها داخل (information security, 2021)

٧/٦/١ مر افق المعلومات: لأغراض الدراسة الحالية يتم تعريف مر افق المعلومات تعريفًا إجر ائيًا بأنها كل الهيئات والمؤسسات ذات الكيان المادى أو الرقمى التى توفر مصادر المعلومات وخدماتها للمستفيدين منها أيًا كانت تخصصاتهم وأهدافهم، ويشمل ذلك المكتبات بأنواعها المختلفة، ومر اكز المعلومات، والبو ابات الإلكترونية.

٧/١عينة الد راسة:

اتخذت الدراسة عينة عمدية من مو اقع مر افق المعلومات المصرية على شبكة الإنترنت وقد تم اختيارها وفقًا للمعايير التالية:-

١- أن تكون مُمثِّلة لكل فئات مر افق المعلومات بمفهومها الإجر ائي الذى تبنته الدراسة سلفًا والذى يشمل المكتبات بأنواعها المختلفة، ومر اكز المعلومات، والبو ابات الإلكترونية.

٢-أن تشمل مر افق حيوية فى طبيعة نشاطها وبارزة بدورها المجتمعى والحكومى وبالتالى تُشكل القرصنة خطرًا كبيرًا يُهددها.

٣- المو افقة على إجراء الدراسة والتعاون مع الباحثة – ويعد من أهم العوامل الحاكمة فى اختيار العينة - حيث رفضت عدة مر افق التعاون مع الباحثة لطبيعة الموضوع ونظرًا لسياستها التى تحظر تداول بيانات تخص أمن الموقع ومنها بنك المعرفة المصرى، ومكتبة الجامعة الأمريكية بالقاهرة، وبو ابة الحكومة المصرية، ومكتبة الجامعة البريطانية، ولهذا فقد تم استبعادهم من العينة.

٤-أن يكون لها مو اقع نشطة وثابتة على شبكة الإنترنت، وقد تبين للباحثة عدم استقرار موقع المكتبة القومية الزراعية أثناء فترة إجراء الدراسة لهذا فقد تم استبعاده من العينة، ويوضح الجدول رقم (١) مو اقع مر افق المعلومات التي شملتها عينة الدراسة:

جدول رقم (١) مو اقع مر افق المعلومات المصرية على الإنترنت عينة الدراسة

جدول رقم (١) مو اقع مر افق المعلومات المصرية على الإنترنت عينة الدراسة

مجتمع الدراسة	الفئة النوعية	الموقع

مكتبات مصر العامة.	مكتبة عامة	http://www.mpl.org.eg
مكتبة الاسكندرية.	مكتبة عامة	https://www.bibalex.org/ar
المكتبة المركزية لجامعة القاهرة	مكتبة جامعية	http://www.cl.cu.edu.eg/
دارالكتب و الوثائق القومية	مكتبة وطنية	http://www.darelkotob.gov.eg
مكتبة معهد الدراسات الشرقية للآباء الدومنيكان.	مكتبة متخصصة	https://www.ideo-cairo.org/ar/library
مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى.	مركز معلومات	https://www.idsc.gov.eg/IDSC/Default
بو ابة دار الافتاء المصرية.	بو ابة إلكترونية	http://www.dar-alifta.gov.eg
بو ابة جامعة طنطا	بو ابة الكترونية	https://www.tanta.edu.eg
اتحاد المكتبات الجامعية المصرية	بو ابة إلكترونية	http://main.eulc.edu.eg/eulc_v5/Libraries

لتحقيق أهداف الدراسة والإجابة على تساؤلاتها، استخدمت الباحثة المنهج الوصفى التحليلى لدراسة مو اقع الإنترنت لمر افق المعلومات واعتمدت على الأدوات التالية:-

- قائمة مراجعة: وهى الأداة الرئيسة لجمع البيانات عن حوادث القرصنة التي استهدفت المو اقع موضوع الدراسة ،وأساليب التأمين المتبعة بها، وقد تكونت من(١٠) بنود رئيسة متفرعة إلى(٤٧)عنصرًا فرعيًا شملت المحاور التالية:– حوادث القرصنة الإلكترونية على مو اقع الدراسة– سياسات أمن المعلومات- خطط الاستجابة للحوادث واستعادة النظام بعد الكارثة–أساليب التأمين المتبعة– اختبارات الاختراق– النسخ الاحتياطى– نوع الاستضافة– لغات البرمجة- الكوادر البشرية المسئولة عن أمن المو اقع– التحديات التى

تواجه تأمين مو اقع الدراسة. وقد كانت البيانات المطلوبة فى الحدود المسموح بتداولها من جانب المسئولين بالمر افق المدروسة حتى يتحقق الهدف من الدراسة دون المساس بأمن المو اقع، وقد قامت الباحثة بالزيارات الميدانية ومقابلة السادة العاملين بإدارات تقنيات المعلومات بالمر افق موضوع الدراسة لتطبيق قائمة المراجعة وجمع المعلومات اللازمة لإجراء الدراسة.

- تحليل المحتوى: قامت الباحثة بفحص المو اقع موضوع الدراسة للتعرف على مدى تطبيق بعض إجراءات التأمين والتى يمكن ظهورها بالموقع كبروتوكول HTTPS وشهادات الحماية SSL .

١/١٩الد راسات السابقة.

أولاً: الدراسات العربية.

استعانت الباحثة بالمصادر التالية للبحث عن الإنتاج الفكري الخاص بالموضوع:

- محرك البحث جوجل Google باللغة العربية.
- الفهرس الموحد لاتحاد المكتبات الجامعية المصرية .
- بنك المعرفة المصري خاصة قاعدة بيانات دار المنظومة ،والكشاف العربى للاستشهادات المرجعية.
- قاعدة بيانات الهادي المتاحة بموقع الاتحاد العربي للمكتبات والمعلومات (أعلم) .
- قواعد بيانات البو ابة العربية للمكتبات والمعلومات (Cybrarians).
- بو ابة البحث ResearchGate.

وقد أجُرى البحث باستخدام المصطلحات التالية:-

القرصنة الإلكترونية -الهجمات الإلكترونية -الجر ائم السيبر انية -اختراق مو اقع الانترنت -حماية البيانات -الأمن السيبر انى -مر افق المعلومات أو المكتبات.

وبمراجعة الإنتاج الفكرى الخاص بموضوع القرصنة الإلكترونية، يمكن تقسيمه إلى مستويين كما يلى:

المستوى الأول:الدراسات التي تناولت القرصنة الإلكترونية كموضوع خاص.

أظهرت نتائج البحث دراسة واحدة تناولت هذا الموضوع قدمها (أحمد م.، ٢٠١٦) دراسة تناولت أمن المعلومات وأهميته ودوره في الحد من مخاطر القرصنة الإلكترونية، وعرض نتائج تنفيذ عمليات القرصنة الإلكترونية للوقوف على مدى حجمها و آثارها السلبية، ثم دراسة حالة للمركز القومى للمعلومات بوزارة الاتصالات بأم درمان بالسودان للوقوف على

إجراءات التأمين المتبعة بالمركز ضد مخاطر القرصنة.استخدم الباحث منهج دراسة الحالة من خلال إعداد استبيان كأداة رئيسة وتم توزيعه على منسوبى المركز بأقسامه المختلفة و انتهى إلى عدة نتائج من أبرزها مايلى: تعرض المركز موضوع الدراسة للاختراق عدة مرات، أنسب الطرق المتبعة للتأمين هى:الجدران النارية، برامج الحماية من الفيروسات، أنظمة الحماية، من أهم دو افع القرصنة هى الأسباب السياسية والأمنية، كما صمم الباحث برنامج Spam Dedication كمقترح للإسهام في الحد من هذه المشكلة.

- المستوى الثانى:هو الأوفر عددًا وتُمثل الدراسات الى تناولت أمن المعلومات وهو المجال الموضوعى العام الذى يندرج منه القرصنة الإلكترونية، وتستعرض الباحثة أهم الدراسات التى تغطى هذا المستوى و أقربها للدراسة الحالية مرتبة زمنيًا من الأقدم للأحدث على النحو التالى:-

- دراسة (حسن ا.، ٢٠٠٥) وسعت إلى تحديد مفهوم أمن المعلومات وأهميته وأهدافه التى تسعى المؤسسات لتحقيقها ثم عرضت طرق اختراق أمن المعلومات وقسمتها إلى السرقة المتعمدة، والتخريب، وتدمير المعلومات عن طريق نشر الفيروسات، التجسس الصناعى، وسوء استخدام المعلومات، الإهمال، تدميرالمعلومات، كما تناولت مجالات اختراق أمن المعلومات وقسمتها إلى وباء أجهزة الفاكس، الملفات الورقية، الهاتف النقال، الثرثرة، التجسس و انتحال الصفة، الملفات الإلكترونية، ثم قدمت آليات تعزيز أمن المعلومات وتكونت من ثلاثة اتجاهات: الاتجاه الأول كان صياغة الإستر اتيجية الأمنية، الاتجاه الثانى التشريع والقانون، الاتجاه الثالث الأفراد العاملون فى المنظمة، ووضع الإجراءات الصحيحة فى التعامل مع الملفات الورقية، ومواجهة الفيروسات، و إنشاء وحدات أمن المعلومات.

- قام (النقيب، ٢٠١٠) بدراسة المخاطر التى استهدفت نظم إدارة المحتوى الرقمى بمشاريع الرقمنة بمؤسسات المعلومات العربية، والتعرف على إجراءات التأمين والحماية المطبقة بهذه المؤسسات للتصدى للمخاطر التى تتعرض لها نظم إدارة المحتوى الرقمى ومدى فعاليتها، وإستر اتيجيات الحماية والتأمين ضد المخاطروالاختراق المتبعة بمشاريع الرقمنة بمختلف القطاعات.وتمت الدراسة على أهم مشروعات الرقمية بالوطن العربى وتتمثل فى دار الكتب المصرية ،والمستودع الرقمى لمكتبة الإسكندرية، مكتبة الملك فهد الوطنية، ومكتبة المدينة الرقمية، والوراق، وبيليوإسلام، مركز توثيق التراث الحضارى والطبيعى.وقد اعتمدت الدراسة على أداة رئيسة هى الاستبيان حيث تم توزيعه على جميع العاملين بالمؤسسات موضوع الدراسة و انتهت الدراسة إلى عدة نتائج من أبرزها ما يلى:أن أكثر

مشـــروع رقمنة عرضـــة للمخاطر والاختر اقات هو دار الكتب المصـــرية، ومكتبة الملك فهد الوطنية، ثم مكتبة الإسكندرية، أن المخاطر التى تأتى من داخل المؤسسات أكثر خطورة من التى تأتى من خارجها ويتمثل ذلك فى الإدخال غير المتعمد لبيانات غير ســـليمة و التدمير المتعمد للبيانات من جانب العاملين وإدخال الفيروسات لأنظمة الحاسب .

- استهدفت دراسة (إسماعيل، ٢٠١٠) التعريف بالمخاطر التى يمكن أن تهدد النظم الآلية المتكاملة المتو افرة بالمكتبات الحكومية بمصر، و أنواعها، وأسبابها، وطرق الحماية منها. وقد استخدمت الباحثة المنهج الوصفى التحليلي واعتمدت على الاستبيان وتوجيهه إلى من عينة من مديرى المكتبات موضوع الدراسة، ومسئولي تأمين النظم والشبكات ومسئولى الدعم الفنى، واختصاصيى المكتبات، والمبرمجين للحصول على البيانات عن المخاطر التى تهدد المكتبات موضوع الدراسة وكذلك أساليب الحماية المتبعة بها.
- تناولت دراسة (حسنين ، ٢٠١٢) مفهوم الشبكات والأسباب التى أدت إلى ظهورها، ثم مفهوم أمن شبكات المعلومات وأسبابه والتى أرجعها الباحث إلى التقدم التكنولوجى، والطفولية والاندفاع لبعض الأشخاص للحصول على معلومات بطرق غير مشروعة، و انتشار جر ائم المعلومات، ثم تطرق إلى مكونات أمن شبكات المعلومات، وأسباب الهجوم عليها والتى حددها فى الأسباب التالية:١- وجود الدافع كأن يكون سياسيًا وماديًا أوالتحدى و إثبات الذات أوالانتقام ٢- وجود ثغرات بالنظام تسمح بالاختراق٣ - وجود خطة للهجوم، ثم تطرق إلى مصادر الخطر علىأمن الشبكة وقسمها إلى نوعين: داخلى وخارجى، ثم عرض أساليب الحماية والتأمين، وأخيرًا حدد متطلبات أمن شبكات المعلومات فى سبعة مطالب من أهمها العنصر البشرى، بروتوكولات التحقق والتشفير، وحسن اختيار مو اقع نقاط الشبكة.
- سعى الباحثان (أصيل و العي، ٢٠١٤) فى دراستهما إلى تقييم الأساليب والوسائل المستخدمة والإجراءات المتو افرة لحماية أمن المعلومات بجامعة الملك عبد العزيز والكشف عن مدى تو افر خطط للطوارئ ثم الوقوف على المشكلات والتحديات التى تواجه منظومة الأمن بالجامعات السعودية، حيث اعتمدا على منهج دراسة الحالة و انتهت إلى عدة نتائج من أبرزها ما يلى:افتقار إدارة أمن المعلومات والجودة إلى العدد الكافي من العاملين المؤهلين في مجال أمن المعلومات، عدم وجود ميز انية ثابتة أو ميز انية سنوية مخصصة لإدارة أمن المعلومات، وجود سياسة مكتوبة للأمن المعلوماتي بجامعة الملك عبد العزيز، بالإضافة إلى اعتماد مجموعة متنوعة من الوسائل والأساليب والإجراءات لتوفير الأمن

المعلوماتي بالجامعة، تتمثل فى توفير برامج الحماية ضد الفيروسات، والجدران النارية، والتوقيع الرقمي، والتشفير،والنسخ الاحتياطي، تقييد النفاذ إلى خوادم الملفات، والمجلدات، وتخصيص اسم مستخدم وكلمة مرور لكل مستخدم.

- استهدف الباحث (حمودة،ب.ا، ٢٠١٤) دراسة سياسة أمن المعلومات ومدى تو افرها بشبكات المعلومات بالمكتبات حيث قدم تعريفًا لأمن المعلومات، و أنواع التهديدات والمخاطر التي يمكن أن تواجهها أنظمة المعلومات في المكتبات، ثم عرض مفهوم السياسات الأمنية وأهميتها والعناصر التى ينبغى أن تغطيها، يليها دراسة وثيقة سياسة أمن المعلومات بشبكة المكتبات بجامعة النيلين، ثم قدم مجموعة من التوصيات من أهمها:الحاجة لزيادة وعى أعضاء هيئة التدريس والطلاب والعاملين بأمن المعلومات وأهميته ومخاطر عدم تو افره، ضرورة إعداد وثيقة لأمن المعلومات تتضمن عناصر تتفق مع السياسات على أن يتم مراجعتها بصورة دورية، ضرورة تو افر المكونات المادية والبرمجيات اللازمة للتأمين.
- قدم (العربى، ٢٠١٥) دراسة عرض فيها معايير ٢٧٠٠٢ الصادر عن المنظمة الدولية للتوحيد والقياس (الأيزو) والسياسات والبنود التى تنص عليها سعيًا للتعرف على مدى تو افرها بمو اقع أفضل الجامعات العربية والتى تم تحديدها وفق تصنيف ويبو ميتركس لعام ٢٠١٢ وقد أعتمدت الدراسة على قائمة المراجعة كأداة أساسية لجمع البيانات عن عناصر معايير تقييم أمن المعلومات والوقوف على مدى تطبيقها بالجامعات موضوع الدراسة، و انتهت الدراسة إلى عدة نتائج من أبرزها مايلى: كان معيار السياسات الأمنية هو أقل المعاييرتو افر ابنسبة ١٩,٠٥٪

تطبق جامعة الملك عبد العزيز ٩٥ معيارًا بنسبة ٧١,٤٣٪ من أجمالى المعايير وبذلك تأتى فى المرتبة الأولى يليها جامعة الملك فهد للبترول والمعادن ٥٨,٦٥٪ وبلغت نسبة الجامعات التى لم تطبق ٥٠٪ من المعايير الفرعية ٨٠,٩٥٪ من إجمالى الجامعات.

- أعدت (يس، ٢٠١٥) دراسة استهدفت البنية الأمنية للحوسبة السحابية، والمزايا والتحديات الأمنية لاستخدام المكتبات للحوسبة السحابية وكيفية تحليل المخاطر الأمنية للسحابة، والمعايير الأمنية الخاصة بإدارة البيانات بالسحابة والسياسات الواجب على المكتبات مراعاتها لحماية بياناتها وخدماتها الحساسة المستضافة بالسحابة التى يتم استخدامها فى نفس الوقت من قبل مستأجرين متعددين.اتبعت الباحثة المنهج الوصفى التحليلي لتحديد الو اقع الحالى للوضع الأمنى للسحابة وتقديم المقترحات التى تساعد المكتبات عند انتقالها لاستخدام السحابة، و انتهت إلى عدة نتائج من أهمها ما يلى: يعد

التحليل العميق لمخاطرالاخفاقات الأمنية للخصوصية والنزاهة والسرية التى يمكن أن تحدث لموفر السحابة تبعًا لمستوى حساسية المعلومات من أهم الاعتبارات التى تحمى المكتبات من الكثير من المشكلات، هناك عدة أساليب لحماية بيانات السحابة كالمصادقة، والتشفير والجدران النارية الافتراضية والمادية، ضرورة اهتمام المكتبات باستراتيجيات الخروج من السحابة كاهتمامها بإستراتيجيات الدخول فيها فى حال فك الارتباط مع موفر الخدمة أو دمجها مع خدمة مؤسسة أخرى.

- قدما(كوبى و خالد، ٢٠١٧) دراسة حالة حول أهمية أمن المعلومات في المكتبات ومراكز المعلومات، وتناولت التهديدات لأمن المعلومات، والمخاطر التي تجعل المكتبات ومراكز المعلومات أكثر عرضة لهذه التهديدات.وتكونت الدراسة من جزأين: الأول يتضمن تعريف وأهمية أمن المعلومات، والمبادئ الأساسية لأمن المعلومات ومجالاته وتخصص أمن المعلومات، والمخاطر التى يشكلها الإنترنت على أمن المعلومات، وتصنيف الجرائم الإلكترونية والطرق ووسائل الحفاظ على أمن المعلومات، وأخيرًا توعية الطلاب بأمن المعلومات والأخلاق. أما الجزء الثاني فيتناول سياسات أمن المعلومات في المكتبات ومراكز المعلومات وتطبيقها على مكتبات جامعة زاخو فى إقليم كوردستان العراق كدراسة حالة. يؤكد البحث على ضرورة وجود وثيقة سياسة أمن المعلومات في المكتبات ومراكز المعلومات متبوعة بمجموعة من الإجراءات والتعليمات. كما يقدم مجموعة من التوصيات لتحديد مدى ملاءمة هذه السياسات لتحقيق أمن المعلومات في المكتبات ومراكز المعلومات.
- قدم (زيدان، ٢٠١٨) دراسة تناولت تحليل الثغرات الأمنية التي تهدد مو اقع أقسام المكتبات والمعلومات المصرية على الإنترنت وتحديد أنواعها وعددها بكل موقع وتقديم الإجراءات الضرورية اللازمة لإصلاح هذه الثغرات، فضلاً عن تحديد أخطر أنواع الثغرات التي تهدد مو اقع الويب على مستوى العالم والتعرف على البرامج والأدوات المستخدمة في عملية اختبار تطبيقات الويب والحماية من الثغرات. استخدم الباحث المنهج الوصفى التحليلي لرصد وتجميع الثغرات الأمنية بالمو اقع موضوع الدراسة من خلال تطبيق برنامج Vega للفترة من ١-١-٢٠١٨ إلى ١٥-٣-٢٠١٨، و انتهى إلى عدة نتائج من أبرزها مايلى: أن ٩٤٪ من مو اقع أقسام المكتبات والمعلومات بالجامعات المصرية يتضمن ثغرات أمنية وأن ٦٪ لايوجد به أى ثغرات، يوجد أكبر عدد من الثغرات الأمنية بموقع قسم المكتبات والمعلومات بجامعة المنوفية بنسبة ١٨٪ من اجمالى الثغرات، تعد ثغرة (حقن الأوامر) أعلى نسبة

للثغرات عالية الخطورة بنسبة (٣٢٪)، يوجد(٢٤) نوع من الثغرات بمو اقع الدراسة منها (تسعة) أنواع عالية الخطورة، و(ثلاثة) متوسطة الخطورة، و(ثلاثة) منخفضة الخطورة.

- قام (حسن و الجوهرى، ٢٠٢٠) بإعداد دراسة استهدفت التعرف على المخاطر التي تهدد أمن المعلومات فى البيئة الرقمية بمختلف أنواعها وصورها، ثم الوقوف على المقومات الواجب تو افرها لمواجهة هذه المخاطر ومنها المقومات المادية والتقنية والتنظيمية والتشريعية على المستوى الوطنى و أيضًا الدولى مع إلقاء الضوء على المعايير الدولية الصادرة عن منظمة الأيزو لضبط إجراءات أمن المعلومات. و انتهت الدراسة إلى عدة نتائج من أبرزها مايلى: ضعف التشريعات والقو انين الموجودة على أرض الو اقع مع وجود بطء ملحوظ في مدى كفاية التشريعات الموجودة للحد من عمليات التعدى على أمن المعلومات، يتعرض أمن المعلومات للعديد من المخاطر والتهديدات التى تتم في بيئة الإنترنت مع صعوبة مو اكبة أساليب التأمين لسرعة تطور الأساليب المستخدمة في عمليات الاعتداءات على أمن المعلومات.

ثانيا : الدراسات الأجنبية :

كما قامت الباحثة بالقراءة الاستطلاعية لتحديد المصطلحات المناسبة، ثم أجرى البحث باستخدام المصطلحات التالية:

information security--Hacking –cyberattacks- Data protection- penetration cybersecurity - websites threats- system Vulnerability

وقد تم البحث عنها بالمصادر التالية:-

١- محرك البحث Google باللغة الإنجليزية وجوجل الباحث الأكاديمي Google Scholar.

٢- بو ابة البحث ResearchGate.

٣- بنك المعرفة المصري وتحديدًاقواعد بيانات :

Proquest theses, ERIC, SAGE Emeralled, Science Direct, EBSCO LISTA.

٤- قاعدة بيانات سكوبس SCUPES.

و قد أسفر البحث عن عدد من الدراسات الأجنبية،قسمت وفقاً للمستويين السابقين وُرتبت داخل كل مستوى زمنيًا من الأقدم للأحدث على النحو التالى:-

المستوى الأول: :الدراسات التي تناولت القرصنة الإلكترونية كموضوع خاص.

- عام ٢٠١٤ قدمت منجال (Munjal, 2014) دراسة استهدفت التعريف بالجانب الإيجابى للقرصنة والتى يطلق عليها القرصنة الأخلاقية وعرفتها بأنها طريقة للكشف عن نقاط

الضعف والثغرات الأمنية بالأنظمة ومو اقع الإنترنت و والاستعداد لها والتغلب عليها قبل الوقوع بالفعل فى بر اثن المجرمين، ولهذا تسعى كافة المؤسسات حاليًا للتعامل مع القراصنة الأخلاقيين سعيًا لحماية أفضل. كما تعرضت لمفهوم القراصنة الأخلاقيين و أنواعهم فى مقابل المعنى السلبى الضار المتعارف عليه للقرصنة من الاختراق غير القانونى للأنظمة بغرض السطو أو التدمير أو السرقة. وقد أظهرت الدراسة عدة نتائج من أهمها أن هناك تأثيرًا سلبيًا للقرصنة غير الأخلاقية على المجتمع، وأن ما يقرب من(٩٠٪) من الهجمات تحدث من داخل المؤسسات مما يدل على سهولة اختراق النظام أو الشبكة من الداخل.

