الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

National Agency for Network Services
Information Security Center

مركز أمن المعلومات

التقرير الإحصائي السنوي لعام

2017

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 2017.

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:

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 2017

المسح الأمني للمواقع الإلكترونية والشبكات والمنظومات المعلوماتية الحكومية:

قام المركز خلال عام 2017 باختبار 50 موقعاً حكومياً وتم إعداد تقارير المسح الأمني لـ 26 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 25 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 سوريا قام المركز بتنفيذ مجموعة من النشاطات:

- 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 تحديث وتطوير الصفحات الخاصة بالمركز على الموقع الجديد للهيئة الوطنية لخدمات الشبكة وذلك من أجل العمل على نشر 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 لأمن المعلومات، إلا أن المركز لكم يتمكن 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 2017 إلى /7/ 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 50 موقعاً إلكترونياً من مختلف القطاعات الحكومية من وزارات ومؤسسات وهيئات وجامعات وتم إعداد تقارير المسح الأمني للمواقع التي تحوي ثغرات هامة فقط وهي 26 موقعاً بالمسح الدوري المجاني، وموقع واحد بالمسح الاحترافي، وسوف نبين تالياً من خلال المخططات البيانية جميع نتائج عمليات المسح.

معلومات عامة عن المواقع الإلكترونية

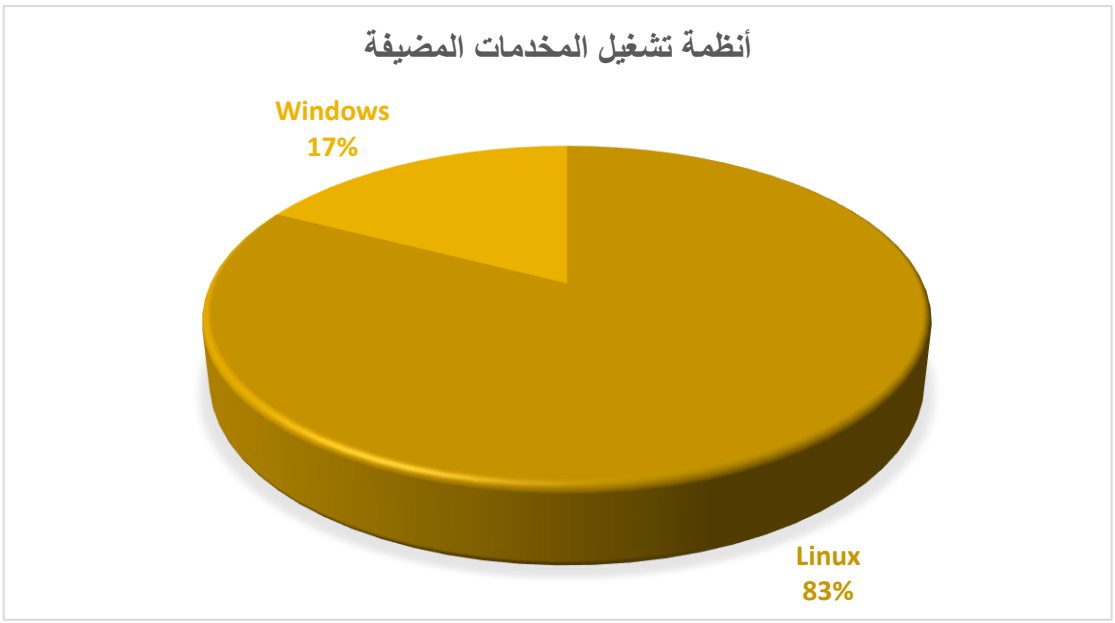
- يظهر الشكل التالي النسبة المئوية للمواقع الإلكترونية التي أعد لها تقارير مسح دوري (مجاني) وأرسلت إلى الجهات صاحبة هذه المواقع، أما المواقع التي أظهرت نتائج المسح عدم وجود ثغرات هامة تعرضها لخطر الاختراق فيجري الاحتفاظ بنتائج المسح الخاص بها في المركز للرجوع اليها عند الضرورة.

