الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

National Agency for Network Services
Information Security Center

الهيئة الوطنية لخدمات الشبكة

مركز أمن المعلومات

التقرير الإحصائي السنوي

لعام 2016

Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

قائمة المحتويات:

Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

تعريف بمركز أمن المعلومات حسب النظام الداخلي للهيئة الوطنية لخدمات الشبكة "المادة 24":

"هو الوحدة التنظيمية المسؤولة عن وضع المواصفات والمعايير وكافة الوثائق الخاصة بأمن وحماية المعلومات والشبكات بما فيها المواقع الالكترونية على الشابكة والإشراف على حُسن الالتزام بها، وإنجاز الأبحاث والاختبارات اللازمة والممكنة في إطار تأمين بيئة عمل آمنة ومناسبة، ووضع المعايير الخاصة بمواجهة حالات الطوارئ على الشبكة أو غيرها من الشبكات المعلوماتية واتخاذ ما يمكن من إجراءات وقائية وعلاجية وإدارة فرق عمل للتصدي لها".

لقد دأب مركز أمن المعلومات منذ تأسيسه على تطوير واقع أمن المعلومات على مستوى الجمهورية العربية السورية، من خلال وضع السياسات والمعايير والمواصفات الوطنية الخاصة بأمن المعلومات، وإجراء الاختبارات الأمنية للمنظومات المعلوماتية الحكومية، والعمل على نشر ثقافة أمن المعلومات والتوعية الأمنية، والاستجابة لحالات الطوارئ المعلوماتية التي تتعرض لها الشبكة والمنظومات المعلوماتية، وأدى ذلك إلى رفع سوية الأمان المعلوماتي ضد الهجمات الإلكترونية في الفضاء السيبراني وفيما يتعلق بمحاولات الاختراق بشكل ملحوظ، كما بينت الدراسات الإحصائية التي يعدها المركز سنوياً، وفيما يلي سنعرض التقرير السنوي لمجمل أعمال ونشاطات المركز خلال العام 2016.

Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

نظام خدمات مركز أمن المعلومات

مع بداية العام 2015 انتهى المركز من تجهيز المخبر الوطني لاختبار الاختراق والتحليل الجنائي للشبكات بأحدث التجهيزات والتطبيقات البرمجية المطورة من قبل شركات عالمية متخصصة بأمن المعلومات والتي تمكن المركز من تطوير الخدمات التي يقدمها كماً ونوعاً، ولاستثمار المخبر بالشكل الأمثل كان لا بد من تنظيم عملية تقديم هذه الخدمات من خلال إصدار نظام خاص بالخدمات التي يقدمها المركز، حيث يقدم هذا النظام توصيفاً دقيقاً للخدمات والجهات المستهدفة بالإضافة للأجور المترتبة للحصول عليها من قبل الجهات العامة والخاصة.

ونوجز فيما يلي الخدمات التي يقدمها المركز حسب هذا النظام:

خدمات المسح الأمني واختبار الاختراق الاحترافية:

1. خدمة المسح الأمني العادية: يقدم المركز هذه الخدمة عند الطّلب لجميع المواقع الإلكترونية العامة والخاصة، وهي مجاناً للجهات العامة ولمرة واحدة خلال العام.
2. خدمة المسح الأمني الاحترافية: يقدم المركز هذه الخدمة عند الطّلب للجهات العامة والخاصة، وتقسم إلى ثلاثة أنواع:
   أ. خدمة المسح الأمني الاحترافية للمواقع الإلكترونية ومخدمات الويب.
   ب. خدمة المسح الأمني الاحترافية للبرمجيات.
   ت. خدمة المسح الأمني الاحترافية للشّبكات.
3. خدمة اختبار الاختراق الاحترافية: تتضمن خدمة المسح الأمني الاحترافية السّابقة، ويضاف إليها اختبار اختراق منظومة العميل بطرق تحاكي هجوم حقيقي بالتنسيق مع الجهة صاحبة المنظومة.

خدمات الاستجابة للطوارئ المعلوماتية CERT:

1. استعادة بيانات أو معلومات مفقودة Data Recovery.
2. التعامل الفوري مع الحوادث المعلوماتية Incident Handling.
3. استخراج الدليل الرقمي لجريمة معلوماتية أو تقليدية Computer Forensics.

Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

نشاطات المركز خلال عام 2016

المسح الأمني للمواقع الإلكترونية والشبكات والمنظومات المعلوماتية الحكومية:

قام المركز خلال عام 2016 باختبار 150 موقعاً حكومياً وتم إعداد تقارير المسح الأمني لـ 46 موقعاً وإرسالها الى الجهات الحكومية صاحبة المواقع لتتم معالجة الثغرات المكتشفة. وتم مخاطبة جميع الجهات التي أرسلت لها تقارير المسح لعرض الخدمات الاحترافية التي يقدمها المركز، بلغ عدد المواقع التي تمت محاولة مسحها ولم نتمكن من ذلك حوالي 70 موقعاً، وذلك لكون عدد من هذه المواقع خارج الخدمة متوقف عن العمل أو بسبب استخدام الجهات المضيفة للمواقع تجهيزات حماية خاصة بتطبيقات الويب مثل WAF، والذي يوقف عمليات المسح الأمني، علماً بأن معظم هذه المواقع مستضاف لدى الجمعية السورية للمعلوماتية والتي تمت مخاطبتها والاتصال بها عدة مرات للسماح بعمليات المسح دون جدوى حتى تاريخ إعداد التقرير.