- عام ٢٠١٧ قدم سميث (SMITH F. A., 2017) دراسة تناول فيها مفهوم القرصنة الإلكترونية، وصورها فى المكتبات ومر افق المعلومات كهجمات الحرمان من الخدمة، وحقن SQL، أو إيجاد منفذ مفتوح أو ثغرة فى النظام. كما استعرض حوادث القرصنة الشهيرة لمو اقع الإنترنت لكثير من المؤسسات ومنها حادث اختراق موقع معهد ماساتشوستس للتكنولوجيا(MIT) على الإنترنت عام ٢٠١٣ وغيرها، كما تناول أشهر القراصنة الذين استهدفوا القرصنة على الكتب الإلكترونية و أكدت الدراسة فى نتائجها أن المكتبات ومر افق المعلومات تواجه تحديًا أمنيًا من نوع فريد لتأمين المجموعات الرقمية التى تم انتاجها إلكترونيًا من الأصل مع الأخذ فى الاعتبار حماية المجموعات التاريخية الهامة التى يمكن استهدافها من قبل قراصنة سياسيين.
- عام ٢٠٢١ أعدت ريشمى (Reshmi , 2021) دراسة عن هجمات برامج الفدية باعتبارها أخطر المهددات و أكثرها انتشاراً فى البيئة الرقمية حيث تقوم بتشفير الملفات الهامة وتصبح عديمة الفائدة ثم طلب دفع مبالغ مالية مقابل فك التشفير واستعادة الملفات والبيانات مما يشكل عبئًا ماليًا ضخمًا على المؤسسات. استخدمت الباحثة منهج المراجعة المنظمة للإنتاج الفكرى المنشور عن هجمات برمجيات الفدية فى العشر سنوات من ٢٠١٠ حتى ٢٠٢٠ حيث تناولت مفهومها و الأنواع المختلفة منها ونقاط الضعف في نظام التشغيل Windows، وأساليب الهجوم المستخدمة لتنفيذ هذا النوع من الهجمات، والآثار المترتبة عليها وسبل الحماية منها. تم رصد ٤٦ نوعاً لبرامج الفدية ظهرت من عام ٢٠١٣ وحتى ٢٠١٩ من أشهرها WannaCry GandCrab and BitPaymer، أن Wannacry Ransomware يستهدف بشكل أساسي أجهزة Windows 7 لشن الهجمات حيث يقوم بتشفير الوثائق والملفات ونقلها إلى مجلد مؤقت باسم وامتداد جديد، وقد رصدت الدراسة

١٥ أداة للحماية من برامج الفدية من أمثلتها Cryptodrop، و File Finger Printing Technique (FFT)

ثانيا: الدراسات التى تناولت أمن المعلومات: وتستعرض الباحثة الأقرب للدراسة الحالية على النحو التالى:

- هدفت دراسة كوزما (Kuzma, 2010) إلى التعرف على ثغرات الويب الموجودة في مو اقع المكتبات الأوروبية على الإنترنت وكيف يمكن أن تؤثر هذه المشكلات على حماية بيانات مستفيديها. تم استخدام أداة اختبار ثغرات الويب لتحليل مو اقع الويب ٨٠ مكتبة أوروبية في أربع دول هى إنجلترا وفرنسا وألمانيا و إيطاليا للكشف عن مستوى الأمان الموجود بمو اقع مكتبات الدراسة وتحديد نقاط الضعف وعدد الثغرات الأمنية بكل منها والوقوف على الاختلافات بين الدول فى توفير أنظمة أمنية للمكتبات. وقد انتهت الدراسة إلى عدة نتائج - أن الغالبية من مو اقع الدراسة لديها عيوب خطيرة فى تأمين تطبيقات الويب الخاصة بهم، و أنه على الرغم من فرض قو انين الحماية والتأمين الخاصة بكل دولة، لم يقم أمناء المكتبات بتنفيذ التدابير المناسبة لتأمين مو اقعهم على الإنترنت .
- قدم أوبر اين وأخرون (O'Brien , 2018) دراسة عن حماية الخصوصية لمو اقع الويب للمكتبات الأكاديمية واستكشاف مدى تطبيق برتوكول تشفير HTTPS وشهادات الأمان SSL وخدمات تحليلات جوجل Google Analytics ومميزات حماية الخصوصية الموجودة شملت الدراسة ٢٧٦ موقع للويب للمكتبات الأكاديمية، أظهرت نتائج الدراسة محدودية تطبيق بروتوكول HTTP على مو اقع مكتبات الدراسة بنسبة بلغت ٣٪ ويشير ذلك إلى تقديم اتصالات غير مؤمنة. فى حين تستخدم (٣٤,١٤٪) Google IP Anonymization على الرغم من أن غالبية مو اقع المكتبات المُدرجة في الدراسة تطبق Google Analytics و/ أو Google Tag Manager إلا أن عدد قليل جدًا من الأشخاص يتصلون اتصال آمن بـ Google عبر تطبيق برتوكول HTTPS أو اخفاء الهوية لتحليلات جوجل Google Analytics IP anonymization.
- عام ٢٠٢٠ أعد فافوسيس وأخرون (Vavousis & ect, 2020) دراسة استهدفت تحليل تطبيق اللائحة العامة لحماية البيانات (GDPR) لتأمين مو اقع الانترنت لشبكة المكتبات اليونانية التابعة لمكتبة اليونان الوطنية Greek Libraries Network of NLG البالغ عددهم ٢٣٣ مكتبة باليونان بالاضافة إلى مكتبة واحدة بقبرص. حيث ناقشت الدراسة أهمية اللائحة العامة لحماية البيانات كأداة هامة لتأمين المو اقع لاعتمادها على أسلوب

الخصوصية على حسب التصميمprivacy by design وليس افتراضيًا privacy by defaultبمو اقع الدراسة كما ألقت الضوء على الثغرات الامنية التى قد تهدد مو اقع المكتبات اليونانية كالحقن بأنواعه المختلفة، و انتهت الدراسة إلى عدة نتائج من أبرزها مايلى: قامت ١٧ مكتبة أن من إجمالي ٧٣ مكتبة لديها مو اقع على الإنترنت بتحديث سياسات الخصوصية كما أن ٢٥ منهم فقط تستخدم SSL لتأمين البيانات المرسلة، توصلت اللائحة العامة لحماية البيانات إلى وضع قواعد جديدة فيما يتعلق بكيفية إدارة البيانات الشخصية على مو اقع الويب كما تفرض غرامات على المؤسسات التى لا تمتثل مو اقعها لقو انين اللائحة.

- هدفت دراسة (Amini, Vakilimofrad , & Saber, 2021)إلى تصميم نموذج لتحديد العوامل البشرية المؤثرة فى أمن المعلومات بالمكتبات العامة والأكاديمية بمدينة همذان بإيران، فنجاح أمن المعلومات يعتمد على السلوك البشرى الصادر من العاملين والمسئولين والمستفيدين.استخدم الباحثان لاستبيان كأداة لجمع البيانات من ١٠٠ من المديرين والعاملين، وتم تحليلها باستخدام smart PLS SPSS 16 وقد اعتمد النموذج على ستة متغيرات هى: مستوى المهارة، احترام الذات، الخبرات، ثقافة الأمن، مستوى التعليم، الأخلاق. وأظهرت نتائج التجربة أن أعلى درجة من بين مكونات أمن المعلومات للمكتبات الإير انية كانت المخصصة لتقدير الذات ومستوى المهارة فى حين أن أدنى درجة كانت لمستوى التعليم، وجاءت الخبرات فى المرتبة الأولى، فى حين أن مستوى المهارة كان له أقل تأثير على أمن المعلومات.

التعقيب على الدراسات السابقة.

من العرض السابق يتبين ندرة الدراسات العربية التى تناولت القرصنة الإلكترونية كموضوع خاص على عكس الدراسات الأجنبية التى أهتمت بمعالجة هذا الموضوع بشكل أكبر، حيث اتجهت الدراسات العربية نحو موضوع أمن المعلومات بمحاوره المختلفة، لذا تأتى الدراسة الحالية لسد هذه الثغرة فى الإنتاج الفكرى العربى والتعرف على و اقع القرصنة بعينة الدراسة من مر افق المعلومات المصرية والتى لم تخضع لهذه الدراسة من قبل .

ثانياً : الإطار النظري

١/٢ دوافع القرصنة :

هناك العديد من الدو افع التى تقف وراء هجمات القرصنة على مو اقع الإنترنت ويمكن حصرها فيما يلى:

١- دو افع اقتصادية: ويقصد بذلك الاختراق نظير الاستفادة المالية والحصول على مبالغ كبيرة كأن يكون الاختراق مدفوع الأجر من جهات أخرى منافسة بغرض الإضرار أو سرقة المعلومات ثم استخدامها للابتزاز المادى للمؤسسة المسئولة عن الموقع .

٢-التحدى التقنى و إثبات الذات: تشكل الرغبة فى إثبات الكفاءة و القدرة التقنية للمخترق أحد دو افع القرصنة، فتتولد أحيانا بعض لحظات الأنانية التى يسعى فيها المخترق إلى إثبات ذاته ومهاراته فى اختراق المو اقع المحصنة و اكتشاف نقاط ضعفها واشباع غروره وقدرته على التحدي التقنى والنجاح فى انتهاك إجراءات الحماية و الخصوصية المتبعة بها، أو للشهرة كما يحدث فى حالات كثيرة من القرصنة على مو اقع الحكومية فى كافة أنحاء العالم .

٣- دو افع سياسية وعسكرية: ويستهدف ذلك الهجوم على مو اقع الإنترنت كمو اقع الحكومات والأجهزة الحساسة بالدول لتحقيق أهداف ومخططات سياسية وعسكرية، فمحرك أنشطة الإرهاب الإلكتروني وحروب المعلومات على سبيل المثال هى الدو افع السياسية والعسكرية حيث أصبحت المعرفة والمعلومات سلاح العصر الرقمى والمعيار الذى يحكم توازنات القوة العسكرية والسياسة والاقتصادية على الصعيد الدولى.

٤-دو افع أمنية: وتعنى دو افع إيجابية حيث تضطر بعض الحكومات لمر اقبة تدفق البيانات والاتصالات لبعض الأشخاص أو جماعات معينة من أجل منع بعض العمليات الإجرامية أو الإرهابية التى قد تمس الأمن القومى للدول أو عمليات غسيل الأموال المشبوهة ...وغيرها من الأعمال الإجرامية. (أحمد أ.، ٢٠١٤).

٥-الرغبة فى الانتقام: ويتولد هذا الدافع لدى أحد العاملين بمؤسسة ما بهدف الانتقام من قياداته أو زملائه نتيجة لعدم الرضا الوظيفى أو المادى أولوجود خلافات شخصية مما يدفعه إلى الانتقام واختراق الموقع والشبكة الداخلية للمؤسسة وإظهار ضعفهم والثغرات الأمنية الموجودة بالموقع .

٦-التسلية واللهو وحب المغامرة: فى بعض الأحيان يكون الدافع لاختراق مو اقع الإنترنت هو التسلية أو الفضول للتعرف على الأنظمة الأمنية لمو اقع الآخرين على الإنترنت واللعب دون إحداث ضرر أو مخاطر تُذكر.

٧-الرغبة في جمع المعلومات وتعلمها: للقراصنة منطق خاص بهذه النقطة حيث يرون أن اختراق نظم الحاسبات ومو اقع الإنترنت يساعد فى فهم العالم مؤمنين بضرورة إتاحة تداول وجمع ونسخ المعلومات المفيدة دون قيود.

٨-التطرف الدينى ونشر الفتن الطائفية والعرقية. (Cekerevac & ect, 2018)

٢/٢أنواع القرصنة الإلكترونية .

يمكن حصر أهم أنواع القرصنة الإلكترونية فيما يلي :

١-القرصنة العبثية التخريبية :وتستهدف التخريب والتدمير عن طريق نشر الفيروسات أو البرامج التخريبية .

٢-القرصنة العدائية:وهى أخطر أنواع القرصنة التى تحدث إما بدافع السطو وسرقة الأموال والابتزاز المادى.

٣-القرصنةالسياسية والاجتماعية Hacktivism الهاكتيفيزم: ظهر هذا المصطلح فى بداية القرن الواحد والعشرين بفعل تز ايد معدلات الهجمات الإلكترونية التي تحمل أبعادًا سياسية واجتماعية حيث يشير إلى استخدام القرصنة الإلكترونية لتحقيق أهداف ومخططات سياسية أو للاحتجاج وليس لدافع شخصى السرقة أو الابتزاز المادى. ومن أشهر ممارسات الهاكتيفيزم تسريب وثائق "ويكيليكس" والتى تُعُد أكبر عملية قرصنة شهدتها الشبكة العنكبوتية وكذلك تسريبات وثائق بنما وتعد مجموعة" آنونيموس "إحدى أشهر المجموعات الإلكترونية النشطة التي تندرج تحت مفهوم "الهاكتيفزيم".

٤- القرصنة الأخلاقية :هي طريقة لمعرفة نقاط الضعف والثغرات في النظام أو شبكة الحاسب الآلى وهى وصف لإجراء القرصنة بطريقة أخلاقية ويطلق عليها أيضًا اختبارات الاختراق. (Cekerevac & ect, 2018)- وسيتم تناول هذه المصطلح بشيءٍ من التفصيل فى ثنايا الدراسة التطبيقية.

٣/٢ أساليب القرصنة الإلكترونية.

تتعدد أنواع الآليات والأساليب المستخدمة لشن الهجمات الإلكترونية على مو اقع الإنترنت، كما تتفاوت فى حجم الضرر الناجم عنها ومن أشهرها ما يلى:-

❖ البرمجيات الخبيثة Malware Attacks

تعد أشهر أنواع الهجمات وتشمل البرامج الضارة بما فى ذلك الفيروسات(Viruses) والديدان (Worms) وأحصنة طروادة (Trojan) وملفات التعريف والارتباط الكوكيزCookies وبرامج التجسس وبرامج الفدية (Chapman , 2016).

وطبقًا للتقرير السنوي للتأمين السيبر انى العالمى لعام ٢٠٢٠ بلغ عدد البرمجيات الخبيثة (٧٧,٦٦) مليون برنامج (Johnson، ٢٠٢١)، وُقدرت عدد الهجمات الإلكترونية التى تمت عبرهذه البرمجيات (٥٥) بليون (Joseph Johnson, Annual number of malware attacks worldwide from 2015 to 2020, 2021)

❖ هجمات التصيد الاحتيالي Phishing Attack

تعد هجمات التصيد الاحتيالي من أكثر أنواع الهجمات الإلكترونية انتشارًا حيث تم تحديد(637,302) موقع للتصيد في الربع الأخيرمن عام ٢٠٢٠ (Joseph Johnson, Number of unique phishing sites detected worldwide from 3rd quarter 2013 to 2nd quarter 2020, 2021) وهى نوع من هجمات الهندسة الاجتماعية يقوم المهاجم فيه بانتحال صفة جهة اتصال موثوقة ويُرسل للضحية رسائل بريدية مزيفة.

❖ هجمات كلمات السر:هو شكل من أشكال الهجوم حيث يقوم أحد المتطفلين باختراق كلمة المرورالخاصة بالضحية باستخدام العديد من البرامج وأدوات اختراق كلمة المرورمثل Aircrackو Cain وAbel و John the Ripper و Hashcat وما إلى ذلك. وهناك أنواع مختلفة من هجمات كلمات المرورمثل هجمات القوة الغاشمة وهجمات القاموس.

❖ هجوم الرجل فى المنتصف Man-in-the-Middle Attack

يُعرف هجوم الرجل في المنتصف (MIT)أيضًا بهجوم التصنت في هذا الهجوم حيث يدخل المهاجم فى اتصال بين طرفين، أى أن المهاجم يخطف الجلسة بين العميل والمضيف ثم يقطع الاتصال بين الخادم والعميل وبالتالى يمر خط الاتصال عبر المتسلل والذى يقوم بسرقة البيانات والتلاعب بها.

❖ هجمات حقن SQL Injection Attack

تهدف إلى المساس بصفحات الويب وقواعد البيانات عن طريق استغلال ثغرة أمنية وحقن رمز خبيث في مربع بحث موقع الويب وبهذه الطريقة يمكن خداع الموقع لتنفيذ

الأوامروالوصـول لقاعدة البيانات مما يجعل الخادم يكشـف عن معلومات مهمة ويعرض أمن وخصوصية البيانات لخطر السرقة أو التعديل أو الحذف.

❖ هجمات حجب الخدمة Denial-of-Service Attack (DOS)

يعد هجوم حجب الخدمة تهديدًا كبيرًا للشـركات والذى يسـتهدف الأنظمة أو الخوادم أو الشبكات ويغمرها بحركة المرورلاستنفاد مواردهم ونطاقهم الترددي وتصبح تلبية الطلبات الواردة أمرًا مُربكًا للخوادم مما يؤدى إلى إغلاق موقع الويب الذي يسـتضـيفه أو إبطائه، ويجعل طلبات الخدمة المشـروعة دون رقابة. وعندما يسـتخدم المهاجمون أنظمة متعددة لشن هذا الهجوم يسمى هجمات حجب الخدمة الموزعة (DDoS Distributed Denial-of-Service)

❖ استغلال يوم الصفر Zero-Day Exploit

هو الهجوم الذى يحدث فى نفس يوم اكتشاف ثغرة بنظام التشغيل أوالشبكة ولم يمضى على اكتشافها ولا يوم واحد، ويتم استغلالها قبل اكتشافها من الجهة المُطورة نفسها أن يصبح الإصلاح متاحًا من منشئه. يمكن للمتسللين استخدام عمليات استغلال لليوم صفر للوصول إلى البيانات أو الشبكات أو تثبيت البرامج الضارة على جهاز (Chapman , 2016)

❖ التهديدات الداخلية Insider Threats

تأتى الهجمات السابقة من خارج المؤسسة،أما التهديدات الداخلية فُينفذها فردُ من داخل المؤسسة يمتلك إمكانية الوصول لحسابات متعددة دون ضو ابط ويترتب على ذلك أضرارجسيمة من حذف أوتعديل أو تزوير أوسرقة للبيانات أو إيجاد ثغرات فى النظام الأمنى ولهذا، يعد أكثرخطورة من الهجمات الخارجية لسهولة حدوثها وصعوبة اكتشافها أو التنبؤ بها وقد تحدث هذه الخدمات بدافع الجشع أو الحقد أوالانتقام أوحتى الإهمال والخطأ غير المتعمد.

٤/٢:سياسة أمن المعلومات Information Security Policy

هى سياسة مكتوبة ومعلنة تتضمن تفصيليًا التوجيهات واللو ائح والقواعد المتعلقة بأمن المعلومات بالمؤسسة من خلال البنود التالية: (Library Computer And Network Security; Library Security. Principles; Creating A Security policy, 2010):

أ- الأهداف: وتشمل حصرلكافة أنواع الأصول والممتلكات التي تحتاج المؤسسة إلى حمايتها وإجراءات ذلك.

ب- المجال: ويشمل تحديد الأصول المطلوب حمايتها من خلال السياسة ونتائج تحليل المخاطر فضلاً عن تحديد الأشخاص المسئولين عن الالتزام بهذه السياسة .

ج- المسئوليات: وتتضمن تحديد دقيق لمسئولية كل شخص عبر توصيف محدد للوظائف.

د- إجراءات التأمين: وتتضمن ذلك إجراءات التأمين ومستوياته ومنها التأمين المادى، وتأمين الأجهزة، والعاملين، والشبكة، والنظام.

هـ – العقوبات: تشمل العقوبات التى يتم اتخاذها في حالة عدم الامتثال للضو ابط الأمنية و انتهاك السياسات ومنها على سبيل المثال:(فقدان المستخدم التمتع ببعض امتيازاتها) (منع الاتصال بالشبكة).

ويعد وجود سياسة أمنية موثقة بمثابة حجر الزاوية لتحقيق منظومة أمنية سليمة وتحديد المسؤولية في حالة وقوع حادث ولا توجد سياسة توفر تأمينًا كامًلا ولكن على كل مؤسسة أن تسعى للاقتراب من الكمال، ونظرًا للتغير المستمر للمخاطر والتهديدات فمن الضرورى مراجعة السياسة وتحديثها سنويًا للمساعدة على إبقاء نظام أمن المعلومات محدثًا ويمكنه التعامل مع أى حوادث مستقبلية.

٥/٢خطط الاستجابة للحوادث واستعادة النظام بعد الكارثة:-

تتطلب إدارة الأزمات والمخاطر الإلكترونية وضع سياسات قوية ومحكمة لضمان استئناف العمل فى أقل وقت وخسائرممكنة، حيث تعد قدرة أى مؤسسة على السرعة والكفاءة فى الاكتشاف والاستجابة واستعادة النظام بعد حادث إلكترونى طارئ من مؤشرات نضجها الأمنى، ويتمثل ذلك فى تطوير خطط الاستجابة للحوادث والتعافي أواستعادة النظام بعد الكوارث.

١/٥/٢ خطة الاستجابة للحوادث Incident Response plan. (IR)

هى خطة مكتوبة موثقة تعمل على تحديد الأفراد وأدوارهم والإجراءات المعمول بها فى حالة حدوث أى هجمة إلكترونية، وترجع أهمية وجود هذه الخطة إلى الاستعداد المسبق لأى هجوم واكتشافه واحتوائه ومنع تصعيده وإزالته ثم استعادة النظام بسرعة وفعالية، وبالتالي تقليل وقت التوقف عن العمل والأضرار الناتجة عنه، وتشمل الخطة الناجحة العناصر التالية :

- إجراءات كل خطوة من خطوات الاستجابة للحوادث.
- أدوار ومسؤوليات كل قسم للاستجابة للحوادث.
- قنوات الاتصال بين فريق الاستجابة للحوادث وبقية أفراد المؤسسة.

- وضع مقاييس لتحديد فعالية الاستجابة للحوادث .
- تخصيص فريق الاستجابة للحوادث المعروف أيضًا باسم فريق الاستجابة لحوادث أمان الحاسب الآلى [Computer Security Incident Response Team [CSIRT مسئول عن توفير خدمات الاستجابة للحوادث لجزء من المؤسسة أوكلها حيث يقوم بتلقى معلومات عن الحوادث المحتملة والتحقيق فيها، و اتخاذ الإجراءات اللازمة لضمان تقليل الضررالناجم عن الحوادث إلى الحد الأدنى (centre, 2020)

٢/٥/٢ خطة استعادة النظام بعد الكارثة Disaster Recovery (DR)

هى خطة تعد بمثابة نموذجًا أو دليلاً إرشاديًا مكتوبًا ومُلزمًا للمؤسسة ومعد مسبقًا لكيفية مواجهة الكوارث أو أى حدث غير مخطط له يمكن أن يُعطل قدرة هذه المؤسسة عن القيام بمهامها وسير العمل لمدة أسبوع أو أكثر كالكوارث الطبيعية، و انقطاع التيار الكهربائي، والهجمات الإلكترونية وأى أحداث تخريبية أخرى، ويشمل ذلك من وجهة نظر تكنولوجيا المعلومات مايلى:-

١- تسجيل أنظمة تكنولوجيا المعلومات الهامة التى يجب حمايتها كالاتصال بالشبكة، وقنوات الاتصالات الصوتية والبريد الإلكتروني، والخوادم وخدمات تكنولوجيا المعلومات، ومصادر الطاقة الاحتياطية والمخاطرالمحتملة وتصنيفها.

٢- تحديد الإجراءات الواجب إتباعها في مواجهة حالة الطوارئ، والإجراءات الوقائية التي يمكن اتخاذها للتخفيف من حدته.

٣- قائمة بأسماء كافة أعضاء فريق (مواجهة الكوارث) الذي يتولى إدارة الأزمات بحيث تتضمن بوضوح مسئولية كل فرد خلال جميع مراحل وقوع الكارثة.

٤- التدريبات الافتراضية المنتظمة للعاملين بالمؤسسات على كيفية مواجهة كافة أنواع الكوارث للتأكد من كفاءة تدريبهم وإدارتهم للأزمات، وسلامة المعدات ووسائل التأمين والإنقاذ المتو افرة لديهم (Kaur, 2009)

٦/٢الإجراءات التأمين ضد القرصنة الإلكترونية.

١/٦/٢ جدران الحماية Firewalls

تعد جدران الحماية حجر الزاوية بمنظومة تأمين المو اقع والشبكات لأى مؤسسة وقد يكون جهازًا و/أو برنامجًا يعمل على فرزوتصفية حركة البيانات الواردة من وإلى الشبكة من

خلال الفصل بين المناطق الموثوق بها في شبكات الحاسب، ومر اقبة العمليات التي تمربها ثم الرفض او السماح فقط بمرور برنامج طبقاً لسياسات وضو ابط الأمان المحددة بالمؤسسة. وهناك العديد من أنواع جدران الحماية اعتمادًا على مميزاتها ومستوى الأمان الذي توفره وفيما يلي أهم أنواع تقنيات جدار الحماية التي يمكن تنفيذها كبرامج أو أجهزة (Hayajneh، ٢٠١٣):

١/١/٦/٢ جدران الحماية لتصفية الحزم Packet-filtering Firewalls

وهو النوع الأساسى لجدار الحماية حيث يعمل كبرنامج إدارة ير اقب حركة مرور الشبكة ويقوم بتصفية الحزم الواردة بناءً على قواعد الأمان التي تم تكوينها. تم تصميم جدران الحماية لحظر بروتوكولات IPالحركة مرور الشبكة وعنوان IP ورقم المنفذ إذا كانت حزمة البيانات لا تتطابق مع مجموعة القواعد المحددة.

٢/١/٦/٢ بو ابات مستوى التطبيق (جدران حماية الوكيل) Application-level Gateways (Proxy Firewalls)

تعمل جدران حماية الوكيل في طبقة التطبيق كجهاز وسيط لتصفية حركة المرور الواردة بين نظامين طرفيين (على سبيل المثال، أنظمة الشبكة وحركة المرور) ولهذا السبب تُسمى "بو ابات مستوى التطبيق" وبمجرد إنشاء الاتصال، يقوم جدار الحماية الوكيل بفحص حزم البيانات الواردة من المصدر إذا كانت محتويات حزمة البيانات الواردة محمية، يقوم جدار الحماية الوكيل بنقلها إلى العميل. يُنشئ هذا الأسلوب طبقة إضافية من الأمان بين العميل والعديد من المصادر المختلفة على الشبكة.

