



*National Agency for Network Services
Information Security Center*

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

التقرير الإحصائي السنوي 2018



National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

قائمة المحتويات

3	تعريف بمركز أمن المعلومات.....
3	نظام خدمات مركز أمن المعلومات.....
4	نشاطات المركز خلال العام 2018.....
4	البيانات الإحصائية لعمليات المسح.....
5	مخطط نسبة المواقع التي تم مسحها.....
5	نسبة أنظمة تشغيل المخدمات المضيفة.....
6	لغات تطوير المواقع.....
6	أنواع مخدمات الويب.....
7	نسب الثغرات المكتشفة.....
8	نسب أنواع الثغرات عالية الخطورة.....
9	نسب أنواع الثغرات متوسطة الخطورة.....
10	نسب أنواع الثغرات منخفضة الخطورة.....
11	مقارنة الثغرات العالية مع أعوام سابقة.....
11	الاستجابة للطوارئ المعلوماتية.....
12	آلية الهجمات.....
12	مقارنة الحالات الطارئة بين عامي 2017 / 2018
13	الدراسات البحثية للمركز.....
13	أعمال أخرى.....
13	الصعوبات التي واجهت عمل المركز.....
15	التوجهات المستقبلية للمركز.....
15	الخاتمة



National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

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 الإلكترونية على الشبكة والإشراف على حسن 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 وإتخاذ 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 يُعدها المركز سنوياً، وفيما يلي سنعرض التقرير السنوي لمجمل أعمال ونشاطات المركز خلال العام 2018.

نظام خدمات مركز أمن المعلومات

مع بداية العام 2015 انتهى المركز من تجهيز المخبر الوطني لاختبار الاختراق والتحليل الجنائي للشبكات بأحدث التجهيزات والتطبيقات البرمجية المطوّرة من قبل شركات عالمية متخصصة بأمن المعلومات والتي تمكّن المركز من تطوير الخدمات التي يقدمها كماً ونوعاً، ولإستثمار المخبر بالشكل الأمثل كان لا بدّ من تنظيم عملية تقديم هذه الخدمات من خلال إصدار نظام خاص بالخدمات التي يُقدّمها المركز، حيث يُقدّم 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 الطلب لجميع المواقع الإلكترونية العامة والخاصة، وهي مجاناً للجهات العامة ولمرة واحدة خلال العام.
2. خدمة المسح الأمني الاحترافية: يقدم المركز هذه الخدمة عند الطلب للجهات العامة والخاصة، وتقسّم إلى ثلاثة أنواع:
 - أ. خدمة المسح الأمني الاحترافية للمواقع الإلكترونية ومخدمات الويب.
 - ب. خدمة المسح الأمني الاحترافية للبرمجيات.
 - ج. خدمة المسح الأمني الاحترافية للشبكات.
3. خدمة اختبار الاختراق الاحترافية: تتضمن خدمة المسح الأمني الاحترافية السابقة، 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.



National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

نشاطات المركز خلال عام 2018

المسح الأمني للمواقع الإلكترونية والشبكات والمنظومات المعلوماتية الحكومية:

قام المركز خلال عام 2018 باختبار 150 موقعاً حكومياً وتم إعداد تقارير المسح الأمني لـ 74 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 يتمكن من ذلك حوالي 50 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 مستضافة لدى الجمعية السورية للمعلوماتية والتي تمت مخاطبتها والاتصال بها عدة مرات للسماح بعمليات المسح دون جدوى حتى تاريخ إعداد هذا التقرير، وتم إجراء مسح عادي بناء على طلب من الجهة صاحبة الموقع (مرصد سوق العمل) و (تطبيق الDmail)، وخمسة مواقع بالمسح الاحترافي، واختبار اختراق احترافي عدد 1.

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.

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 لم 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 2018 إلى 5/ حالات 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 74 موقعاً بالمسح الدوري المجاني، وإجراء مسح عادي بناء على طلب من الجهة صاحبة الموقع (مرصد سوق العمل) و (تطبيق الDmail)، وخمسة مواقع بالمسح الاحترافي، واختبار اختراق احترافي عدد 1 وسوف نبين تالياً من خلال المخططات البيانية جميع نتائج عمليات المسح.