التوعية الأمنية:

في إطار التحذير المبكر من الأخطار المعلوماتية على الشبكة ونشر ثقافة أمن المعلومات في القطر قام المركز بتنفيذ مجموعة من النشاطات:

- إصدار نشرة التنبيهات الدورية الشهرية التي تتضمن أحدث الثغرات المكتشفة في أنظمة التشغيل والتطبيقات البرمجية بالإضافة إلى أخطر البرمجيات الخبيثة.
- تقديم استشارات أمنية للجهات العامة حول معالجة الثغرات الأمنية وقضايا تتعلق بأمن المعلومات بشكل عام.
- المشاركة في ورشات عمل في مجالات أمن المعلومات المختلفة.
- العمل على تطوير موقع إلكتروني خاص بالمركز سيتم استخدامه لنشر التوعية الأمنية والاستجابة لحالات الطوارئ على الشبكة والتعريف بخدمات المركز.

Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

الاستجابة للطوارئ المعلوماتية:

نظراً لاضطلاع المركز بالتصدي لحالات الطوارئ المعلوماتية على الشبكة، برزت الحاجة لاستخدام برمجيات وتجهيزات احترافية يعتمد عليها فريق الاستجابة للطوارئ المعلوماتية، لذلك أعد المركز دفتر شروط خاص باستكمال تجهيز المخبر الوطني لاختبار الاختراق والتحليل الجنائي للشبكات، إلا أن المركز لكم يتمن من تأمين هذه التجهيزات والبرمجيات بعد، ولذلك يعتمد فريق الاستجابة حالياً في عمله على برمجيات غير مرخصة تعمل ضمن فترة تجريبية مؤقتة أو مفتوحة المصدر، وهي غير كافية وذات أداء محدود.

وقد استجاب فريق الطوارئ المعلوماتية في مركز أمن المعلومات خلال العام 2016 إلى /15/ حالة طارئة في الجهات الحكومية تتعلق بحالات اختراق وإصابة ببرمجيات خبيثة وتم تحليلها ومعالجتها واستعادة الخدمات المتأثرة وإعداد تقارير بها وإرسالها الى الجهات المعنية.

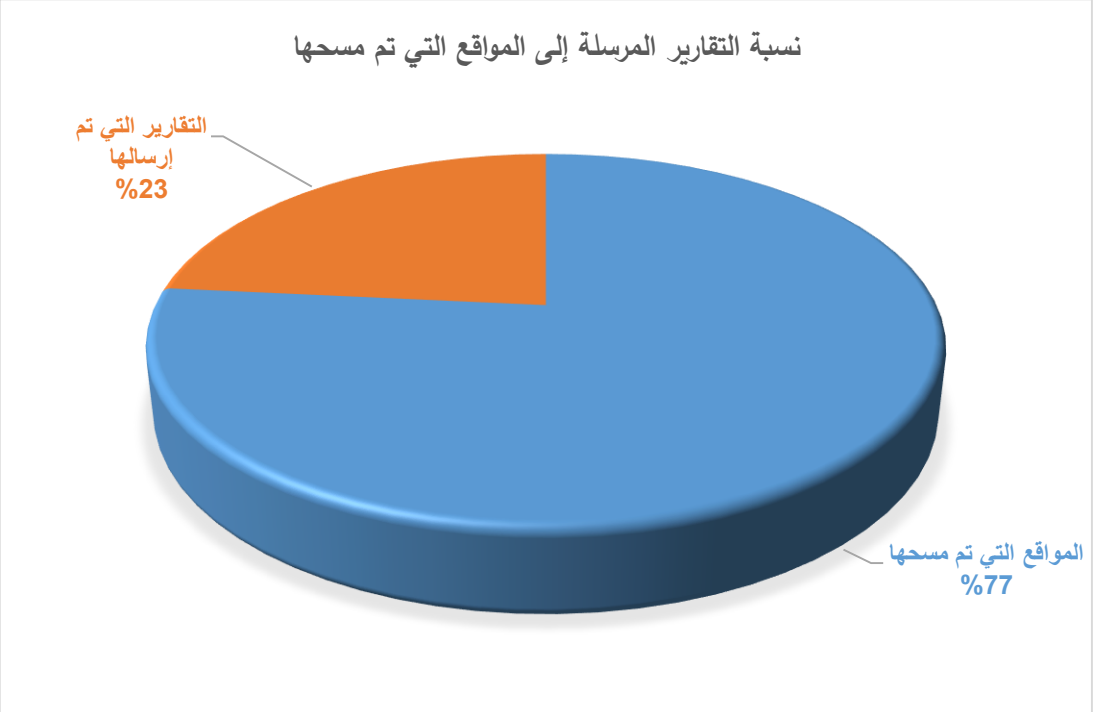
إحصائيات التقرير

شملت عمليات المسح الإلكتروني كما ذكر سابقاً 150 موقعاً إلكترونياً من مختلف القطاعات الحكومية من وزارات ومؤسسات وهيئات وجامعات وتم إعداد تقارير المسح الأمني للمواقع التي تحوي ثغرات هامة فقط وهي 46 موقعاً مسح دوري مجاني، وموقع واحد مسح احترافي، وسوف نبين تالياً من خلال المخططات البيانية جميع نتائج عمليات المسح.

معلومات عامة عن المواقع الإلكترونية

- يظهر الشكل التالي النسبة المئوية للمواقع الإلكترونية التي أعد لها تقارير مسح دوري (مجاني) وأرسلت إلى الجهات صاحبة هذه المواقع، أما المواقع التي أظهرت نتائج المسح عدم وجود ثغرات هامة تعرضها لخطر الاختراق فيجري الاحتفاظ بنتائج المسح الخاص بها في المركز للرجوع اليها عند الضرورة.

Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

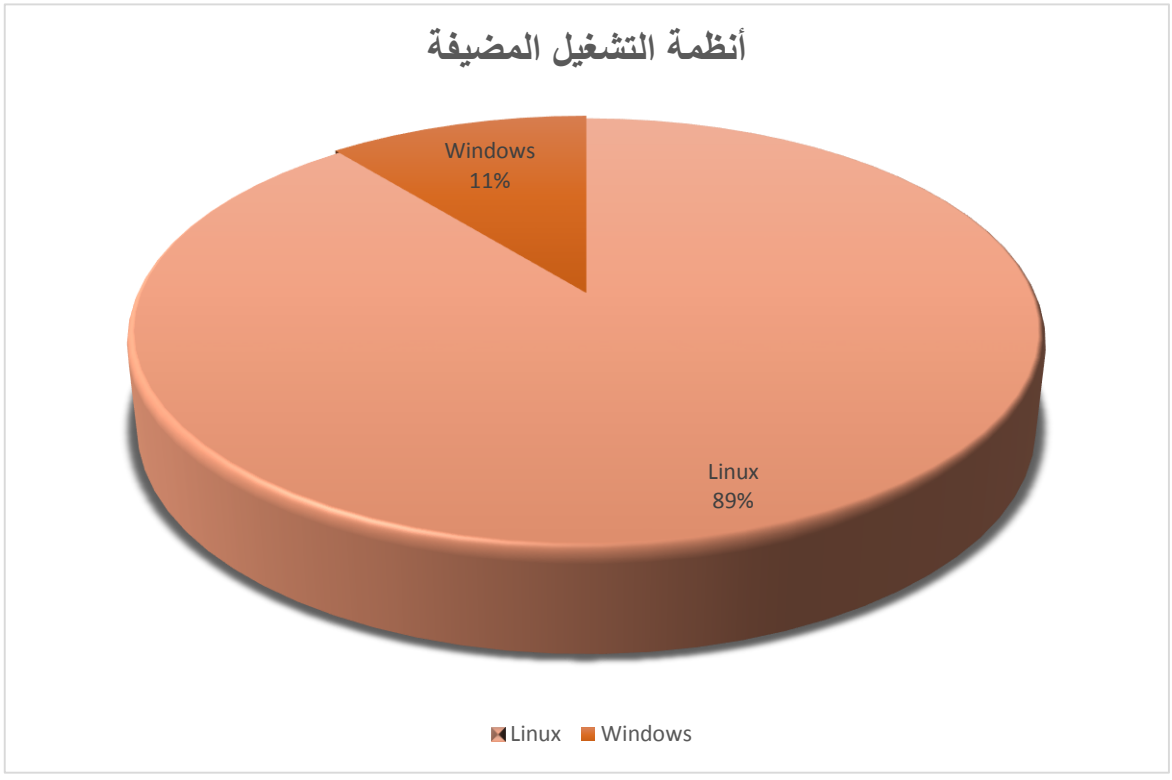


كما يظهر المخطط أن نسبة المواقع الإلكترونية التي احتاجت لإعداد تقارير مسح أمني بلغت 23% بتراجع ملحوظ عن العام 2015 حيث بلغت هذه النسبة 32% أي هناك تحسن بنسبة 9% ويعود ذلك لاستجابة الجهات صاحبة الموقع لتقارير المسح ومعالجة الثغرات المكتشفة.

- يظهر المخطط التالي أن معظم المواقع التي تم اختبارها تعمل على مخدمات ضمن الأراضي السورية، سواءً كانت المخدمات محلية لدى الجهة صاحبة الموقع أو لدى مزودات خدمة حكومية أخرى أو لدى مزودات خدمة خاصة، ويقوم المركز بمراسلة أصحاب المواقع الحكومية التي تعمل خارج الأراضي السورية لنقلها لداخل الأراضي السورية عملاً بالبلاغ رقم 15/7944 تاريخ 7-6-2012 الصادر عن رئاسة الحكومة والذي يلزم الجهات الحكومية بنقل مواقعها الإلكترونية للعمل داخل أراضي سوريا.

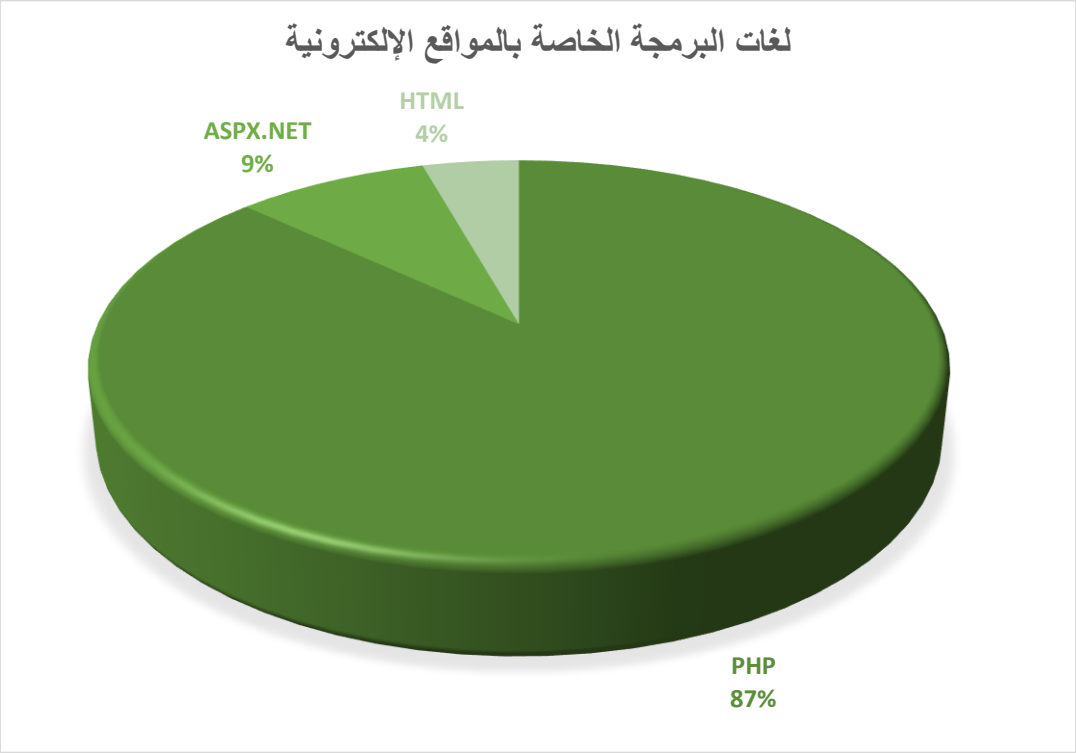
Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