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

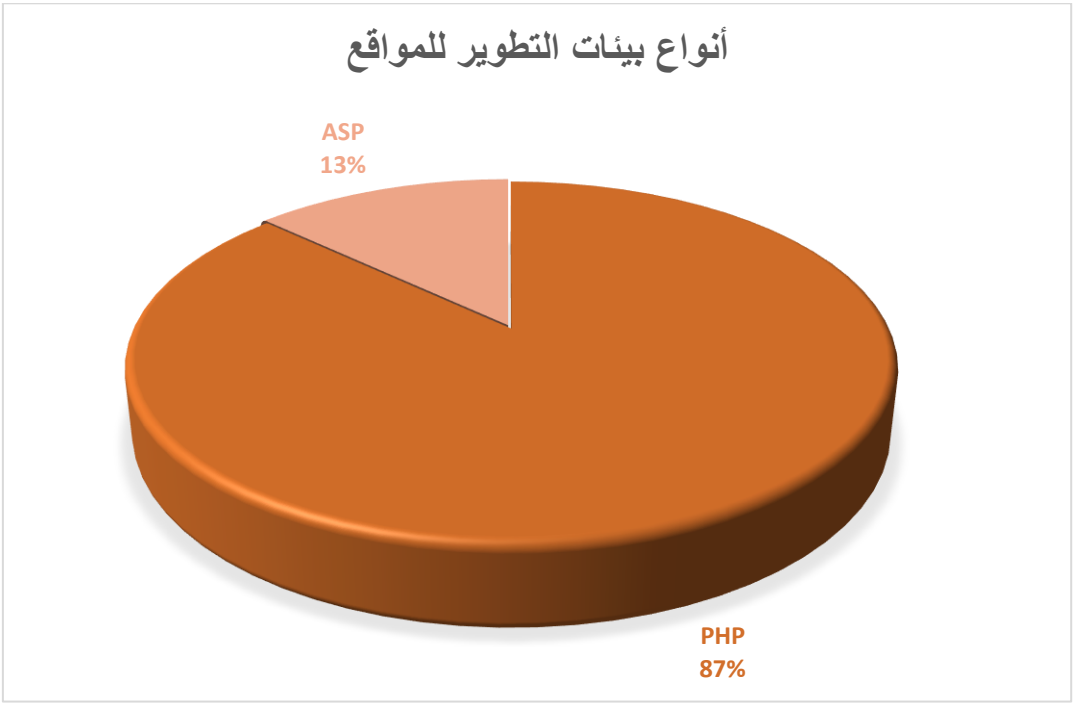
- إن جميع المواقع التي تم اختبارها تعمل على مخدمات تعمل ضمن الأراضي السورية، سواءً كانت المخدمات محلية لدى الجهة صاحبة الموقع أو لدى مزودات خدمة حكومية أخرى أو لدى مزودات خدمة خاصة.

