الجمهورية العربية السورية
وزارة الاتصالات والتقانة
الهيئة الوطنية لخدمات الشبكة

الهيئة الوطنية لخدمات الشبكة
National Agency For Network Services

نظام خدمات

مركز أمن المعلومات

المحتويات

الفصل الأوّل: تعاريف ومصطلحات

المادة (1): تعاريف

الهيئة: الهيئة الوطنيّة لخدمات الشّبكة، المحدَثة بموجب قانون التّوقيع الإلكتروني وخدمات الشبكة رقم /4/ لعام 2009.

المركز: مركز أمن المعلومات في الهيئة الوطنيّة لخدمات الشّبكة.

الثغرة الأمنيّة: خلل أو ضعف يمكن أن تتعرّض له إجراءات أو تصميم أو تنفيذ أو الضوابط الداخلية لحماية المنظومات المعلوماتيّة وينتج عنها خرقاً أو انتهاكاً لسياسة حماية المنظومات المعلوماتيّة.

المسح الأمني :عملية البحث عن الثغرات الأمنية في المنظومات المعلوماتيّة.

اختبار الاختراق الاحترافي: خدمة متقدّمة تتضمّن خدمة المسح الأمني الاحترافي ويُضاف إليها اختبار اختراق منظومات الزّبون بطرق تحاكي هجوم حقيقي بالتنسيق مع الزّبون ولا تسبب ضرراً لأنظمته.

جهاز شبكي: جهاز حاسوبي يعمل ضمن الشبكة موجهات، مبدلات، جدران نارية، أجهزة كشف التطفل أو منع الاختراق...

منظومات معلوماتيّة: مجموعة منّسقة من الأجهزة والبرمجيات الحاسوبية والمعدّات الملحقة بها، ومن الأمثلة على المنظومات المعلوماتيّة: جهاز حاسوبي مع برمجياته المضمّنة سواءً كانت أساسية أو تطبيقية، مجموعة من الأجهزة الحاسوبية المترابطة في منظومات موزّعة، مخدّم تتصل به حواسب طرفية أو حاسب مع المعدّات الملحقة به كالطابعة والماسح الضوئي أو هاتف جوال.

جهاز حاسوبي: أي جهاز يستخدم التقانات الإلكترونية أو الكهرومغناطيسية أو الضوئية أو الرقمية أو أي تقانات أخرى مشابهة بغرض توليد المعلومات أو جمعها أو حفظها أو الوصول إليها أو معالجتها أو توجيهها أو تبادلها.

الجرائم المعلوماتية: هي الجرائم المعرفة بقانون تنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية لعام 2012.

الطوارئ المعلوماتية: هي الحوادث الطارئة التي تؤدي لتهديد أو لتعطل جزئي أو كلي للمنظومات المعلوماتية أو الشبكات أو الخدمات الإلكترونية المقدّمة للعاملين أو للمواطنين والتي تقدمها جهات عامة أو خاصة.

الطوارئ الخاصة بالأفراد: الحوادث الطارئة الخاصة بالأفراد والمتعلقة بالجرائم المعلوماتية والتحليل الجنائي الرقمي والتي يتمّ التكليف بمعالجتها أو تحليلها من قبل إدارة الهيئة.

الدليل الرقمي: البيانات الرقمية المخزّنة في الأجهزة الحاسوبية أو المنظومات المعلوماتية، أو المنقولة بواسطتها، والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية.

السياسة الوطنية لأمن المعلومات واللوائح التنظيمية الملحقة: الوثائق ذات الصلة الصادرة عن الهيئة.

الخدمة الاستشارية: خدمة يقدمها المركز تتعلق بتقديم استشارات خاصة بأمن المعلومات وتصميم الشبكات وتطوير المنظومات المعلوماتية والخدمات الإلكترونية الآمنة.

الزبون: قطاع عام أو قطاع خاص أو أفراد.

طلب الخدمة: وثيقة إلكترونية أو ورقية تتضمن المعلومات الأساسية الواجب تقديمها للبدء بالخدمة.