- يوضح المخطط التالي أنواع أنظمة تشغيل المخدم المضيف حيث أن معظم المخدمات تعتمد على نظام التشغيل Linux والذي يوفر بيئة أكثر أماناً من نظام التشغيل Windows

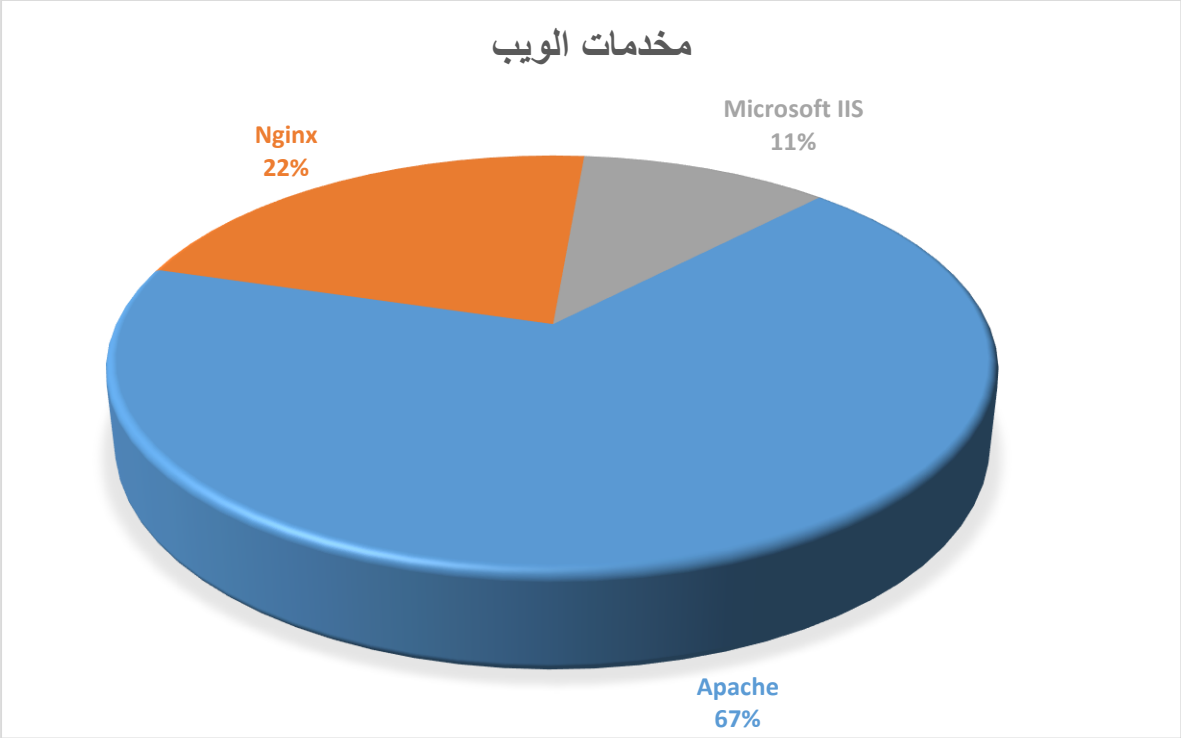


Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

- لغات البرمجة التي تم برمجة المواقع الإلكترونية بواسطتها:



- يبين المخطط التالي نسبة توزع أنواع مخدمات الويب:

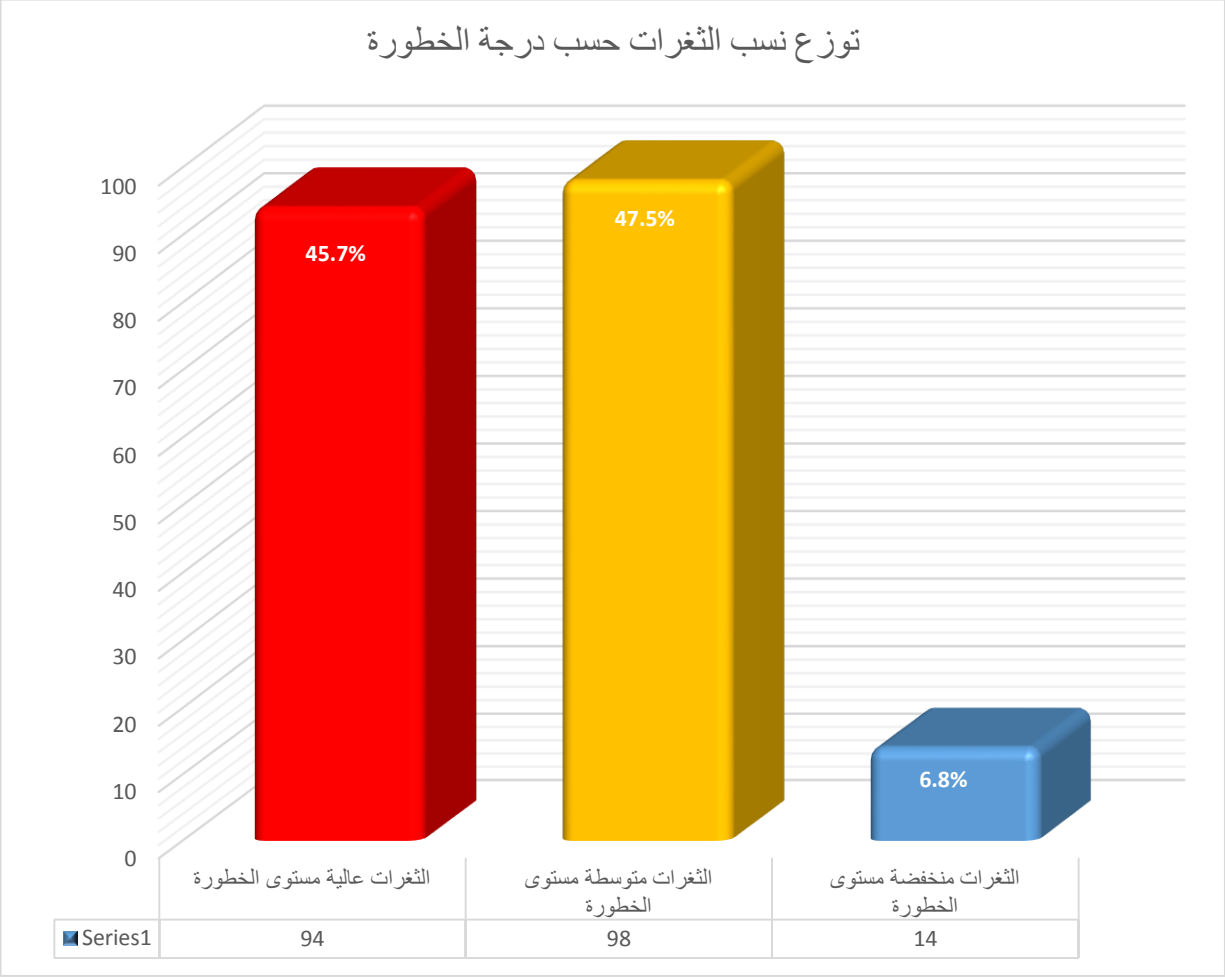


Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

الثغـــــــــــــــــرات

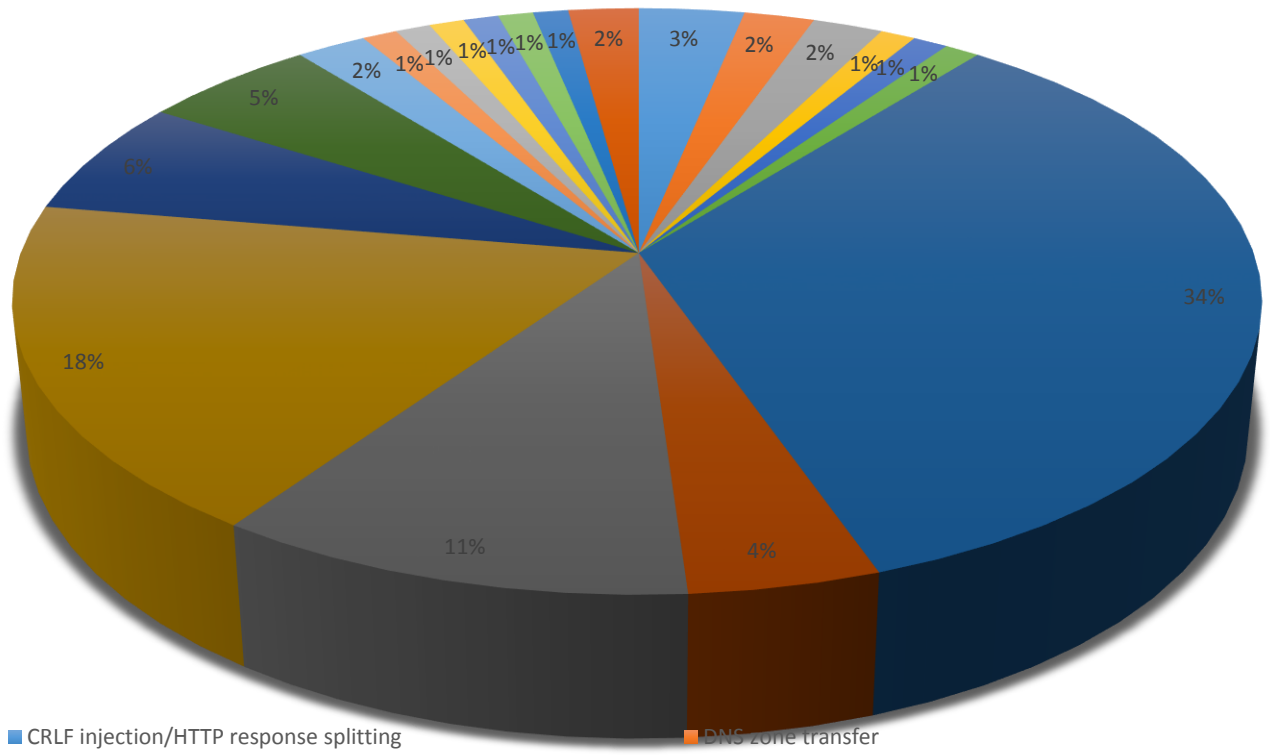
تصنف الثغرات الأمنية حسب التصنيفات العالمية إلى ثغرات عالية مستوى الخطورة وثغرات متوسطة مستوى الخطورة وثغرات منخفضة مستوى الخطورة.