- 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

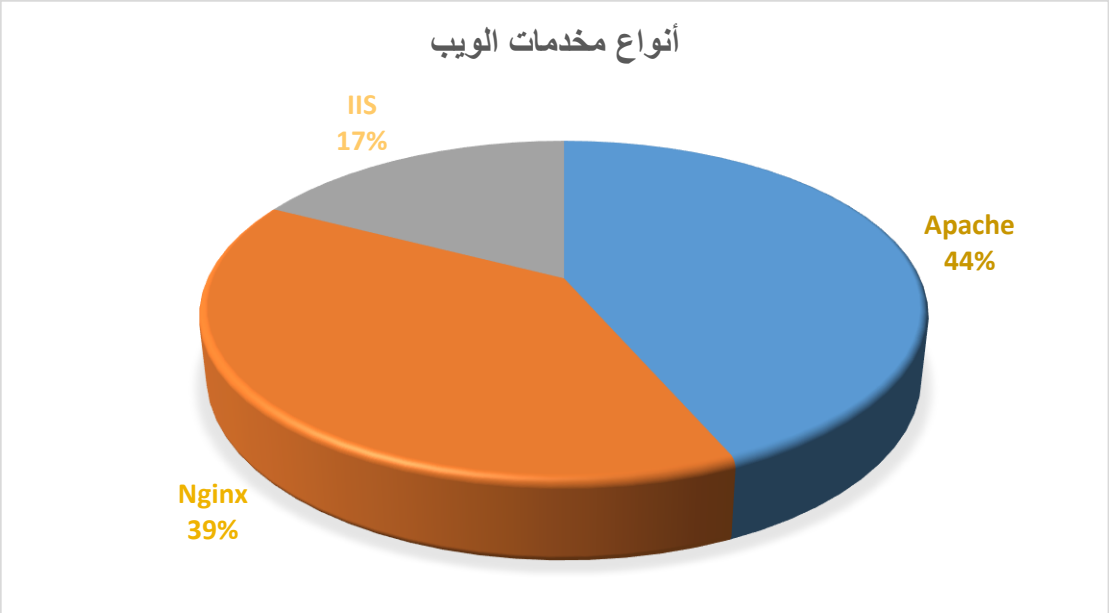


- لغات البرمجة التي تم تطوير المواقع الإلكترونية بواسطتها:



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

- يبين المخطط التالي نسبة توزع أنواع مخدمات الويب:

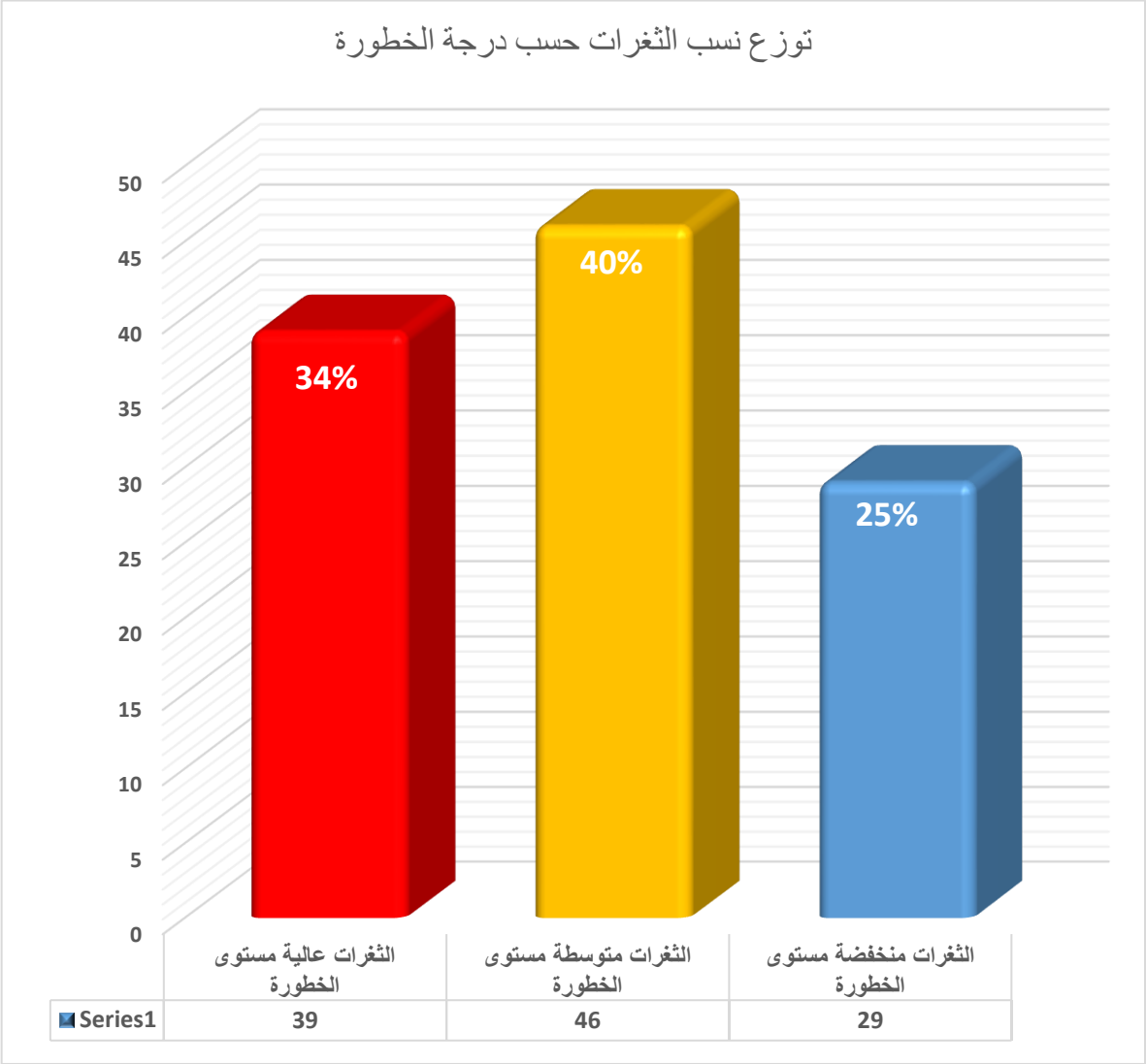


الثغـــــــــــــــــرات

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

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

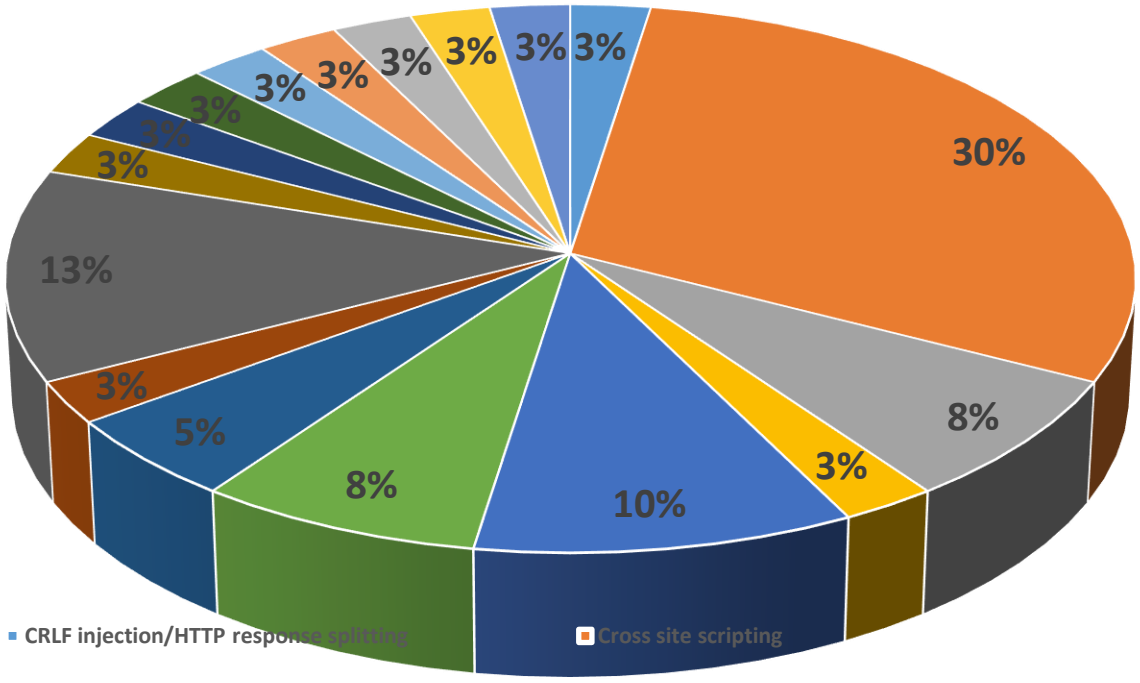
- يبين المخطط التالي نسب توزع الثغرات المكتشفة بمستويات الخطورة الثلاثة:



- يبن المخطط التالي نسب توزع أنواع الثغرات عالية 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