٣/١/٦/٢ جدار حماية تطبيقات الويب Web Application Firewall (WAF)

يحمي جدار حماية تطبيق الويب WAF) طبقة التطبيق فهو مصمم خصيصًا لتحليل كل طلب HTTP / S في طبقة التطبيق و تضمن WAFs التقليدية إمكانية تنفيذ الإجراءات المسموح بها بناءً على سياسة الأمان للمؤسسة ويعد خط دفاع أول موثوق به للحماية من قائمة العشر ثغرات الأمنية الأولى الأكثر ظهورًا OWASP Top 10 كهجمات البرمجة النصية عبر المو اقع (XSS) وحقنSQL كما يعمل WAF بطريقة مماثلة لخادم البروكسى ولكن فى الاتجاه المعاكس حيث يعمل كوسيط يحمى خادم تطبيق الويب من عميل يُحتمل أن يكون ضارًا حيث يقوم بتحليل جميع الاتصالات قبل أن تصل إلى التطبيق أو المستخدم. (Best Practice: Use of Web Application Firewalls. OWASP Papers Program)

٤/١/٦/٢جدران الحماية من الجيل التالى Next-generation Firewalls (NGFW)

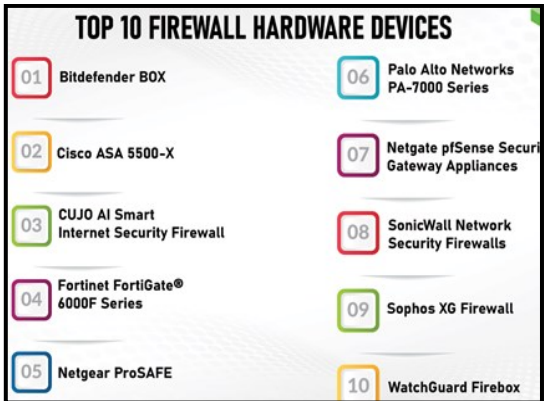
أحدث جدران الحماية التي تم إصدارها، و يُعرَّف هذا النوع من جدار الحماية بأنه جهاز أمان يجمع بين ميزات ووظائف جدران الحماية الاخرى والتى تتضمن الفحص العميق لمحتويات حزمة البيانات والتحقق من المصادقة وقد تتضمن تقينات اخرى مثل أنظمة منع الإختراق (IPSs) بالإضافة إلى ذلك، فإنها توفر أيضًا اكتشافًا متقدمًا للتهديدات وعلاجها والرد السريع على الهجمات من خلال أتمتة الأمان الذكية مما يزيد من أمن نظام الدفاع العام (Next-generation Firewalls (NGFW), 2021).

٥/١/٦/٢ جدران الحماية السحابية Cloud Firewalls

هى أجهزة شبكة قائمة على البرامج ويتم نشرها عبر السحابة، وهى مصممة لإيقاف أو تخفيف الوصول غير المرغوب فيه إلى الشبكة. وباعتبارها تقنية جديدة، فقد تم تصميمها لتلبية احتياجات العمل الحديثة، وتقع ضمن بيئات التطبيق عبر الإنترنت.

٦/١/٦/٢ جدران الحماية الموحدة لإدارة التهديدات Unified Threat Management (UTM) Firewalls

تعد جدران حماية UTM نوعًا خاصًا من الأجهزة التي تتضمن ميزات جدار حماية فحص الحالة مع دعم مكافحة الفيروسات ومنع التطفل IPS وقد تم تصميمها لتوفير البساطة وسهولة الاستخدام. ويمكن أن تضيف جدران الحماية هذه أيضًا العديد من الخدمات الأخرى، مثل إدارة السحابة وعلى المؤسسة التى تتطلع لاستخدام جدران الحماية أن تكون على دراية باحتياجاتها وفهم لبنية الشبكة الخاصة بها حتى يتثنى لها اختيار النوع الملائم لاحتياجاتها (Hayajneh، ٢٠١٣) ويوضح الشكل رقم (٢) قائمة بأعلى (١٠) أنواع للأجهزة المادية للجدران النارية بعام ٢٠٢١.



شكل رقم (٢) قائمة بأعلى (١٠) أنواع للأجهزة المادية للجدران النارية لعام ٢٠٢١ (BasuMallick, 2021)

٢/٦/٢-أنظمة كشف ومنع التسلل Intrusion detection and prevention systems IDPs

١/٢/٦/٢ نظام كشف التسلل intrusion detection system (IDS)

هو نظام ير اقب حركة مرور الشبكة بحثًا عن أى نشاط مشبوه أوحركة مرور غير طبيعية وتسجيله والتنبيه عند اكتشاف مثل هذا النشاط والإبلاغ عنه.ويوفر استخدامها المميزات التالية:-

- الكشف عن المتسللين وحوادث الاختراق الأمنى.

- المساعدة في التحليل العددى والنوعى للهجمات، وبِناءً عليه يمكن لهذه المعلومات أن تساعد المؤسسة فى تطوير أنظمتها الأمنية وتطوير ضو ابط أكثر فعالية .

- تحديد الأخطاء أوالمشكلات المتعلقة بتهيئة أجهزة الشبكة الخاصة بالمؤسسة وتساعد هذه البيانات فى تقييم المخاطر مستقبلاً

- تحسين الاستجابات الأمنية حيث تعمل المُستشعرات الموجودة بأنظمة كشف التسلل على فحص البيانات داخل حزم الشبكة (Khraisat و ect، ٢٠١٩)

٢/٢/٦/٢ نظم منع التسلل Intrusion prevention System (IPS)

- هى أحد أدوات تأمين الشبكات (ويمكن أن تكون جهازًا أو برنامجًا) هدفها الأساسى هو منع التهديدات بمجرد اكتشافها حيث تعمل على المر اقبة المستمرة للشبكة بحثًا عن أى نشاط ضار أومشبوه ثم اتخاذ إجراءات منعها بما في ذلك الإبلاغ عنها وحظرها أوإسقاطها عند حدوثها.ويمكنها تحديد التهديدات التي يصعب تحديدها بواسطة الإجراءات الأخرى، وفى بعض الأحيان يتم تضمين هذه الأنظمة كجزء من الجيل التالي لجدار الحماية (NGFW) next-generation firewall أو حل إدارة التهديدات الموحدة (UTM) ويجب أن تكون قوية بما يكفي لمسح حجم كبير من حركة المرور دون إبطاء أداء الشبكة (Farhaoui, 2016.)

٢ /٣/٦-أنظمة إدارة ومر اقبة الشبكات Network Management and Monitoring System

يقصد بها مجموعة الاجهزة والبرامج التى تعمل على مر اقبة الجو انب المختلفة للشبكة وتشغيلها، مثل حركة المرور ووقت التشغيل بالاضافة الى تقديم رؤية واضحة لجميع الأجهزة والعناصر الأخرى التي تتكوَّن منها الشبكة أو تتصل بها والتعرُّف على كيفية انتقال البيانات فيما بينها والتحديد السريع لتهديدات الأمان للشبكة من خلال فهم الأداء الطبيعى للشبكة فعند حدوث نشاط غير معتاد كزيادة مفاجئة غير مبررة فى مستويات حركة المرور فى

الشـبكة وبالتالى تنبيه المسـئولين لوجود مشـكلة وتحديدها بسـرعة ما إذا كانت اختراق او تهديدًا أمنيًا أم لا.ومن أمثلة برامج مر اقبة الشبكات:

PRTG Network Monitor –OpenNMS- Nagios- HP Network Node Manager i Software

CA Spectrum (Network Management and Monitoring System, 2021)

٤/٦/٢إجراءات الاتصال الآمن بالخادم :Secure Server Connectivity

وتتضمن استخدام البرتوكولات المسئولة عن تحقيق الاتصال الآمن والمشفر بالخادم ومن أهمها:

١/٤/٦/٢ شهادة الحمايةSSL

هي اختصار لكلمة (Secure Socket Layer) وترجمتها باللغة العربية(بروتوكول طبقة المنافذ الآمنة)أو بروتوكول طبقة المقابس الآمنة وهى شهادة رقمية تصادق على هوية موقع ويب وتتيح اتصالاً مشفرًا بين متصفح جهاز المستخدم وبين خادم الويب Web Server وحيث توفر طبقة تعمل على تشفير المعلومات المتبادلة بين الأجهزة المتصلة بالإنترنت. وفي حالة المو اقع الإلكترونية Https فإنه بروتوكول يعمل على تشفير المعلومات بين المتصفح (المستخدم) وخادم الاستضافة لمنع المخترقين من قراءتها أو تعديلها ويظهر مؤشر يوضح للمستخدم أنه محمي بواسطة جلسة SSL المشفرة، ورمز القفل في أعلى المتصفح في جهة اليمين وبالضغط على رمز القفل يعرض شهادة SSL ومعلومات عنها وتوجد نوعان لشهادات الحماية: مجانية ومدفوعة الأجر يتم الحصول عليها بموجب ترخيص وفق مدة زمنية محددة وتمتاز بخصائص أمنية أكبر و أقوى من الشهادات المجانية (امبابى و الغثبر، ٢٠٢١).

٢/٤/٦/٢ بروتوكول النقل الأمن Secure Shell (SSH)

يُشار إلى Secure Shell أحيانًا باسم Secure Socket Shell، ويعد هذا البروتوكول أفضل طريقة لإنشاء اتصال محمي وآمن بالخادم باستخدام واجهة تستند إلى نص بشكل افتراضي، ويستخدم SSH المنفذ ٢٢ ولهذا يعد تغيير رقم المنفذ طريقة سهلة لتقليل فرص مهاجمة القراصنة للخادم.

٣/٤/٦/٢ بروتوكول نقل الملفات الآمن Secure File Transfer Protocol (SFTP)

يسـتخدم لنقل الملفات من وإلى الخادم دون التعرض لخطر اختراق المهاجمين للبيانات أو سـرقتها عن طريق تشـفير ملفات البيانات ومعلومات المصـادقة الخاصـة بالمسـتخدم، يوفر هذا البرتوكول نقل آمن للبيانات ولكن بمجرد وصولهم إلى الخادم، لم تعد البيانات مشفرة

لهذا السبب فإن تشفير الملفات قبل إرسالها يضيف طبقة أخرى من الأمان (phoenixnap, 2019)

٥/٦/٢ الشبكة الافتراضية الخاصة Virtual Private Network (VPN)

تقدم وصفاً لكيفية إنشاء اتصال شبكي محمي عند استخدام الشبكات العامة. تقوم شبكات VPN بتشفير حركة البيانات الخاصة بالمستخدم على الإنترنت وإخفاء هويته الإلكترونية، مما يجعل تتبع أنشطته عبرالإنترنت وسرقة بياناته أمرًا فى غاية الصعوبة بالنسبة للآخرين. ويوفراستخدامها المميزات التالية:-

-تشفيرعناوين Ip الخاصة بالمؤسسة واخفائها عن مزود خدمات الانترنت: ويوفرذلك إرسال واستقبال المعلومات على الإنترنت دون التعرض لخطر رؤيتها بواسطة أي طرف عدا المؤسسة نفسها .

-المصادقة ثنائية العوامل: من خلال استخدام مجموعة متنوعة من أساليب المصادقة، تقوم شبكات VPN القوية بفحص كل من يحاول تسجيل الدخول.

-تشفيرالبروتوكولات: تعمل VPN على إخفاء أى أثرللمستخدم، مثل تاريخ التصفح، أوتاريخ البحث، أوملفات تعريف الارتباط. ويعد تشفير ملفات تعريف الارتباط مهمًا بشكل خاص لأنه يمنع الجهات الخارجية من الوصول إلى المعلومات السرية مثل البيانات الشخصية والمعلومات المالية والمحتويات الأخرى على مو اقع الويب. (Massis, 2017)

٦/٦/٢ بيئة الخوادم المتعددة Multi-Server Environment:

تسمح بيئات الخوادم المتعددة بما يسمى فصل المهام(SOD Separation of Duties)، ويعدعزل خادم قواعد البيانات وخادم تطبيقات الويب من الممارسات الأمنية القياسية وأكثر الإعدادات موثوقية ومصداقية خاصة للمؤسسات كبيرة الحجم التي لا تستطيع تحمل أى انتهاكات أمنية حيث تقوم خوادم قواعد البيانات المستقلة بتأمين المعلومات الحساسة وملفات النظام من المتسللين الذين يتمكنون من الوصول إلى الحسابات الإدارية. كما يتيح العزل لمسئولى النظام تكوين أمان تطبيق الويب بشكل منفصل وتقليل سطح الهجوم عن طريق تعيين جدارحماية لتطبيق الويبWAF. (phoenixnap, 2019)

٧/٦/٢ برامج الحماية من الفيروسات Antivirus Software

تعد من الممارسات الأمنية القياسية والأساسية لأى جهاز حاسب آلى وهى برامج تقوم بمر اقبة الحاسب أو الشبكة للتعرف على كل أنواع البرمجيات الخبيثة ومنع أو عزل ما يظهر من أعراضها. ويمكن الحصول على هذه البرامج مجانًا على الإنترنت أوالحصول على نسخ مرخصة لمدة محددة مدفوعة الأجروهى الأفضل من الناحية الأمنية من اشهر البرامج لعام Total AV, Bitdefender, NORTON, McAFee, Kaspersky (Rubenking, 2022)

٨/٦/٢ القياسات الحيوية Biometric

يقصد بها القياسات المعتمدة على التعرف الآلى على الأفراد من خلال الخصائص البيولوجية والسلوكية القابلة للقياس لتحديد الهوية والمصادقة وضبط الوصول.

شكل رقم (٣)المحددات الفسيولوجية والـ ت الحيوية.

ويتم التحقق من هوية المستخدم من خلال إجراء مضاهاة بين الخصائص المسجلة والقالب المُدخل. وتنقسم المحددات الحيوية إلى نوعين رئيسين هما: المحددات الفسيولوجية والسلوكية كما أوضح الشكل رقم(٣).

ويعد البرنامج القائم على التعرف على بصمة الإصبع من أنجح البرامج وأكثرها دقة ومعيارية وغير قابلة للتغير مع تقدم العمر، على عكس محددات التعرف على الصوت والوجه و لا تتطلب تذكر كلمات سر فضلاً عن أنها طريقة سهلة ورخيصة وأسرع فى التجهيز، إلا أن تأمين قواعد البيانات الضخمة يتطلب التوقيع الرقمى بجانب بصمة الإصبع كما يمكن تعطيل و إفساد عمل البصمة بفعل العرق أو الماء أو الغبار (Abdulrahman & Alhayani, 2021).

٩/٦/٢ كلمات السر.

يعد استخدام كلمات السر من أشهر أساليب التأمين وأخطرها فى نفس الوقت حيث كشف استطلاع الرأى الذى قامت به مؤسسة جوجل إلى أن ٦٥٪ من الأشخاص يعيدون استخدام كلمات المرور الخاصة بهم بحسابات متعددة، وأن ٢٣ مليون شخص من ضحايا القرصنة قد استخدموا سلسلة الأرقام المتتابعة ككلمات سر لهم مما ساعد على تخمينها

وكسرها بسهولة (Jastra, WannaCry Virus Was the Most Common Crypto Ransomware Attack in 2019, 2020) ولهذا تُقدِّم مؤسسة مايكروسوفت عدة توصيات لممارسات آمنة لكلمات السر تتمثل فيما يلى:-

- عدم استخدام البيانات الشخصية كالاسم أو أسماء افراد العائلة أو تاريخ الميلاد أو اللقب أو أى بيانات شخصية أو الحصول عليها من وسائل التواصل الاجتماعى، وتجنب استخدام الكلمات الشائعة التى يسهل تخمينها كاسم المؤسسة أوكلمة " كلمة المرور" نفسها وتعيين نظام تاريخ انتهاء صلاحية كلمات السر.
- الحفاظ على الحد الأدنى من ٨ تمثيلات طولا مع تجنب الطول الزائد(كاستخدام أكثر من ١٠ أحرف)
- استخدام عبارات مرور معقدة ومركبة بحيث تجمع بين الحروف الكبيرة والصغيرة والكلمات والرموز والأرقام والمسافات، ويفضل تضمين كلمات أجنبية، واستخدام برامج مديرکلمات السرPassword Manager لتوليد واسترجاع كلمات السر المعقدة.
- توعية العاملين بعدم استخدام نفس كلمة السرلأكثرمن حساب، أو استخدام كلمات السر الخاصة بالمؤسسة فى مكان أخرخارج نطاق العمل أوبمو اقع الويب الخارجية.
- استخدام المصادقة الثنائية Use two-factor authentication (2FA وتسمى ايضا التحقق من خطوتين وهى حماية أمنية تتطلب من المستخدم إدخال جزء ثانٍ من المعلومات التي يمتلكها هو فقط (عادةً ما يكون رمزًا لمرة واحدة) قبل أن يقوم التطبيق أو الخدمة بتسجيل دخول وبالتالى تمنع الوصول غيرالمصرح به للحسابات حتى وإن نجح المهاجمون فى سرقة كلمة السر. .(Password policy recommendations, 2021)

١٠/٦/٢تحديث البرامج وترقيتها بانتظام Update and Upgrade Software Regularly

يعد التحديث المنتظم للبرامج أحد أكثر ممارسات التأمين فعالية حيث يستغل المهاجمون نقاط الضعف المعروفة والمرتبطة بالبرامج القديمة لشن هجوم وبالتالى فإن عدم مواكبة التحديثات والترقيات للنظم يفتح الباب على مصراعيه لأبسط الاختراقات ويُزيد من نقاط الضعف بشكل كبير.ويتضمن كل إصدارجديد تصحيحات أمان لإصلاح مشكلات الأمان المعروفة ويشمل ذلك تحديث نظم تشغيل الخادم ونظم إدارة المحتوى وبرامج الحماية ضد الفيروسات وجميع تطبيقات الويب.ولهذا يجب أن توثق سياسة أمن المعلومات بوضوح إجراءات إدارة التصحيح وتكرارالتحديثات.

١١/٦/٢اختبارالاختراق Penetration testing

ويطلق عليها أيضـــاً القرصـــنة الأخلاقية وهى أداة فعالة لتقييم واختبار مدى اكتمال وفعالية وسـلامة المنظومة الأمنية بالمؤسـسـة من حيث الأجهزة والبرمجيات والأشـخاص، حيث تحدد درجة الصـعوبة التى يواجهها أى مهاجم عن طريق سـلسـلة من الإجراءات التى تحاكى تنفيذ هجمة الكترونية حقيقية لتحقيق هدف رئيس هو تحديد الثغرات الأمنية ونقاط الضعف ومعالجتها استباقياً قبل استغلالها فعلياً من قبل المهاجمين مع التركيز على الثغرات شـــديدة الخطورة، ومن ثَم تقديم التوصـــيات التى من شـــأنها رفع كفاءة اللأمن السيبر انى بالمؤسسة (Bacudio & Ect, 2011)

أنواع اختبارات الاختراق: يقوم بالاختبار فريق من المتخصصين في مجال الأمن قد يكون على معرفة مسبقة بالبيئة والأنظمة التي يحاولون اختر اقها وقد لا يكون كذلك، وبناء عليه يمكن تقسيمها إلى نوعين رئيسين:-

اختبار الاختراق الخارجى External Penetration testing

ويعرف أيضا باختبار الصندوق الأسود و يستهدف الكشف عن الثغرات الأمنية ونقاط الضعف بالموقع وبنظام أمن المعلومات بالمؤسسة عامةً، واحتمالات التعرض لهجوم خارجى عن طريق إجراءات يتم تنفيذها من خارج المؤسسة حيث يكون منفذ الاختبار على غير علم أو ذو معرفة ضئيلة بالبنية التحتية لتكنولوجيا المعلومات المتو افرة بالمؤسسة ثم يُنفذ محاكاة هجوم إلكتروني في العالم الحقيقي، ومن أمثلة المعلومات التى يتم جمعها فى هذا الاختبار:-

- الكشف عن أنظمة التشغيل المستخدمة Linux - macOS - Windows

- تحديد طراز ونموذج معدات الشبكات (الخوادم، والجدران النارية، والمحولات، والموجهات، ونقاط الوصول، وأجهزة الحاسبات الآلية، وما إلى ذلك ..).

- التعرف على الضو ابط المادية المستخدمة كالأبواب، الأقفال، الكاميرات، أفراد الأمن.

- التعرف على المنافذ المفتوحة / المغلقة بجدار الحماية للسماح / حظر حركة مرور معينة .

-إنشاء خريطة للشبكة لتحديد الجهة المستضيفة للموقع فضلاً عن جهة مكان إرسال حركة المرور (Weidman, 2014)

-اختبار الاختراق الداخلى Internal Penetration testing

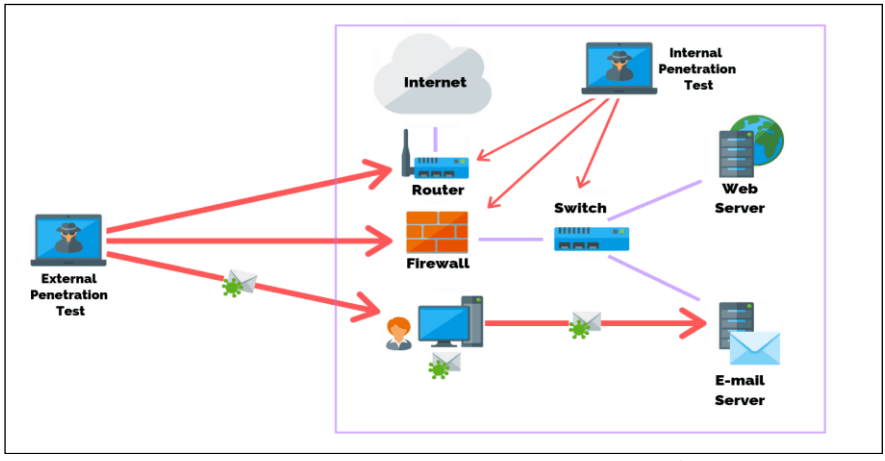
ويطلق عليه أيضا اختبار الصندوق الأبيض، فيأتى تنفيذه بعد اجراء الاختبار الخارجى ويكون منفذى هذا الاختبار على معرفة كاملة ببيئة النظام وكود المصدر وإجراءات الحماية المتبعة وذلك لتحقيق الأهداف التالية:

- التعامل مع الهجمات التى قد تأتى من داخل المؤسسة وما يمكن أن ينجزه مهاجم مصرح له بالدخول أو لديه امتيازات الوصول الداخلي للشبكة كأن يكون موظف ساخط لديه القدرة على الوصول لمناطق أعمق.

-حماية الأصول الهامة والحيوية للمؤسسة من أى تهديد من خلال جمع البيانات وتوثيق ما يجب حمايته بالضبط من الأصول الحيوية وتحديد أولوياتها بالنسبة لعمل المؤسسة والتأثير المحتمل حال غياب هذه الأصول، وفي سياق أمن المعلومات، تعد المعلومات أصلاً أساسيًا بل من أهم الأصول وأكثرها حساسية.

- إجراء تقييم للمخاطر Risk Assessment من خلال تحديد التهديدات التى تهدد كل أصل ونقاط الضعف التي يمكن استغلالها ثم حساب الخسارة في حالة حدوث التهديد استنادًا إلى تحليل التكلفة والعائد.

ولهذا يفضل وضع استراتيجية للجمع بين النوعين لتحقيق الفحص الشامل والتحسين المستمر في الوضع الأمني للمؤسسة، وتعد أفضل الممارسات الأمنية إجراء اختبارات الاختراق على الأقل مرة إلى مرتين فى السنة وقد يتطلب اجراء تغيير فى البنية التحتية تكرارها عدة مرات فى السنة (Bacudio و Ect، ٢٠١١) ويوضح الشكل رقم (٤) أنواع اختبارات الاختراق .



شكل رقم (٤) أنواع اختبارات اختراق الثغرات الامنية (Weidman, 2014).

١٢/٦/٢النسخ الإحتياطى Backup

ويقصد به إنشاء نُسخ للبيانات باستخدام وسائط متعددة ثم الاحتفاظ بهذه النُسخ واستخدامها في حالة فقد البيانات الأصلية أوضياعها نتيجة لتعطل أحد الأجهزة، أو

البرمجيات، أو شن هجمات إلكترونية على النظام واختر اقه، حيث تتيح النسخ الاحتياطية تخزين آمن للبيانات الهامة لسيرالعمل بالمؤسسات وامكانية استردادها من نقطة زمنية سابقة، لذلك يعد وجود سياسة للنسخ الاحتياطى بالمؤسسات من أهم عناصر خطط الاستجابة للحوادث (IRP) واستعادة النظام بعد الكارثة (DRP)- كما ذكر سلفاً.

١/١٢/٦/٢ سياسة النسخ الاحتياطى :

للحصول على أفضل ممارسات للنسخ الاحتياطى يجب إعداد سياسة واضحة وموثقة للنسخ الاحتياطى تتضمن العناصر التالية. (Zhao & Lu, may2018):-

١- حلول وأدوات النسخ الاحتياطي Backup solutions and tools

على الرغم من إمكانية نسخ البيانات الاحتياطى يدويًا، تفضل معظم المؤسسات حلاً تقنيًا لنسخ بياناتها آليا وذلك لضمان نسخ الأنظمة احتياطيًا بشكل منتظم ومتسق ومحدث باستمرار.

٢- مسؤول النسخ الاحتياطي Backup administrator

-يتم تحديد موظف مسئول عن النسخ الاحتياطية. يتولى التأكد من إعداد أنظمة النسخ الاحتياطي بشكل صحيح ، واختبارها بشكل دوري والتأكد من نسخ البيانات الهامة بالفعل.

٣- نطاق وجدول النسخ الاحتياطي Backup scope and schedule

فى هذا العنصر يتم تحديد نوعية الملفات والبيانات المستهدف نسخها وتأمينها وفق أهميتها لدى المؤسسة ويتم ذلك من خلال تصنيف البيانات ومراجعة أصول المعلومات وتحديد البيانات الهامة والحرجة بحيث تأتى فى الأولوية أثناء عملية النسخ الاحتياطي. كما يحدد المعدل الزمنى لتكرار نسخ الاحتياطى بحيث يتم جدولة مواعيد مناسبة لعملية النسخ الاحتياطي متسقة مع طبيعة عمل المؤسسة.