المادة (2): مصطلحات

المصطلح باللغة العربية	المصطلح باللغة الانكليزية
المسح الأمني	Vulnerability Scanning
اختبار الاختراق الاحترافي	Penetration Testing
منظومات معلوماتية	Information Systems
جهاز حاسوبي	Computer Device
عملية التحقق من الوجود الحقيقي للثغرة	Elimination of false positive
نسخ احتياطي	System Backup
جمع معلومات	Information Gathering
خدمة المسح الأمني الاحترافية للمواقع ومخدمات الويب	Web Vulnerability Scanning
خدمة المسح الأمني الاحترافية للبرمجيات	Application Vulnerability Scanning
خدمة المسح الأمني الاحترافية للشبكات	Network Vulnerability Scanning

الفصل الثاني: خدمات المسح الأمني واختبار الاختراق الاحترافيّة

توصيف الخدمات

المادة (3): الهدف من الخدمات

رفع مستوى الأمان ضدّ الهجمات الالكترونيّة ومحاولات الاختراق، من خلال كشف الثغرات الأمنيّة المعلوماتيّة الموجودة لدى الجهات التي تطلب الخدمات والتي يمكن استغلالها من قبل المهاجمين وقراصنة المعلوماتية ويتمّ ذلك بالاعتماد على مجموعة من أفضل البرامج والتجهيزات الاحترافية المرخصة من أفضل الشركات العالمية بالإضافة إلى تقديم أفضل الحلول الممكنة لمعالجة هذه الثغرات.

المادة (4): أنواع الخدمات

1. **المسح الأمني العادي:** يقدّم المركز هذه الخدمة عند الطلب لجميع المواقع الالكترونيّة العامة والخاصة، وهي مجاناً للجهات العامّة ولمرةٍ واحدة في العام.
2. **المسح الأمني الاحترافي:** يقدّم المركز هذه الخدمة عند الطلب للجهات العامة والخاصة وتقسّم إلى ثلاثة أنواع:
   أ. المسح الأمني الاحترافية للمواقع ومخدّمات الويب.
   ب. المسح الأمني الاحترافية للبرمجيات.
   ت. المسح الأمني الاحترافية للشبكات.
3. **اختبار الاختراق الاحترافي:** تتضمّن خدمة المسح الأمني الاحترافية السابقة ويُضاف إليها اختبار اختراق منظومة الزّبون بطرقٍ تحاكي هجوم حقيقي بالتنسيق مع الزّبون.

المادة (5): طرق تقديم الخدمات

يتمّ تقديم الخدمة بإحدى الطرق التالية، ويعود لإدارة المركز تقدير ذلك بالاتفاق مع الزّبون بحسب ماتتطلبه ظروف المسح:

1. المسح الأمني عن بعد من خلال المركز.
2. المسح الأمني لموقع العمل من خلال زيارة فريق متخصص من المركز للزبون.
3. المسح الأمني في موقع العمل وعن بعد بحسب متطلبات العمل.

المادة (6): مخرجات الخدمات

يحصل الزبون على تقرير تفصيلي يتضمن ما يلي:

1. جميع المعلومات التي تمّ الحصول عليها من خلال المسح الأمني مثل: منظومات التشغيل المستخدمة، التقنيات والبرمجيات المستخدمة وإصداراتها، الخدمات الإلكترونية والمنافذ المفتوحة والعناوين الشبكية (IPs) وغيرها.
2. الثغرات الأمنية المكتشفة، ودرجة خطورتها وتأثيرها على العمل.
3. الحلول المقترحة لمعالجة الثغرات الأمنيّة.
4. أيّة معلومات تفيد الزّبون في تحسين واقع أمن المعلومات لديه.

طرق طلب الخدمة

المادة (7): خدمة المسح الأمني العادي

1. تقدّم الخدمة مجاناً للجهات العامّة مرة واحدة في العام ودون طلب من الزبون.
2. تقدّم الخدمة بناءً على طلب مباشر من الزبون، أو من مزوّد خدمة الاستضافة أو من خلال ملء طلب الخدمة المتوفّر على الموقع الالكتروني للهيئة أو للمركز وإرساله إلكترونيّاً أو عن طريق الفاكس.
3. يلتزم الزبون بتقديم إشعار، يُفيد بتسديده لرسوم الخدمة عند ملء طلب الخدمة.

المادة (8): خدمة المسح الأمني الاحترافي وخدمة اختبار الاختراق الاحترافي

1. تقدّم الخدمة من خلال ملء طلب الخدمة المتوفّر على الموقع الالكتروني للهيئة وإرساله إلكترونيّاً أو عن طريق الفاكس.
2. يقوم المركز بدراسة الطلب وإعداد العقد اللازم.
3. توقيع العقد من قِبل الطرفين.
4. واجبات الزّبون:

- تقديم كافّة المعلومات والبيانات التي يطلبها المركز والتي تمكّنه من تقديم الخدمة بالشكل الأمثل.
- تحضير بيئة العمل للمسح الأمني وفق ما يطلبه المركز والوارد في العقد مثل:

أ. نسخ احتياطي للمنظومات المعلوماتيّة التي سيتمّ مسحها.