- يبين المخطط التالي نسب توزع الثغرات المكتشفة بمستويات الخطورة الثلاثة:



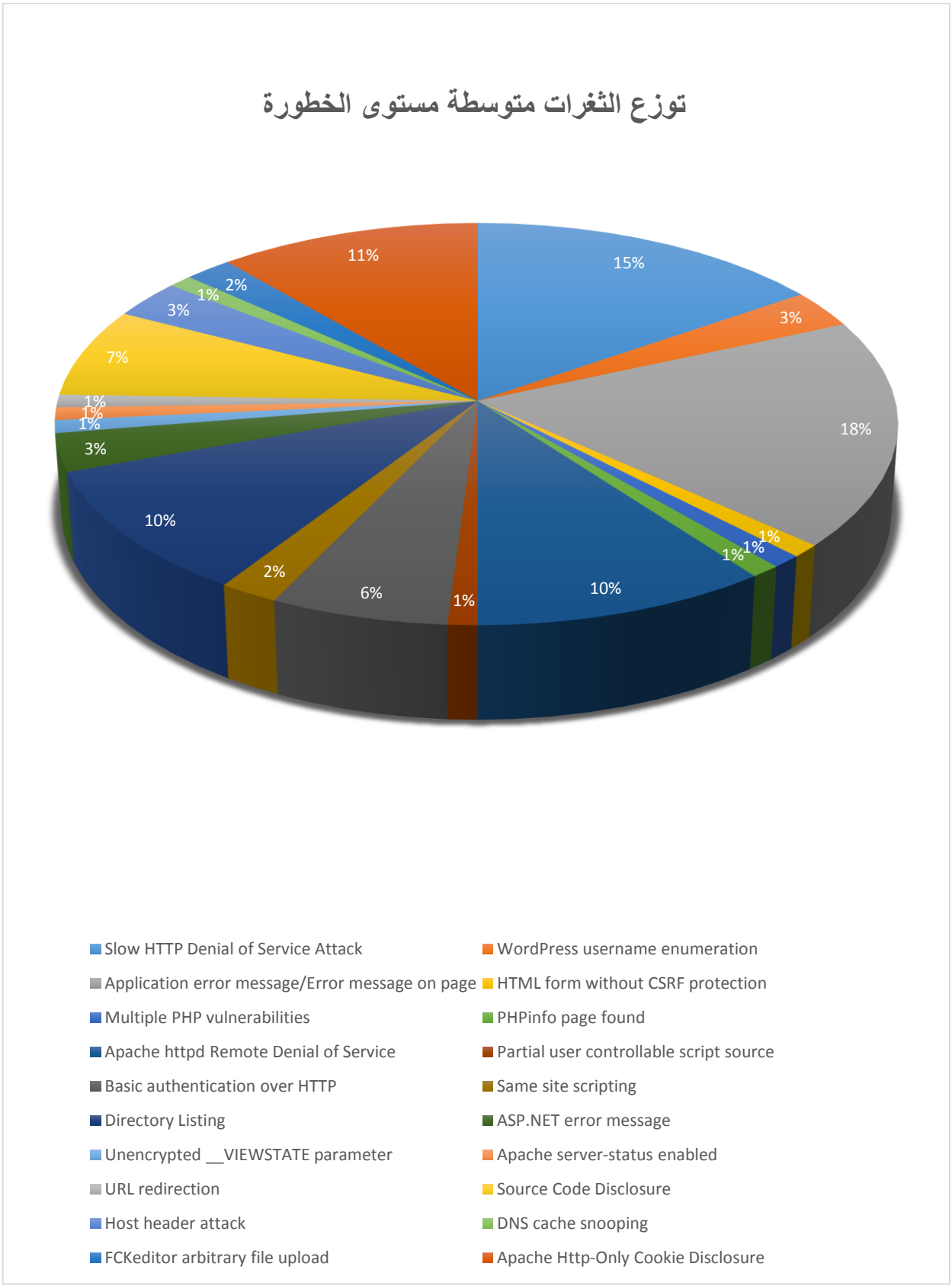
Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