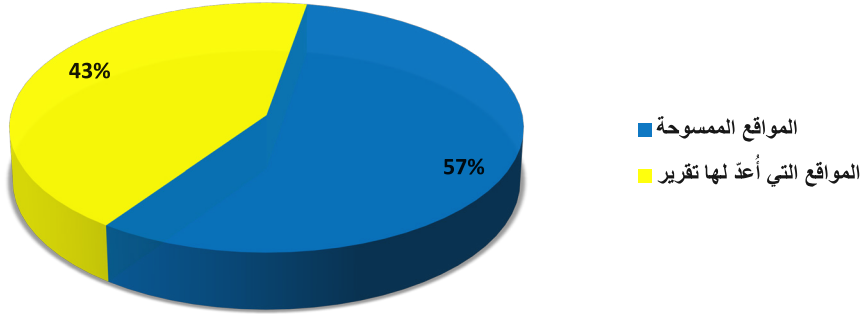
يظهر الشكل التالي النسبة المئوية للمواقع الإلكترونية التي أعد لها تقارير مسح دوري (مجاناً) وأرسلت إلى الجهات صاحبة هذه المواقع، أما المواقع التي أظهرت نتائج المسح عدم وجود ثغرات هامة تعرضها لخطر الاختراق فيجري الاحتفاظ بنتائج المسح الخاص بها في المركز للرجوع إليها عند الضرورة.



National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

نسبة المواقع الممسوحة إلى المواقع التي أعد لها تقرير

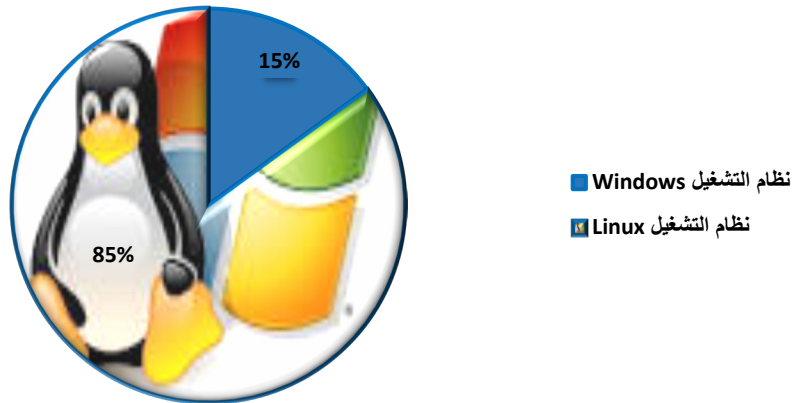


إن معظم المواقع التي تم اختبارها تعمل على مخدمات تعمل ضمن الأراضي السورية، ويوجد بعضها يعمل خارج الأراضي السورية، سواء كانت المخدمات محلية لدى الجهة صاحبة الموقع أو لدى مزودات خدمة حكومية أخرى أو لدى مزودات خدمة خاصة.

• أنواع أنظمة التشغيل:

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

أنظمة تشغيل المخدمات المضيفة

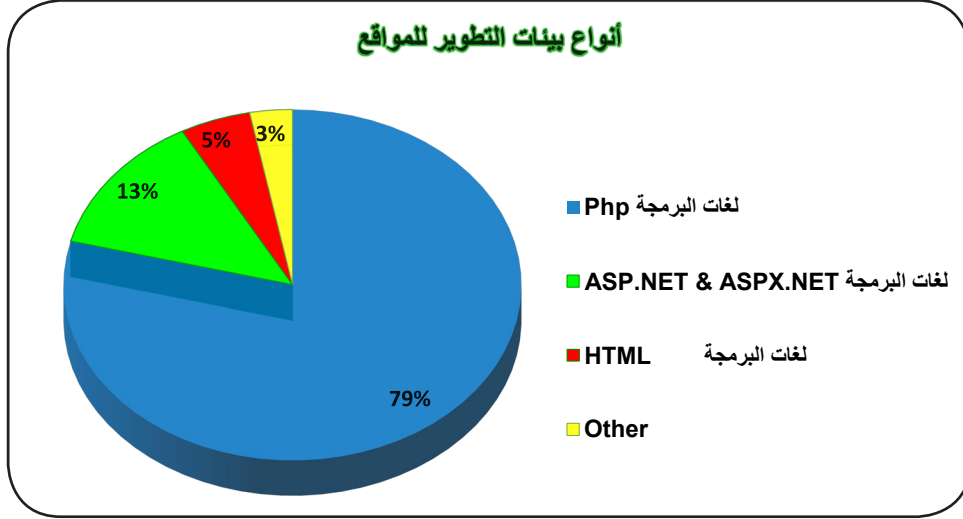




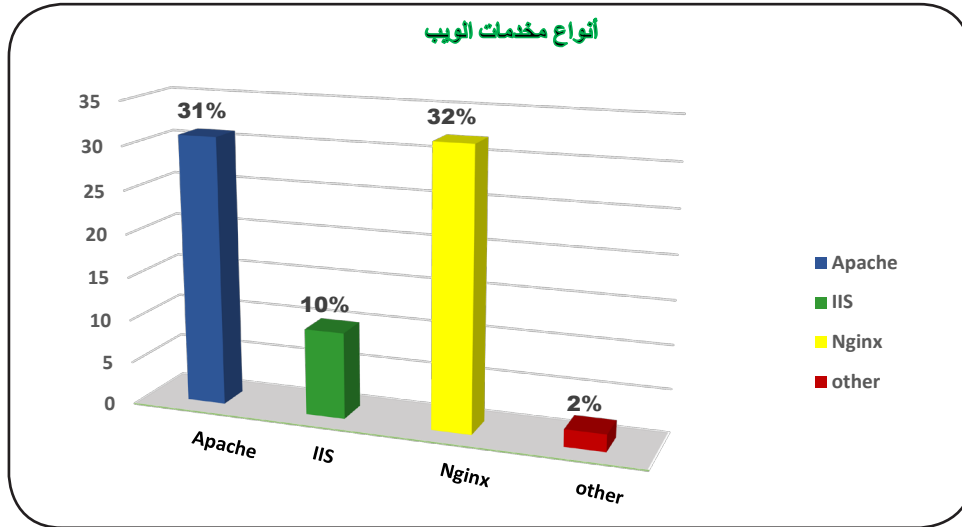
National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

- لغات البرمجة التي تم تطوير المواقع الإلكترونية بواسطتها:



- يبين المخطط التالي نسبة توزيع أنواع مخدمات الويب:



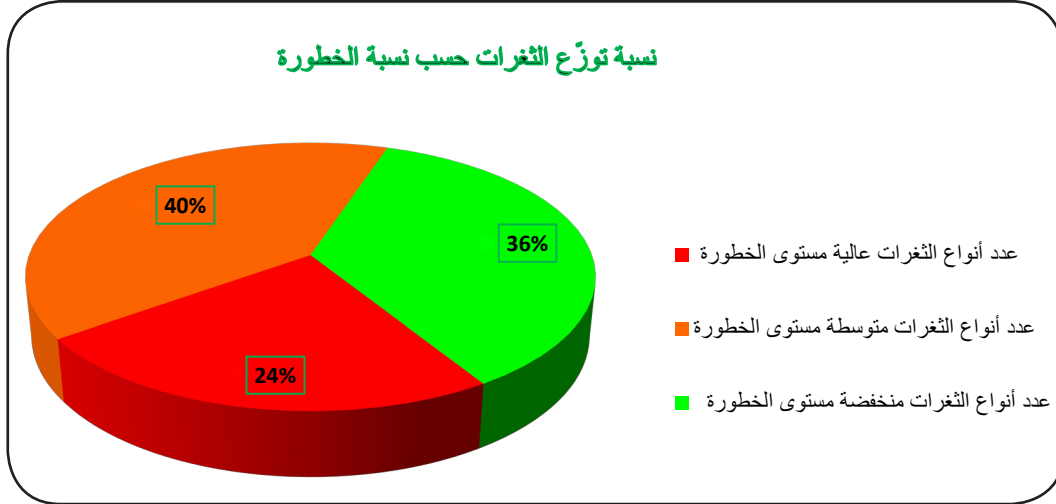


National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

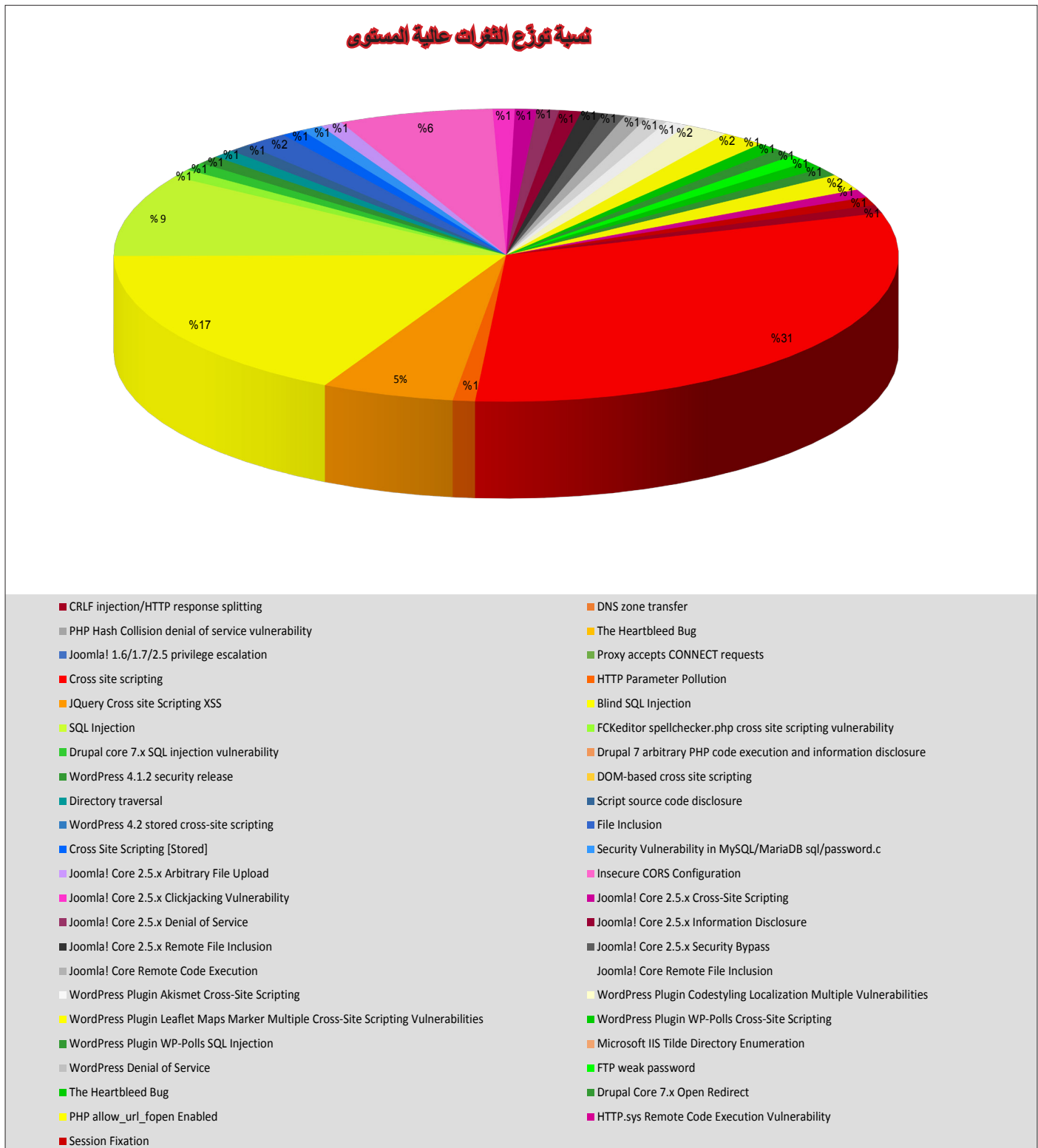
الثغرات

تصنّف الثغرات حسب التصنيفات العالمية إلى ثغرات عالية مستوى الخطورة وثغرات متوسطة مستوى الخطورة وثغرات منخفضة مستوى الخطورة. • يبيّن المخطط التالي نسب توزّع الثغرات المكتشفة بمستويات الخطورة الثلاثة:





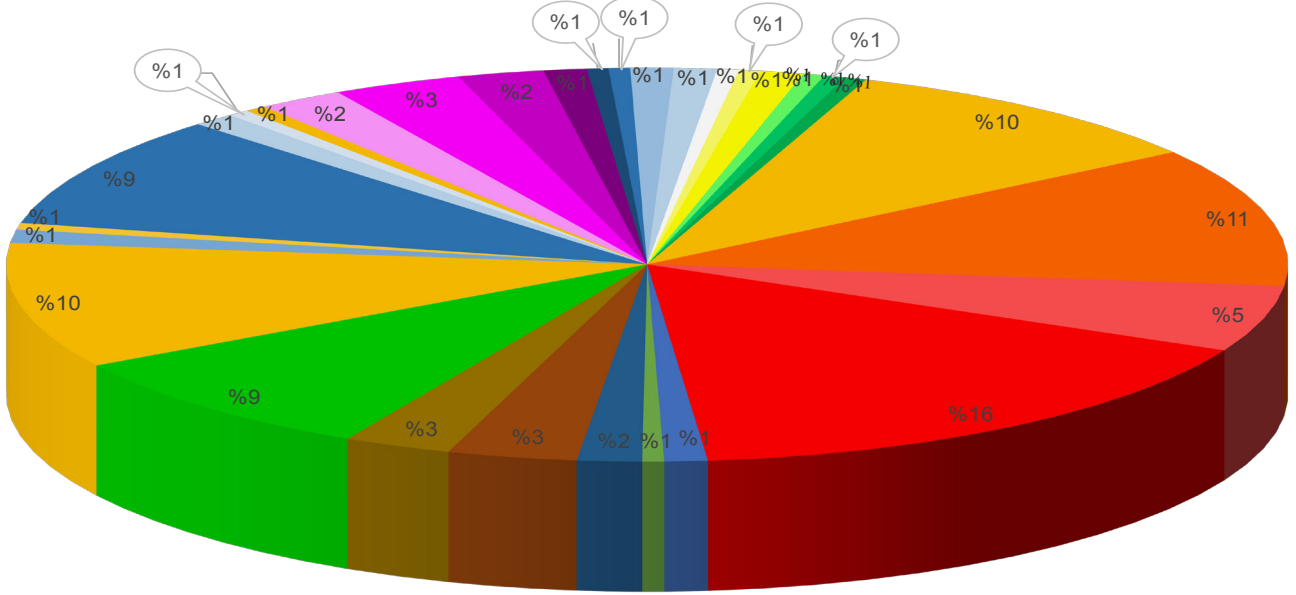
1- يبين المخطط التالي نسب توزع أنواع الثغرات عالية مستوى الخطورة في المواقع المختبرة:





2- يبين المخطط التالي نسب توزيع أنواع الثغرات متوسطة مستوى الخطورة في المواقع المختبرة:

نسبة توزيع الثغرات متوسطة الخطورة



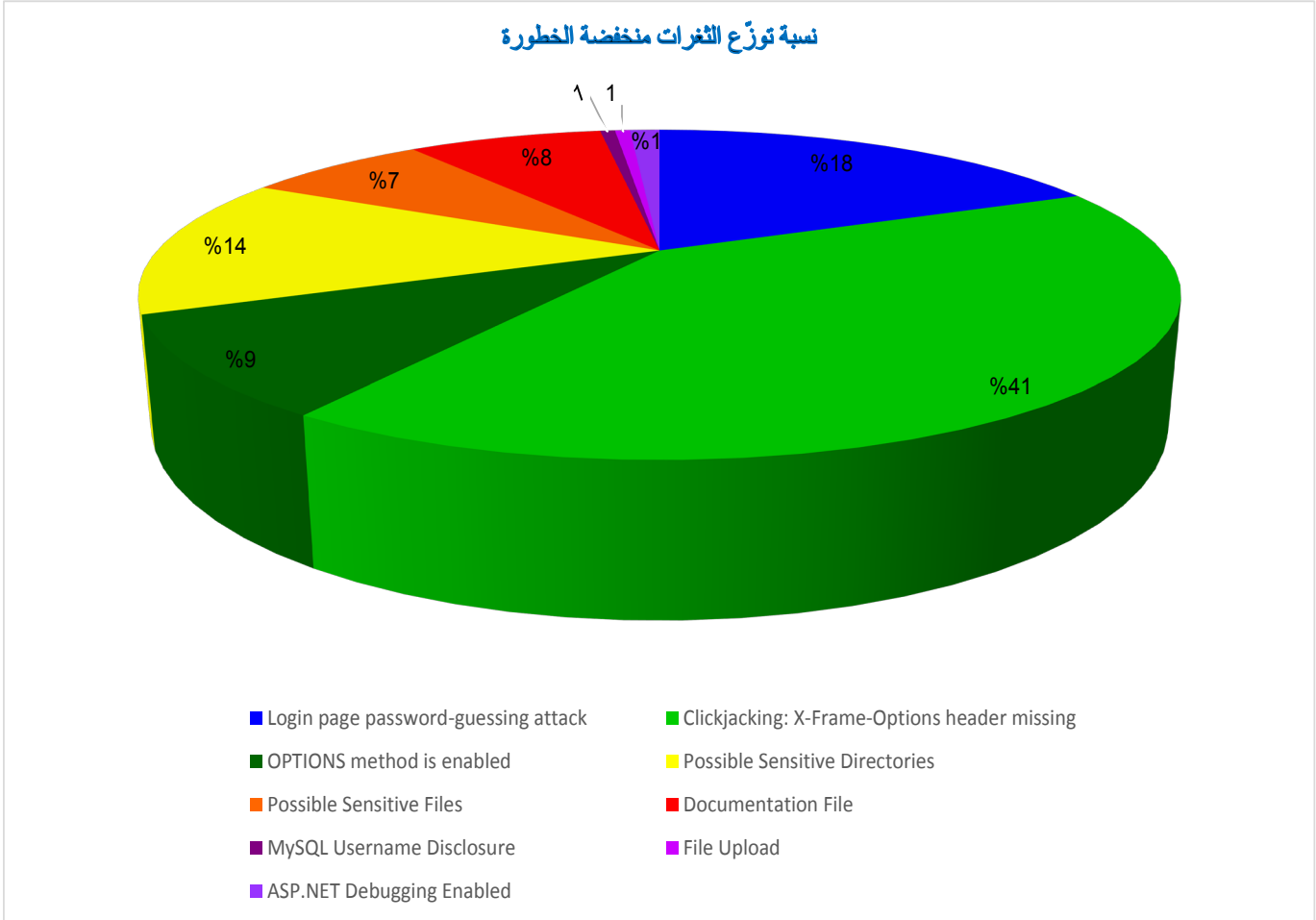
- Slow HTTP Denial of Service Attack
- WordPress username enumeration
- HTML form without CSRF protection
- PHPinfo page found
- Partial user controllable script source
- Same site scripting
- ASP.NET error message
- Apache server-status enabled
- Source Code Disclosure
- Host header attack
- FKEditor arbitrary file upload
- HTTP Parameter Pollution
- Cross Site Scripting(content-Sniffing)
- WordPress XML-RPC authentication brute force
- RC4 Cipher Suites Detected
- JetBrains .idea project directory
- PHP multiple vulnerabilities
- BREACH attack
- Vulnerable Javascript Library
- Application error message/Error message on page
- Multiple PHP vulnerabilities
- Apache httpd Remote Denial of Service
- Basic authentication over HTTP
- Directory Listing
- Unencrypted __VIEWSTATE parameter
- URL redirection
- User Credentials are Sent in Clear Text
- DNS cache snooping
- Apache Http-Only Cookie Disclosure
- Apache Multiple Vulnerabilities
- Webalizer Script
- Insecure Transition From HTTP to HTTPS in Form Post
- The POODLE Attack (SSLv3 Supported)
- HTML injection
- PHP Hangs on Parsing Particular Strings as Floating Point
- Cross domain data hijacking



National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

3- يبين المخطط التالي نسب توزيع أنواع الثغرات منخفضة مستوى الخطورة في المواقع المختبرة:



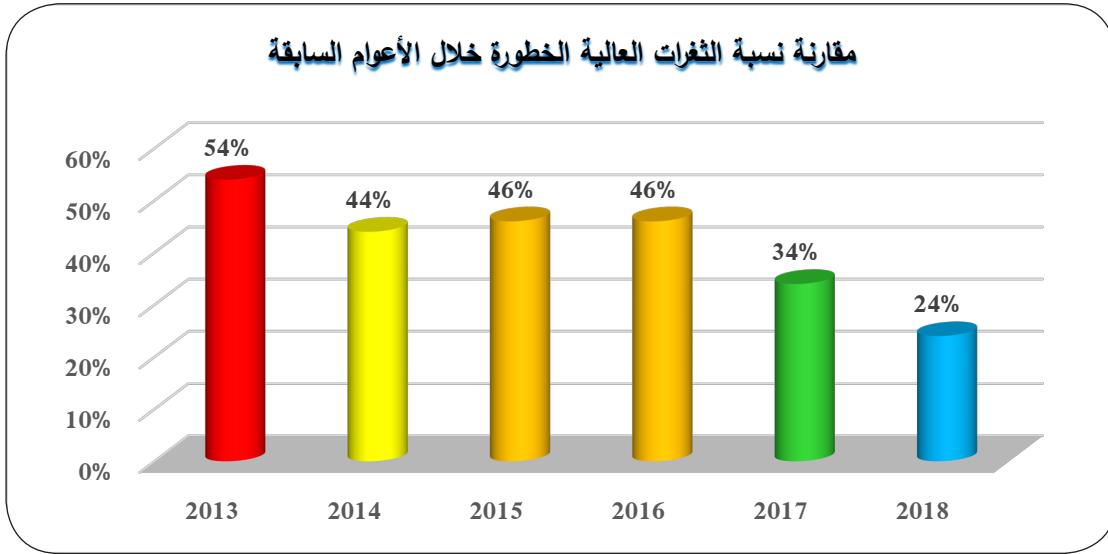


National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

مقارنة نسب الثغرات عالية مستوى الخطورة للأعوام 2018-2017-2016-2015-2014-2013

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 10% تقريباً في نسبة الثغرات العالية الخطورة مقارنة بالعام 2017 مما يشير إلى ارتفاع سوية أمن المواقع الالكترونية الحكومية.

الاستجابة للطوارئ المعلوماتية

تم خلال العام 2018 الاستجابة لـ 5 حالات طارئة (اختراق + هجمات أخرى)، جميعها في الجهات الحكومية، حالات اختراق مواقع الكترونية وحالة واحدة هجوم فيروسى 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.

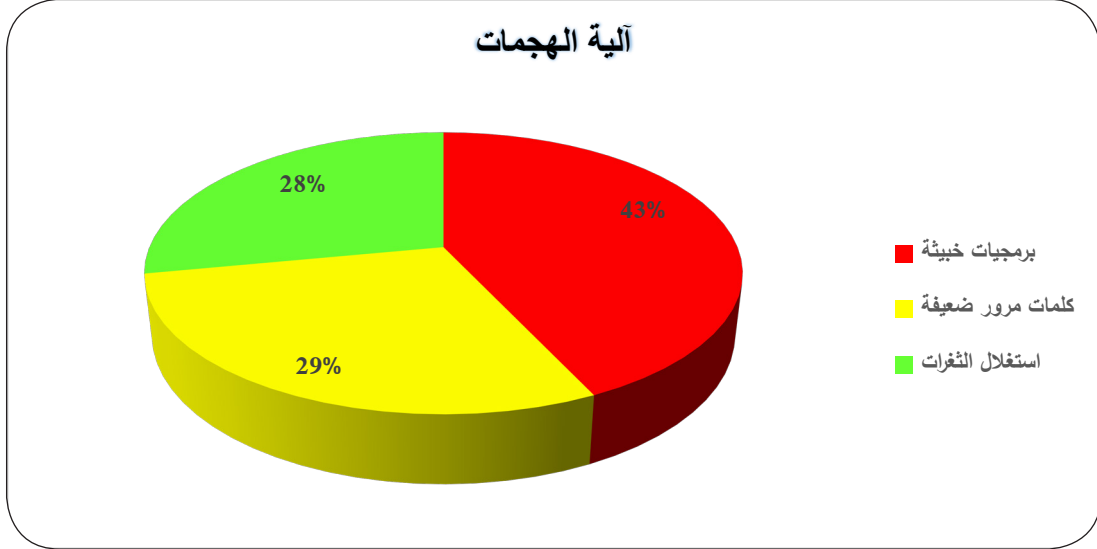
وقد توزعت أسباب هذه الحالات على ثلاث فئات رئيسية هي: قيام المهاجمين باستغلال بعض أنواع البرمجيات الخبيثة. قيام المهاجمين باستغلال وجود ثغرات ضمن بنية البيئة المستهدفة. استغلال وجود كلمات مرور ضعيفة.



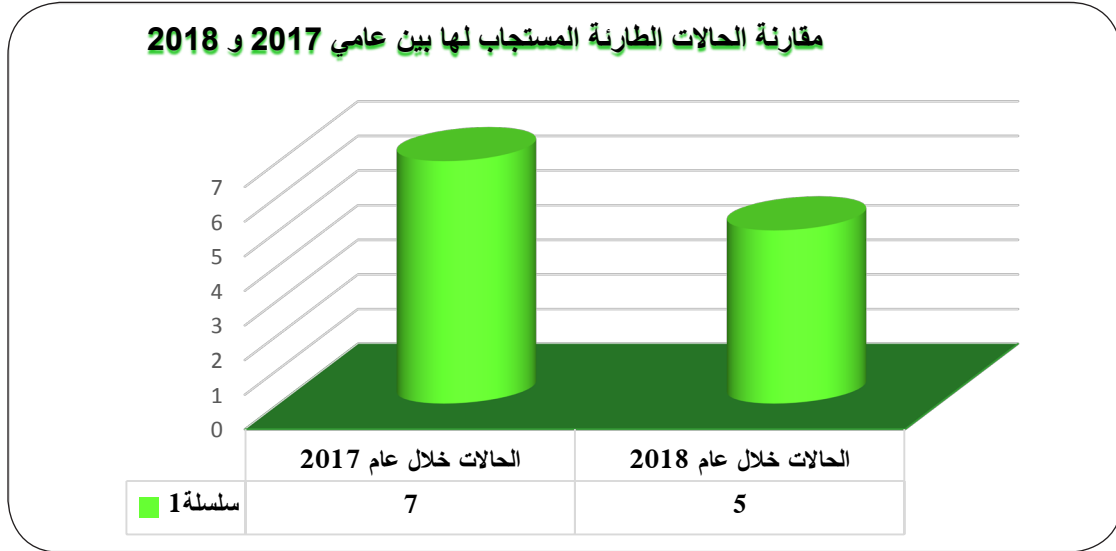


National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات



مقارنة الحالات الطارئة التي استجاب لها المركز في العام 2018 مع العام 2017:



نلاحظ بأن الحالات الطارئة التي استجاب لها المركز في العام 2017 هي 7 حالة أي أنه في العام 2018 انخفض عدد الحالات إلى 5 حالات فقط.





National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

الدراسات البحثية لمركز أمن المعلومات :

- 1- برنامج خبيث جديد من النوع "برمجيات الفدية" **New Malware: SamSam Ransomware** للتعرف على هذه الدراسة الرجاء زيارة الرابط التالي:
<http://www.nans.gov.sy/ar/file/5c07b6a2879eb>
- 2- المخاطر المحدقة بنظم تخطيط موارد المؤسسة **Systems EPR**: للتعرف على هذه الدراسة الرجاء زيارة الرابط التالي:
<http://www.nans.gov.sy/ar/file/5bb1c0353084a>
- 3- دراسة بحثية عن البرنامج الخبيث **The VPNFilter Malware**: للتعرف على هذه الدراسة الرجاء زيارة الرابط التالي:
<http://www.nans.gov.sy/ar/file/5b618a1777adf>
- 4- برنامج الخبيث **The Slingshot APT**: للتعرف على هذه الدراسة الرجاء زيارة الرابط التالي:
<http://www.nans.gov.sy/ar/file/5af2b33cdc771>
- 5- التحذير من ثغرة خطيرة في قواعد بيانات **oracle**: للتعرف على هذه الدراسة الرجاء زيارة الرابط التالي:
<http://www.nans.gov.sy/ar/file5/b73ed5c59327>

أعمال أخرى:

- المشاركة في ورشتي عمل، الأولى في وزارة الاتصالات والتقانة عن الشبكة الحكومية الآمنة في إطار الحكومة الالكترونية، والأخرى في المركز الثقافي بطرطوس حول الجريمة المعلوماتية في إطار التوعية الأمنية.
- ترجمة السياسة الوطنية لأمن المعلومات واللوائح التنظيمية لها إلى اللغة الإنكليزية
- مراجعة وتدقيق الوثائق الفنية الخاصة بترخيص /9/ شركات دفع الكتروني.

الصعوبات التي تواجه عمل المركز

واجه المركز خلال العام 2018 - كما في الأعوام السابقة - جملةً 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 إلى عدم تعاون هذه الجهات مع المركز ويجعل الخدمات الإلكترونية التي تقدمها عرضةً لكل أنواع الهجمات الإلكترونية.
- عدم تأمين التجهيزات والبرمجيات الخاصة باستكمال مشروع الاستجابة للطوارئ المعلوماتية **CSIRT-SY**.
- نقص الكادر البشري المدرب للعمل في 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.





National Agency for Network Services
Information Security Center

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

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 سواءً من خلال الدورات التدريبية أو المحاضرات أو المشاركة بورشات العمل التي تقوم بها الهيئة لشريحة واسعة من المسؤولين عن تقديم وإدارة 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 ضدّ 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 2019.
- 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 الإلكترونية التي تُمسح وفق خطة المسح الأمني السنوية من خلال تخفيض نسبة الثغرات العالية مستوى الخطورة عن العام 2018.





*National Agency for Network Services
Information Security Center*

الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

الخاتمة

شهد المركز في العام 2018 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 والاعون 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 بتذليل 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.