ب. السماح لبرمجيات المركز الوصول إلى المنظومات المعلوماتيّة المستهدَفة عبر تجهيزات الحماية إن وجدت وذلك في حال تمّ المسح عن بعد.

ت. إنشاء حسابات مؤقتة خاصة بعملية المسح وبصلاحيات إدارية على المنظومات المعلوماتيّة التي سيتمّ مسحها.

ث. إلغاء جميع الصلاحيات والإجراءات والحسابات التي تم إنشاؤها لغرض المسح بعد الانتهاء التّام من عمليات المسح الأمني.

مراحل المسح الأمني

المادة (9): خدمات المسح العادي للمواقع الالكترونيّة

1. يتمّ المسح من خلال برمجيّات احترافية لدى المركز.
2. إعداد تقرير بالنتائج التي تمّ الحصول عليها.
3. إرسال التقرير للزبون من خلال البريد الرّسمي والإلكتروني.

المادة (10): خدمة المسح الاحترافي

يتمّ المسح من خلال برمجيّات احترافيّة لدى المركز وفق المراحل التالية:

1. جمع المعلومات عن المنظومات المراد مسحها.
2. إجراء المسح الأمني للمنظومات.
3. تحليل الثغرات المكتشفة من خلال عملية المسح وفق خطورتها وتأثيرها.
4. اختبار كلّ ثغرة على حدا بحسب درجة الخطورة والتحقق من وجودها الفعلي.
5. إعداد تقرير تفصيلي يتضمّن ما يلي:
   أ. الهدف من المسح
   ب. الثغرات المكتشفة لدى الزّبون ونوعها ودرجة خطورتها وتأثيرها.
   ت. الحلول المقرحة والجهة المسؤولة عن تنفيذها.
   ث. نصائح ومعلومات هامّة للزبون مثل مخطط الأجهزة والخدمات وغيرها.
6. تقديم التقرير للزبون ومناقشته معه.

المادة (11): خدمة اختبار الاختراق الاحترافي

يتمّ المسح واختبار الاختراق الاحترافي من خلال برمجيّات احترافيّة لدى المركز وفق المراحل التالية:

1. جمع المعلومات عن المنظومات المراد اختبارها.
2. إجراء المسح الأمني.
3. تحليل الثغرات المكتشفة من خلال عمليّة المسح وفق خطورتها وتأثيرها.
4. اختبار كلّ ثغرة على حدا بحسب درجة الخطورة والتحقق من وجودها الفعلي.
5. تحضير الأدوات والبرمجيّات المناسبة لاختبار الاختراق الاحترافي.
6. التعاون مع الزبون لإعلامه ببدء اختبار الاختراق الاحترافي والإجراءات الواجب اتّخاذها من قبله.
7. إجراء الاختراق الاحترافي.
8. إعداد تقرير تفصيلي يتضمّن ما يلي:
   أ. الهدف من اختبار الاختراق.
   ب. الخطوات المتّبعة في الخدمة.
   ت. مخططات البنية التحتية العاملة لدى الزبون.
   ث. الثغرات المكتشفة لدى الزّبون ونوعها ودرجة خطورتها وتأثيرها.
   ج. الحلول المقرحة والجهة المسؤولة عن تنفيذها.
   ح. نصائح ومعلومات هامّة للزبون
9. تقديم التقرير للزبون ومناقشته معه.

المادة (12): أجور خدمة المسح واختبار الاختراق

الخدمة	الأجر بالليرة السورية		الملاحظات
المسح العادي	12000		تقدّم الخدمة مجاناً للجهات العامّة مرة واحدة في العام
المسح الاحترافيّ	90000	المواقع الالكترونيّة	في حال خدمة مسح البرمجيّات أو الشبكات يُضاف عن كلّ مخدّم 12000 وعن كلّ جهاز شبكي 2400 وعن كلّ شبكة محليّة 30000
	150000	مخدّمات الويب والبرمجيّات	
	300000	الشبكات	
اختبار الاختراق الاحترافي	120000	المواقع الالكترونيّة	في حال خدمة اختبار الاختراق للبرمجيّات أو الشبكات يُضاف عن كلّ مخدّم يخضع للاختبار 24000 وعن كلّ جهاز حاسوبي يخضع للاختبار 6000
	240000	مخدّمات الويب والبرمجيّات	
	360000	الشبكات	