٤-هدف نقطة الاسترداد – Recovery Point Objective (RPO)

هو مقدار البيانات التي تكون المنظمة على استعداد لخسارتها في حالة حدوث كارثة، ويتم تحديدها من خلال تكرار النسخ الاحتياطي.إذا تم نسخ الأنظمة احتياطيًا مرة واحدة يوميًا يكون RPO 24 ساعة وكلما انخفض RPO، زادت الحاجة إلى تخزين البيانات فكلما تباعدت الفترة بين النسخ الاحتياطية كلما زادت احتمالات فقدانها عند استردادها.

٥-هدف وقت الاسترداد Recovery Time Objectiv RTO

هو الوقت الذي تستغرقه المؤسسة لاستعادة البيانات من النسخ الاحتياطي بعد أى كارثة أو توقف واستئناف الخدمة فبالنسبة لأحجام البيانات الكبيرة والنسخ الاحتياطية المخزنة خارج أماكن العمل، يمكن أن يستغرق استعادة البيانات وقتًا أطول.

٦- اعتماد سياسة ٣-٢-١ للنسخ الاحتياطى: هي طريقة لضمان الاحتفاظ بنسخ متعددة من البيانات على وسائط مختلفة لرفع مستوى التأمين وتوفير مرونة أكثر عند استعادة البيانات دون فقد أوتأثر بهجمات القرصنة الإلكترونية حيث تعمل هذه الإستر اتيجية على إنشاء ثلاث نسخ من البيانات تتضمن النسخة الأصلية ونسختين مكررتين منسوختين على نوعين مختلفين من الوسائط وذلك للتغلب على العيوب المتعلقة بوسيط معين، على أن يتم تخزين نسخة واحدة على الأقل عن بُعد خارج الموقع.

٧- تحديث إجراءات استعادة البيانات واختبارها بشكل دورى للتحقق من فعاليتها وإمكانية إتمام عملية الاستعادة فى الوقت المحدد.

٢/١٢/٦/٢ أنواع النسخ الاحتياطى (Gotseva, Georgiev , & Gancheva, 2011)

النسخ الاحتياطى الكامل **Full backup**: وهو الحصول على نسخة احتياطية من البيانات كاملة تمامًا، ويتميز بتوفير حماية أفضل و إتاحة جميع البيانات فى نسخة واحدة كاملة ويستغرق وقتًا أقل فى استعادة البيانات مقارنًة بإستر اتيجيات النسخ الأخرى، إلا أن معظم المنظمات خاصة الكبيرة لا تستخدمها إلا على أساس دورى، حيث أنها تستغرق وقتًا طويلاً، وغالباً ما تتطلب مساحة تخزينية كبيرة وعددًا كبيرًا من الوسائط كالأشرطة أو الأقراص.

النسخ الاحتياطي التز ايدى **Incremental backup**: يحفظ البيانات المتغيرة أو الإضافات التى حدثت منذ آخر مهمة نسخ احتياطى سواء كان تفاضليًا أو كاملاً أى أن البيانات غير المتغيرة لن تتو افر فى هذه النسخة، ويتميز هذا النوع بوقت أقل من النسخ الكامل، وتقليل حمل الشبكة ومساحة تخزينية أقل ولكن لابد أولاً من الحصول على نسخة احتياطية كاملة تمثل نقطة انطلاق للبدء بالعمل، كما أنه يستغرق وقت أطول لاستعادة البيانات مقارنة بالنسخ الاحتياطى الكامل حيث يتطلب الحصول على النسخة الكاملة وجميع النسخ التز ايدية.

النسخ الاحتياطى التفاضلى **differential backup**: يحتفظ فقط بالتغييرات التي حدثت منذ آخر عملية نسخ احتياطي كامل ويعد حلاً وسط بين النسخ الاحتياطى الكامل والتز ايدى فيسمح باستعادة البيانات بشكل أبطأ من النسخ الاحتياطى الكامل وأسرع مقارنة بالنسخ

الاحتياطي التزايدي لأنه لا يتطلب سوى جزأين من النسخة الاحتياطية:النسخة الاحتياطية الكاملة والنسخة الاحتياطية التفاضلية الأخيرة.

ومن حيث الموقع يمكن تقسم النسخ الاحتياطى للأنواع التالية (Kumara , Rajb, & Jelcianac , 2018):

- النسخ الاحتياطى داخل المقر On-Site Backup
- النسخ الاحتياطى خارج المقر Off- Site Backup
- النسخ الاحتياطى المستند إلى السحابة Cloud-Based Backup
- النسخ الاحتياطى بالمقر

ويعتمد على تخزين النُسخ الاحتياطية على أساس دورى بمعدلات ثابتة منتظمة داخل المقر على نفس الجهاز أو باستخدام وسائط تخزين محلية كالأقراص الصلبة والأشرطة، وأسطو انات الليزر DVD ويتميز هذا النوع بإمكانية الوصول الفورى للبيانات واستعادتها بسرعة عند الحاجة فضلاً عن قلة التكلفة، وتو افروسائط التخزين المحلية، وعدم الحاجة للاتصال بالإنترنت، ولكن من عيوبه احتمالات تعرض الموقع لوقوع الكوارث الطبيعية كالحر ائق أو الفياضانات أو السرقة أو تخريب الأجهزة والبرمجيات مما يعرض المؤسسة لخطر فقدان كافة البيانات سواء الأصلية أو النسخ الاحتياطية فى ذات الوقت

-النسخ الاحتياطي خارج المقر

وهو عكس نظام النسخ الاحتياطي داخل الموقع ويعنى تخزين نسخة من البيانات في مكان خارج الموقع كتخزين نسخ من البيانات على شر ائط أو اسطو انات ليزرونقلها إلى مكان بعيد يفضل أن يكون على بُعد ١٠٠ ميل على الأقل من موقع البيانات الأصلى.

-النسخ الاحتياطى المستند إلى السحابة: وقد تناولته الدراسة بشئ من التفصيل.

ولهذا من الأفضل الجمع على الأقل بين نوعين سابقين من التخزين الاحتياطى لتحقيق التكامل فيما بينهم والاستعاضة عن عيوب أحدهما بمميزات الآخر.

٣/١٢/٦/٢ طرق (وسائط) النسخ الاحتياطي (Gotseva, Georgiev , & Gancheva, 2011).

أ-الوسائط القابلة للإزالة Removable Media

وهى وسائط قابلة للإزالة كأقراص الليزر، ودى فى دى، والراى بلو، والأشرطة Tapes وتتميز هذه الطريقة بسهولة الحمل ورخص التكلفة وسهولة نقل البيانات إلى مصادر أخرى، إلا أنها ستحتاج إلى وسائط متعددة إذا ما استخدمت لنسخ بيانات كبيرة، كما أنها معرضة للفقد

عند تعرض المكان نفسه لأية كارثة لذلك تحتاج إلى تخزينها خارج موقع المر افق مما قد يعقد عملية استرداد البيانات، كما أنها تتطلب محرك شر ائط وجهاز تحميل تلقائى لإجراء النسخ الاحتياطي والاسترداد، وهذه المعدات باهظة الثمن.

ب-خادم للنسخ الاحتياطى Backup server

وهو الخيار الأكثر شيوعاً ويتمثل فى تخصيص خادم ويب احتياطى يعمل كآلية نسخ احتياطي كاملة طبق الأصل ويكون فى وضع الاستعداد فى حالة تعرض الخادم الرئيسي لأى كارثة أو هجمة ألكترونية ويتم بنسخ البيانات من الخادم الأصلى للاحتياطى بشكل آلى، وتتميز هذه التقنية بالقوة والثبات وسرعة استرداد البيانات وتجاوز توقف الخدمة إلا أنها معقدة فى إدارتها.

ج-محرك القرص الخارجى External hard drive

هو محرك أقراص ثابت متصل بجهاز الحاسب الآلى من الخارج ويتميز بسهولة الاستخدام وإمكانية حمله إلى أى مكان ونقله كما أنه رخيص نسبيًا مقارنة بوسائط أخرى ويوفر سعة تخزينية كبيرة، ومع ذلك يمكن اختراق البيانات المخزنة عليه بسهولة أكبر نظرًا لطبيعته المتنقلة وسهولة الوصول إليه والتقاطه وسرقته.

د-أجهزة المادية Hardware Appliances

يوفر العديد من الموردين أجهزة نسخ احتياطي كاملة، بسعة تخزين كبيرة وبرامج نسخ احتياطي مدمجة مسبقًا وتقوم تثبيتها على الأنظمة المراد نسخها إحتياطيًا وتحديد جدول وسياسة النسخ وتبدأ البيانات في التدفق إلى جهاز النسخ الاحتياطي كما هو الحال مع الخيارات الأخرى.

هـ- برامج النسخ الاحتياطى Backup Software

تعد حلول النسخ الاحتياطي المستندة إلى البرامج أكثر تعقيدًا من الأجهزة، ولكنها توفر قدرًا أكبر من المرونة و تسمح بتحديد البيانات المطلوب نسخها احتياطيًا وإدارة عملية النسخ الاحتياطي آليًا.

و-النسخ الإحتياطى كخدمة(Backup as a Service (BaaS: يقدم مزودى السحب النسخ الاحتياطى كخدمة للبيانات المرفوعة لديه لضمان إتاحة البيانات عن بُعد واستردادها فى حالة وقوع كارثة. ويتميز النسخ الإحتياطى المعتمدعلى السحابة بتوفيرالوقت والتكلفة المستغرق فى إعداد النُسخ الاحتياطية وإدارتها وغالباً ما يتم النسخ على السحابة آليا لضمان بقائها محدثة.

ز-مزامنة الخادم Server synchronization

يتم فى هذه الطريقة مزامنة قاعدة البيانات الخاصة بخادمين موجودين على أنظمة مختلفة ،وُتستخدم هذه التقنية بشكل نموذجى فى نقل نفس حالة الخادم لخوادم أخرى متعددة وإمكانية تشغيل أى منهم كبديل فورى فى حالة تعرض الخادم الرئيس لأى هجوم أو تعطل.

٧/٢ استضافة خادم الويب وأثره على أمن المواقع.

يعد اختيار نوع استضافة خادم الويب من أهم القرارات التكنولوجية التى تتخذها المؤسسات وتنعكس على أمن الموقع حيث توجد عدة أنواع للاستضافة ولكل منها مميز اته وعيوبه، وتقوم الجهة المستضيفة للموقع بدور محورى فى تأمينه، فكلما كانت جهة الاستضافة موثوقة وجيدة السمعة كلما وفرت استضافة قوية وآمنة.ويتوقف الاختيار الأمثل لهذه الجهة على مدى قدرتها على تلبية احتياجات المؤسسة بفعالية ووفقًا للإمكانات البشرية والتقنية والمادية المتاحة للمؤسسات نفسها.وتتمثل أنواع الاستضافة فيما يلى:

١/٧/٢ الاستضافة المشتركة Shared web hosting

ويقصد بها استضافة أكثرمن موقع على نفس خادم الويب بحيث تتشارك هذه المو اقع فى المكونات المادية للجهازكوحدة المعالجة المركزية والذاكرة. ويتميز هذا النوع من الاستضافة بانخفاض التكلفة -مقارنة بأنواع الاستضافات الأخرى- ولهذا فهو الأكثر انتشارًا خاصة لمو اقع الأفراد والمؤسسات الصغيرة، فضلاً عن أن المسئولية التقنية تُلقى كاملةعلى عاتق جهة الاستضافة، ولكن فى المقابل تعد أكثر عرضة لهجمات القرصنة لإمكانية استخدامها كوسيلة لنشر البرمجيات الضارة وأساليب التصيد ويشير"كانالى" Canali إلى تز ايد هذه الخطورة إذا لم يكن لدى المسئول عن إدارة هذه المو اقع الخلفية الكافية بطرق التأمين بالإضافة إلى الدور الرئيسى لشركات الاستضافة فى التأمين والمر اقبة وبدون دعمها لن يتمكن عملائهم من تحقيق الحماية والمر اقبة الكاملة، ولهذا لابد من إلزام الجهة المضيفة للموقع بتقديم خدمات التأمين والمر اقبة بموجب بند واضح مُدرج فى التعاقد القانونى.) Canal, Balzarott, & Francil, May 2013)

٢/٧/٢ الاستضافة المستقلة: Dedicated web Hosting

وتعنى استضافة الموقع على خادم مستقل غيرمرتبط بأى مو اقع أخرى ويتم تأجيره بأكمله لهذا الموقع وحده ويوفر هذا النوع من الاستضافة أعلى درجات التأمين والاعتمادية والثبات والتحكم فى الخادم من خلال المرونة فى تخصيص مساحات القرص الصلب ووحدة المعالجة المركزية وفقاً لاحتياجات المؤسسة- وإن كان أكثرهم تكلفة مقارنة بأنوع الاستضافات الأخرى- لهذا فهو الحل الأمثل للبيانات الحساسة والهامة وللمؤسسات ذات البيانات الضخمة والتى تشهد مو اقعها ارتفاع معدلات المرور اليومى، كما لا تتطلب اعتماد المؤسسات كاملاً على الجهة المضيفة لتوفير عناصر التأمين للموقع على عكس الاستضافات المشتركة- وإن كان ذلك يعد من العيوب فى حالة عدم تو افرالكفاءات الفنية المتخصصة بهذه المؤسسات .

٣/٧/٢ الاستضافة الافتراضية الخاصة: (Virtual private server (vps

فى هذا النوع من الاستضافة يتم تقسيم الخادم الرئيسى إلى عدة خوادم افتراضية بحيث يخصص لكل موقع الخادم الخاص به ولكن فعلياً يتشارك أكثرمن موقع على نفس الخادم، لهذا فهى تجمع بين خصائص الاستضافة المستقلة والمشتركة فضلاًعن كونها افتراضية كالاستضافة السحابية، ولهذا تعد أفضل من الاستضافة المشتركة من حيث الأمان والثبات والتحكم فى الخادم وتخصيص المساحة والذاكرة مع تكلفة أقل من الاستضافة المستقلة ولكنها أكثر عُرضة لاحتمالات تأثر الخادم الرئيس الافتراضى فى حالة تعرض أحد الخوادم الإفتراضية الموجودة عليه لهجمات القرصنة. (Molnar, 2010)

٤/٧/٢الاستضافة السحابية: Cloud Hosting

ويقصد بذلك تخزين البيانات على بيئة الإنترنت عن طريق عدة خوادم مادية مختلفة ومتصلة جميعًا معًا لُتشكل شكل سحابة ولهذه سميت بالاستضافة السحابية، حيث يتم تخزين ومعالجة البيانات افتراضيًا عبرآلة افتراضية تصل إلى جميع الخوادم المختلفة. وبدلاً من تخزين البيانات على خادم واحد، تقوم الاستضافة السحابية بنشر البيانات عبرعدد من الأجهزة المختلفة وفي حالة تعطل أحد الخوادم تعمل الخوادم الأخرى بنسخة احتياطية لتوفير الموارد المطلوبة لضمان العمل المستمر لخدمات استضافة الويب، وتقدم هذه الاستضافة من خلال شركات تقوم بتأجير مساحات للاستضافة السحابية للمؤسسات وفق احتياجاتهم، وتوفرالاستضافة السحابية العديد من المميزات من أهمها :خفض التكلفة وإمكانية الوصول إلى الموارد من أي مكان على أي جهاز عبر الإنترنت، المرونة والسهولة فى

الاشتراك بالخدمة أو إيقافها، وامكانية قياس مدى استخدام الخدمة وإعداد تقاريرالخدمة (Kumara , Rajb, & Jelcianac , 2018).

وعلى الرغم من المميزات السابقة، يوجد العديد من المخاطر الأمنية المحتملة التي يجب أخذها بالاعتبار ومنها تهديد سرية وخصوصية وسلامة البيانات نتيجة لتزايد مستخدمى السحابة بشكل كبير واستضافة عدد هائل من التطبيقات وتخزينها على خوادم مشتركة خارج السيطرة الفعلية للمستخدم، وإمكانية استرجاع البيانات الخاصة بمستفيد ما بفترة زمنية سابقة من قبل مستخدمين آخر، فضلاًعن أن نقل البيانات إلى مو اقع جغر افية مختلفة يمكن أن يتسبب فى مشكلة قانونية بسبب تغييرالأنظمة القانونية والتنظيمية التى تخضع لها هذه البيانات ولهذا يجب إخطارهم بذلك من قِبل مُزود الخدمة.كما يفضل تشفير البيانات قبل رفعها على السحابة بحيث يتم تخزينها لدى مقدمى الخدمة فى صورة مشفرة تماماً كما يجب توخى الحذر فى نوعية البيانات التى يتم نقلها للسحابة والابتعاد عن رفع البيانات الهامة ذات الطبيعة السرية(Sun , 2020) ،

٨/٢ لغات البرمجة المستخدمة وأثرها على أمن المواقع .

تعد لغة البرمجة المستخدمة فى بناء مو اقع الويب من العوامل المؤثرة من الناحية الأمنية، حيث يسعى المطورون دوماً لاستخدام اللغة الأكثرقوة وأمانًا ضد الهجمات الإلكترونية، ولكن لكل لغة ثغراتها وعلى مطورى المو اقع الوقوف عليها ومعرفة أنماط التصميم العامة التي يجب تجنبها والوظائف التي تنتج هذه الثغرات حتى يتثنى لهم اتخاذ الاحتياطات اللازمة لتأمين الأكواد. ووفقًا للدراسة التى قام بها موقع Whitesource لأشهر لغات البرمجة وما تتضمنه من ثغرات أمنية موثقة ومعروفة طبقاً لمواصفة تعداد نقاط الضعف الشائعة[١](CWEs) Common Weakness Enumeration (CWE the Common Weakness Enumeration.CWE List Version 4.6, 2021)، فقد تبين أن لغة سى (C) هى الأعلى من حيث الثغرات الأمنية التى تتضمنها، يليها لغة بى اتش بىPHP وتتضمن(١٧٪) من مجموع الثغرات، ثم لغة جافاسكريبت JavaScript وتحتوى على نسبة(١١٪) ثم سى شارب C# بنسبة (٦٪) (What are the most secure Programming languages, 2022).

٩/٢ نماذج لأبرز حوادث القرصنة الإلكترونية لمواقع مرافق المعلومات الأجنبية على شبكة الإنترنت:

١- موقع مكتبة معهد ماساتشوستس للتكنولوجيا: (MIT)

فى مارس٢٠١٣ قام قرصان شهير من قراصنة القبعات السوداء يدعى(أيرون سوارتز.Aaron Swartz) بالهجوم على موقع معهد ماساتشوستس للتكنولوجيا(MIT) واختراق قاعدة بيانات JSTOR وقاعدة بيانات المكتبة واستطاع تنزيل أكثر من(٤) ملايين مصدر.اتهمه المدعون الفيدراليون بالاحتيال و١١ تهمة أخرى من جر ائم انتهاكات الحاسب الآلى وقد أدى ذلك إلى عقوبة قصوى تمثلت فى غرامة قدرها مليون دولار و٣٥ سنة في السجن، ومصادرة الأصول. (SMITH F. A., 2017, p. 15)

٢- اختراق موقع شركة ياهو: yahoo.com

فى ديسمبر٢٠١٦ صرحت شركة ياهو بتعرضها لهجمة الكترونية شرسة عام ٢٠١٣ تعد أكبر اختراق تم الكشف عنه فى التاريخ أدت إلى اختراق حسابات ما يقرب من مليار شخص والقرصنة عليها والسطو على بيانات شخصية كالأسماء و تواريخ الميلاد، وأرقام الهاتف، والبريد الإلكترونى، وكلمات سر مشفرة فضلاً عن أسئلة وأجوبة أمنية مشفرة. ويرجح أنه هجوم سياسي برعاية دولة لأنه مشابه لعمليات قرصنة سابقة ارتبطت بوكالات استخبارية روسية. ويفوق حجم خسائر هذه الحادثة حوادث اختراق سابقة كما هى الحال مع ماي سبيس (٣٥٩ مليونًا) ولنكند إن (١٦٤ مليونًا) وأدوبى (١٥٢ مليون (Timberg, 2016)

٣- موقع مكتبة الكونجرس الأمريكية: Library of Congress

كان موقع مكتبة الكونجرس هدفاً للقرصنة الإلكترونية حيث انطلقت هجمات حجب الخدمة فى ١٧ يوليو ٢٠١٦ الذى أدى إلى تعطيل موقع الكونجرس الحكومى، وموقع مكتب حقوق الطبع والنشر الأمريكى، و انقطاع الخدمة في المو اقع الأخرى التي تستضيفها المكتبة بما فى ذلك تعطل أنشطة المكتبة وخدماتها، والشبكة الداخلية، والبريد الإلكترونى للعاملين، واستمر قر ابة ٢٤ ساعة حتى تم استعادة النظام وتشغيل الخدمة مرة أخرى، ومن المرجح أن يكون الدافع هو التحدى و اثبات القدرات التكنولوجية (Mazmanian , 2016)

٤- موقع مكتبة مقاطعة آن أروندل موقع: Anne Arundel County library

فى ٧ أكتوبر ٢٠١٨ تعرضت أجهزة الحاسبات الآلية بمكتبة مقاطعة آن أروندل لهجمات القرصنة الإلكترونية، حيث تعرضت جميع أجهزة الحاسبات سواء للعاملين أو المستفيدين البالغ عددها حوالي ٦٠٠ جهاز لفيروس يسمى Emotet من خلال خداع البريد الإلكتروني

المعقدة مما دفع المسؤولين إلى إخراج أجهزة الحاسبات المصابة من الخدمة ومطالبة المستفيدين بمر اقبة معلوماتهم الشخصية تحسبًا لأي نشاط احتيالى. وقد تم الإخطار بالحادث للمستفيدين البالغ عددهم ٤٧٦٨ الذين استخدموا أجهزة الحاسبات العامة منذ ١٧ سبتمبر والذين قاموا بتسجيل الدخول لفهرس المكتبة (MD: 600 Anne Arundel County library computers affected by "Emotet" virus, 2018)

٥-موقع مكتبة مقاطعة سبارتانبيرج العامة: Spartanburg County Public Library (SCPL)

فى ٢٩ يناير ٢٠١٨ ، تلقى الفريق الفنى بمكتبة مقاطعة سبارتانبورغ العامة (SCPL) إشعارًا على موقع مكتبة على الإنترنت يعلن أن أجهزة الحاسب الآلى الخاصة بها قد تم تشفيرها باستخدام برامج الفدية، والتى جاءت عبر رسالة بريد إلكترونى مصابة فتحها أحد العاملين بها حيث تم تشفير ٢٣ خادمًا servers الموجودة بالمكتبة وفروعها، كما تأثرت أيضًا العديد من أجهزة الكمبيوتر العميلة clients. ولم يتمكن المهاجمون من التقاط أى بيانات شخصية للمستفيدين حيث يتم التخزين خارجيا لدى مورد third – party vendor، وقد أغلقت المكتبة على الفور موقعها على الويب وفهرسها العام والمجموعات الرقمية وشبكة الإنتر انت الداخلية، وتوقفت الإعارة وجميع الخدمات الإلكترونية لعزل البرامج الضارة ومنع انتشارها، واضطر العاملين لإجراء الإعارة يدويًا لمدة ٤٨ ساعة، وقد طالب المهاجمون دفع فدية ٣,٦ إلى ٣,٨ بيتكوين بقيمة قدرها حوالي ٣٦ ألف دولار إلا أن المكتبة رفضت الخضوع للابتزاز والدفع لعدم ضمان الحصول على بيانات سليمة (US libraries hit by ransomware attack. ، ٢٠١٧).

٦- موقع مكتبة براونسبيرج العامة: Brownsburg (Ind.) Public Library: تعرضت مكتبة براونسبيرج العامة بولاية أنديانا الأمريكية لهجوم برنامج الفدية في ٢٦ يونيو ٢٠١٨ ، فعند إعادة تشغيل الخادم لتحديث Windows أصيبت قاعدة بيانات SQL الخاصة بالنظام الآلى المتكامل للمكتبة، لذلك توقف الاتصال بقاعدة البيانات والبحث في الفهرس أو الإعارة. وبعد محاولة غير ناجحة لاستعادة النظام المشفر استجابت المكتبة في النهاية لمطالب المهاجمين بالحصول على نصف عملة بيتكوين بلغت قيمتها حوالي ١٥٠٠ دولار في ذلك الوقت لأن أحدث نسخة احتياطية كاملة للموقع كانت قبل ثلاثة أشهر، وقد تلقت المكتبة رمز إلغاء قفل التشفير بعد ساعات قليلة من قيامها بالدفع واستعادت الأنظمة واستأنفت العمل فى غضون ثلاثة أسابيع (US libraries hit by ransomware attack. ، ٢٠١٧).

٧-موقع مكتبة مجلس مدينة ساندر لاند: Sunderland City Council's library database

فى ٢١ مايو ٢٠١٩ تعرض موقع مكتبة مجلس مدينة ساندرلاند إلى هجوم إلكترونى حيث تمكن القراصنة من استغلال خطأ فى التهيئة واختراق قاعدة بيانات المستفيدين والنجاح فى الوصول غير المصرح به إلى ٤٥ من حسابات المستفيدين البالغ عددها ١٤٥٠٠٠ والحصول على بيانات شخصية كالأسماء، وتواريخ الميلاد، وأرقام الهو اتف والتى تعد كنقطة بداية للحصول على مزيد من المعلومات حول الأشخاص لارتكاب جر ائم سرقة الهوية و الاحتيال. وعلى الرغم من التحقيق فى الحادث من جهات متعددة إلا أن الشركة المستضيفة للموقع لم تتمكن من تحديد الحسابات المخترقة على وجه الدقة وبالتالى ناشد المجلس جميع المستفيدين من توخى الحذر واليقظة مما تسبب فى قلق بالغ للمستفيدين (Robertson, 2019).

٨-موقع المكتبات العامة بمقاطعة كونترا كوستا: Contra Costa County Libraries community

فى ٣ يناير ٢٠٢٠ تعرضت ٢٦ مكتبة عامة بمقاطعة كونترا كوستا بولاية كاليفورنيا الأمريكية لهجوم إلكترونى حيث ضرب فيروس الفدية Ransomware المكتبة وفروعها وتسبب فى تعطيل الخوادم وإغلاقها و انقطاع الإنترنت مما أدى إلى تعطيل خدمات الإعارة والإنترنت والطباعة، وقد قامت المكتبة المركزية بفصل الخوادم المصابة، ثم استعادة النظام ومحاولة تشغيل الخدمات الإلكترونية، كما قامت المقاطعة بتحذير المستفيدين لحماية حساباتهم عبرالبريد الإلكترونى.ومن نتائج هذا الهجوم تخوف وقلق كثير من المستفيدين على بياناتهم الشخصية المخزنة بالمكتبة كبطاقات الائتمان والتأمين الاجتماعى وكما كانت فى السابق عام ٢٠١٩ تسجل بيانات رخصة القيادة مما اضطرها لحذف بعض هذه البيانات بناء على رغبة المستفيدين.ولم يتم طلب مبالغ محددة لفتح الخوادم التى تم إغلاقها بفعل الفيروس مما يشير إلى أن الدافع هو الرغبة فى التحدى و إثبات الذات (Pena, 2020)

٩-موقع برنامج مكتبة الإيداع الفيدرالية الأمريكية(FDLP) Federal Depository Library Program's site

فى صباح السبت٤ يناير٢٠٢٠ شهد موقع برنامج مكتبة الإيداع القانونى الفيدرالية الأمريكية هجوما إلكترونيًا من قبل قراصنة "مجموعة الأمن الإلكترونى الإير انية" كرد على

مقتل اللواء الإير انى "قاسم سليمانى" قائد فيلق القدس التابع للحرس الوطنى الإير انى، والذى قتل فى غارة جوية أمريكية بدون طيار وسط موجة الاضطر ابات السياسية التى شهدها العالم فى هذه الفترة، حيث ظهر موقع المكتبة عليه صور مركبة لخريطة الشرق الأوسط مؤيدة لإيران وتُكرم اللواء قاسم سليمانى وتتعهد بالانتقام من قاتليه ومصحوبة بصورة مزيفة للرئيس الأمريكى "ترامب" وهو يتعرض للضرب.و قد ترتب على ذلك تعطيل الموقع لمدة ٢٤ ساعة كاملة قبل النجاح فى السيطرة عليه واستعادته فى اليوم التالى. وقد أظهرت التحقيقات عدم المساس بالبيانات التى يتضمنها الموقع الذى يتيح الوصول الحر إلى مجموعة ضخمة ومتنوعة من الوثائق الحكومية المودعة فى ١١٠٠ مكتبة إيداع منتشرة في جميع أنحاء الولايات المتحدة. وقد كان الدافع هو استعراض القدرة التقنية للمهاجمين ويؤكد ذلك الجملة التى ظهرت على الموقع" ليس هذا سوى جزء صغير من قدرة إيران الإلكترونية. (Zaveri, 2020)، ويوضح الشكل التالى رقم (٥) صورة للموقع بعد اختر اقه.

شكل رقم(٥) صورة لموقع برنامج مكتبة الإيداع الفيدرالية الأمريكية بعد اختر اقه من قبل قراصنة ايرانيين لأهداف سياسية ويظهر عليه رسالة القراصنة (Zaveri, 2020).

١٠-موقع مكتبة البرازيل الوطنية National Library of Brazil (Biblioteca Nacional do Brasil)

فى صباح يوم الأحد المو افق ١١ أبريل ٢٠٢١ تمكن قراصنة مجهولون من اختراق موقع المكتبة الوطنية للبرازيل عبر إرسال فيروس الفدية الذى تسبب فى تشفير بيانات الخودام وتعطيلها وتوقف الخدمة لمدة ٤٨ ساعة إلى أن استطاع الفريق الفنى من إعادة تشغيل

النظام فى الثلاثاء ١٣ ابريل، ثم تعرض الموقع لهجمة ثانية فى نفس اليوم طلباً للفدية ولكن رفضت المكتبة الاستجابة لمطالب القراصنة ونجح الفريق الفنى فى تحرير الموقع والوصول لبعض الملفات واستعادة الباقى بفضل نسخ الاحتياطى الكامل للموقع. (Price, 2021)

وبالنظر لحوادث القرصنة السابق عرضها يتضح ما يلى :

١- يعد قطاع مر افق المعلومات بمختلف فئاته هدفاً للقرصنة الإلكترونية، فلم تسلم كبرى المر افق العالمية كمكتبة الكونجرس ومحرك البحث جوجل من حوادث الاختراق، كما اختلفت الدو افع الكامنة ورائها، فتارة كان الغرض منها سياسيًا، وتارة أخرى ماديًا، وأخرى للتحدى التقني و اثبات الذات مما يؤكد أنه لا يوجد مرفق أيًا كان فئته ونشاطه وإمكاناته بعيداً عن أيدى القراصنة ومطامعهم، وهى الحقيقة التى ينبغى أن يدركها مسئولو أمن المو اقع ويستعدوا لها بيقظة مستمرة.ويؤكد ذلك ما ذكره سميث SMITH من حاجة المكتبات ومر افق المعلومات إلى الاستعداد للهجمات الإلكترونية التى لا مفر منها والتى تهدد بالحفاظ على مصادرها عبر الإنترنت والمجموعات الرقمية خاصة التى أنتجت من الأصل رقمية وليس لها نظير ورقى، فضل عن ضرورة وضع خطط واضحة لاسترداد النظام بعد أى كارثة .(SMITH F. A., 2017, p. 15)

٢-الأهمية القصوى للنسخ الاحتياطى المستمر فقد كان لوجود نسخة احتياطية كاملة وفق آخر تحديث للموقع عاملاً فارقاً فى عدم رضوخ المؤسسات الضحايا للابتزاز المادى ودفع الفدية المطلوبة، و أيضاً القدرة على استعادة البيانات بعد الحادثة وتشغيل النظام بنجاح والعكس صحيح، كما يعد فيروس الفدية أكثر الأساليب المستخدمة فى الهجمات السابقة.

٣- للعامل البشري دور كبير فى حدوث الثغرات الأمنية كأخطاء التعامل مع رسائل البريد الإلكترونى وعيوب التهيئة، وكذلك مهاراتهم التكنولوجية فى كيفية استعادة النظام بعد الكارثة.

٤-يعد تأمين الحسابات الشخصية للمستفيدين من أخطرالقضايا التى يتضمنها تأمين مو اقع مر افق المعلومات السابق عرضها وقد كان حفظها خارج المر افق نفسها إجراء أكثر ضماناً.

وكما شهدت مو اقع مر افق المعلومات الأجنبية حوادث قرصنة الكترونية، فقد تعرضت أيضا مو اقع المر افق المصرية على الإنترنت بأنواعها المختلفة للعديد من هجمات القرصنة، كما ستوضح الدراسة الميدانية فى الإطار التطبيقى.

ثالثاً:الإطار التطبيقى.

يعرض الجزء التالى الجانب التطبيقى للدراسة من حيث الوقوف على جر ائم القرصنة التى استهدفت مجتمع الدراسة ودو افعها، وإجراءات والتعرف على سياسات وإجراءات التأمين المتبعة، والكوادر البشرية المسئولة عن تأمين المو اقع، والتحديات التى تواجه هذه المؤسسات لتحقيق منظومة أمنية متكاملة، ثم الخروج بالتوصيات التى من شأنها الارتقاء بمنظومة أمن المو اقع بمر افق الدراسة

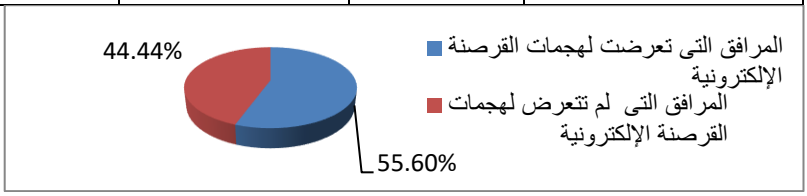
١/٣حوادث القرصنة الإلكترونية على مرافق المعلومات موضوع الدراسة

يوضح الجدول رقم (٢) والشكل رقم (٦) حوادث القرصنة الإلكترونية التى استهدفت مو اقع مر افق المعلومات المصرية على الإنترنت حتى أكتوبر ٢٠٢١.

جدول رقم (٢) حوادث القرصنة الإلكترونية التى تعرضت لها مو اقع مر افق المعلومات المصرية موضوع الدراسة على الإنترنت حتى أكتوبر ٢٠٢١

عينة الدراسة	الدو افع	الأساليب المستخدمة	الخسائر الناجمة عنها
مكتبات مصر العامة		----	----
مكتبة الإسكندرية	-التحدى و اثبات الذات التدميروتخريب البيانات	هجمات حجب الخدمة	تغييروحذف البيانات - حجب الخدمة بالموقع تنزيل عدد من النصوص الكاملة للكتب الرقمية.
المكتبة المركزية لجامعة القاهرة	--	--	---
دار الكتب والوثائق القومية	التدميروتخريب البيانات	فيروس تروجان	تغييروحذف البيانات
مكتبة معهد الدراسات الشرقية للاباء الدومنيكان	---	---	---
مركز معلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى	تخريب وتدمير البيانات	التصيد والخداع	تغييروحذف البيانات
بو ابة دارالافتاء المصرية	----	-----	----
بو ابة جامعة طنطا	-التدمير تخريب وتدمير البيانات	حجب الخدمة- حقن Injection	تدميروحذف البيانات - تعطيل الخدمة بالموقع.

	التحدى و إثبات الذات		حداث خلل بالشبكة الدخلية للحاسبات و لإتصالات.
اتحاد المكتبات الجامعية المصرية	التحدى إثبات الذات	حجب الخدمة - التصيد والخداع حقن	حجب الخدمة بالموقع



شكل رقم (٦) حوادث القرصنة الإلكترونية التى استهدفت مو اقع مر افق المعلومات موضوع الدراسةعلى الإنترنت حتى أكتوبر ٢٠٢١

ويتبين من الجدول رقم (٢) والشكل رقم (٦) ما يلي:

-تعرضت بالفعل(٥) مو اقع بنسبة ٥٥,٥٦٪من مو اقع الدراسة لهجمات القرصنة الإلكترونية وتمثل أنواع مختلفة لمر افق المعلومات وهى مكتبة الإسكندرية، ودار الكتب والوثائق القومية، ومركز معلومات مجلس الوزراء، وبو ابة جامعة طنطا و اتحاد المكتبات الجامعية المصرية.

- تعرض موقع مكتبة الإسكندرية لعدة هجمات إلكترونية أشهرها عام ٢٠٠٩، ٢٠١٣ وترتب عليها تدمير وتخريب فى البيانات، وتنزيل عدد من النصوص الكاملة للكتب الإلكترونية التى قامت المكتبة برقمنتها، وحجب الخدمة لعدة ساعات وبِناء عليه فقد اهتمت المكتبة اهتمامًا بالغًا برفع مستوى الحماية وتنويع أساليب التخزين الاحتياطى والوسائط المستخدمة به- كما سيرد بالعنصر الخاص بالنسخ الاحتياطى، أيضاً تعرض موقع جامعة طنطا لعدة هجمات معظمها من طلاب بغرض تغيير البيانات وتخريبها، كذلك كان موقع اتحاد المكتبات الجامعية المصرية هدفاً للقرصنة حيث تعرض لهجمات إلكترونية متعددة استهدفت المستودع الرقمى للرسائل الجامعية.

- تعرض موقع دار الكتب والوثائق القومية لهجمة إلكترونية عام ٢٠١٣ وقد كان هذا الحدث سبباً فى الانتباه لضرورة الارتقاء بآليات التأمين المتبعة، ونظراً لضعف الامكانيات التقنية والبنية التحتية المتاحة للدار، فقد تولت وزارة الاتصالات المصرية مسئولية استضافة خادم الموقع وتأمينه وتطوير بنيته وذلك فى إطار بروتوكول التعاون المبرم بين وزارة الاتصالات ووزارة الثقافة التابعة لها الدار.

- شهد موقع مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى عدة محاولات للاختراق من أشهرها هجمة عام ٢٠٠٩ نجح فيها المهاجمون فى اختراق الموقع ورفع صورهم الشخصية وتغيير وحذف بيانات. وقد كان هذا الحدث نقطة تحول استدعت تغيير البنية التحتية للموقع ورفع مستوى آليات التأمين ومواكبة الجديد في أساليب التأمين والوقوف على أحدث التقنيات ومتابعة المؤتمرات الدولية فى مجال أمن المعلومات، خاصة مع رصد محاولات يومية لاختراق الموقع -نظراً لطبيعة المركز التى تجعله مستهدفاً - ويتم التصدى لها.
- كان" تدميروتخريب البيانات " هو الدافع الأكثر انتشـــارًا وراء الهجمات الإلكترونية على مو اقع مر افق الدراســـة حيث تكررفى (٤) مر افق بنســـبة ٤٤,٤٤ % وقد يرجع الســـبب فى ذلك إلى طبيعة المر افق نفســـها وما تتضـــمنه من بيانات تجعلها هدفاً للتدميروالتخريب المتعمد، يليه التحدى التقنى و إثبات الذات وتكررفى (٣) مر افق بنسبة ٣٣,٣٣٪ وقد توصل الفريق الفنى المســـئول عن أمن موقع الدراســـة لتحديد هذه الدو افع من خلال تحليل سلوك المهاجمين وتتبع الآثاروالخسائر الناجمة عنهم .
- اختلفت الأساليب المستخدمة فى الهجمات الإلكترونية على مو اقع مر افق المعلومات موضوع الدراسة، ويعد هجمات حجب الخدمة أكثر الأساليب استخداماً فى(٣) مر افق بنسبة ٣٣,٣٣٪، يليه التصيد والخداع phishing، وحقن sql وتم استخدام كل منهما فى مرفقين بنسبة ٢٢,٢٢٪، ثم فيروس تروجان فى مرفق واحد بنسبة ١١,١١٪، على عكس المر افق الأجنبية التى تعرضت لهجمات فيروس الفدية بشكل أكبر- كما تبين بالعنصر رقم ٩/٢.
- كان تغيير وحذف البيانات من أهم الخسائر والآثارالناجمة عن حوادث القرصنة الإلكترونية على مو اقع مر افق المعلومات موضوع الدراسة حيث تكررفى(4) مر افق بنسبة ٤٤,٤٤٪، يليه حجب الخدمة عن الموقع وتكرر فى (٣) مو اقع بنسبة ٣٣,٣٣ %، ثم كان الحصول على النصوص الكاملة للكتب الرقمية، وإحداث خلل بالشبكة الداخلية بمرفق واحد بنسبة (١١,١١٪) ويؤكد ذلك أهمية النسخ الاحتياطى للبيانات خاصة النسخ اليومى والتخزين بأشكال ووسائط مختلفة لاسترداد البيانات واستعادة النظام بأقل وقت وخسائر ممكنة .

٢/٣سياسة أمن المعلومات بمرافق المعلومات موضوع الد راسة

تبين بالدراسة الميدانية لهذا العنصر مايلى:- افتقرت جميع مر افق الدراسة لوجود سياسات موثقة وفعالة لأمن المعلومات، حيث توجد أجزاء مكتوبة تغطى إجراءات الاستجابة للحوادث- كماذكر سلفاً- وذلك بمكتبة الإسكندرية ومركز معلومات مجلس الوزراء، أما العناصر الأخرى المفترض أن تغطيها سياسة أمن المعلومات فيتم توثيق ضو ابطها وإدارتها بقرارات الإدارية أثناء العمل اليومى ويرجع السبب فى ذلك فى رأى العاملين بمر افق الدراسة إلى صعوبة توثيق وصياغة سياسة محددة نتيجة لمستجدات ومتطلبات العمل المتغيرة باستمرار.

- توجد سياسات مكتوبة للخصوصية، واستخدام الإنترنت، والبريد الإلكترونى، والتحكم فى الوصول بكافة مر افق الدراسة، والتى تخضع للمراجعة والتحديث سنويًا ببو ابة جامعة طنطا، بينما تتم المراجعة بمعدل غيرثابت ببو ابة دارالإفتاء المصرية، ومكتبة الاسكندرية، والمكتبة المركزية لجامعة القاهرة، ومركزالمعلومات ودعم اتخاذ القرار، وعند الحاجة بمكتبة الدومنيكان، و اتحاد المكتبات الجامعية المصرية، ودارالكتب المصرية، ولم يتم تحديثها أو مراجعتها منذ إقرارها بمكتبات مصر العامة.

٣/٣ خطط الاستجابة للحوادث واستعادة النظام بعد الكارثة بمرافق المعلومات موضوع الد راسة.

تبين بالدراسة الميدانية لهذا العنصر مايلى :-

- لاتوجد خطط مكتوبة للاستجابة للحوادث أو التعافى بعد الكارثة فى أى من مر افق الدراسة، باستثناء مكتبة الإسكندرية ومركز معلومات مجلس الوزراء التى يتو افر بهما تعليمات مكتوبة بالإجراءات اللازم اتخاذها عقب أى هجمة أو حادث إلكترونى، أما بقية المر افق فتفتقر لتوثيق الاجراءات ويتم الاستجابة للحوادث واستعادة النظام بشكل متفق عليه بين العاملين بإدارات تكنولوجيا المعلومات، وقد تم الاستجابة لحوادث القرصنة التى تعرضت لها مر افق الدراسة بالفعل وفق الإجراءات التالية:

- إغلاق المخارج المتسببة فى الاختراق.

- فصل الخوادم المخترَقة عن باقى الشبكة ومراجعتها وفحصها وتحليلها لمعرفة كيفية حدوث الاختراق، و اكتشاف الثغرة المستخدمة وتحديد مصدرها، ثم إغلاق المخارج التي تم تنفيذ الهجوم من خلالها.

- استعادة البيانات عن طريق الحصول على نسخة من وسائط التخزين الاحتياطي وإعادة تشغيل الموقع، ويوضح ذلك أهمية النسخ الاحتياطى للبيانات كخطوة رئيسة لاستعادة البيانات وتشغيل المو اقع بمر افق الدراسة، وسوف تتناول الدراسة هذا العنصر بشيء من التفصيل بالعنصر رقم(٦/3).

٤/٣الإجراءات المتبعة لتأمين مواقع مرافق المعلومات موضوع الد راسة.

ويوضح الجدول رقم (٣) الأساليب المستخدمة لتأمين مو اقع مر افق المعلومات المصرية موضوع الدراسة حتى أكتوبر ٢٠٢١.

مجتمع الدراسة	الجدران النارية	شهادات الحماية ssl	برتوكول ssH	بروتوكول SFTP	انظمة كشف ومنع التسلل		النسخ الاحتياطي اسطى	تحديث البرامج وترقيتها	انظمة مراقبة الشبكات	برامج الحماية ضد الفيروسات	VPN	كلمات السر	SODف من لمهام	اسالیب اخرى	اختبارات الاختراق	الإجمالى
					IDS	IPS										
مكتبات مصر العامة	√	—	-	-	-	√	√	—	√	√	—	√	√	—	-	٧
مكتبة الاسكندرية	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	١٥
المكتبة المركزية لجامعة القاهرة	√	---	√	—	√	-	√	√	√	√	√	√	√	—	√	١١
دار الكتب الوثائق القومية	√	—		√	√	√	√	√	√	√	√	√	√	—	√	١٢
مكتبة معهد الدراسات الشرقية للاباء الدومنيكان	√	√	√	√	√	√	√	√	√	√	—	√	√	—	—	١٢
مركز معلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	١٥
بوابة دار الافتاء المصرية	√	—	—	—	√	√	√	√	√	√	√	√	√	√	√	١٢
بوابة جامعة طنطا	√	√		√	√	—	√	√	√	√	√	√	√	—	√	١٢
اتحاد المكتبات الجامعية	√	—		-	-	√	√	—	√	√	—	√	√	-	-	٧

الاجمالى	٩	4	٤	٥	٧	٧	٩	٧	٩	٩	٦	٩	٩	3	٦	–
النسبة المئوية	٪١٠٠	٤٤,٤ ٪٤	٪٤٤,٤	٪٥,٦	٧٧, ٪٨	٧٧, ٪٨	٪١٠٠	٧٧,٨ ٪	٪١٠٠	٪١٠٠	٦٦, ٪٧	٪١٠٠	١٠٠ ٪	١٠٠ ٪	3,33 3%	٪٦٦,٧	–

ويتبين من الجدول رقم (٣) مايلى :

- تتعدد أساليب وممارسات التأمين المتبعة بمو اقع مر افق المعلومات موضوع الدراسة، وتأتى مكتبة الإسكندرية، ومركز معلومات مجلس الوزراء فى مقدمة مر افق الدراسة من حيث تو افر هذه الأساليب ويرجع ذلك لتو افر الإمكانات البشرية والتقنية والمادية والسعى الدائم لرفع إجراءات الحماية بهذين المرفقين خاصةً بعد حوادث هجمات الإلكترونية السابقة التى استهدفت موقعيها، ثم تأتى دار الكتب، ومكتبة الدومنيكان، وبو ابة جامعة طنطا، وبو ابة دار الإفتاء المصرية وتو افر بكل منهم نسبة ٨٠٪ من الأساليب المدروسة، ثم المكتبة المركزية لجامعة القاهرة بنسبة٧٣٪، ومكتبات مصر العامة فى الترتيب الأخير بنسبة٤٦,٧٪.

- يوجد العديد من نقاط القوة التى تُميز الأساليب والممارسات المتبعة للتأمين بالمو اقع موضوع الدراسة كمايلى:

- تُستخدم جدران الحماية فى جميع المر افق بنسبة ١٠٠٪، وتبين تو افر أربعة من ضمن قائمة أعلى (١٠) أنواع للأجهزة المادية للجدران النارية علي مستوى العالم وفقًا لإحصائيات عام ٢٠٢١، فضلاً عن استخدام الأجيال الحديثة للجدران كما يلى:-

- سيسكو: Cisco من أشهر أنواع الجدران النارية ويأتى ثانى أفضل نوع، ويستخدم تقنية جدار الحماية من الجيل الثانى (NGFW) بكل من مكتبة الإسكندرية، والمكتبة المركزية لجامعة القاهرة، ومركزالمعلومات ودعم اتخاذ القرار، ودارالكتب، ومكتبة الدومنيكان.

- فورتيجات Fortigate: يتو افر ببو ابة جامعة طنطا، و اتحاد المكتبات الجامعية المصرية وتستخدم تقنية WAF.

- بالو ألتو Palo Alto: يتو افر ببو ابة دارالإفتاء المصرية، وتستخدم تقنية جدار الحماية من الجيل الثانى (NGFW).

- سوفوس Sophos: يتو افر بمكتبات مصر العامة وتستخدم تقنية الجيل الثانى (NGFW).

- تقوم جميع `مر افق الدراسة بنسبة ١٠٠٪ بالنسخ الاحتياطى لبياناتها تحسبًا لأى هجوم على مو اقعها وما قد يترتب علي ذلك من فقدان أوتخريب للبيانات، وسوف تُعالج هذه الجزئية بشئ من التفصيل بالعنصر رقم (١٢/٦/٣)

- يتم تطبيق سياسة كلمات السر بمر افق الدراسة بنسبة ١٠٠٪ حيث تخصص كلمات سر للعاملين المصرح لهم بالوصول لخادم الموقع وقواعد البيانات، وأجهزة الشبكة الداخلية، وفق ضو ابط تراعى جانبًا كبيرًا من التوصيات السابق ذكرها فيتم تغيير الكلمات الخاصة بأجهزة الحاسبات الشخصية للشبكة بشكل منتظم كل ٣٠ يوم وكل ٦٠ يوم للعاملين من لهم صلاحيات الدخول على الموقع وإدارته ويتم ذلك فى(٦) مر افق بنسبة٦٦,٦٧٪ وهى بو ابة دارالإفتاء المصرية، ومكتبة الدومنيكان، ومكتبة الإسكندرية، ومركز المعلومات ودعم اتخاذ القرار، والمكتبة المركزية لجامعة القاهرة، و اتحاد المكتبات المصرية، بينما يتم تغييرها بمكتبات مصر العامة، ودار الكتب، وجامعة طنطا بمعدلات غير ثابتة، أو فى حالة تغير أحد المسئولين المصرح لهم بالدخول على الموقع أو قواعد البيانات أو أحد أعضاء الفريق التقنى .أما من حيث متطلبات الطول والتعقيد، فهناك(٥) مر افق تستخدم كلمات سر مكونة من (٨) تمثيلات مع مراعاة استخدام العبارات المعقدة التى تجمع بين الحروف الصغيرة والكبيرة والكلمات والرموزوهى مكتبة الإسكندرية، ومركز معلومات مجلس الوزراء، وبو ابة دارالإفتاء المصرية، ودار الكتب المصرية، و اتحاد المكتبات الجامعية المصرية، أما بقية المر افق فتفضل استخدام الكلمات المكونة من (١٦) حرف بأنماط متكررة مع استخدام برامج مدير كلمات السر لإنشائها وحفظها آليا، و تطبق أساليب المصادقة الثائية ب(٧) مر افق بنسبة(٧٧,٨٪) مما يزيد من ضو ابط التحكم فى الوصول.

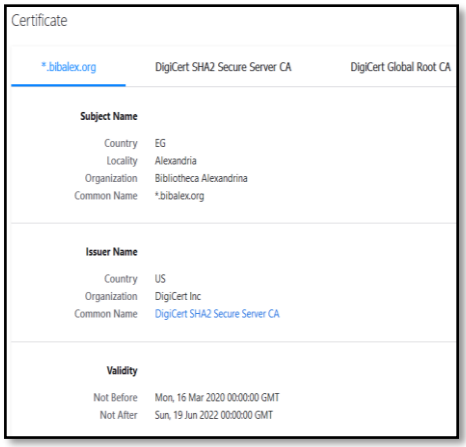
- تستخدم كافة مر افق الدراسة نسخ مرخصة من برامج الحماية ضد الفيروسات ويتم تجديدها وتحديثها سنويًا حيث يستخدم مركز المعلومات برامج مكافى McAFee، وتستخدم مكتبة الإسكندرية Symantec Endpoint Protection وتستخدم مكتبات مصر العامة، وبو ابة دار الإفتاء المصرية، وبو ابة جامعة طنطا، و اتحاد الجامعات المصرية برنامج كاسبرسكىKaspersky، وتسخدم مكتبة الدومنيكان حزم برامج تأمين نظام التشغيل لينكس الأصلية، وتسخدم دارالكتب نظام فورتيجات، أما المكتبة المركزية لجامعة القاهرة فتستخدم Microsoft security Ethintial، وE TRUST CA وهى نقطة قوة تحسب لمر افق المعلومات موضوع الدراسة.

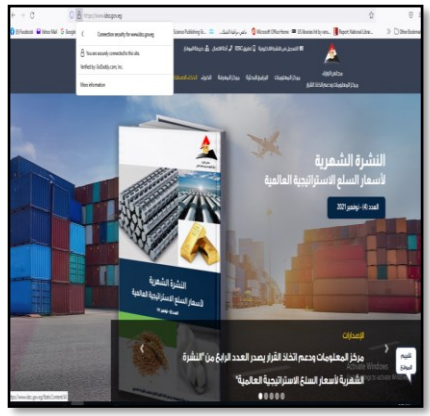
- تُستخدم أنظمة مر اقبة الشبكات فى جميع مر افق بنسبة ١٠٠٪ ومن أمثلة النظم المتو افرة بمر افق الدراسةspectrum ،PRTG Network Monitor- CA diagram - Spicework

- تقوم جميع المر افق موضوع الدراسة بفصل المهام SOD عن طريق عزل الخوادم الخاصة بقواعد البيانات على خوادم داخلية حيث تخصص دار الكتب خادمًا داخليًا منفصل لقواعد بيانات المخطوطات والمهاديات والكتب النادرة والمصكوكات، وكذلك يتم عزل خادم قواعد بيانات النصوص الكاملة لمستودع الرسائل الجامعية اتحاد المكتبات الجامعية المصرية، كما تعمل دارالإفتاء على عزل قواعد البيانات الداخلية الخاصة بالفتاوى والرد على أسئلة الجمهور، وكذلك قواعد بيانات مستودع (دار)، والنصوص الكاملة للمجموعات والكتب النادرة والمخطوطات بمكتبة الأسكندرية، كما يتم فصل قواعد بيانات الجهات الحكومية والهيئات المستضافة بمركز المعلومات مجلس الوزراء، وكذلك تقوم مكتبة الدومنيكان بفصل قواعد البيانات الداخلية الخاصة المخطوطات والمهاديات، ويتم فصل قواعد بيانات المجموعات بالمكتبة المركزية لجامعة القاهرة، هذا بجانب قواعد البيانات المالية والإدارية الخاصة بكل المر افق موضوع الدراسة، وبعد ذلك من نقاط القوة بالممارسات الأمنية بمر افق الدراسة -أما الأساليب الأخرى الوارد بالجدول فلا تتو افر فى كل المر افق موضوع الدراسة أو تتضمن ممارسات غير مكتملة وهى كالتالى :

- تستخدم الشبكات الخاصة الافتراضية VPN فى(٦) مر افق بنسبة ٦٦,٦٦٪، و أنظمة منع وكشف التسلل فى (٧) مر افق بنسبة(٧٧,٨٪).

- تتو افر شهادات الحماية (SSL) فى(٤) مو اقع بنسبة ٤٤,٤٤٪% وتستخدم جميع هذه المر افق شهادات مدفوعة الأجر مرخصة من شركات GoDaddy، وDigicert inc، وBluehost، وGlobalSign nv-sa- باستثناء المكتبة المركزية التى تستخدم النسخ المجانية وبعد ذلك من الممارسات القياسية التى تفتقدها النسبة الأكبر من مجتمع الدراسة لما لها من أهمية، لهذا توصى الباحثة باستخدام شهادات الحماية المرخصة بجميع مر افق الدراسة. ويوضح الشكل رقم (٧) استخدام شهادات SSL بموقعى مركز معلومات مجلس الوزراء ودعم اتخاذ القرار، ومكتبة الاسكندرية.





شكل رقم (٧) شهادات الحماية SSL المستخدمة بموقعى مركز معلومات مجلس الوزراء ودعم اتخاذ القرار المصرى ومكتبة الإسكندرية

- فيما يتعلق بتحديث البرامج وترقيتها، فقد تبين للباحثة اختلاف سياسة التحديث المتبعة بمر افق الدراسة، فيتم التحديث بشكل منتظم وفق آخر إصدار لنظم التشغيل ببو ابة جامعة طنطا وبو ابة دار الإفتاء ٢٠١٩ windows، كذلك توفر المكتبة المركزية لجامعة القاهرة، ومكتبة الإسكندرية، ومركز معلومات مجلس الوزراء، ومكتبة الدومنيكان إصدار Kali Linux 2021.1، ودار الكتب SharePoint Server 2019 ولا يتم التحديث بشكل منتظم بل وفقًا للحاجة باتحاد المكتبات الجامعية المصرية ومكتبات مصر العامة ويستخدم كلاهما نسخة Windows Server ٢٠١٢.

- هناك أساليب أخرى للتأمين تستخدمها مكتبة الإسكندرية، ومركز المعلومات ودعم اتخاذ القرار فقط وتتمثل فى خدمات مدفوعة الأجر تُقدمها شركات الأمن السيبر انى وهى cloud flare [٢]، وAnti-DDoS [3]

- لم تتو افر أساليب التقنيات البيومترية فى أى من المر افق موضوع الدراسة لعدم قناعة العاملين بالحاجة لاستخدامها، ولصعوبة التنفيذ فى ظل اللو ائح والإجراءات الروتينية الخاضعة لها مر افق الدراسة.

١٥/٣اختبار الاختراق Penetration testing بمرافق المعلومات موضوع الدراسة:-

بالرجوع للجدول رقم (٣) يتبين قيام (٦) مر افق بنسبة (٦٦,٦٧٪) من مر افق الدراسة بإجراء اختبار الثغرات الأمنية لمو اقعها وهى مكتبة الإسكندرية، والمكتبة المركزية لجامعة القاهرة، ودار الكتب والوثائق القومية، ومركز المعلومات ودعم اتخاذ القرار، وبو ابة دار الإفتاء المصرية، وبو ابة جامعة طنطا- ويتناول الجزء التالى هذا العنصر بشىء من التفصيل .ويوضح الجدول رقم(٤) مدى تطبيق أنواع اختبارات الاختراق بمر افق المعلومات موضوع الدراسة.

جدول رقم (٤) مدى تطبيق أنواع اختبارات الاختراق Penetration testing بمر افق المعلومات موضوع الدراسة حتى اكتوبر ٢٠٢١

مجتمع الدراسة	الاختبار الخارجى	اختبار الداخلى
مكتبات مصر العامة	-----	---
مكتبة الاسكندرية	√	√
المكتبة المركزية لجامعة القاهرة	√	---
دار الكتب الوثائق القومية	√	---
مكتبة معهد الدراسات الشرقية للآباء الدومنيكان	----	--
مركز معلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى	√	
بو ابة دارالافتاء المصرية	√	---
بو ابة جامعة طنطا	---	√
اتحاد المكتبات الجامعية المصرية	---	---
الإجمالى	٥	٢
النسبة	٥٥,٦٪	٢,٢٢٪

وبالرجوع للجدول رقم (٤) يتضح الأتى :

- تقوم (٥) مر افق بنسبة (٨٣,٣٣٪) من المر افق التى تقوم بإجراء اختبارات الاختراق ونسبة (٥٥,٦٪) من إجمالى مر افق الدراسة بالاختبار الخارجى فقط، والسبب فى ذلك فى اعتقاد العاملين بأنه أكثر أهمية وإجراء كافى فى حد ذاته لتحقق الهدف المطلوب.
- تعد مكتبة الإسكندرية المرفق الوحيد الذى يقوم بإجراء اختبار الثغرات الأمنية بنوعيه بمعدلات ثابتة حيث يتم الاختبار الخارجى سنويًا عن طريق الاستعانة بشركات دولية

للقراصنة الأخلاقيين white hacker ومنها شركات رايا وميكروسوفت، وسيسكو وتتغير كل عام حرصًا على تنوع الخبرات والمصداقية، أما الاختبار الداخلى فيتم أسبوعيًا بواسطة فريق أمن الموقع security officer داخل المكتبة المسئول عن مراجعة كافة إجراءات التأمين وفحصها وتقييمها ثم رفع تقرير لمطورى الموقع لتلافى العيوب ورفع مستوى الحماية.

- تعد بو ابة جامعة طنطا المرفق الوحيد الذى يقوم بإجراء الاختبار الداخلى فقط، ويرجع ذلك لصعوبة الإجراءات المالية والإدارية الخاصة بالاختبار، ويقوم به الفريق الفنى لأمن الموقع ولكن بمعدل غير ثابت عند الضرورة كرصد محاولات متعددة للاختراق أو فترات انتشار حوادث القرصنة بشكل عام.

- ويتم هذا الاجراء بشكل دورى ثابت فى(٥) مر افق حيث يتم كل (٦) شهورفى بو ابة دار الإفتاء المصرية، وموقع دار الكتب والوثائق القومية وفق بروتوكول تعاون مع وزارة الاتصالات التى تتولى إجراء الاختبار، كما يتم هذا الإجراء كل(٣) أشهر بالمكتبة المركزية لجامعة القاهرة التى تستعين بشركات محلية للقراصنة الأخلاقيين لإجراء الاختبار ويتم تغييرها باستمرار سعيًا للموضوعية.

- يقوم مركز المعلومات بإجراء هذا الاختبار(شهريًا) بمعدل ثابت لموقع المركز نفسه و أيضًا لمو اقع الجهات والهيئات الحكومية المستضافة بالمركز ويتم ذلك عن طريق الاستعانة بشركات القراصنة الأخلاقيين.

٦/٣النسخ الاحتياطى لمواقع مرافق المعلومات موضوع الدراسة:-

وقد تبين للباحثة بالدراسة الميدانية ما يلى:

- تتو افر سياسة مكتوبة وموثقة للنسخ الاحتياطى ب(٣) مر افق فقط بنسبة (٣٣,٣٣٪) وهى مركز المعلومات ودعم اتخاذ القرار ومكتبة الإسكندرية، ومكتبة معهد الدراسات الشرقية للآباء الدومنيكان وتتضمن البنود التالية:-

- تحديد المسئول عن النسخ الاحتياطى. - طرق ووسائط التخزين المستخدمة.

- معدلات النسخ المتبعة ونوعية البيانات المحدد نسخها وفق كل معدل.

- كما تبين أن السياسة الخاصة بمركز المعلومات ودعم اتخاذ القرار تخضع للمراجعة والتقييم سنويًا بشكل دورى بينما تتم مراجعتها وفق الحاجة بمكتبة الاسكندرية ومكتبة الدومنيكان.

-أما بقية مجتمع الدراسة فلا تتبع خطط مكتوبة، ويتم النسخ الاحتياطى وفق الممارسات التى يتم إقرارها من العاملين وبذلك فقد تُصبح عرضة للاهتزاز فى حالة تغير الأشخاص-حتى وإن كانت ممارسات قوية، ولهذ توصى الباحثة بضرورة وجود سياسات مكتوبة للنسخ الاحتياطى متكاملة تتضمن العناصر السابق ذكرها وأن تخضع للمراجعة والتقييم الدورى؛ حفاظاً على ثباتها ولضمان نجاح هذه العملية الحيوية وفق مستجدات العمل والتطور التقنى لطرق وأدوات النسخ، ويوضح الجدول رقم (٥) طرق (وسائط) النسخ الأحتياطى المستخدمة بمو اقع مر افق المعلومات موضوع الدراسة.

جدول رقم (٥) طرق (وسائط) النسخ الأحتياطى المستخدمة بمر افق المعلومات موضوع الدراسة حتى أكتوبر ٢٠٢١

م	مر افق المعلومات	الوسائط القابلة للإزالة	برامج النسخ الآلى	الأقراص الصلبة	خادم احتياطى	خادم متزامن	التخزين السحابى
١	مكتبات مصر العامة	√	√	---	-	-	-
٢	مكتبة الإسكندرية	√	√	√	-	√	√
٣	المكتبة المركزية لجامعة القاهرة	---	√	---	√	-	√
٤	دار الكتب الوثائق القومية	---	√	---	√	-	√
٥	مكتبة معهد الدراسات الشرقية للاباء الدومنيكان	---	√	---	√	-	√
٦	مركز معلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى	---	√	----	-	√	√
٧	بو ابة دارالإفتاء المصرية	√	√	---	-	-	√
٨	بو ابة جامعة طنطا	√	√	√	√	√	-

٩	اتحاد المكتبات الجامعية المصرية	√	√	--	-	√	-
	الإجمالى	٥	٩	٢	٤	4	6

يتبين من الجدول رقم (٥) ما يلى:-

١- تطبق إستر اتيجية ١-٢-٣ للنسخ الإحتياطى فى (٧) مر افق بنسبة ٧,٧٨٪ حيث يتم إنشاء نسختين و أكثر للبيانات الأصلية باستخدام طرق مختلفة ويعد ذلك من نقاط القوة التى تشير إلى وعى العاملين بأهمية النسخ الإحتياطى فى استعادة البيانات بعد أى كارثة و أيضًا مميزات الجمع بين أكثر من وسيط للنسخ - وقد تبين بالدراسة الميدانية حفظ نسخة خارج الموقع فى جميع مر افق الدراسة، وتعد مكتبات مصر العامة الوحيدة التى تُنشئ نسخة واحدة فقط؛ لذلك توصى الباحثة بضروة مراعاة توصيات النسخ الاحتياطى السابق ذكرها، كما كانت مكتبة الإسكندرية وبو ابة جامعة طنطا أكثر المر افق التى تنشئ نُسخًا إحتياطية حيث تستخدم (٥) طرق مختلفة للنسخ الاحتياطي.

٢- تتعدد طرق التخزين الاحتياطى المستخدمة بمر افق الدراسة حيث تستخدم البرامج الآلية للنسخ الاحتياطى فى جميع مر افق الدراسة بنسبة (١٠٠٪) ويعد ذلك من مواطن القوة بممارسات التخزين الإحتياطى حيث تكفل هذه البرامج إجراء النسخ الاحتياطى آليا بشكل دورى، يليه التخزين السحابى ويستخدم فى(٦) مر افق بنسبة(٦٦٪) ويرجع ذلك إلى مميزات التخزين السحابى السابق ذكرها، يليه (الوسائط القابلة للإزالة) وتستخدم فى(5) مر افق بنسبة(55.55%) ثم الخادم المتزامن فى(٤) مر افق بنسبة (٤٤,٤٤٪) وهى المر افق التى تسمح إمكاناتها وطبيعتها بوجود خادم آخرمتزامن مع الخادم الرئيسى، وتستخدم كل من الخوادم الاحتياطية والأقراص الصلبة فى (٣) مكتبات بنسبة (33,33%) وقد تبين للباحثة أن لكل من هذه الوسائط استخداماته بمر افق الدراسة على النحو التالى:-

أ- وسائط تخزين قابلة للإزالة: تستخدم الأشرطة Taps وأسطو انات DVD بمكتبات مصر العامة، وبو ابة دارالإفتاء لنسخ البيانات المطلوب نسخها يومياً، أما مكتبة الإسكندرية، وبو ابة جامعة طنطا، و اتحاد المكتبات الجامعية المصرية فتستخدمها للتخزين بمعدلات أبعد أسبوعياً وشهرياً.

ب- أما الخوادم الإحتياطية فتعمل على التخزين اليومى من الخادم الرئيس ب(٤) مر افق بنسبة ٤٤,٤٤٪ وهى المكتبة المركزية لجامعة القاهرة، ودار الكتب والوثائق القومية، وبو ابة جامعة طنطا التى تخصص خادمين لهذا الغرض يتم حفظهما خارج مقرها، و أيضًا مكتبة

الدومنيكان والتى تخصص خادمين احتياطيين الأول موجود لديها، والثانى بمعهد الدراسات الشرقية للآباء الدومنيكان بالقاهرة حيث يتم يوميًا إرسال نسخة كاملة من البيانات الأصلية من الخادم الرئيس الموجود بباريس للخادمين بشكل آلى، كما يوجد الخادم الاحتياطى الخاص بدار الكتب بوزارة الاتصالات التى تتولى العملية كلها نظرًا لعدم وجود إمكانات أو أجهزة خوادم متطورة داخل الدار يمكن تخصيصها لهذا الغرض، ويعد وجود الخوادم الاحتياطية خارج المقار العمل من عناصر القوة التى تُحسب لمر افق الدراسة.

ج- تُستخدم الأقراص الصلبة Hard disks لتخزين بيانات المو اقع يوميًا ثم أسبوعيًا فى (مرفقين) بنسبة (٣٣,٣٣٪) وهى مكتبة الإسكندرية، و اتحاد المكتبات الجامعية المصرية وعلى قدر مميزاتها فإن لها عيوبًا - قد أشارت إليها الدراسة سلفًا.

د-تُستخدم الخوادم المتزامنة بمكتبة الإسكندرية، ومركز المعلومات ودعم اتخاذ القرار- و اتحاد المكتبات الجامعية المصرية، وبو ابة جامعة طنطا و بالتالى يتم تشغيلها فور حدوث أى هجوم أو تعطل فى الخدمة، ومن الممارسات الإيجابية وجود هذه الخوادم خارج مقار المر افق سعياً لتوفير المزيد من الحماية.

هـ- يُستخدم التخزين السحابى كشكل من أشكال النسخ الاحتياطى خارج الموقع ب(٦) مر افق هى مكتبة الإسكندرية والمكتبة المركزية لجامعة القاهرة، ودار الكتب والوثائق القومية، ومكتبة الدومنيكان، ومركز المعلومات ودعم اتخاذ القرار وبو ابة دار الإفتاء المصرية – وقد تناولته الدراسة بشىء من التفصيل -كما يقدم (٣) من مزودى الخدمة خدمات النسخ الاحتياطى للبيانات المخزنة على سُحُبِها سنويًا وذلك مركز المعلومات ودعم اتخاذ القرار، مكتبة الإسكندرية، وبو ابة دار الإفتاء المصرية والمفترض أن يوفر مزودو الخدمة هذه الإمكانية وأن يُذكر ذلك فى العقد القانونى.ويوضح الجدول رقم(٦) معدلات النسخ الاحتياطى بمر افق المعلومات موضوع الدراسة حتى أكتوبر ٢٠٢١.

مر افق المعلومات	يوميا	أسبوعيا	شهريا	معدلات أخرى
مكتبات مصر العامة	√	√	√	--
مكتبة الإسكندرية	√	√	-	√
المكتبة المركزية لجامعة القاهرة	√	√	-	--
دار الكتب الوثائق القومية	√	√	--	√
مكتبة معهد الدراسات الشرقية للاباء الدومنيكان	√	√	√	--

مركز معلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى	√	√	√	--
بو ابة دارالإفتاء المصرية	√	√	-	√
بو ابة جامعة طنطا	√	√	--	--
اتحاد المكتبات الجامعية المصرية	√	√	-	--
	٩	٩	٣	٣
	٪١٠٠	٪١٠٠	٪٣٣	٪٣٣

بالرجوع للجدول رقم (٦) يتضح مايلى:-

- تقوم جميع مر افق الدراسة بالنسخ الاحتياطى بمعدلين ثابتين هما (يوميًا) و(أسبوعيًا) وتقوم(٣) مر افق بالنسخ الشهرى و(٣) مر افق أخرى بمعدلات أخرى غير ثابتة كالنسخ السنوى، قد تبين للباحثة بالدراسة الميدانية اختلاف نوع النسخ المتبع ونوعية ومعدل البيانات التى يتم نسخها وفق كل نوع من مرفق لآخر وفقاً لأولوياته على النحو التالى:-

-النسخ الكاملFullBackup : يعد النسخ الكامل هوالنوع السائد للنسخ الاحتياطى بمر افق الدراسة حيث يتم الحصول على نسخة كاملة يومياً لمحتوى المو اقع وقواعد البيانات فى (٧) مر افق بنسبة (٧٧,٨٪) وهى مكتبات مصرالعامة، و اتحاد المكتبات الجامعية المصرية، وبو ابة جامعة طنطا، ومكتبة الدومنيكان، ومركز المعلومات ودعم اتخاذ القرار، وبو ابة دارالإفتاء المصرية، والمكتبة المركزية لجامعة القاهرة ويعد ذلك من نقاط القوة بممارسات تأمين المو اقع المدروسة حيث يسمح بتكرار النسخ بمعدلات متقاربة وضمان انخفاض حجم البيانات المحتمل خسارتها، و إتاحة أسرع للبيانات عند استردادها. وبالنسبة للعيوب المصاحبة له كتضخم حجم الملفات، فتقوم مر افق الدراسة بالتخلص من النسخ الأقدم فالقديمة فالأحدث.

- كما يتم أيضا النسخ الكامل شهريًا لبيانات الموقع بمكتبات مصر العامة، أيضاً مكتبة الدومنيكان، ومركز المعلومات ودعم اتخاذ القرار، وهناك معدلات أخرى للنسخ الكامل تتبعها بعض المر افق موضوع الدراسة حيث يتم تخزين نسخة كاملة كل (٥) شهور من محتويات موقع دارالكتب والوثائق القومية، وسنويًا ببو ابة دار الإفتاء المصرية، وعلى فترات متباعدة غير ثابتة بمكتبة الإسكندرية.وتدعم هذه الممارسات نقاط القوة للنسخ الاحتياطى وتأمين البيانات المتبعة بمجتمع الدراسة.

- النسخ التفاضلى : تقوم مكتبة الإسكندرية بالنسخ التفاضلى للإضافات المستحدثة والتغيرات اليومية على الموقع وقواعد البيانات، أما المواد الأرشيفية والتاريخية الثابتة

تؤخذ منها نسخة مرة واحدة فقط سنويًا، كذلك تنسخ دار الكتب التغيرات اليومية التى تطرأ على قواعد البيانات وهى الخاصة بخدمات الإيداع والإصدارات.

٧/٣ استضافة خادم الويب بمرافق المعلومات موضوع الدراسة

يوضح الجدول رقم (٧) استضافة خادم الويب المتبعة بمر افق المعلومات موضوع الدراسة.

جدول رقم (٧) استضافة خادم الويب بمر افق المعلومات موضوع الدراسة حتى أكتوبر ٢٠٢١

م	مر افق المعلومات	نوع الاستضافة			
		مستقلة Dedicated	مشتركة Shared	VPSالاستضافة الافتراضية الخاصة	سحابية clouding
١	مكتبات مصر العامة.	√	-	√	-
٢	مكتبة الإسكندرية.		-	-	√
٣	المكتبة المركزية لجامعة القاهرة	√	-	-	√
٤	دار الكتب والووثائق القومية	-	√	-	√
٥	مكتبة معهد الدراسات الشرقية لآباء الدومنيكان	√	-	-	√
٦	مركز معلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى	√	-	-	√
٧	بو ابة دارالإفتاء المصرية	√	-	-	√
٨	بو ابة جامعة طنطا	√	-	-	-
٩	اتحاد المكتبات الجامعية المصرية	√	-	-	-
	الإجمالى	٧	١	١	٦

ويتبين من الجدول رقم (٧) مايلى:

- تعد الاستضافة المستقلة النمط الغالب بمر افق الدراسة حيث تتم ب(٧) مر افق تمثل نسبة(٧٧,٨٪) من مجتمع الدراسة ويعد ذلك من عناصر القوة بمنظومة التأمين بمر افق الدراسة لما سبق ذكره من مميزات لهذا النوع، والجدير بالذكر أن مركز المعلومات ودعم اتخاذ القرار هو نفسه جهة مُضيفة حيث يقدم خدمات الاستضافة ل(٦٣)مؤسسة وجهة حكومية وذلك نظرًا لدوره وبالتالى يستوجب ذلك إجراءات تأمينية عالية لموقعه.

-تقدم شركة (ليكويد ويب Liquid web) خدمات الاستضافة لبو ابة دارالإفتاء المصرية، وشركة (أوفى اتش OVH) الفرنسية لموقع مكتبة الدومنيكان، وقد جاء اختيارهذه الشركات وفقاً لمعايير السمعة الجيدة، وجودة الأداء بالمو اقع أخرى، واستقرار الخدمات المقدمة، كما تتم الاستضافة للمكتبة المركزية لجامعة القاهرة، وبو ابة جامعة طنطا، و اتحاد المكتبات الجامعية المصرية بشبكة الجامعات المصرية تحت مظلة المجلس الأعلى للجامعات .

- يعتمد موقع واحد بنسبة (١١,١١٪) وهو موقع دار الكتب والوثائق القومية على الاستضافة المشتركة بوزارة الاتصالات المصرية وذلك فى إطار برتوكول التعاون المبرم بينها وبين وزارة الثقافة بكافة القطاعات التابعة لها، ولهذا تعتمد الدار كاملاً على ما تقدمه وزارة الاتصالات من دعم وتأمين للخادم .

- تتم الاستضافة الافتراضية بموقع واحد بنسبة (١١,١١٪) هو موقع مكتبة مصر العامة حيث تقدم شركة (كورد ديجيتال(cord digital) الفرنسية خدمات الاستضافة لموقع مكتبات مصرالعامة وتأمينه وتقديم الدعم الفني وإجراء التحديثات. وقد تم اختيارها أيضًا وفقًا للمعايير السابقة .

- تُستخدم الاستضافة السحابية كشكل من أشكال النسخ الاحتياطى لتخزين نسخة من البيانات خارج مو اقعها الجغر افية ويتم ذلك ب(٦) مر افق بنسبة (٦٦,٧٪) وهى مكتبة الإسكندرية، والمكتبة المركزية لجامعة القاهرة، ودار الكتب والوثائق القومية، ومركز معلومات ودعم اتخاذ القرار، والبو ابة الالكترونية لدارالإفتاء المصرية، ومكتبة معهد الدراسات الشرقية للآباء الدومنيكان. كما تبين بالدرسة الميدانية مايلى:-

أ- أن جميع هذه المر افق تستأجر سُحباً خاصة Private Clouds ويعد ذلك من نقاط القوة لما لهامن مميزات أمنية حيث تعدأكثر أماناً و أقل عرضة للاختراق من السحب العامة وتتم المصادقة فى السحب الخاصة نفس الطريقة المتبعة فى vpnولهذا تختلف السياسات والإجراءات الأمنية من نموذج إلى آخر(Kumara , Rajb, & Jelcianac , 2018)

ب- تقع مسئولية تأمين جميع السُحب على مزودى الخدمة بموجب بند موثق بالعقد القانونى من حيث تأمين البنية التحتية ،ويتم إنشاء حساب وتحديد اسم مستخدم وكلمة مرور لكل مرفق للحفاظ على سرية بياناته والتحكم فى الوصول ومن أمثلة مقدمى الخدمة شركة Global protect التى توفر السحابة ببو ابة دار الإفتاء المصرية، وشركة Microsoft Azur التى توفر السحابة الخاصة بدار الكتب، والجدير بالذكر أن وزارة الثقافة فى طريقها لتأجير سحابة خاصة بقطاعاتها ومنها دار الكتب وذلك عن طريق شركة وى (WE)للاتصالات.

ج- يتم رفع البيانات للسحابة بمعدل ثابت على مدار الساعة يوميًا ب(٤) مر افق بنسبة (٦٦,٧٪) وهى مكتبة الإسكندرية، مركز المعلومات ودعم اتخاذ القرار، وبو ابة دار الإفتاء المصرية، والمكتبة المركزية لجامعة القاهرة، ويتم بمعدل غير ثابت بدار الكتب، ومكتبة معهد الدراسات الشرقية للآباء الدومنيكان ويتم رفع البيانات للسحب آليا بجميع المر افق- فيما عدا مكتبة الدومنيكان فيتم يدوياً.

هـ- أن (٣) مر افق بنسبة ٥٠٪ من المر افق المؤجرة للسحب لاتعلم الأماكن الجغر افية للخوادم المخزنة عليها بياناتها بالسحابة وهى المكتبة المركزية لجامعة القاهرة، ودار الكتب، وبو ابة دار الإفتاء المصرية وجميع المر افق موضوع الدراسة المستخدمة للمنصات السحابية لا تعلم هل يقوم مزودى الخدمة بتشفير بياناتها بمرحلة التخزين أم لا - باستثناء مكتبة الإسكندرية ومركز المعلومات ودعم اتخاذ القرار.

و- يعد مركز المعلومات المرفق الوحيد الذى يقوم بتشفير بياناته قبل رفعها للسحابة حفاظاً على سريتها وسلامتها، وتشيد الباحثة بهذه الخطوة نظرًا لطبيعة عمل المركز ونوعية البيانات الحكومية الهامة التى يتم رفعها –أما بقية مر افق الدراسة فلا تقوم بالتشفير قبل الرفع.

ز- فيما يتعلق بنوعية البيانات التى يتم رفعها للسُحب فتختلف من مرفق لآخر حيث يتم رفع بيانات الموقع كاملاً بالمكتبة المركزية لجامعة القاهرة، ومركز المعلومات ودعم اتخاذ القرار وبو ابة دار الإفتاء المصرية، وترفع دار الكتب بيانات الأرشفة الإلكترونية لخدمات الإيداع والكتب الإلكترونية المتاحة مجاناً فقط والسبب فى ذلك هو صغر المساحة التخزينية المخصصة للدار، كما ترفع مكتبة الإسكندرية بيانات الكتب الإلكترونية ومستودع دار والمواد الأرشيفية والتاريخية لقلة التغيرات بها، وتتفق جميع المر افق فى عدم رفع بيانات الحسابات الشخصية للأشخاص وأسماء المستخدمين وكلمات السر، وتشيد الباحثة بهذا الإجراء والوعى فى انتقاء البيانات التى يتم رفعها للمنصات وفقا لما ذكر سلفاً من توصيات.

٨/٣ لغات البرمجة المستخدمة بمواقع المرافق موضوع الدراسة:-

يوضح الجدول رقم (٨) لغات البرمجة المستخدمة بمو اقع مر افق المعلومات موضوع الدراسة:

جدول رقم (٨) لغات البرمجة المستخدمة بمو اقع مر افق المعلومات موضوع الدراسة حتى أكتوبر ٢٠٢١

م	مجتمع الدراسة	لغة البرمجة
١	مكتبات مصر العامة	PHP
٢	مكتبة الاسكندرية	PHP
٣	المكتبة المركزية لجامعة القاهرة	Wordpress
٤	دار الكتب الوثائق القومية	SharePoint
٥	مكتبة معهد الدراسات الشرقية للآباء الدومنيكان	PHP
٦	مركز معلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى	PHP
٧	بو ابة دارالإفتاء المصرية	javascript #C
8	بو ابة جامعة طنطا	PHP javascript
9	اتحاد المكتبات الجامعية المصرية	#C

ويتبين من الجدول رقم (٨) مايلى:

-تعد لغة PHP أكثر اللغات استخداماً بمو اقع الدراسة حيث تُستخدم فى (٦) مو اقع بنسبة (٦٦,٦٧٪) من مو اقع الدراسة فضلاً عن أنها النواة لبرنامج Wordpress وتتميز بأنها لغة مفتوحة المصدر يتمّ تطويرها وصيانتها من قبل مجتمع كبير وواسع من المطوّرين والمتطوعين تحت رخصة PHP ممّا يسمح للجميع بالتعاون والعمل عليها، ونظراً لوجودها منذ سنوات فقد تبلورت خبرات المطورين بها وتم اكتشاف معظم ما يحويه من عيوب وأخطاء ووفقًا لما ورد بإحصاءات Whitesource فإن ثغرة البرمجة عبر الموقع Cross-Site Scripting-XSS CWE-79 هى الأعلى بهذه اللغة بنسبة ٤٠٪ من إجمالى الثغرات التى تتضمنها، يليها حقن SQL Injection CWE-89 بنسبة (١٥٪)، يليها تخطى الأذونات والامتيازات والتحكم فى الوصول Permissions Privileges, and Access Control CWE-264 بنسبة(١٢%) وعلى هذه النحو يتعين على العاملين بمو اقع الدراسة المبنية بهذه اللغة التعرف على هذه الثغرات و اتخاذ للإجراءات اللازمة لصد الهجمات التى قد تحدث من خلالها ورفع مستوى تأمين الأكواد.

- تستخدم لغة جافا سكريبت بموقعين بنسبة (٢٢,٢٢٪) وهى المكون الأساس لتصميم وتطوير تطبيقات الويب حيث تضيف التفاعل إلى صفحات المو اقع الإلكترونية بشكل يجذب المستخدمين، ولهذا أصبحت تستخدم بشكل مكثف وواسع فى تطويروبرمجة المو اقع ووفقًا لCWE فإن ثغرة" فشل آليات التشفير Cryptographic Issues CWE-310 "هى الأعلى بهذه اللغة بنسبة (٢٥٪)، وحقن SQL Injection CWE-89 بنسبة(٢٢%) وعلى هذه النحو يتعين على العاملين بمو اقع الدراسة المكتوبة بهذه اللغة التعرف على هذه الثغرات و اتخاذ الإجراءات اللازمة لمنعها. (What are the most secure Programming languages, 2022)

-تستخدم لغة (C#) بموقعين من مجتمع الدراسة بنسبة ٢٢,٢٢٪ وهى أحد أشهر لغات البرمجة على الإطلاق حيث تسمح للمطورين بإنشاء تطبيقات قوية وآمنة وتدعم خدمات تطوير.ASP.NET ويتم دعمها وتطويرها من شركة ميكروسوفت ووفقا لCWE فهى تتضمن ثغرات بنسبة أقل من الموجودة فى اللغات مفتوحة المصدر. (What are the most secure Programming languages, 2022)

٣/١٩الكوادر البشرية المسئولة عن أمن وإدارة مواقع مرافق المعلومات موضوع الدراسة .

تعد الكوادر البشرية حجر الزاوية لأى مؤسسة حيث يؤكد خبراء الأمن السيبر انى وأن الحلقة الأضعف في عملية الاختراق هو العنصر البشري، وأن الأخطاء البشرية هى القاسم المشترك فى كافة عمليات الاختراق الواسعة كقيام الموظف بالنقرعلى ر ابط أو ملف فى رسالة بريد إلكتروني ضارة، أو استخدام كلمات مرور ضعيفة، أو عدم تحديث تأمين البرمجيات فى الوقت المناسب وتشيرالدراسة التى أجرتها شركة IBM عام ٢٠٢١ إلى أن إزالة الخطأ البشرى والتغلب عليه سيؤدى إلى منع حدوث ٩٥٪ من اختراق البيانات (Why Human Error is #1 Cyber Security Threat to Businesses in 2021, 2021)

ويؤكد ذلك نتائج الدراسة التى أجراها موقع PreciseSecurity.com عام ٢٠١٩ و انتهت إلى أن كلمات المرور الضعيفة هي السبب الرئيس الثالث لشن هجمات برامج الفدية الضارة، وذلك عقب نقص تدريب العاملين على الأمن السيبر اني، والتصيد الاحتيالي – وجميع هذه الأسباب ناجمة عن الأخطاء البشرية. (Jastra, Spam Messages Make 55 % of Global E-mail Traffic in 2019, 2020) ويوضح الجدول (٩) أعداد ومؤهلات العمالة البشرية المسئولة عن أمن وإدراة المو اقع موضوع الدراسة.

جدول رقم (٩) الكوادر البشرية المسئولة عن أمن وإدارة المو اقع موضوع الدراسة حتى اكتوبر ٢٠٢١

م	مر افق المعلومات	العدد	المؤهل	الدورات التدريبية
١	مكتبات مصر العامة	١	هندسة اتصالات	MCSA- Red hat Admin IC3- VMware- ICDL Default A+
٢	مكتبة الاسكندرية	١٢	هندسة اتصالات	CSSP- Ethical Hacking
٣	المكتبة المركزية لجامعة القاهرة	٥	هندسة اتصالات-حاسبات ومعلومات	1-Microsoft security routing & switching 2-Sna ISA SECURITY
٤	دار الكتب الوثائق القومية	٣	٢ -مهندسين اتصالات +١- اداب تخصص مكتبات إدارة محتوى الموقع	CSSP
٥	مكتبة معهد الدراسات الشرقية للآباء الدومنيكان	٣	هندسة اتصالات	- Ethical Hacking
٦	مركز معلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى	١٩	هندسة اتصالات-حاسبات ومعلومات	CCNA & CCNP
٧	بو ابة دار الإفتاء المصرية	١٢	هندسة اتصالات-حاسبات ومعلومات	Ethical Hacking
٨	بو ابة جامعة طنطا	٤	هندسة اتصالات	FG &F5big ip
٩	اتحاد المكتبات الجامعية المصرية	٦	هندسة اتصالات	CSSP

ويتبين من الجدول رقم (٩) ما يلى:-

- تو افر كوادر بشرية من المهندسين المتخصصين بكافة المر افق موضوع الدراسة تتولى تأمين المو اقع و الشبكات وتشغيلها والدعم الفنى، كما يقوم بتشغيل وإدارة موقع دار الكتب فرد واحد حاصل على ماجستير مكتبات وتقنيات المعلومات ويتولى مسئولية تأمين إدارة موقع مكتبات مصر العامة مهندسًا متخصصًا واحدًا.
- تتفاوت أعداد الكوادر البشرية المتو افرة لكل مرفق ويرجع ذلك لاختلاف حجم وطبيعة المر افق ونشاطها وأهدافها، حيث تضم مكتبة الإسكندرية قطاعاً كبيراً لتكنولوجيا

المعلومات يتكون من (١٥٠) فرد من التخصصات المختلفة للقيام بالمهام التقنية والمشروعات الرقمية بالمكتبة ويتولى (١٢) منهم مسئولية أمن وإدارة الموقع والدعم الفنى وإدارة البرمجيات مركز معلومات ودعم اتخاذ القرار بمجلس الوزراء قطاعًا كبيرًا لتقنية المعلومات يتكون من ١٩ متخصص، بينما نجد مهندسًا واحدًا مسئولاً عن أمن وإدارة موقع مكتبات مصر العامة.

- يسعى الفريق الفنى التقنى بكافة مر افق الدراسة للتطوير المهنى والتدريب على أحدث أساليب الأمن السيبر انى من خلال الحصول على دورات متخصصة كما ورد بالجدول رقم (٩)، وقد تبين أن (٥) مر افق بنسبة ٥٥,٦٪ تقدم الدعم المالى والإدارى للعاملين بها من خلال الالتحاق بالدورات المهنية المتخصصة وهى مكتبة الإسكندرية، ومركز معلومات مجلس الوزراء وبو ابة دارالإفتاء المصرية كما بدأ العاملون ببو ابة جامعة طنطا، والمكتبة المركزية، و اتحاد المكتبات الجامعية المصرية فى الحصول على دورات تدريبية من قِبل المجلس الأعلى للجامعات بدايةً من عام ٢٠٢٠ فقط لرفع كفاءة التأمين والحماية فى ظلال جائحة كورونا ومستجداتها واعتماد أساليب التعليم عن بعد وزيادة الضغط على استخدام بو ابة الجامعة، بينما يفتقد العاملون فى بقية مر افق الدراسة للدعم المؤسسى ويتم السعى بشكل شخصى.

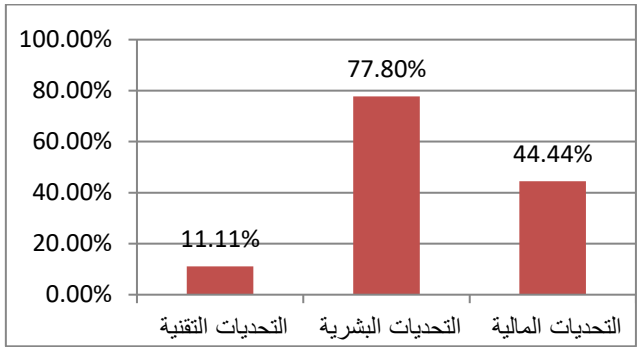
- لم يتلق بقية قطاعات العاملين بمر افق الدراسة على أى دورات تدريبية متعلقة بالأمن السيبر انى وارشاداته – باستثناء مكتبة الأسكندرية ومركز معلومات مجلس الوزراء، بينما يتم توجيه العاملين بمكتبات مصر العامة للإرشادات الأمنية عن طريق البريد الإلكترونى والاجتماعات الافتراضية.

- من الممارسات الإيجابية اشتراك أعضاء الفريق الفنى بدارالإفتاء المصرية ومركز المعلومات ومكتبة الاسكندرية بمو اقع دولية متخصصة فى أمن المعلومات للإحاطة بكل ماهو جديد فى مجال الأمن السيبر انى والثغرات الأمنية ومشاركة الخبرات الخاصة بأساليب القرصنة وهى نقطة قوة تحسب لمر افق الدراسة.

١٠/٣تحديات القرصنة الإلكترونية بمواقع مرافق المعلومات موضوع الد راسة:-

يواجه العاملون المسئولون عن أمن المعلومات تحديات كبيرة لحماية البيانات وتأمين المو اقع من أخطار القرصنة الإلكترونية ولا يمكن النجاح بهذا الدور الملقى على عاتقهم دون إدراك عوامل النجاح والوقوف على هذه الصعوبات التى تنعكس سلبًا على توفير منظومة

أمنية ناجحة وليست كلها تقنية، فمنها ماهو إدارى، ومنها ماهو بيئى، أومادى ولهذا لابد من الوقوف على التحديات والعوامل التى تؤثرعلى نجاح تأمين المو اقع. ويوضح الشكل رقم (٨) والجدول رقم (١٠) التحديات القرصنة الإلكترونية بمر افق المعلومات موضوع الدراسة.



شكل رقم (٨) التحديات القرصنة الإلكترونية بمر افق المعلومات موضوع الدراسة

جدول رقم (١٠) تحديات القرصنة الإلكترونية بمو اقع مر افق المعلومات موضوع الدراسة حتى أكتوبر ٢٠٢١

م	مر افق المعلومات	تحديات تقنية	تحديات بشرية	تحديات مالية	الإجمالى
١	مكتبات مصر العامة	---	√	--	١
٢	مكتبة الاسكندرية	----	√	-	١
٣	المكتبة المركزية لجامعة القاهرة	---	---	√	١
٤	دار الكتب الوثائق القومية	√	√	√	٣
٥	مكتبة معهد الدراسات الشرقية للآباء الدومنيكان	---	√	-	١
٦	مركز معلومات ودعم اتخاذ القرار بمجلس الوزراء المصرى	---	√	-	١
٧	بو ابة دارالإفتاء المصرية	---	√	-	١
٨	بو ابة جامعة طنطا	---	√	√	٢
٩	اتحاد المكتبات الجامعية المصرية	--	---	√	١
	الإجمالى	١	٧	٤	١٢
	النسبة المئوية	٪١١,١	٪٧٧,٧	٪٤٤	

وبناء على الجدول رقم (١٠) والشكل رقم (٨) يتضح الأتى:-

- تأتى التحديات البشرية فى مقدمة التحديات التى تواجه المر افق موضوع الدراسة بنسبة ٧٧,٧٨٪ وتتمثل فى نقص الكوادر البشرية المتخصصة المسئولة عن أمن وإدارة المو اقع، والأخطاء البشرية عن غير عمد والحاجة للتطوير المهنى والتوعية المستمرة بأساليب التخزين الاحتياطي والتعرف على أحدث التطورات في مجال تأمين المو اقع ضد القرصنة والأمن السيبر انى وأهمية كل منها ولتقليل نسبة الأخطاء البشرية التى قد ينتج عنها ثغرات بالموقع وبالتالى احتمالات للاختراق. وتتفق هذه النتيجة مع دراسة أحمد عبد الرازق حيث يرى (٦٢٪) من منسوبى المركز القومى للمعلومات أن فقدان البيانات والمعلومات نتيجة لأخطاء العامل البشرى سواء عن عمد أو غير عمد تأتى المقام الأول.

- تأتى التحديات المالية فى المرتبة الثانية بنسبة٤٤٪ وتتمثل فى عدم كفاية المخصصات المالية المرصودة للتأمين، وإن تو افرت الميز انيات الكافية عند التأسيس فلا تزال هناك صعوبة في توفيرها للتحديث والمتابعة، وقد يتأثر هذا العامل بمدى تقدير الإدارات العليا للمر افق موضوع الدراسة لأهمية بند التأمين ومستحدثاته. ولهذا توصى الباحثة بضرورة توفير الموارد المالية اللازمة لتوفير منظومة دفاع إلكترونى متكاملة ومواكبة كل ما هو جديد فى هذه المجال .

- تأتى التحديات التقنية فى المرتبة الثالثة والأخيرة بنسبة (١١,١١٪) وتتمثل فى الحاجة لأجهزة خوادم بمواصفات متطورة لقواعد البيانات الداخلية بدار الكتب والوثائق القومية والتى تعانى من التقادم وسوء حالتها المادية.

- تعد دار الكتب والوثائق القومية أكثر المر افق موضوع الدراسة التى تواجه تحديات أمنية حيث بلغت ٢٥٪ من إجمالى التحديات التى تواجه مر افق الدراسة، لهذا توصى الباحثة بضرورة الاهتمام بحل المشكلات التى تواجهها للارتقاء بمنظومة التأمين والحماية لموقعها لما لها من مكانة متفردة باعتبارها مكتبة مصر الوطنية.

١١/٣النتائج والتوصيات :

١/١١/٣ ملخص نتائج الدراسة:

تناولت الدراسة القرصنة الإلكترونية على مو اقع الإنترنت والتطبيق على عينة من مو اقع مر افق المعلومات المصرية، هنا تم ترتيب (ملخص النتائج) وفقا لترتيب التساؤلات الواردة في الإطار المنهجي لهذه الدراسة بحيث يأتي كل تساؤل متبوعاً بملخص النتائج المرتبطة به على النحو التالي:-

التساؤل الأول :ما حوادث القرصنة التى استهدفت مو اقع مر افق المعلومات المصرية على الإنترنت؟ وما الدو افع ورائها ؟وهل اختلفت باختلاف طبيعة نشاط المرفق نفسه؟ وما الخسائر الناجمة عنها؟ وكيف تم التعامل معها ؟

- تعرض بالفعل (٥) مو اقع بنسبة ٥٥,٥٦٪ من مو اقع مر افق المعلومات موضوع الدراسة لهجمات القرصنة الإلكترونية وهى مكتبة الإسكندرية، ودار الكتب والوثائق القومية ،مركز معلومات مجلس الوزراء، وبو ابة جامعة طنطا و اتحاد المكتبات الجامعية المصرية.

- كان" تدمير وتخريب البيانات "هو الدافع الأكثر انتشارًا وراء الهجمات الإلكترونية على مو اقع مر افق المعلومات موضوع الدراسة، حيث تكررفى (٤) مر افق بنسبة٤٤ ,٤٤٪، يليه التحدى التقنى و اثبات الذات وتكررفى (٣) مر افق بنسبة ٣٣,٣٣٪.

- كانت هجمات حجب الخدمة" أكثر الأساليب المستخدمة ب(٣) مر افق بنسبة ٣٣,٣٣٪، يليه "التصيد والخداع "phishing، وحقن Injection واستخدم كل منهما فى مرفقين بنسبة ٢٢,٢٢٪، وتم استخدام فيروس "تروجان" فى مرفق واحد بنسبة ١١,١١٪.

التساؤل الثانى : هل تتو افر سياسات وخطط موثقة وفعَّالة لأمن المعلومات، والاستجابة للحوادث، واستعادة النظام بعد الكارثة بمر افق الدراسة؟ وما الإجراءات المتبعة لتأمين مو اقع مر افق المعلومات المصرية على شبكة الإنترنت؟ وإلى أى مدى تُمثل نقاط قوة أو ضعف فى تأمين المو اقع المدروسة؟

- افتقرت جميع مر افق الدراسة لوجود سياسات موثقة وفعالة لأمن المعلومات، حيث توجد أجزاء مكتوبة تغطى إجراءات الاستجابة للحوادث- كماذكر سلفًا- وذلك بمكتبة الإسكندرية ومركز معلومات مجلس الوزراء.

- تعددت الأساليب والممارسات الأمنية المتبعة بمر افق الدراسة، وتأتى مكتبة الإسكندرية، ومركز معلومات مجلس الوزراء، فى مقدمة مجتمع الدراسة من حيث تو افر هذه الأساليب.

- تتو افر (٦) أساليب أمنية بجميع مر افق الدراسة بنسبة ١٠٠٪ وهى الجدران الحماية، وكلمات السر، وبرامج إدارة الشبكات، والنسخ الاحتياطى، وفصل المهام ، وبرامج الحماية ضد الفيروسات.

- تقوم (٦) مر افق بنسبة (٦٦,٦٧٪) من مر افق الدراسة بإجراء اختبار الثغرات الأمنية بمو اقعها وتطبق(٥) منها الاختبار الخارجى فقط.

-تو افرت إستر اتيجية ١-٢-٣ للنسخ الإحتياطى فى (٧) مر افق بنسبة ٧٧,٧٪ وتقوم جميع مر افق الدراسة بنسبة ١٠٠٪ بالنسخ الإحتياطى بمعدلين ثابتين هما (يوميًا) و(أسبوعيًا).

- يعد النسخ الكامل FullBackup هو النوع السائد للنسخ الاحتياطى حيث يتم الحصول على نسخة كاملة لمحتوى المو اقع وقواعد البيانات يومياً فى (٧) مر افق بنسبة ٧٧,٨٪.

التساؤل الثالث: ما نوع الاستضافة لمو اقع مر افق المعلومات المصرية على شبكة الإنترنت، وما لغات البرمجة المستخدمة لبناء هذه المو اقع وإلى أي مدى تُمثل نقاط قوة أو ضعف في تأمين المو اقع المدروسة؟

- تعد الاستضافة المستقلة النمط السائد بمر افق الدراسة حيث تتم ب(٧)مر افق تمثل نسبة (٧٧,٧٪) ويعد ذلك من عناصر القوة لما تتميز به مميزات ذُكرت فى الإطار النظرى .

-تعد لغة PHP أكثر اللغات استخداماً بمو اقع الدراسة حيث تُستخدم فى (٦) مو اقع بنسبة (٦٦,٦٧٪) من مو اقع الدراسة ووفقا لما ورد بإحصاءات Whitesource فإن ثغرة البرمجة عبر الموقع Cross-Site Scripting-XSS CWE-79 هى الأعلى بهذه اللغة بنسبة ٤٠٪ من إجمالى الثغرات التى تتضمنها.

التساؤل الرابع: ما أعداد ومؤهلات الكودار البشرية المسئولة عن أمن مو اقع مر افق المعلومات المصرية على الإنترنت؟ وهل يتم تدريبهم وتنمية مهاراتهم بالشكل الملائم وإلى أي مدى تُمثل نقاط قوة أو ضعف لتحقيق أمن هذه المو اقع؟

-تو افرت كوادر بشرية من المهندسين المتخصصين بكافة المر افق موضوع الدراسة تتولى تأمين المو اقع والشبكات وتشغيلها والدعم الفني، كما يقوم بتشغيل وإدارة موقع دار الكتب فرد واحد حاصل على ماجستير مكتبات وتقنيات المعلومات، ويتولى مسئولية تأمين إدارة موقع مكتبات مصرالعامة مهندسًا متخصصًا واحدًا.

- تبين أن (٥) مر افق بنسبة ٥٥,٦٪ من مر افق الدراسة تقدم الدعم المالى والإدارى للعاملين بها من خلال الالتحاق بالدورات المهنية المتخصصة.

التساؤل الخامس: ما التحديات التى تواجه تأمين مو اقع مر افق المعلومات المصرية على شبكة الإنترنت من مخاطر القرصنة ؟

-تأتى التحديات البشرية فى مقدمة التحديات التى تواجه المر افق موضوع الدراسة بنسبة ٧٧,٧٨٪ ، يليها التحديات المالية بنسبة ٤٤,٤٤٪ يليها التحديات التقنية بنسبة ١١,١١٪

- تعد دارالكتب والوثائق القومية أكثر المر افق التى تواجه تحديات أمنية حيث بلغت ٢٥٪ من إجمالى التحديات التى تواجه جميع المر افق موضوع الدراسة.

٢/١١/٣ :التوصيات :

التساؤل السادس:ما التحديات التى تواجه تأمين مو اقع مر افق المعلومات المصرية على شبكة الإنترنت من مخاطر القرصنة؟

قدمت الدراسة العديد من التوصيات من أبرزها مايلى:

١-تطوير سياسة لأمن المعلومات بمر افق الدراسة اعتمادًا على السياسات والإجراءات بمعايير المنظمة الدولية للتوحيد القياسي(آيزو27002 ISO/IEC 27002:)، وأن يتم مراجعتها وتحديثها بصفة دورية سنويًا وفقًا لأحدث الإصدارات وما يستجد من أولويات للمؤسسة بحيث تعكس سياسة واضحة وليست كنتيجة أورد فعل لحادث اوكارثة ما.

٢- ضرورة إعداد خطط لاستعادة النظام بعد الكارثة والاستجابة للحوادث مكتملة وفق المحتوى السابق ذكره على أن يتم مراجعتها بانتظام وتحديثها لمراعاة أي تغييرات فى العاملين أو بيئة تكنولوجيا المعلومات وهناك (٧) خطوات لإعداد خطة ناجحة للاستجابة للحوادث تتمثل فيما يلى :

- التحضيرPreparation:ويشمل التحضير المسبق قبل وقوع الحادثة ويعنى تقييم شامل للمخاطر يتناول جميع العناصر من تدريب العاملين وإعداد قو ائم للاتصال فى حال وقوع حادث وغيرها.

- تحديد الحوادثIdentifying events: وتعنى اكتشاف السلوكيات غير العادية وتصنيفها لاتخاذ الإجراء المناسب ويتم ذلك من خلال اجراء اختبار الاختراق لاكتشاف الثغرات ونقاط الضعف وتقييم المخاطر بمجرد أن يتم تحديد المشكلة يجب فهم طبيعة هذا الحدث واحتمالات الضرر الناتج عنه .

- الاحتواء:Containment:أى تحديد رد الفعل المناسب لاحتواء الأزمة والإجراءات الملائمة للتعامل مع كل هجمة إلكترونية كالفيروسات الضارة أو حجب الخدمة وغيرها، ويساعد اتخاذ الاجراءات الصحيحة على تقليل وقت توقف الخدمة وتسهيل التحقيق فى أسباب الحادث .

- الإزالة والاستردادEradication and restoration:ويتضمن الخطوة الر ابعة والخامسة إزالة التهديد ثم إعادة بيئة العمل للإنترنت مرة أخرى من خلال وجود خطة موثقة ومحكمة للنسخ الاحتياطى.

- التعلم والتكرارLearning and reiteratin: تشمل الخطوتان السادسة والسابعة التوثيق لكل حدث والتعلم منه لتحديد نقاط الضعف ومنع تكرارها من خلال إعداد تقرير ورفعه

للإدارة العليا، فضلاًعن تطوير الإجراءات واختبارها وتدريب العاملين عن طريق محاكاة هجوم حقيقى واختبارات الاختراق. (centre, 2020, pp. 4-11)

٣- توفير أساليب الحماية المختلفة بجميع مر افق الدراسة ومنها شهادات الحماية SSL ونظم IPS ,IDS وبرتوكولات الإتصال الآمن بالخادم.

٤- وضع إستر اتيجية لتطبيق اختبارات الاختراق بنوعيها الداخلية والخارجية وإجراء تقييم المخاطر وتحديد الأصول الرقمية لتحقيق الفحص الشامل والتحسين المستمر للوضع الأمني للمؤسسة.

٥-أن تشمل الدورات التدريبية كافة قطاعات العاملين بمر افق الدراسة وليس المتخصصين بالأمن السيبر انى فقط بهدف التعريف بأنواع الهجمات الإلكترونية والتوعية بالأخطاء البشرية التى يتم استغلالها لشن هجمات كدورهم فى حماية كلمات السر الخاصة بهم، وأساسيات التأمين والحماية.

٦-تقديم الدعم المؤسسى اللازم لتدريب الكوادر المتخصصة بمر افق الدراسة ومتابعة كل ماهو جديد فى مجال الأمن السيبر انى وتحسين مهاراتهم وإعادة تأهيلهم، كما يجب أن يدرك العاملون أن الأمن السيبر انى هي مسئولية الجميع وعلى كافة مستويات الإدارة بالمؤسسة الوقوف على أَهُبة الاستعداد دائما لضمان عدم تعرض بياناتها وعملياتها للخطر، وأنهم بصدد حرب شرسة لن ينتهى بين مهارات المُدافع والمُهاجم.

٧-توفير المتطلبات المادية والبشرية والتقنية اللازمة للتغلب على التحديات الأمنية التى تواجهها دار الكتب والوثائق القومية.

٨- استخدام تقنيات جديدة لأمن البيانات من أهمها القياسات البيومترية- السابق الإشارة إليها، وتقنية سلسلة الكتل (Blockchain) التى تمثل التوجه القادم فى تقنيات تشفير وحماية البيانات، وعلى الرغم من أنها تقنية ناشئة إلا أنها تشهد تحركاً لاستخدامها من قبل العديد من المؤسسات على الصعيد الدولى والعربى فى مختلف المجالات. ولهذا تأمل الباحثة متابعة العاملين لمر افق الدراسة للتطورات وإمكانات التطبيق سعيًا للاستفادة بمميزاتها الفائقة فى تأمين البيانات.

الشكر والعرفان.

تتوجه الباحثة بأسمى آيات الشكروالامتنان للسادة المديرين والمهندسين وجميع العاملين بإدارات تقنيات المعلومات بالمر افق موضوع الدراسة على حسن تعاونهم والعمل الجاد معها، وجزيل الشكروالعرفان لكل من قدم لها يد العون فى سبيل إجراء الدراسة .

قائمة المصادر العربية

- أحمد،م.أ.ع (٢٠١٦). أمن المعلومات ودوره فى الحد من القرصنة الإلكترونية المركز القومى للمعلومات : دراسة حالة. (شراف نصر الدين حسن، المحرر) أم درمان: جامع أم درمان الإسلامية.
- إسماعيل،ن. (أكتوبر, ٢٠١٠). إدارة أمن نظم المكتبات الآلية المتكاملة بطريقة أكثر فعالية : دراسة تطبيقية على المكتبات المصرية . أعلم(ع٧)، الصفحات ٢٤٠-٢٦٦.
- أشرف،ا.أ. (٢٠١٤). استراتيجية أمن المعلومات (الإصدار ط١). القاهرة: مطابع الشرطة للطباعة والنشر والتوزيع.
- أصيل،غ.ع.ع و العي،آ.ع(أكتوبر- ذو الحجة, ٢٠١٤). أمن المعلومات بالجامعات السعودية : دراسة لجامعة الملك عبدالعزيز.-مجلة مكتبة الملك فهد الوطنية. ٢٠(٢)، الصفحات ٢٥٠-٢٨٩.
- الطائي،م.ع.ح. (أغسطس– رجب, ٢٠٠٥) أمن المعلومات. مجالات الاختراق وآلية التعزيز. المجلة العربية للدراسات الامنية والتدريب، ٢٠(٤٠)، الصفحات ص ص ٢٦١ -٢٨٣.
- العربى،أ.ع. (٢٠١٥). معيار المنظمة الدولية للتوحيد القياسى أيزو٢٧٠٠٢ لسياسات أمن المعلومات : دراسة وصفية تحليلية لمو اقع الجامعات العربية. مجلة جامعة طيبة للأداب والعلوم الإنسانية، ٤(٧)، الصفحات ٦٦١-٧٣٨.
- أمبابى،س. والغثبر،خ .ش.بوتوكول طبقات المنافذ الأمنة. قاموس أمن المعلومات.المملكة العربية السعودية. وزارة التعليم العالي. جامعة الملك سعود. مركز التميز لأمن المعلومات.متاح فى: https://coeia.ksu.edu.sa/ar/dictionary
- النقيب، م.م.أ. (سبتمبر, ٢٠١٠). التحديات الأمنية لمشاريع الرقمنة بمؤسسات المعلومات العربية. مجلة بحوث في علم المكتبات والمعلومات(ع٥)، الصفحات ١٠٧-١٥٧.
- حسن،ط.م.ط، والجوهرى،ع.ع.(أبريل, ٢٠٢٠). أمن المعلومات الرقمية وسبل حمايتها في ظل التشريعات الراهنة. المجلة المصرية لعلوم المعلومات، ٧(١)، الصفحات ١٦١-٢٢٢.
- حسنين،ع (ديسمبر, ٢٠١٢). أمن شبكات المعلومات الإلكترونية : المخاطر والحلول. Cybrarian journa(٣)، الصفحات ٧٤-١٠١.
- حمودة،ب. (٢٠١٤).سياسة أمن المعلومات فى شبكة المكتبات بجامعة النيلين: دراسة حالة. المجلة العربيةالدولية للمعلوماتية، ٣(٥)، الصفحات ٥٥ -٦٢.
- خدمة مكافحة هجمات حجب الخدمة (Anti-DDoS). (١٤ ,١ ٢٠٢٢). خدمة مكافحة هجمات حجب الخدمة (Anti-DDoS). تم الاسترداد من umniah: https://www.umniah.com/ar/business.
- زايد،محمد. (٢٠٠٦). الجريمة و القرصنة في مجال المعلوماتيةو الشبكات. المجلة العربية العلمية للفتيان، ١٠(١٩)، الصفحات ٧٣-٨٤.
- زيدان،ع.ع.ط (أكتوبر- ديسمبر,٢٠١٨). الثغرات الأمنية في مو اقع الويب: دراسة تطبيقية على مو اقع أقسام المكتبات والمعلومات المصرية. .لمجلةالدولية لعلوم المكتبات والمعلومات، ٥(٤).
- كوبى،ف،وخالد،ع . (٣١ ديسمبر/كانون الأول, ٢٠١٧). سياسة أمن المعلومات في المكتبات و مراكز المعلومات : دراسة حالة. المجلة الأردنية للمكتبات والمعلومات، ٥٢(٤)، الصفحات ٥٩-٨٦.

○ يس،ن. (مارس, ٢٠١٥). أمن وخصوصية البيانات بالحوسبة السحابية :قضايا وتحديات جديدة للمكتبات. مجلة بحوث في علم المكتبات والمعلومات(١٤)، الصفحات ٢٧٥-٢٩٧.

المصادر الأجنبية

○ Abdulrahman , S. A., & Alhayani, B. (2021). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics Materials Today. Proceedings, 47(19).

○ Amini, M., Vakilimofrad , H., & Saber, M. K. (2021). Human factors affecting information security in libraries. The Bottom Line, 34(1), pp. 45-67.

○ Attacks. (2021, 8 12). Retrieved from Cybersecurity Glossary. NICCS. the Cybersecurity and Infrastructure Security Agency: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

○ Bacudio, A. G., & Ect. (2011, November). AN OVERVIEW OF PENETRATION TESTING. International Journal of Network Security & Its Applications (IJNSA), 3(6), pp. 19-38.

○ BasuMallick, C. (2021, September 2). Top 10 Firewall Hardware Devices in 2021. Retrieved 1 7, 2022, from Network Security: https://www.toolbox.com/it-security/network-security/articles/top-10-firewall-hardware-devices.

○ Best Practice: Use of Web Application Firewalls. OWASP Papers Program. (n.d.). Retrieved 12 22, 2021, from owasp: https://owasp.org/www-pdf-archive/BestPractices_Guide_WAF_v104.en.pdf.

○ Canal, D., Balzarott, D., & Francil, A. (May 2013). The Role of Web Hosting Providers in Detecting Compromised Websites. WWW '13 Proceedings of the 22nd international conference on WorldWide Web, (pp. 177-188). Rio de Janeiro, Brazil.

○ Chapman , C. (2016). Introduction to practical security and performance testing. Retrieved 1 4, 2022, from Network Performance and Security:t esting and Analyzing Using Open Source and Low-Cost Tools: https://www.sciencedirect.com/science/article/pii/B9780128035849000019

○ Cekerevac , Z., & ect. (2018). Hacking, protection and the consequences of hacking. C O M M U N I C A T I O N S, 20(2).

○ centre, N. c. (2020). cyber security Response and Recovery:How to prepare for a cyber incident from response through to recovery ,Small Business Guide Collection. Retrieved 1 8, 2022, from https://www.ncsc.gov.uk/search?q=National%20cyber%20security%20centre.%20cyber%20security%20Response%20and%20Recovery.

- CWE the Common Weakness Enumeration.CWE List Version 4.6. (2021). Retrieved 1 12, 2022, from cwe: http://cwe.mitre.org/data/index.htm.
- cybercrime. (2021, 4 11). Retrieved from Britannica Encyclopedia: https://08107zk4k-1103-y-https-academic-ebcom.mplbci.ekb.eg/levels/collegiate/search/articles?query=cybercrime.
- Cybersecurity (2021, 8 12). Retrieved from Cybersecurity Glossary. NICCS. the Cybersecurity and Infrastructure Security Agency: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.
- Farhaoui, y.(2016.).How to secure web servers by the intrusion prevention system (IPS)? International Journal of Advanced Computer Research, 6(23), pp. 65-71.
- Gotseva, D., Georgiev , I., & Gancheva, V. (2011). DATABASE BACKUP STRATEGIES AND RECOVERY MODELS. Challenges in Higher Education & Researchat, 9, pp. 147-150.
- Hacking.(2021,411). Retrieved from cambridge dictionary :https :// dictionary. cambridge. Org /dictionary/ english/hacker.
- Hacker. (2021, 9 3). Retrieved from Cybersecurity Glossary. NICCS the Cybersecurity and Infrastructure Security: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.
- Hayajneh, Thaier.(2013) Performance and Information Security Evaluation with Firewalls. International Journal of Security and Its Applications. Vol.7, No.6), pp.355-372
- information security. (2021, 8 12). Retrieved from Cybersecurity Glossary. NICCS. the Cybersecurity and Infrastructure Security Agency: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.
- INTERPOL report shows alarming rate of cyberattacks during COVID-19. (2020, August 4). Retrieved from interpol: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.
- Jastra, i. (2020, September 13.). Spam Messages Make 55 % of Global E-mail Traffic in 2019. Retrieved 11 19, 2021, from https://www.precisesecurity.com/articles/spam-messages-make-55-of-global-e-mail-traffic-in-2019.
- Jastra, i. (2020, May 27). WannaCry Virus Was the Most Common Crypto Ransomware Attack in 2019. Retrieved from precisesecurity: https://www.precisesecurity.com/articles/wannacry-virus-was-the-most-common-crypto-ransomware-attack-in-2019.

- Johnson, J. (2021 , Jan 25). Cumulative detections of newly-developed malware applications worldwide from 2015 to March 2020 (in millions). Retrieved 7 6, 2021, from https://www.statista.com/statistics/680953/global-malware-volume.
- Joseph J. (2021, Apr 13). Annual number of malware attacks worldwide from 2015 to 2020. Retrieved 7 15, 2021, from statista.: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide..
- Joseph J. (2021, Feb 27). Number of unique phishing sites detected worldwide from 3rd quarter 2013 to 2nd quarter 2020. Retrieved 7 2021, 5, from https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide.
- Kaur, T. (2009). Disaster planning In University Libraries In India; A Neglected Area. New Library world, 110(4/3,), pp. 175- 187.
- Khraisat, A., & ect. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 20(2), pp. 2-22.
- Kumara , R. P., Rajb, H., & Jelcianac , P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Computer Science, 125, pp. 691–697.
- Kuzma, J. (2010). European digital libraries: web security vulnerabilities. library Hi Tech, 28(3), pp. 402-413.
- Library Computer And Network Security; Library Security.Principles; Creating A Security policy.(2010).Retrieved 8 12, 2021, from esin.bsloan: http://www.u/esin.bsloan/guid/www.infopeople.org.
- Massis, B. (2017).VPNs in the library.Information and Learning Science, 118 No(11/12), pp. 672-674.
- Mazmanian , A. (2016, Jul 18).Library of Congress wracked by DNS attack.Retrieved 8 17, 2021, from fcw: https://fcw.com/portals/security.aspx.
- MD: 600 Anne Arundel County library computers affected by "Emotet" virus. (2018, October 7).Retrieved 8 13, 2021, from DataBreaches.net: https://www.databreaches.net/md-600-anne-arundel-county-library-computers-affected-by-emotet-virus.
- Molnar, D. S. (2010, jun). Self Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud. WEIS, 1.
- Munjal, M. N. (2014, March). ETHICAL HACKING: AN IMPACT ON SOCIETY. Cyber Times International Journal of Technology & Management, 7(1), pp. 922-931

- Network Management and Monitoring System. (2021, 12 4). Retrieved from cisco: https://www.cisco.com/c/ar_ae/solutions/automation/what-is-network-monitoring.htm.
- Next-generation Firewalls (NGFW). (2021, 12 27). Retrieved from .javatpoin: https://www.javatpoint.com/types-of-firewall.
- O'Brien , P. (2018). Protecting privacy on the web A study of HTTPS and Google Analytics implementation in academic library websites. Information Review, 42(6), pp. 734-751.
- Password policy recommendations. (2021, 10 6). Retrieved 12 8, 2021, from microsoft: https://docs.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations?view=o365-worldwide.
- Pena, L. (2020, January Sunday 5). 26 community libraries in Contra Costa County compromised by a ransomware attack. Retrieved from abc7news: https://abc7news.com.
- penetration. (2021, 8 12). Retrieved from Cybersecurity Glossary. NICCS. the Cybersecurity and Infrastructure Security Agency: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary
- phoenixnap. Secure Server Connectivity. 21 Server Security Tips to Secure Your Server. (2019, April 20). Retrieved 7 15, 2021, from phoenixnap: httpshttps://phoenixnap.com/kb/category/security.
- piracy. (2021, 4 11). Retrieved from dictionary.cambridge: https://dictionary.cambridge.org/dictionary/english/piracy.
- Price, G. (2021, 4 18). National Library of Brazil (Biblioteca Nacional do Brasil) Hit with Ransomware Attack. Retrieved 8 13, 2021, from DataBreaches.net. The Office of Inadequate Security.: : https://www.infodocket.com/2021/04/18/report-national-library-of-brazil-biblioteca-naciona.
- Reshmi , T. (2021). Information security breaches due to ransomware attacks - a systematic literature review. International Journal of Information Management Data Insights, 1, pp. 1-10.
- Robertson, R. (2019, 5 21). Cyber attack on Sunderland City Council database: Investigation after library users' personal data accessed by hackers. Sunderland echo. Retrieved 8 16, 2021, from sunderlandecho: https://www.sunderlandecho.com/news/politics/council/cyber-attack-sunderland-city-council-database-investigation-after-library-users-personal-data-accessed-hackers-117103.

- Rubenking, N. J. (2022, 1 16). The Best Antivirus Protection for 2022. Retrieved 1 16, 22, from pcmag: https://www.pcmag.com/picks/the-best-antivirus-protectio.
- SMITH, F. A. (2017, JANUARY/FEBRUARy). Should Libraries Even Consider Hacking Back If Attacked? COMPUTERS IN LIBRARIES., 14-17.
- Steve, M. (2020, Nov 13). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine.
- Sun , P. ((2020) , april). Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Compute Applications, 160.
- Timberg, C. a. (2016, December 14). Yahoo says 1 billion user accounts were hacked. Retrieved 8 13, 2021, from washingtonpost: https//www.washingtonpost.com/business/economy/yahoo-says-1-billion-user-accounts-hacked/2016/12/14/a301a7d8-b986-4281-9b13-1561231417c0..
- Vavousis, K., & ect. (2020). Compliant and secure websites for the Greek Libraries Network of the National Library of Greece and each library-member of this Network in consideration of internet security and GDPR. Qualitative and Quantitative Methods in Libraries(QQML), 9(3), pp. 377-396.
- Weidman, G. (2014). Penetration testing : a hands-on introduction to hacking. San Francisco: William Pollock.
- what-is-cloudflare. (2021, 3 17). Retrieved 11 4, 2021, from cloudflare: https://www.cloudflare.com/what-is-cloudflare.
- What are the most secure Programming languages. (2022, 1 12). Retrieved from whitesourcesoftwares:https://www.whitesourcesoftware.com/most-secure-programming-languages.
- Why Human Error is #1 Cyber Security Threat to Businesses in 2021. (2021, February 4). Retrieved 7 14, 2021, from The Hacker News: https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html accessed on (14-7-2021).
- Zaveri, M. (2020, Jan 6). Government Website Is Hacked With Pro-Iran Messages. Retrieved from THE NEW YORK TIMES: https://www.nytimes.com/section/u.
- Zhao, Y., & Lu, N. (may2018). Research and Implementation of Data Storage Backup. IEEE International Conference on Energy Internet (ICEI), (pp. 21-25).

[1] the Common Weakness Enumeration (CWE): هو نظام لحصر نقاط الضعف بالبرامج والأجهزة صادر قاعدة البيانات الوطنية للثغرات الأمنية التابعة للأمن الوطنى الأمريكى National Cyber Security وقد تم تطويره من خلال مشروع مجتمعى ليصبح لغة معيارية مشتركة لإيجاد العيوب وتحديد الثغرات

الأمنية للبرامج والتعامل معها كما هي موجودة في الكود أو التصميم أو بنية النظام و انشاء أدوات لإصلاحها ومنعها وقياس الأدوات الأمنية. لمناقشة و .تمثل كل مفردة CWE نوعًا واحدًا من الثغرات الأمنية

[٢] هى شبكة إنترنت أمريكية عالمية تستهدف زيادة سرعة مو اقع الويب وحمايتها وتأمينها عبر شبكة ضخمة من الخوادم موزعة على ٢٥٠ مدينة في أكثر من ١٠٠ دولة بجميع انحاء العالم، وتوفر مميزات تأمين مو اقع الويب الخاصة بك وواجهات برمجة التطبيقات وتطبيقات الإنترنت وحماية الشبكات والموظفين والأجهزة خلف جدار الحماية داخل المؤسسة (what-is-cloudflare, 2021)

[3] هى خدمة تعمل على الحماية من الهجمات الموزعة لحجب الخدمات "DDoS" من خلال رصد حركة المرور على الإنترنت، وتحديد وجود هجمات موجهة تستهدف المؤسسة وتقوم الخدمة بإعادة توجيه حركة المرور المشبوهة إلى مركز تنقية حركة البيانات لوقف الهجمات، وفي ذات الوقت يتم إرسال حركة المرور الطبيعية إلى شبكة مؤسستك دون انقطاع في البيانات أو تأخير، وبالتالي تبقى شبكتك متاحة ومستقرة بالكامل ((Anti-DDoS، ٢٠٢٢)