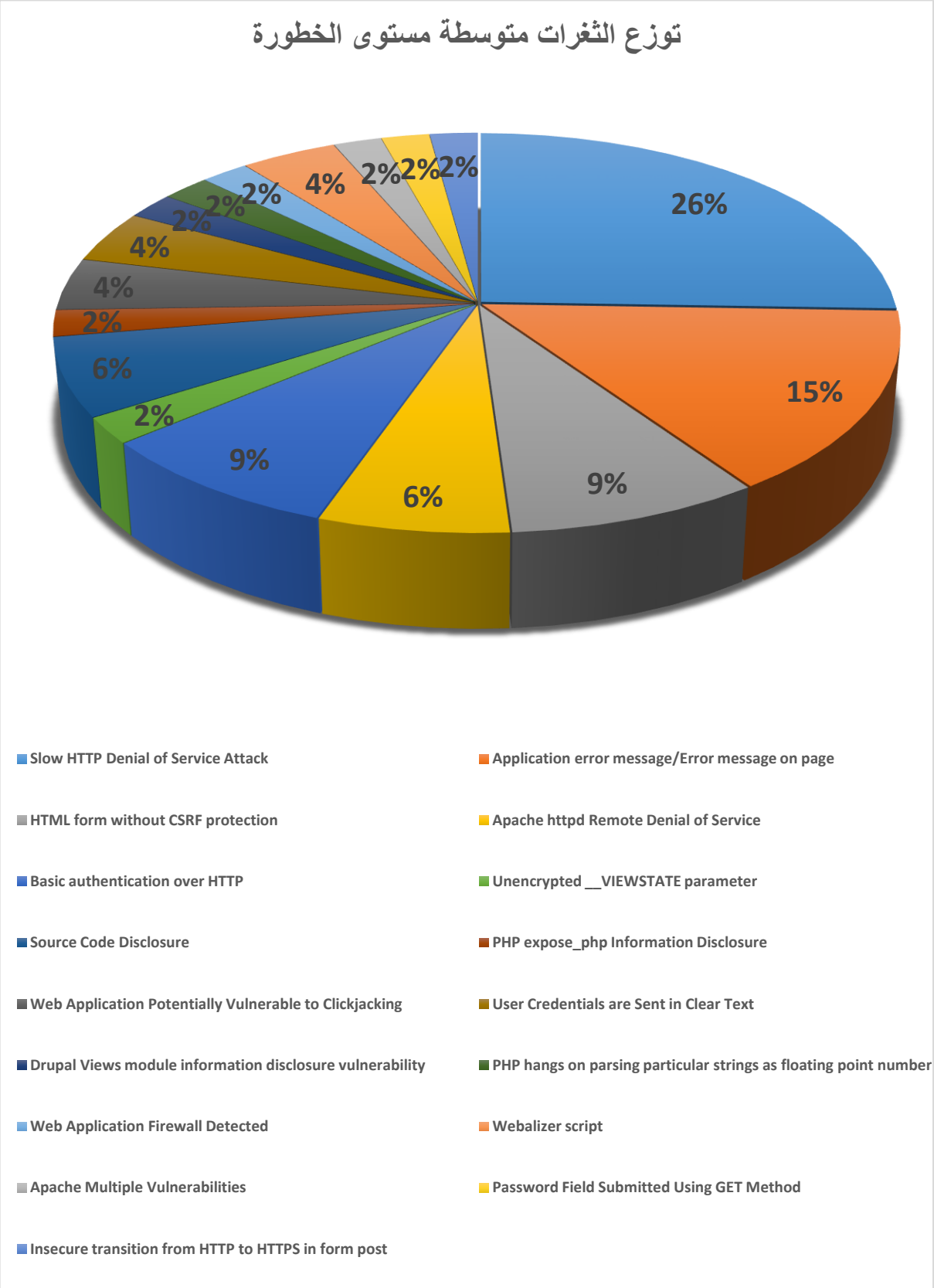
نسب توزع الثغرات عالية مستوى الخطورة



- CRLF injection/HTTP response splitting
- Cross site scripting
- HTTP Parameter Pollution
- JQuery Cross site Scripting XSS
- Blind SQL Injection
- SQL Injection
- Vulnerable Javascript Library
- FCKeditor spellchecker.php cross site scripting
- HTTP.sys remote code execution vulnerability
- PHP Unsupported Version Detectio
- Web Application Potentially Vulnerable to Clickjacking
- Weak Password
- HTML Form Found in Redirect Page
- XML quadratic blowup denial of service attack
- Possible Database Backup
- File Inclusion
- Server Side Request Forgery

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:

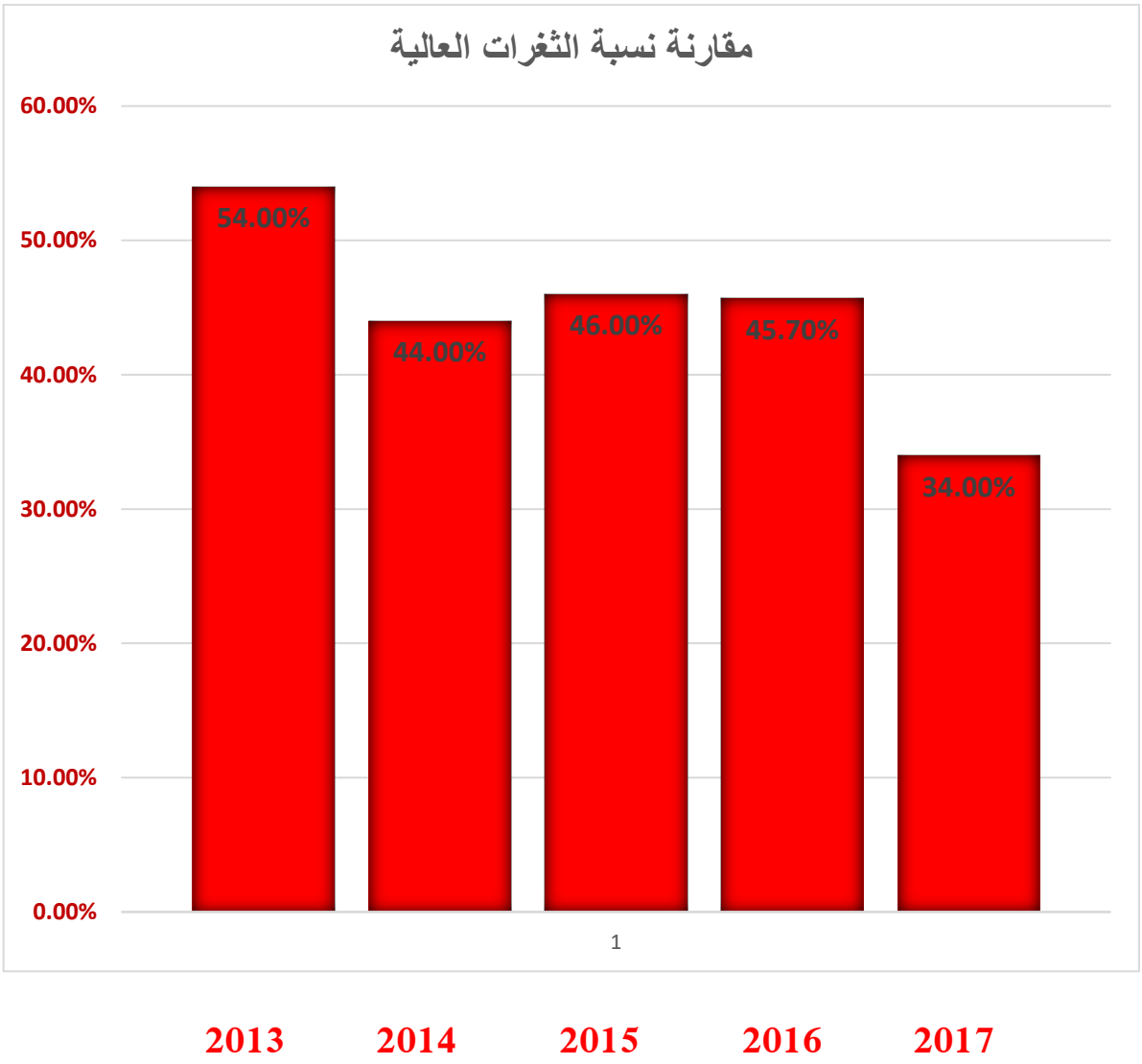


Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

مقارنة نسب الثغرات عالية مستوى الخطورة للأعوام

2017-2016-2015-2014-2013

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



يلاحظ انخفاض قدره 11% تقريباً في نسبة الثغرات العالية الخطورة مقارنة بالعام 2016 مما يشير إلى ارتفاع سوية أمن المواقع الالكترونية الحكومية.

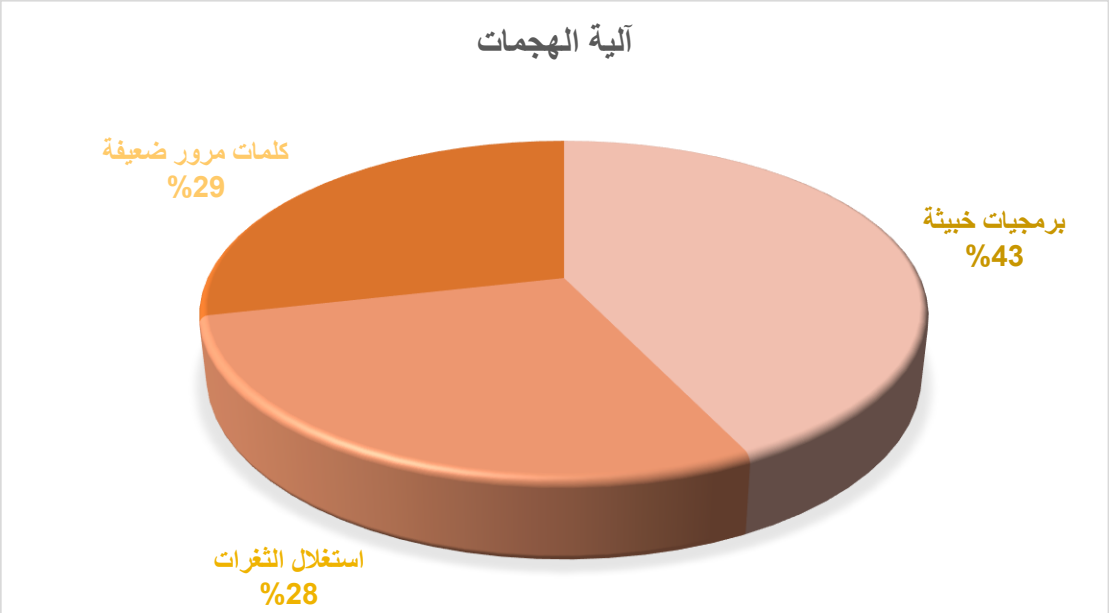
Tel: +963 11 3937032 (Ext: 2210 – 2211) Fax: +963 11 3937079 E-mail: infosec@nans.gov.sy Website: www.nans.gov.sy

الاستجابة للطوارئ المعلوماتية

تم خلال العام 2017 الاستجابة لـ 7 حالة طارئة (اختراق + هجمات أخرى)، جميعها في الجهات الحكومية، ست حالات اختراق مواقع الكترونية وحالة واحدة هجوم فيروسي على مخدم بريد الكتروني، حيث قام الفريق التقني في المركز بالتعامل مع هذه الحالات تباعاً واتخاذ الإجراءات اللازمة وإعداد التقارير الفنية.

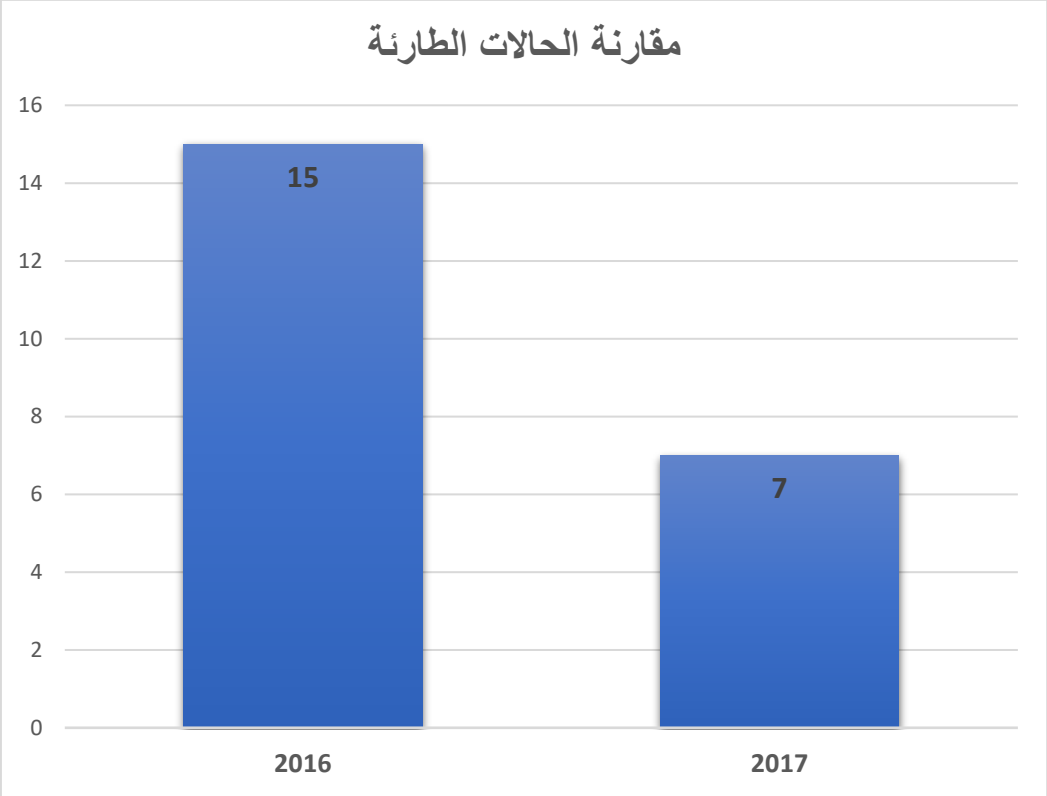
علماً بأن مركز أمن المعلومات يتعامل مع الحالات الطارئة التي يتم تبليغه بها رسمياً.

وقد توزعت أسباب هذه الحالات على ثلاث فئات رئيسية هي قيام المهاجمين باستغلال بعض أنواع البرمجيات الخبيثة، قيام المهاجمين باستغلال وجود ثغرات ضمن بنية البيئة المستهدفة واستغلال وجود كلمات مرور ضعيفة:



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

مقارنة الحالات الطارئة التي استجاب لها المركز في العام 2017 مع العام 2016:



نلاحظ بأن الحالات الطارئة التي استجاب لها المركز في العام 2016 هي 15 حالة أي أنه في العام 2017 انخفض عدد الحالات إلى 7 حالات فقط.

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

أعمال أخرى:

- تجديد تراخيص البرمجيات الخاصة بالمسح الأمني.
- تقديم خبرة فنية للقضاء بمجال التحليل الجنائي الرقمي في إحدى القضايا المعروضة على القضاء والمتعلقة بجريمة الكترونية.
- عضـوية لجنة إعداد دفتر الشـروط الخاصـة الفنية لمخبر الشـرعية الرقمية الخاص بوزارة الداخلية كأعضاء استشاريين ضمن اللجنة.
- ترأس الفريق التقني الخاص بتنفيذ مشـروع الشـبكة الحكومية الآمنة في الهيئة وتنفيذ المطلوب.
- ورشات عمل ومحاضرات واجتماعات حول مشروع الشبكة الحكومية الامنة.
- إعداد دفاتر الشـروط الفنية الخاصـة بمشـروع الاسـتجابة للطوارئ المعلوماتية في المركز، بالإضافة لشراء تجهيزات جديدة للمركز.
- المشاركة باللجان المشكلة ضمن الهيئة.
- تدريب وتأهيل العاملين الجدد في المركز (عاملين اثنين).
- تحديث التجهيزات والبرمجيات الخاصـة بتقديم خدمات المركز بشكل دوري واصـلاح الأخطاء والمشاكل.
- توعية أمنية عن طريق التنبيه من مخاطر البرمجيات الخبيثة والهجمات الالكترونية خلال 2017.

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

واجه المركز خلال العام 2017 –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 CSIRT-SY.
- نقص الكادر البشري وتسرب العاملين من المركز نتيجة مفرزات الأزمة التي تعاني منها البلاد.
- 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 ومناسبة.

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 وتحسين جودة الخدمات التي يقدمها المركز.
- 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.
- تنفيذ ما يلزم من المركز في إطار مشروع الشبكة الحكومية الآمنة.
- تنفيذ المشاريع والأعمال المشار إليها في خطة عمل المركز لعام 2018.
- تقديم الخدمات الاستشارية والخبرات الفنية للجهات العامة التي ترغب بذلك.
- تطبيق السياسة الوطنية لأمن المعلومات في الهيئة الوطنية لخدمات الشبكة تمهيدا لتطبيقها في كافة الجهات العامة.
- رفع سوية أمن المواقع الالكترونية التي تمسح وفق خطة المسح الأمني السنوية من خلال تخفيض نسبة الثغرات العالية مستوى الخطورة عن العام 2017.

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

شهد المركز في العام 2017 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