الفصل الثالث: خدمات الاستجابة للطوارئ المعلوماتيّة

المادة (13): طرق طلب الخدمة

يمكن للزبون التقدّم بطلب الخدمة بإحدى الطّرق التالية:

1. طلب خطي للهيئة من قبل الزبون يوضّح الحادثة التي يطلب الاستجابة لها.
2. الاتصال الهاتفي بالمركز بحيث يقوم الموظفون المكلفون بتلقي الطلبات بتعبئة طلب الخدمة والتي يمكن توقيعها لاحقاً من الزبون.
3. ملء طلب الخدمة المتوفر على الموقع الإلكتروني للهيئة أو للمركز وارساله عن طريق البريد الالكتروني أو عن طريق الفاكس.

المادة (14): واجبات الزبون

1. تقديم كافة المعلومات والبيانات التي يطلبها المركز والتي تمكنه من الاستجابة للحادثة.
2. السماح لفريق المركز بالوصول للملفات والتجهيزات المتعلقة بالحادثة.

المادة (15): مخرجات الخدمة

تقرير تفصيلي من قبل المركز يتضمّن تفاصيل الحادثة والحلول الإسعافية الآنية والاحترازية المستقبلية المقتَرحة.

المادة (16): أجور الاستجابة للطوارئ المعلوماتيّة

1. الخدمة مجانية للجهات الحكومية.
2. تحدد الأجور للأفراد والجهات الخاصة كما يلي:

الخدمة	الأجر حسب سعة التخزين			ملاحظات
	من GB	إلى GB	الأجر بالليرة السورية	
استعادة بيانات أو معلومات مفقودة Data Recovery	--	64	2400	يقصد بالبيانات المفقودة: ملفات إلكترونية بكافة أنواعها، منظومات تشغيل، تطبيقات وغيرها من البيانات المخزنة إلكترونياً
	64	500	6000	
	500	1000	8400	
	1000	ما فوق	8400 لكلّ 1TB	
طوارئ معلوماتية	12000 لكلّ جهاز حاسوبي			كل جهاز حاسوبي يقوم فريق المركز بفحصه
استخراج الدليل الرقمي لجريمة معلوماتية أو تقليدية	12000 للأفراد عن كلّ جهاز 24000 عن كلّ جهاز للجهات الخاصة			كل جهاز حاسوبي يقوم فريق المركز باستخراج أدلة رقمية منه

الفصل الرابع: أحكام عامّة

1. يمكن لإدارة الهيئة تخفيض الأجور الواردة في هذا النظام لبعض الجهات وفق ما تقتضيه المصلحة العامّة، وذلك بموافقة من مجلس إدارة الهيئة.
2. تخفّض أجور الخدمات المقدّمة للقطاع العام بنسبة 20% عن الأجور الواردة في هذه الوثيقة.
3. يتم تسديد الأجور لحساب الهيئة في المصرف التجاري السّوري كما يلي:

أ. خدمة المسح الأمني العادي: يجب تسديد كامل الأجر قبل البدء بالخدمة.

ب. خدمات الاستجابة للطوارئ المعلوماتية: يُسدّد 10% من الأجور قبل البدء بالخدمة ويتمّ تسديد باقي الأجور في حال الوصول لنتيجة وقبل تسليم التقرير النّهائي ويُستثنى من هذا البند خدمة طوارئ المعلوماتيّة.

ت. باقي الخدمات يجب على الزبون تسديد 50% من قيمة الأجور عند مباشرة المركز بتقديم الخدمة، على أن يتمّ تسديد باقي الأجور عند انتهاء المركز من تقديم الخدمة بالكامل بحسب بنود العقد مع الزبون.

ث. يُستثنى الزبون إذا كان إحدى جهات القطاع العام من أحكام الفقرة ت السابقة، ويقوم بتسديد 50% من قيمة الأجور عند إنجاز المركز للمراحل 1، 2، 3 من مراحل تقديم خدمة المسح الأمني الاحترافي وخدمة اختبار الاختراق الاحترافي المشار إليهما في المادتين 10، 11 وتستكمل باقي الأجور عند إنجاز المركز لباقي مراحل تقديم الخدمتين.

4. جميع المعلومات الخاصّة بالزّبون بما في ذلك نتائج الاختبارات هي معلومات سريّة ويحق للمركز استخدامها لغرض إجراء الدّراسات الإحصائية لتقييم واقع أمن المعلومات في سورية فقط.