توزع الثغرات عالية الخطورة



Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

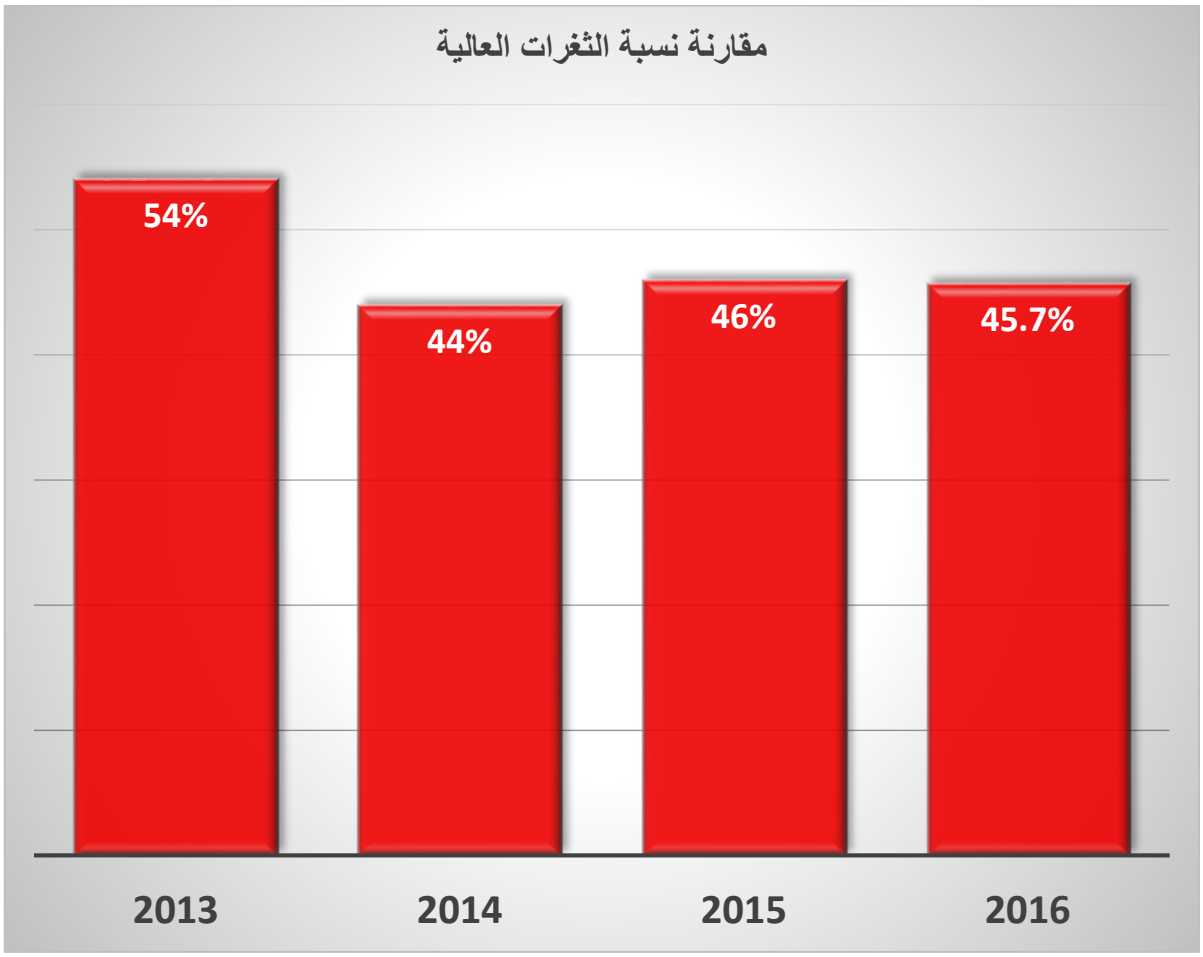
- يبن المخطط التالي نسب توزع أنواع الثغرات متوسطة مستوى الخطورة في المواقع المختبَرة:



Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

مقارنة نسب الثغرات عالية مستوى الخطورة للأعوام 2013-2014-2015-2016

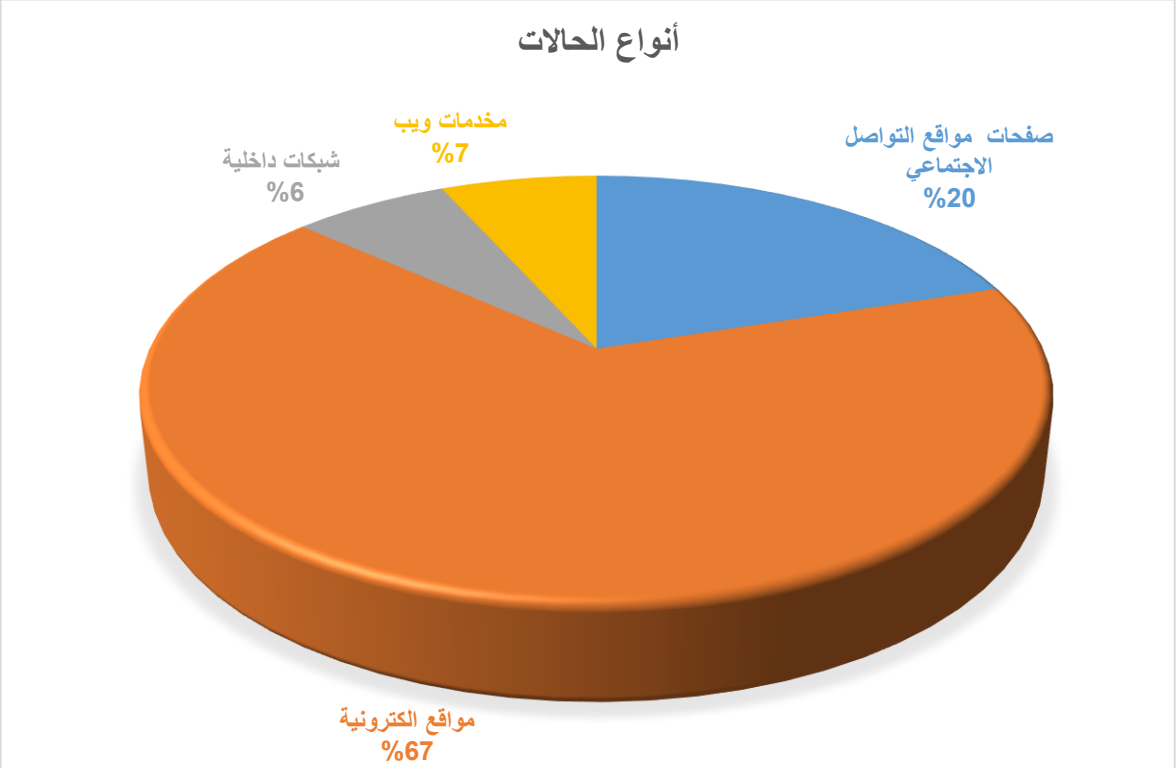
يوضح المخطط البياني التالي مقارنة نسبة الثغرات عالية مستوى الخطورة إلى نسبة الثغرات ذات مستوى الخطورة الأقل وذلك بين الأعوام المبينة تالياً:



Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

الاستجابة للطوارئ المعلوماتية

تم خلال العام 2016 الاستجابة لـ 15 حالة طارئة (اختراق + تعطل الخدمة)، جميعها في الجهات الحكومية، ثلاث حالات منها اختراق لصفحات التواصل الاجتماعي من خلال اختراق الحواسب الشخصية لمدراء هذه الصفحات عن طريق برمجيات خبيثة و10 حالات مواقع إلكترونية وحالة واحدة اختراق شبكة داخلية بالإضافة الى حالة اختراق مخدم ويب واحدة كما يوضح المخطط التالي:



Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

وقد توزعت أسباب هذه الحالات على فئتين رئيسيتين هما قيام المهاجمين باستغلال بعض أنواع البرمجيات الخبيثة أو قيام المهاجمين باستغلال وجود ثغرات ضمن بنية البيئة المستهدفة (مواقع إلكترونية):

Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

الصعوبات التي تواجه عمل المركز

واجهت المركز خلال العام 2016 –كما في الأعوام السابقة–جملة من الصعوبات والتحديات:

- عدم وجود تعاون من بعض الجهات العامة التي تم تحذيرها مسبقاً من خلال إرسال تقارير مسح لها وتحوي ثغرات خطيرة، مما أدى إلى اختراق هذه المواقع فيما بعد، وكانت سبباً في اختراق مواقع أخرى آمنة ضمن بيئة المخدم المضيف نفسه.
- عدم تطبيق سياسات وطنية لأمن المعلومات تلزم كل من يقدم خدمات إلكترونية بالحد الأدنى من معايير أمن المعلومات على مستوى التطبيقات والشبكات، وغياب إشراف المركز على تطبيق الحد الأدنى لمعايير أمن المعلومات، مما يؤدي الى عدم تعاون هذه الجهات مع المركز ويجعل الخدمات الإلكترونية التي تقدمها عرضة لكل أنواع الهجمات الإلكترونية.
- عدم تأمين التجهيزات والبرمجيات الخاصة باستكمال مشروع الاستجابة للطوارئ المعلوماتية CERT-SY.
- نقص الكادر البشري وتسرب العاملين من المركز نتيجة مفرزات الأزمة التي يعانيها القطر.
- عدم وجود دورات تدريبية تخصصية في مجال أمن المعلومات لتطوير الكادر البشري وتحسين جودة الخدمات، والاكتفاء بالتعلم الذاتي.
- نقص الوعي في مجال أمن المعلومات عند القائمين على تقديم الخدمات الإلكترونية في معظم الجهات العامة.
- تكتفي الجهات العامة بتقارير المسح المجاني والتي تتطلب وقتاً وجهداً من طاقم المركز التقني ولا تطلب خدمات المسح الاحترافي رغم أن أسعار هذه الخدمات رمزية جداً.

Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

التوصيات والتوجهات المستقبلية

- تأمين الموارد البشرية اللازمة التي يحتاجها المركز لتقديم خدماته بالشكل الأمثل بالإضافة إلى العمل على تأهيل وتدريب الكادر التقني في المركز بشكل مستمر.
- تطبيق سياسة خاصة بأمن المعلومات على المستوى الوطني ووضع معايير خاصة بأمن المعلومات لجميع الجهات العامة والخاصة المعنية بتقديم الخدمات الإلكترونية للحد من الهجمات الإلكترونية وعمليات الاختراق التي تتعرض لها.
- تفعيل مركز الاستجابة للطوارئ المعلوماتية للقيام بمهامه على أكمل وجه.
- الاستمرار بنشر الوعي وثقافة أمن المعلومات، سواء من خلال الدورات التدريبية أو المحاضرات أو المشاركة بورشات العمل التي تقوم بها الهيئة لشريحة واسعة من المسؤولين عن تقديم وادارة الخدمات الإلكترونية في الجهات العامة، أو من خلال التوعية الأمنية من خلال النشرات الدورية التي يصدرها المركز.
- التواصل مع الجهات العامة والخاصة لتقديم خدمات المسح الاحترافي وخدمة اختبار الاختراق الاحترافي لزيادة مناعتها ضد الهجمات الإلكترونية ومحاولات الاختراق من خلال كشف مواطن الضعف والثغرات الأمنية التي لا يتيحها المسح العادي.

الخلاصة

شهد المركز في العام 2016 تطوراً في الخدمات التي يقدمها كماً ونوعاً، ولوحظ ذلك من خلال انخفاض ملموس في حالات الاختراق والهجمات على المواقع الإلكترونية الحكومية بشكل خاص ومن خلال تزايد الثقة التي يبديها أصحاب المواقع الإلكترونية من خلال طلب تكرار الحصول على خدمات المسح الأمني بعد استلام تقارير المسح ومعالجة الثغرات المكتشفة لديهم وطلب المشورة والعون في كثير من الحالات المستجدة التي لم يوثقها هذا التقرير لأنها تتم عبر الاتصال الهاتفي المباشر مع فريق العمل التقني في المركز، وسيستمر المركز بتقديم خدماته وتطويرها كماً ونوعاً رغم كل الصعوبات التي تمت الإشارة إليها، كما يأمل المركز تذليل الصعوبات التي تحول دون قيامه بجميع المهام الموكلة إليه بالشكل الأمثل، وضمن الإمكانيات المتاحة لجهة توفير بيئة عمل أكثر أماناً لتقديم الخدمات الإلكترونية الحالية والمستقبلية على الشبكة.

Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy