الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

National Agency for Network Services
Information Security Center

الرقم: ١/٢٠١٤
التاريخ: ٢٠١٤/١/٧

التقرير السنوي الإحصائي
الخاص باختبارات أمن المواقع الإلكترونية الحكومية
لعام ٢٠١٣

GOVERNMENTAL WEBSITE SECURITY STATISTICS REPORT 2013

لمحة عن مركز أمن المعلومات:

مركز أمن المعلومات هو مركز جديد من نوعه في الجمهورية العربية السورية، قامت الهيئة الوطنية لخدمات الشبكة التابعة لوزارة الاتصالات والتقانة بإحداثه في منتصف العام ٢٠١١ م، بهدف تحسين معايير وممارسات أمن المعلومات وحماية البنية التحتية لتقنية المعلومات والاتصالات من تهديدات الجرائم الأمنية على شبكة الإنترنت، وبناء ثقافة آمنة ومحمية من جرائم تقنية المعلومات، وتعزيز الوعي حول أمن المعلومات على مستوى القطر.

يُعنى المركز عموماً بتحديد المواصفات والمعايير الخاصة بأمن وحماية الشبكات ومواقع الإنترنت، والإشراف على حسن الالتزام بها، ووضع المعايير الخاصة بمواجهة حالات الطوارئ على الإنترنت وغيرها من الشبكات الحاسوبية ونظم المعلومات، والإشراف على حسن الالتزام بها. كما يقوم المركز بحكم طابعه الوطني بدور المستجيب الأول لحوادث أمن المعلومات والمسؤول عن إرشاد الجهات الحكومية المختلفة في كيفية حماية نظمها وشبكاتها المعلوماتية قبل وبعد حدوث أي جريمة أو حادثة أمنية إلكترونية. يعمل المركز على تأمين الخدمات المختلفة في المجالات الرئيسية التالية:

المركز عضو في فريق منظمة التعاون الإسلامي للاستجابة لطوارئ الحاسوب OIC-CERT

أنشطة وخدمات المركز:

يقوم المركز بوضع وتحديد السياسيات والنواظم والمعايير لضمان تحقيق أمن المعلومات والإشراف على تحقيقها وفق آلية محددة تساعد جميع الجهات الحكومية في القطر على تنفيذها. يعمل المركز حالياً على تقدم الخدمات والأنشطة التالية بشكل مجاني:

(١). اكتشاف الثغرات الأمنية في المواقع الإلكترونية الحكومية

- تهدف هذه الخدمة إلى مساعدة الجهات الحكومية السورية – فقط – في تجنب أية تهديدات أو اختراقات مستقبلية قد تتعرض لها مواقعها الإلكترونية من خلال إجراء اختبارات أمنية أولية لهذه المواقع باستخدام برمجيات مفتوحة المصدر وعبر فريق تقني مختص. يتم خلال الاختبار الأمني اكتشاف نقاط الضعف والثغرات الأمنية والبرمجية الواضحة والمحتملة في لغات البرمجة ونظام التشغيل الخاص بمخدّمات الاستضافة وبرمجيات إدارة الموقع وقاعدة المعطيات، ومن ثم تقييم خطورتها، ووضع التوصيات والحلول المقترحة لمعالجة هذه الثغرات.

(٢). تحليل البرمجيات الخبيثة (فيروسات – ديدان – تروجان)

- خدمة مجانية مخصصة للأفراد والجهات الحكومية والمؤسسات الخاصة، تعتمد على اكتشاف الملفات الخبيثة الجديدة في الفضاء السيبراني بواسطة مجموعة من البرمجيات والتجهيزات المخصصة لهذا الغرض، والتي يتم إرسالها إلى المركز للتحليل، وذلك بهدف التحذير من الأخطار الأمنية المرافقة لهذه الملفات الخبيثة المكتشفة والتقليل من أضرارها ما أمكن من خلال إصدار تقرير تحليلي يتضمن آثار هذه الملفات المؤذية وسلوكها وآلية عملها وكيفية إزالتها وإصدار التوصيات بشأن الإجراءات المضادة وطرق الاستجابة لمعالجة التهديدات المرافقة لهذه الملفات.

(٣). التنبيهات والتحذيرات الأمنية المعلوماتية

- يعمل المركز على توفير خدمة التنبيهات والتحذيرات الأمنية ضد المخاطر والتهديدات الإلكترونية التي قد تشكل ضرراً على الشبكات والنظم. تشمل التحذيرات والتهديدات الأمنية على تفضيل للمخاطر والأضرار الناجمة عنها إضافةً إلى الحلول التي يمكن أن تمنع التعرض لهذه الهجمات والتهديدات. ويعمل المركز على إرسال هذه التنبيهات والتحذيرات إلى جميع الجهات الحكومية عبر القوائم البريدية الإلكترونية الموجودة لديه.

(٤). الاستجابة للحوادث الأمنية المعلوماتية

- بحكم الطابع الوطني للمركز فإنه يتعامل مع العديد من الحوادث الأمنية المعلوماتية التي تستهدف وتتعرض لها الجهات الحكومية في القطر فقط، وبشكل مجاني. تهدف هذه الخدمة إلى تأمين الاستجابة الفورية لحوادث أمن المعلومات وتقديم الدعم الفني للجهات الحكومية في حال طلب المساعدة في الحالات التالية:
  - (١). اختراق الموقع الإلكتروني للجهة الحكومية.
  - (٢). محاولات الاختراق إلى النظام أو البيانات.
  - (٣). نشر البيانات والمعلومات الخاصة بالجهات دون تصريح من الجهة صاحبة الحق في النشر.

إنجازات المركز:

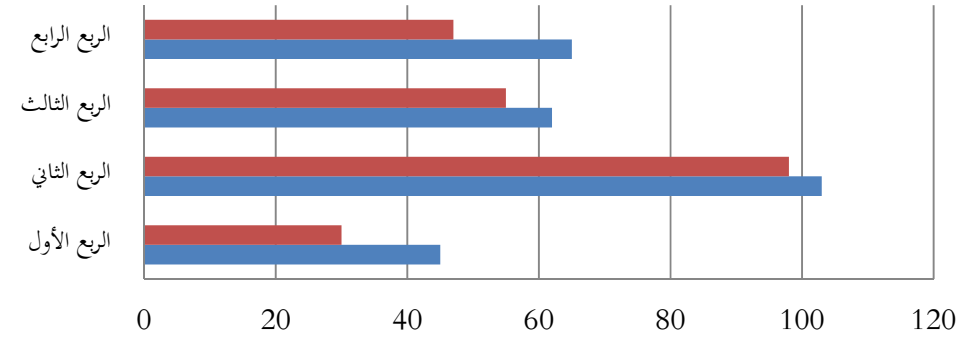
فيما يلي أهم ما تم إنجازه في هذا المركز خلال عام ٢٠١٣ م:

(١). في مجال اكتشاف الثغرات الأمنية في المواقع الإلكترونية الحكومية:

تم في العام ٢٠١٣ م **اكتشاف** (٩٠٠) **ثغرة أمنية** – أغلبها في نطاق التطبيقات ونظم التشغيل – من خلال إجراء الاختبار الأمني لـ (٢٧٥) **موقعاً إلكترونياً** حكومياً، كما تم إرسال (٢٣٠) تقريراً إلى الجهات الحكومية المعنية مع توصيات تفصيلية بكيفية سد الثغرات الأمنية المكتشفة.

يوضح الشكل التالي إحصائية بعدد المواقع الإلكترونية التي تم اختبارها في العام ٢٠١٣ م:

الشكل (١): عدد المواقع الإلكترونية الحكومية التي تم اختبارها



	الربع الأول	الربع الثاني	الربع الثالث	الربع الرابع
عدد التقارير المرسلة	30	98	55	47
عدد المواقع التي تم اختبارها	45	103	62	65

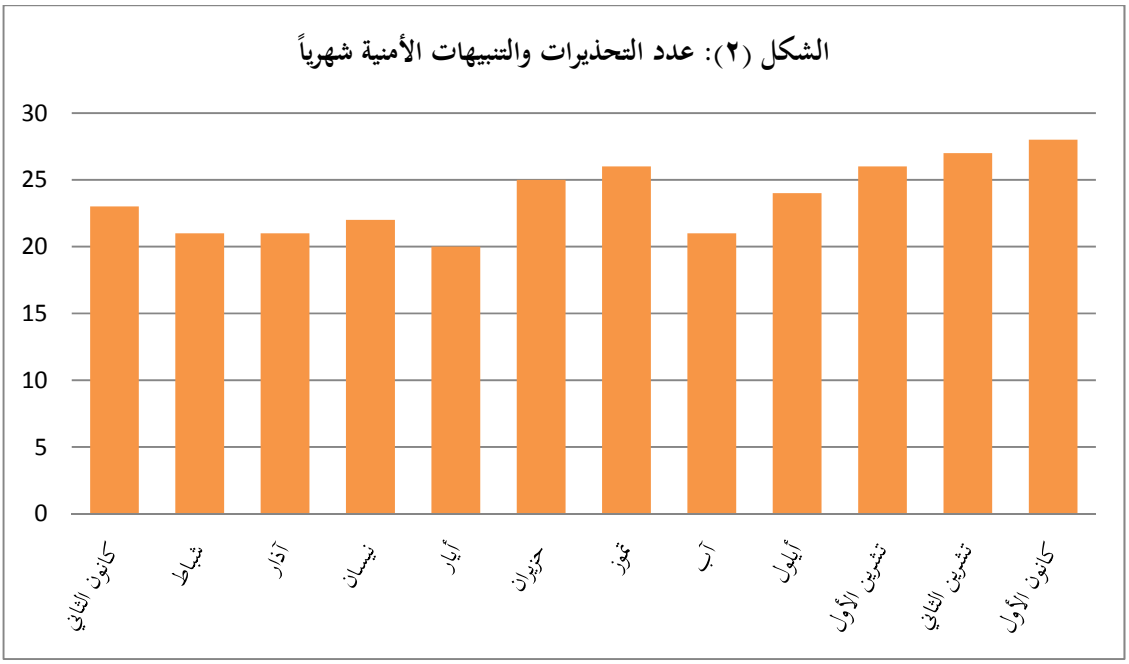
(٢). في مجال التنبيهات والتحذيرات الأمنية المعلوماتية:

تم في العام ٢٠١٣ م إحصاء (٢٨٥) تحذيراً وتنبيهاً أمنياً في مختلف نظم التشغيل والتطبيقات والبرمجيات على شكل (١٢) نشرة شهرية جرى إرسالها إلكترونياً إلى جميع الجهات الحكومية عبر القوائم البريدية الموجودة لدى المركز. بالإضافة إلى نشر هذه النشرات على الموقع الإلكتروني للهيئة الوطنية لخدمات الشبكة.

يوضح الجدول التالي إحصائية بعدد التحذيرات والتنبيهات الأمنية التي قام المركز بإرسالها خلال عام ٢٠١٣ م:

	عدد التحذيرات والتنبيهات الأمنية
الربع الأول	٦٥
الربع الثاني	٦٧
الربع الثالث	٧١
الربع الرابع	٨٢
إجمالي	٢٨٥

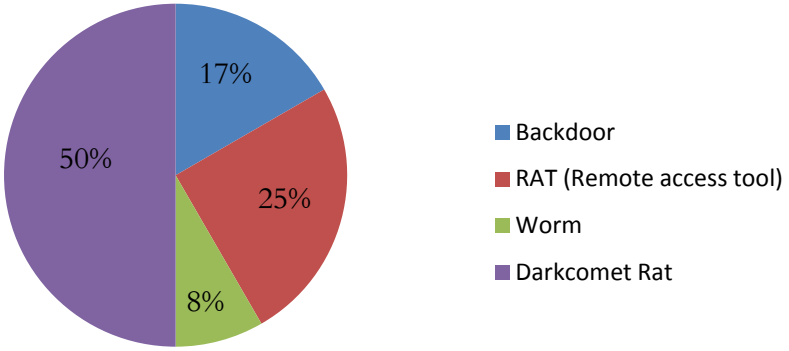
الشكل (٢): عدد التحذيرات والتنبيهات الأمنية شهرياً



(٣). في مجال تحليل البرمجيات الخبيثة:

تم في العام ٢٠١٣ م دراسة وتحليل ما يقارب (١٥) ملفاً خبيثاً تنوعت بين برمجيات تجسس وديدان شبكية وبرمجيات تحكم من بُعد، بالإضافة إلى إعداد تقارير مفصلة بنتائج التحليل. الشكل (٣) يبين النسب المئوية للبرمجيات التي تم تحليلها.

الشكل (٣): أنواع البرمجيات الخبيثة التي تم تحليلها عام ٢٠١٣



(٤). في مجال الاستجابة للحوادث الأمنية المعلوماتية:

- تم التعامل والتجاوب مع (٢٠) حادثة اختراق أمني في مختلف الجهات الحكومية خاصة بالمواقع الإلكترونية العائدة لتلك الجهات. و إعداد تقارير تقنية وبرمجية بأسباب الاختراق.
- تم التعامل والتجاوب مع حادثتي اختراق أمني داخلي في الشبكات الحاسوبية المحلية المستخدمة في جهتين حكوميتين. و إعداد تقارير تقنية وبرمجية بأسباب الاختراق.

(٥). في مجالات أخرى:

- إصدار معجم (إنكليزي – عربي) خاص بمصطلحات أمن المعلومات والاتصالات.
- المساهمة في إعداد مجموعة النواظم والمعايير التقنية اللازمة لتطبيق أحكام المواد (٢-٣) من قانون " تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية " الصادر بالمرسوم التشريعي رقم /١٧/ لعام ٢٠١٢ على شكل ثلاث لوائح تنظيمية هي:

(١). النواظم والمعايير التقنية لمقدمي خدمات الاستضافة على الشبكة.

(٢). النواظم والمعايير التقنية لمقدمي خدمات النفاذ على الشبكة.

(٣). النواظم والمعايير التقنية لمقدمي خدمات التواصل على الشبكة.

التقرير الإحصائي البياني الخاص باختبارات أمن المواقع الإلكترونية الحكومية

المقدمة

يعمل مركز أمن المعلومات في الهيئة الوطنية لخدمات الشبكة، وفق قانون التوقيع الرقمي وخدمات الشبكة رقم /٤/ لعام ٢٠٠٩ م، على وضع المواصفات والمعايير الخاصة بأمن وحماية الشبكات ونظم المعلومات ومواقع الإنترنت، ووضع المعايير الخاصة بمواجهة حالات الطوارئ على الانترنت وغيرها من الشبكات المعلوماتية والحاسوبية، إضافة إلى إجراء الأبحاث الأمنية وتقييم المخاطر على النظم المعلوماتية، وبناء الخبرة في مجال المعلوماتية الشرعية، ونشر ثقافة أمن المعلومات بشكل عام.

ولقد عمل المركز منذ تأسيسه في منتصف العام ٢٠١١ م على تعزيز مستوى أمن وسلامة النظم المعلوماتية لدى الجهات الحكومية، وكان أحد أبرز نشاطاته في هذا المجال إجراء الاختبار الأمني الخارجي الدوري للمواقع الالكترونية الحكومية بشكل مجاني وباستخدام برمجيات مفتوحة المصدر، وإعداد تقارير شاملة بثغراتها الأمنية وطرق حلها ومعالجتها تفادياً لأية تهديدات أمنية أو اختراقات قد تتعرض لها هذه المواقع مستقبلاً. وكنتيجة لهذا الإجراء تم إعداد هذا التقرير الموجز الذي يقدم معلومات إحصائية تقريبية عن مدى انتشار الثغرات الأمنية في المواقع الالكترونية الحكومية ومستوى تأثيرها، وأكثرها خطورة.

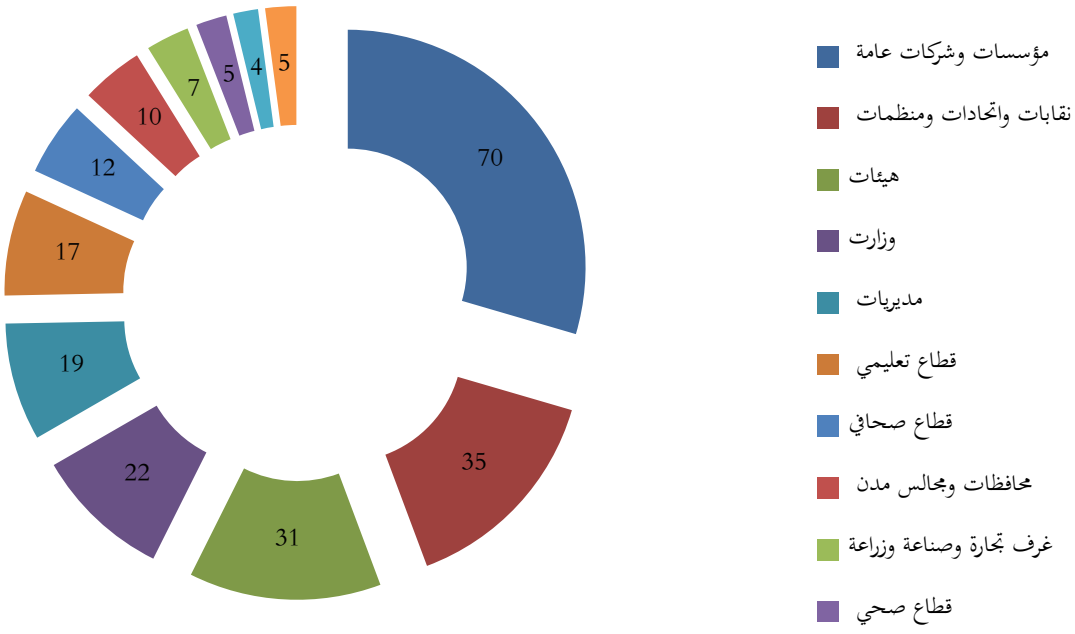
الدراسة الإحصائية:

(١). معطيات الدراسة:

تم الاعتماد أثناء إعداد هذا التقرير على المعطيات التالية:

- نتائج الاختبار الأمني لـ (٢٧٥) موقعاً الكترونياً خلال عام ٢٠١٣ م، والذي شمل مختلف الجهات الحكومية من وزارات وهيئات ومؤسسات وشركات ومديريات ونقابات واتحادات وغرف مهنية ومختلف القطاعات التعليمية والصحية والخدمية، والمبين نسب توزيعها في الشكل (٤).
- إجمالي الثغرات الأمنية المكتشفة أثناء الاختبار الأمني والبالغ عددها (٩٠٠) ثغرة أمنية متعددة مستويات الخطورة.

الشكل (٤): توزع الدراسة على القطاعات الحكومية

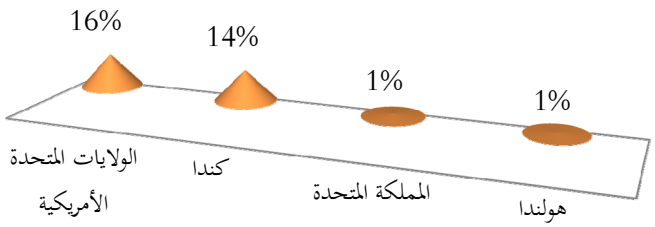


(٢). استضافة المواقع الإلكترونية الحكومية التي تم اختبارها:

(أ). مكان الاستضافة:

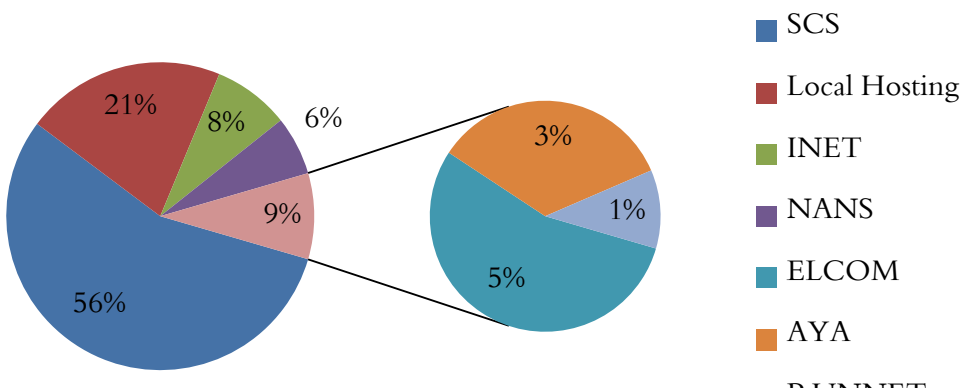
أثناء عمليات الاختبار الأمني للمواقع الإلكترونية الحكومية، لوحظ قيام (٨٨) جهة حكومية باستضافة مواقعها الإلكترونية خارج القطر، أي ما يعادل (٣٢ %) من إجمالي عدد المواقع التي تم اختبارها. هذه المواقع مستضافة في مخدّمات استضافة موزعة على أربعة دول مبين نسب توزعها في الشكل (٥).

الشكل (٥): النسب المئوية لاستضافة المواقع الإلكترونية خارج القطر – حسب الدولة



بينما تمت استضافة النسبة المتبقية (٦٨ %) من الموقع الإلكترونية المدروسة داخل القطر لدى شركات استضافة حكومية وخاصة مختلفة كما هو مبين في الشكل (٦).

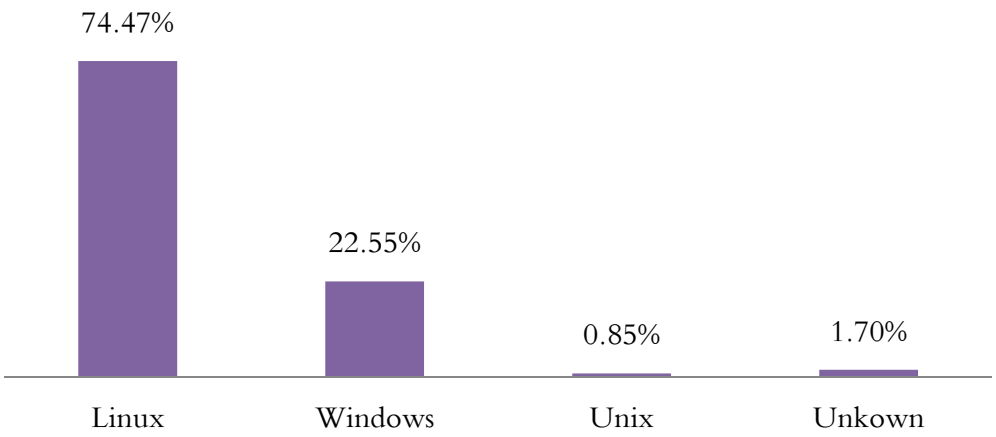
الشكل (٦): النسب المئوية لاستضافة المواقع الإلكترونية داخل القطر – حسب شركة الاستضافة



(ب). نوع نظم تشغيل مخدّمات الاستضافة:

لوحظ أن نظام التشغيل Linux هو الأكثر استخداماً على مخدّمات استضافة المواقع الإلكترونية الحكومية الموجودة داخل أو خارج القطر، بالمقارنة مع نظم التشغيل الأخرى Unix و Windows كما هو مبين في الشكل (٧).

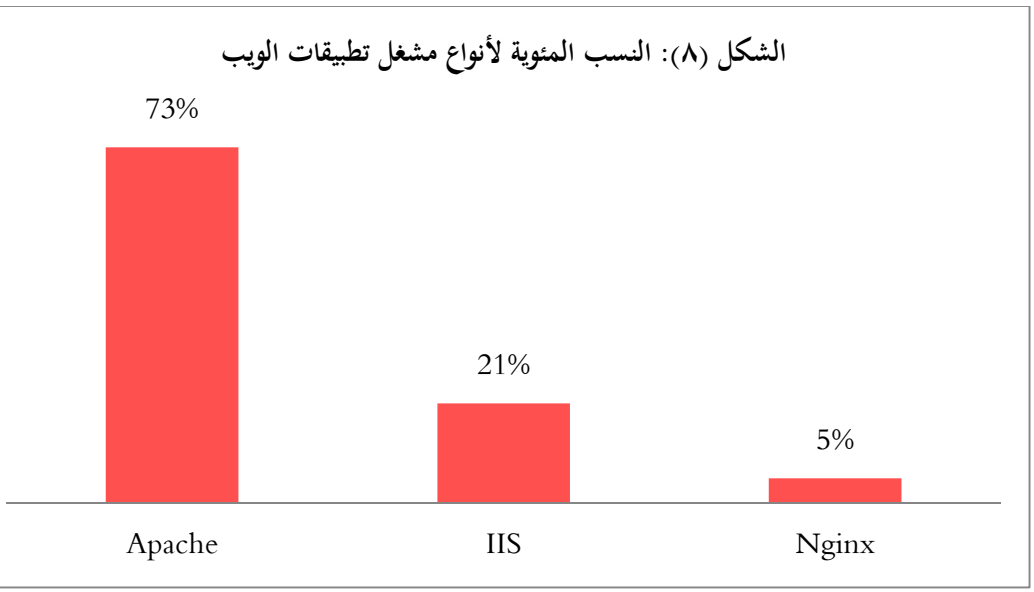
الشكل (٧): النسب المئوية لأنواع نظم تشغيل مخدمات الاستضافة



(ج). نوع مشغل تطبيق الويب المستخدم:

من الدراسة الإحصائية تبين أن مشغل Apache (مفتوح المصدر) قد استحوذ على نسبة مئوية عالية مقارنةً بالمشغلات الأخرى IIS و Nginx . كما هو مبين في الشكل (٨).

الشكل (٨): النسب المئوية لأنواع مشغل تطبيقات الويب

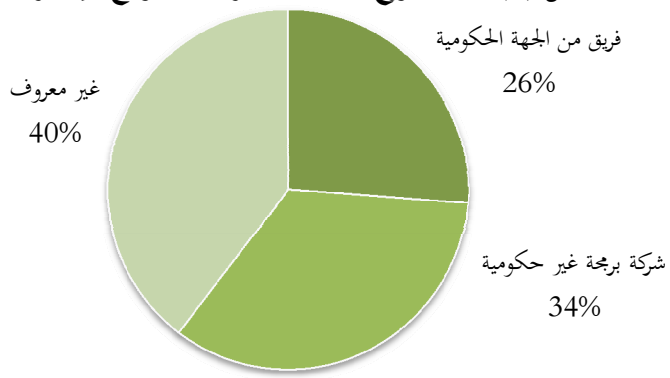


(٣). التصميم البرمجي للمواقع الإلكترونية التي تم اختبارها:

(أ). الجهة المبرمجة للموقع:

من الدراسة الإحصائية وجدنا أن (٢٦ %) من المواقع الإلكترونية التي جرى اختبارها قد تم تصميمها البرمجي بواسطة فريق فني محلي يعمل في الجهة الحكومية صاحبة الموقع الإلكتروني، و أن (٣٤ %) من المواقع قد تم تصميمها البرمجي عن طريق شركة برمجة – غير حكومية – مختصة بتطبيقات الويب كما هو مبين في الشكل (٩).

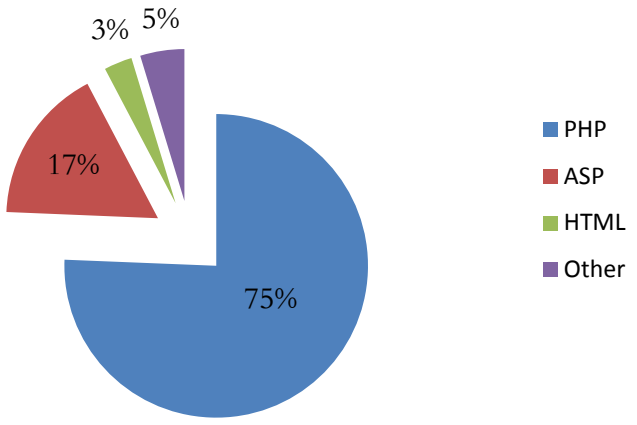
الشكل (٩): نسب توزع الجهات المبرمجة للمواقع الإلكترونية الحكومية



(ب). لغة البرمجة المستخدمة:

تبين من الدراسة أن غالبية الجهات الحكومية تستخدم لغة البرمجة عالية المستوى PHP في برمجة مواقعها الإلكترونية، ونسبة محدودة جداً من الجهات تقدر بـ (٣ %) قامت بالاعتماد على طريقة الصفحات الثابتة Static باستخدام لغة تأشير النص الترابطي HTML في إنشاء مواقعها الإلكترونية. كما هو مبين في الشكل (١٠).

الشكل (١٠): التقنيات المستخدمة في برمجة المواقع

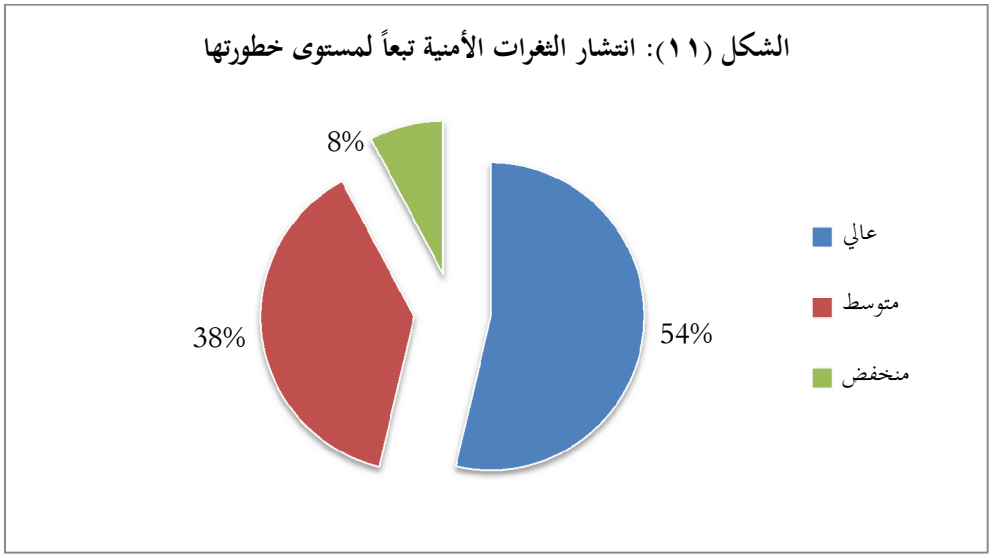


(٤). انتشار الثغرات الأمنية المكتشفة في المواقع الإلكترونية الحكومية التي تم اختيارها:

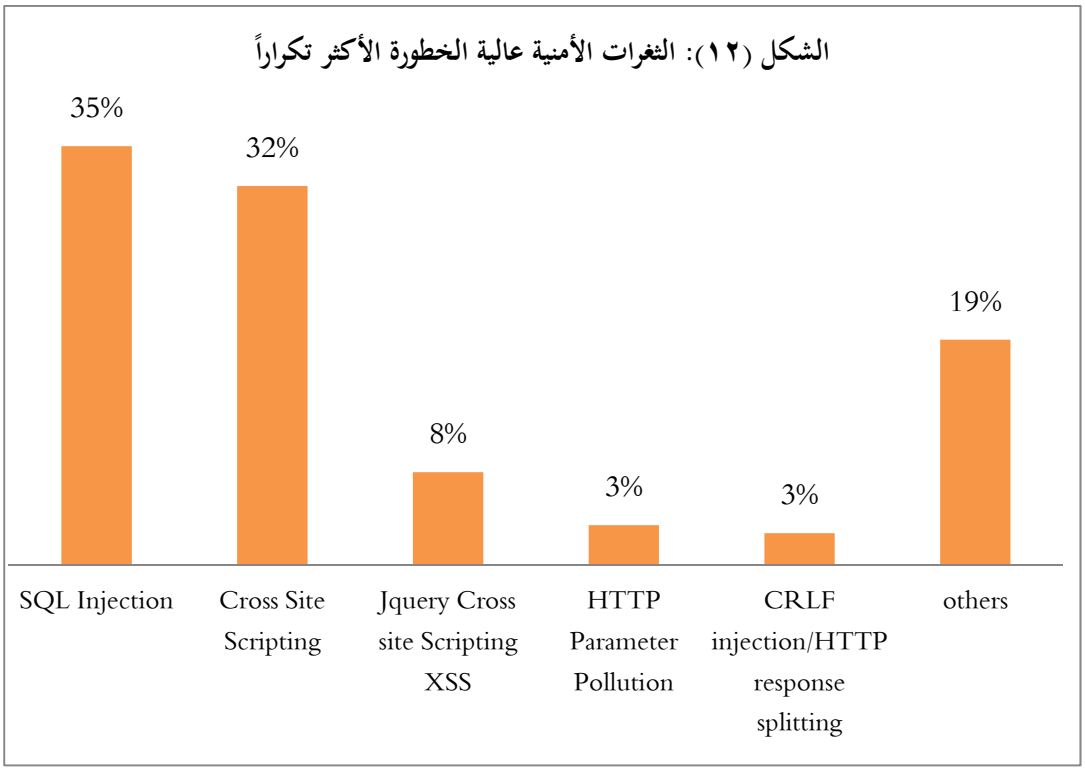
(أ). تبعاً لمستوى الخطورة:

على الرغم من وجود العديد من الثغرات ذات مستوى الخطورة المنخفض (والتي قد لا تتجاوز في بعض الحالات مجرد ثغرات تكشف معلومات قد تكون غير هامة) إلا أننا قد اخترنا في تقارير الاختبار المرسلة إلى الجهات الحكومية التركيز على الثغرات ذات المستوى العالي من الخطورة مما جعل نسبة ورودها يقدر بـ (٥٤ %) ونسبة الثغرات ذات المستوى المتوسط من الخطورة يقدر بـ (٣٨ %). كما هو مبين في الشكل (١١).

الشكل (١١): انتشار الثغرات الأمنية تبعاً لمستوى خطورتها

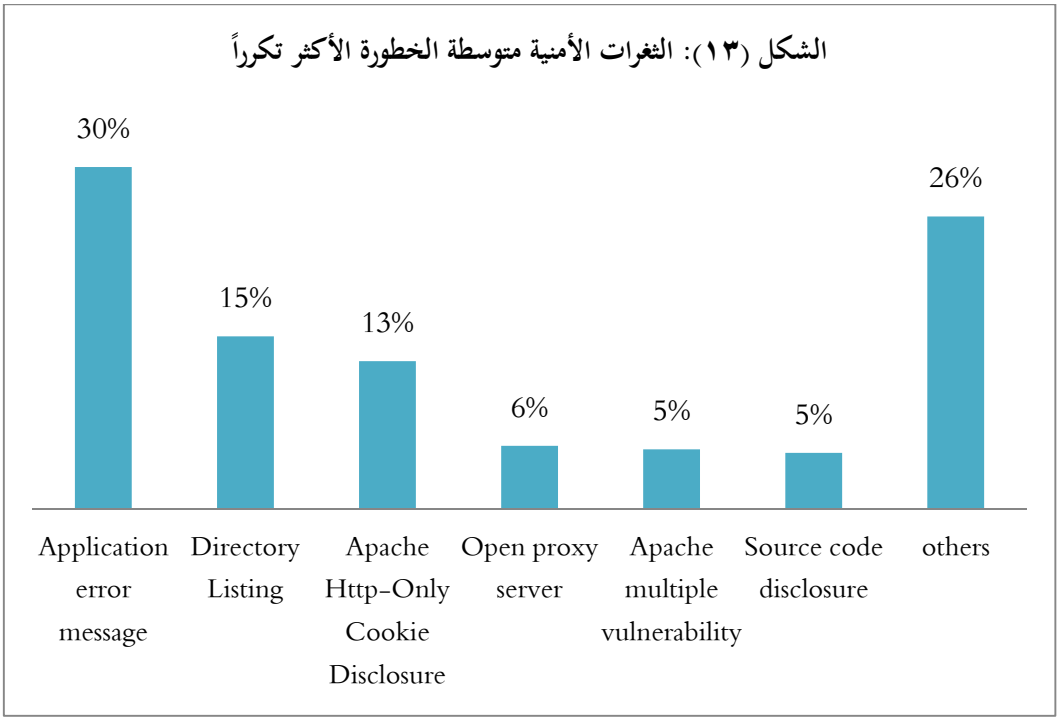


لقد تم تحديد الثغرات الأمنية الأكثر انتشاراً في المواقع الإلكترونية الحكومية والأعلى مستوى خطورة والتي تهدد أمن الموقع الالكتروني بشكل مباشر، ووجدنا أنه لا يكاد يخلو موقع الكتروني حكومي من ثغرة الحقن بلغة الاستعلام البنيوية SQL Injection والتي تكررت بنسبة (٣٥ %) من إجمالي الثغرات عالية الخطورة المكتشفة، يليها ثغرة الحقن البرمجي عبر الموقع Cross Site Scripting (XSS) والتي تكررت بنسبة (٣٢ %). كما هو مبين في الشكل (١٢).



الشكل (١٢): الثغرات الأمنية عالية الخطورة الأكثر تكراراً

أما بالنسبة للثغرات الأمنية المتوسطة الخطورة المكتشفة أثناء الاختبارات فقد تبين أن ثغرة رسالة الخطأ البرمجي Application Error Message هي الأكثر تكراراً بنسبة (٣٠ %). كما هو مبين في الشكل (١٣).

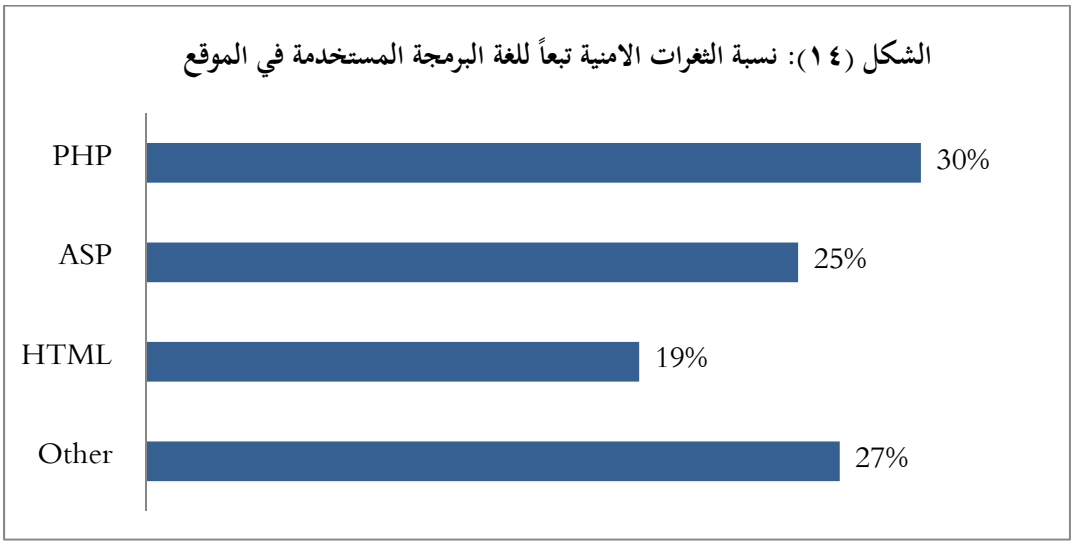


الشكل (١٣): الثغرات الأمنية متوسطة الخطورة الأكثر تكرراً

(ب). تبعاً للغة البرمجة المستخدمة:

إن النسبة العظمى من الثغرات الأمنية المكتشفة تتصل بشكل مباشر بلغة البرمجة PHP، أي أن إجراء تعديلات برمجية على البنية البرمجية للموقع باستخدام هذه اللغة كفيل بسدّ الثغرة الأمنية وإلغاء تأثيرها. الشكل (١٤) يبين مدى انتشار الثغرات الأمنية بالاعتماد على لغة البرمجة المستخدمة.

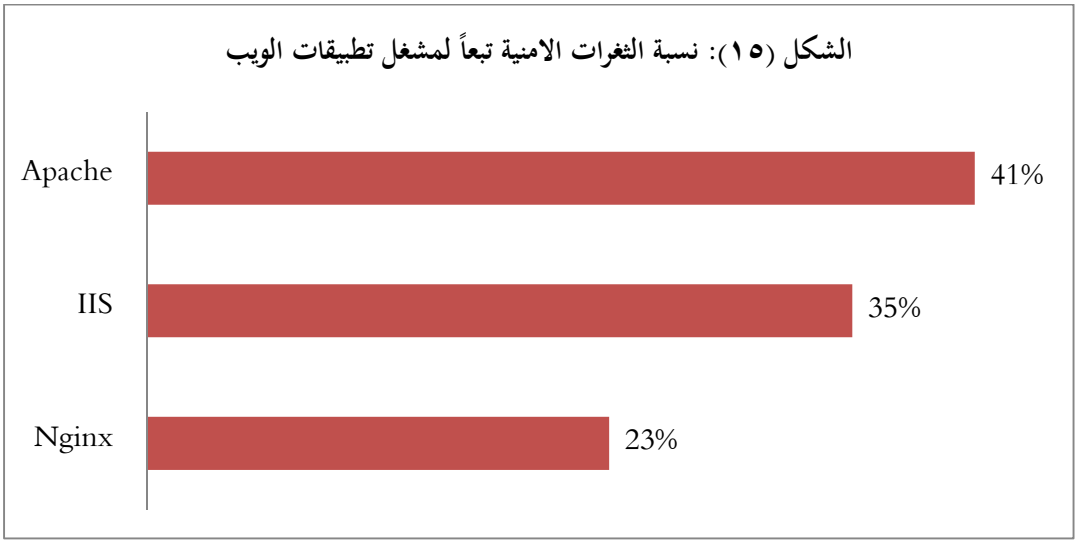
الشكل (١٤): نسبة الثغرات الامنية تبعاً للغة البرمجة المستخدمة في الموقع



(ج). تبعاً لمشغل تطبيقات الويب المستخدم:

إن النسبة العظمى من الثغرات الأمنية المكتشفة تتصل بشكل مباشر بمشغل Apache، مما يتطلب التحديث الدوري لهذا المشغل لسدّ الثغرات الأمنية ذات الصلة به. الشكل (١٥) يبين مدى انتشار الثغرات الأمنية بالاعتماد على مشغل تطبيقات الويب المستخدم في تشغيل الموقع الإلكتروني.

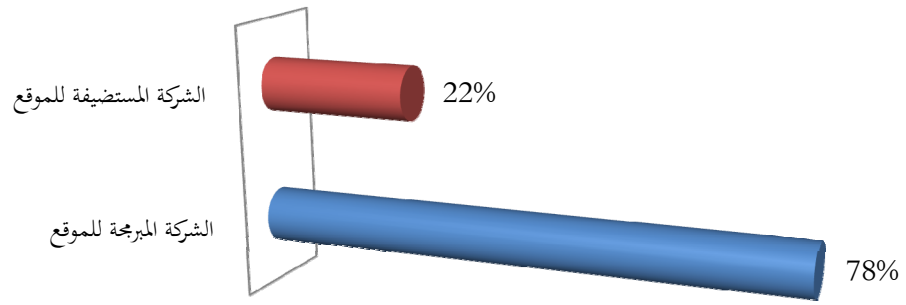
الشكل (١٥): نسبة الثغرات الامنية تبعاً لمشغل تطبيقات الويب



(٥). معالجة الثغرات الأمنية المكتشفة:

من أهم النقاط التي لا بد من الإشارة إليها هي أن غالبية الثغرات الأمنية المكتشفة وأكثرها خطورة تكون معالجتها من مسؤولية الشركة المبرمجة للموقع، في حين يقع على عاتق الشركة المستضيفة للموقع معالجة الثغرات المتعلقة بمشغل تطبيقات الويب والمخدّم المستضيف وإجراءات الترقية والتحديث بشكل دوري، بالإضافة لبعض الثغرات الأمنية التي قد يستطيع حلها أحد الطرفين. كما هو مبين في الشكل (١٦).

الشكل (١٦) :مسؤولية معالجة الثغرات الأمنية



النتائج:

من خلال ما تقدم يمكن تلخيص نقاط الضعف التي تعاني منها غالبية المواقع الإلكترونية الحكومية بالبنود التالية:

- عدم توفّر إجراءات التحقق من مدخلات المستخدم (اختبار نوع المدخل وشكله وطوله) أثناء برمجة الموقع مما يجعله عرضةً للاختراق بأسلوبي الحقن SQL Injection و XSS.
- عدم تنقيذ التحديثات الدورية لنظم تشغيل مخدّمات الاستضافة ومشغل تطبيقات الويب لتفادي الثغرات الأمنية المكتشفة حديثاً، والتي يتم الإعلان عنها في مواقع الشركات المبرمجة للنظم والمشغلات.
- الإعداد غير الصحيح للتطبيقات والبرمجيات ضمن مخدّمات الاستضافة، وعدم تحديد صلاحيات النفاذ إلى ملفات الموقع الحساسة والتي قد تؤدي إلى تسريب معلومات مهمة يمكن استغلالها في تنفيذ هجمات أخرى.
- استضافة عدد من المواقع الإلكترونية الحكومية على مخدّمات استضافة خارج القطر، مما يسبب صعوبات في متابعة إجراءات الأمان الخاصة بمخدّمات الاستضافة.
- عدم إجراء المعالجة البرمجية للثغرات الأمنية المكتشفة، والمراجعة الدقيقة للكود البرمجي المتضمن على ثغرات أمنية واضحة.

التوصيات:

- نقل استضافة المواقع الإلكترونية الحكومية إلى داخل القطر.
- المعالجة الفورية للثغرات الأمنية المكتشفة في المواقع الإلكترونية بالتعاون مع مركز أمن المعلومات.
- التنسيق المستمر بين جميع الجهات الحكومية والشركات المتعاقدة معها لتصميم وبرمجة واستضافة مواقعها الإلكترونية على تنفيذ الإجراءات الأمنية التالية دورياً:

١. الحفاظ على كلمات المرور الخاصة بمخدّم الاستضافة ونظام إدارة المحتوى وبرنامج إدارة قواعد البيانات بشكل موثوق وآمن، والعمل على تغييرها دورياً.
٢. التحديث الدوري لنظام إدارة المحتوى المستخدم ولنظام التشغيل الخاص بمخدّم الاستضافة، وتنصيب الحزم البرمجية الحاوية على ترقيعات الثغرات الأمنية المكتشفة.
٣. المراجعة الدورية لملفات النفاذ للنظام وإجراء فحص شامل ودوري لكافة الملفات الموجودة على مخدّم الاستضافة والتأكد من عدم وجود أي برامج أو ملفات خبيثة.
٤. الفحص الدوري لكافة البرامج والسكريبتات التي تعمل ضمن الموقع والتأكد من خلوها من أوامر برمجية قد تؤدي إلى إضعاف إمكانيات مخدّم الاستضافة أو التسبب في مشاكل أمنية أخرى.
٥. تنصيب برامج مضادة للفيروسات وتطبيقات حماية WAF مُرخصة بشكل نظامي على مخدّم الاستضافة.