



تعليمات ترخيص خدمة فحص الاختراقات لسنة ٢٠٢٦

صادرة بمقتضى المادة (١٥) من نظام ترخيص مقدمي خدمات الأمن السيبراني رقم (٧٦) لسنة ٢٠٢٤

المادة ١ - تسمى هذه التعليمات (تعليمات ترخيص خدمة فحص الاختراقات لسنة ٢٠٢٦) ويعمل بها من تاريخ نشرها في الجريدة الرسمية.

المادة ٢ - أ- يكون للكلمات والعبارات التالية حيثما وردت في هذه التعليمات المعاني المخصصة لها أدناه ما لم تدل القرينة على غير ذلك: -

- | | | |
|---------------------------|---|--|
| القانون | : | قانون الأمن السيبراني. |
| النظام | : | نظام ترخيص مقدمي خدمات الأمن السيبراني. |
| المركز | : | المركز الوطني للأمن السيبراني. |
| خدمة فحص الاختراقات | : | عملية تقييم واختبار مستوى الأمان والحماية لأنظمة وشبكات وتطبيقات متلقي الخدمة ، ومحاكاة الهجمات السيبرانية لتحديد الثغرات الأمنية ونقاط الضعف. |
| فريق فحص الاختراقات | : | مجموعة من الخبراء المعتمدين لدى مقدم الخدمة لتقديم خدمة فحص الاختراقات. |
| أصول المعلومات | : | جميع الموارد التي تحتوي على معلومات ذات قيمة للجهة بغض النظر عن شكلها أو وسيلة تخزينها أو نقلها بما في ذلك المعلومات المكتوبة والمطبوعة والإلكترونية، والأصول الرقمية التي تم إنشاؤها أو تخزينها أو معالجتها باستخدام أنظمة رقمية ويمكن الوصول إليها عبر شبكة الإنترنت أو الشبكات. |
| الأصول المستهدفة | : | أنظمة وشبكات وتطبيقات متلقي الخدمة التي تخضع لفحص الاختراقات. |
| الهجمات السيبرانية | : | الأنشطة الضارة التي تهدف إلى تعطيل أصول المعلومات أو تدميرها أو التلاعب بمحتواها أو الحد من قدرتها أو جمع المعلومات عنها أو الوصول إليها بقصد الإضرار بها دون إذن من مالكها. |
| فحص اختراق الصندوق الأسود | : | فحص الاختراق الذي يملك فيه منفذ الفحص معلومات وصلاحيات محدودة جداً عن الأصول المستهدفة. |
| فحص اختراق الصندوق الأبيض | : | فحص الاختراق الذي يملك فيه منفذ الفحص معلومات وصلاحيات محدودة حول الأصول المستهدفة بما في ذلك بيانات تسجيل الدخول إلى النظام. |

فحص اختراق الصندوق الأبيض : فحص الاختراق الذي يملك فيه منفذ الفحص جميع المعلومات والصلاحيات المتعلقة بالأصول المستهدفة
 رقم الوارد: ١١٧٩
 تاريخ: ٢٠٢٦/٠٣/٢٥





- برمجيات نصية : سلسلة من التعليمات البرمجية البسيطة أو المعقدة ، تكتب بلغات (سكريبت) برمجية خاصة وتستخدم في عمليات فحص الاختراق.
- الثغرات الأمنية: : نقاط الضعف في أصول المعلومات والتي يمكن استغلالها من قبل التهديدات.
- التهديد : أي حدث أو فعل أو حالة قد تؤدي إلى أضرار وتأثيرات وعواقب غير مرغوبة فيها على أصول المعلومات.
- نمذجة التهديدات : إعداد تصور أو نموذج عن التهديدات المحتملة التي قد تستهدف أصول المعلومات.
- المسوحات الأمنية : عمليات فحص تجري على أصول المعلومات بهدف الكشف عن ثغرات أمنية محتملة.
- الاستطلاع : عملية جمع أكبر قدر ممكن من المعلومات عن الأصول المستهدفة بقصد الاستفادة منها في تخطيط فحص الاختراقات وتنفيذه.

ب- تعتمد التعاريف الواردة في النظام حيثما ورد النص عليها في هذه التعليمات ما لم تدل القرينة على غير ذلك.

المادة ٣-أ- على مقدم طلب الحصول على ترخيص خدمة فحص الاختراقات الالتزام بما يلي: -

- ١- شروط ومتطلبات الترخيص المنصوص عليها في النظام.
- ٢- تقديم طلب الترخيص ورقياً أو إلكترونياً إلى المركز على النموذج المعتمد لهذه الغاية مرفقاً به ما يلي: -

- أ- الشهادات والوثائق التي تثبت تحقق الشروط المنصوص عليها في النظام.
- ب- الخبرات السابقة والمشاريع المنفذة من قبل الجهة طالبة الترخيص داخل المملكة وخارجها في مجال خدمة فحص الاختراقات.
- ج- وصف فني لآلية تقديم خدمة فحص الاختراقات وإجراءات العمل والأنظمة والتقنيات التي سيتم استخدامها لهذه الغاية في حال لم تكن لدى الجهة طالبة الترخيص خبرة سابقة.
- د- وثيقة تتضمن أسماء أعضاء فريق فحص الاختراقات مرفقة بها سيرهم الذاتية وصور عن الشهادات المصدقة والوثائق التي تثبت خبراتهم في تقديم خدمة فحص الاختراقات.
- هـ- شهادات اعتماد سارية المفعول صادرة عن المركز ، في حال سبق الحصول عليها تخول فريق الفحص تقديم الخدمة.

و- قائمة بأدوات وبرمجيات فحص الاختراقات التي سيستخدمها مقدم الخدمة عند تقديم الخدمة ، ومميزاتها، ومكان الاستضافة، على أن تكون هذه الأدوات والبرمجيات من مصدر موثوق.

ز- عقد العمل أو الاتفاقية الموقعة مع فريق فحص الاختراقات.

ح- أي شهادات اعتماد دولية سارية المفعول في مجال تقديم خدمة فحص الاختراقات حصل عليها مقدم طلب الترخيص.

ط- وصل مقبوضات بدل دراسة طلب تقديم خدمة فحص الاختراقات.

ي- أي معلومات أو مستندات أو وثائق أخرى يراها المركز ضرورية لإصدار قراره بشأن طلب الترخيص.





الجريدة الرسمية

ب- للمركز إجراء الكشف على مقر مقدم طلب الترخيص في العنوان المحدد في الطلب للتحقق من صحة المعلومات المقدمة وتقييم إمكاناته وقدراته.
المادة ٤- أ- يشترط أن تتوفر لدى مقدم الخدمة منهجية محددة لفحص الاختراقات على أن تتوافق مع ما يلي: -

- ١- الإطار الوطني للأمن السيبراني.
 - ٢- المعايير العالمية القياسية المتعلقة بفحص الاختراقات، بما في ذلك المنهجيات والإرشادات الصادرة عن الدليل الفني لاختبار وتقييم أمن المعلومات الصادر عن المعهد الوطني للمعايير والتكنولوجيا (١١٥-٨٠٠ NIST)، ومعيار تنفيذ فحص الاختراقات (PTES).
 - ٣- أي معايير أخرى يعتمد عليها المركز.
- ب- أن تتضمن منهجية فحص الاختراقات الجوانب التالية:-

- ١- التحضير والتخطيط لفحص الاختراقات.
- ٢- الاستطلاع وجمع المعلومات عن الأصول المستهدفة.
- ٣- تحديد الثغرات الأمنية وتحليلها وإمكانية استغلالها.
- ٤- استغلال الثغرات الأمنية ومحاكاة الهجمات الحقيقية.
- ٥- التوسع في الهجمات وفق مقتضى الحال.
- ٦- إزالة التعديلات التي تم إجراؤها على الأصول المستهدفة.
- ٧- إعداد التقارير وإصدارها.

ج- على مقدم الخدمة القيام بما يلي :-

- ١- تحديد وتخصيص تقنيات وأساليب فحص الاختراقات بما يتناسب مع نطاق الفحص ونوعه سواء كان فحص اختراق الصندوق الأسود أو فحص اختراق الصندوق الرمادي أو فحص اختراق الصندوق الأبيض، وبما يتوافق مع الأصول المستهدفة.
- ٢- الحصول على موافقات جميع الأطراف ذوات الصلة بمن في ذلك متلقي الخدمة وأي جهة أخرى مالكة لأحد الأصول المستهدفة قبل إجراء الفحص.
- ٣- تزويد المركز بأي شروحات أو تفاصيل عن طبيعة البرمجيات النصية (سكريبت) التي يتم تطويرها لتنفيذ الخدمة.
- ٤- الاستخدام الآمن والمشروع للبرمجيات والأدوات اللازمة لتقديم الخدمة، وعدم استخدامها بطرق غير مشروعة، وتحت طائلة المسؤولية القانونية.

المادة ٥ - يشترط في الأدوات والبرمجيات والأجهزة المستخدمة لتقديم خدمة فحص الاختراقات أن تكون ما يلي: -

- أ- مرخصة ومن مصدر موثوق ومنسجمة مع سياسة اعتماد منتجات الأمن السيبراني وأن تتناسب مع نوع الفحص والأصول المستهدفة.
- ب- قادرة على أداء مختلف مهام الفحص بما في ذلك الاستطلاع وجمع المعلومات، وإجراء المسوحات الأمنية، وتحليل الثغرات الأمنية، ونمذجة التهديدات، وتنفيذ مختلف الهجمات السيبرانية، واستغلال الثغرات الأمنية، والتوسع في الهجمات، وفقا لمقتضى الحال.





المادة ٦ أ- يشترط في أعضاء فريق فحص الاختراقات أن يكونوا من ذوي الخبرة والاختصاص والكفاءة على أن لا يقل عدد الفاحصين عن (٣) ثلاثة فاحصين ، ويتولى أحدهم رئاسة الفريق.

ب- يشترط في رئيس فريق فحص الاختراقات أن يكون :-

١- حاصلاً على الشهادة الجامعية الأولى كحد أدنى في مجال تكنولوجيا المعلومات أو في أي تخصص ذي صلة .

٢- حاصلاً على شهادة مهنية واحدة على الأقل من الشهادات المهنية المعتمدة لدى المركز، والمنشورة على الموقع الإلكتروني الخاص به، على أن يتم تحديثها باستمرار.

٣- لديه خبرة عملية في مجال الأمن السيبراني لا تقل عن (٥) خمس سنوات على أن تتضمن تنفيذ ما لا يقل عن (٥) خمسة مشاريع في مجال فحص الاختراقات.

ج- يُشترط في أعضاء فريق فحص الاختراقات ما يلي :-

١- الحصول على الشهادة الجامعية الأولى أو شهادة الدبلوم المتوسط، كحد أدنى من جامعة أو من مؤسسة أكاديمية معترف بها.

٢- الحصول على شهادة مهنية واحدة على الأقل معتمدة لدى المركز، ومنشورة على الموقع الإلكتروني الخاص به.

٣- لديهم خبرة عملية في مجال الأمن السيبراني لا تقل عن (٣) ثلاث سنوات وعلى أن تتضمن تنفيذ ما لا يقل عن مشروعين في مجال فحص الاختراقات.

المادة ٧- يلتزم مقدم الخدمة عند تقديم خدمة فحص الاختراقات بما يلي :-

أ- تصميم وتنفيذ برنامج تدريبي لتطوير مهارات الفريق بشكل مستمر.

ب- توقيع اتفاقية عدم الإفصاح عن المعلومات للحفاظ على سرية المعلومات والبيانات التي يطلع عليها، وعدم إفشائها أو مشاركتها مع أي طرف آخر أو نقلها خارج المملكة ما لم تنص التشريعات النافذة على غير ذلك.

ج- تقديم الخدمة بأمانة ونزاهة واحترافية، والامتناع عن تقديم معلومات غير صحيحة أو مضللة، وعدم استخدام الرخصة لغير الأغراض الممنوحة لأجلها، تحت طائلة المساءلة القانونية.

د- تزويد المركز بتقارير إحصائية سنوية تتضمن معلومات عن المستفيدين من الخدمة والخدمات المقدمة لهم ، وأي قضايا أو حوادث رئيسة ذوات صلة، وحفظ هذه التقارير بشكل آمن وضمان حماية الوصول إليها.

هـ- الامتناع عن التعاقد من الباطن لتقديم خدمة فحص الاختراقات إلا مع جهة مرخصة وفق الأصول من المركز.

و- الربط والتكامل مع أنظمة المركز ومنصاته بهدف إدارة وأتمتة الإجراءات وتزويد المركز بالمعلومات التي يحتاج إليها للقيام بمسؤولياته أو بالطريقة التي يراها المركز مناسبة.

ز- التعاون مع المركز خلال عمليات التدقيق التي يقوم بها وتزويده بأي معلومات أو وثائق يراها ضرورية.





الجريدة الرسمية

المادة ٨ - مع مراعاة أحكام هذه التعليمات، على مقدم الخدمة عند تقديم خدمة فحص الاختراقات، الالتزام بما يلي: -

- أ- المعايير المعتمدة والمنصوص عليها في كافة التشريعات النافذة والمتعلقة بالأمن السبيري، وبالإطار الوطني للأمن السبيري.
- ب- اتخاذ الإجراءات اللازمة لحماية أصول وأنظمة متلقي الخدمة، وعدم إلحاق الضرر بها أو إساءة استخدام المعلومات التي يحصل عليها، ووضع آلية لحماية نتائج الفحوصات وفق الممارسات الفضلى وتزويدها لمتلقي الخدمة، وعدم الاحتفاظ بها.
- ج- أن يكون جمع بيانات متلقي الخدمة ومعالجتها لأغراض محددة وصريحة تتعلق بتقديم الخدمة فقط.

- د- إعلام متلقي الخدمة بأي مخاطر أو تأثيرات محتملة قد تنتج عن تنفيذ فحص الاختراقات.
- هـ- إعلام متلقي الخدمة بأي مشاهدات أو ثغرات أمنية يتم رصدها خلال تقديم الخدمة، والتي قد تؤثر في سلامة متلقي الخدمة وأمنه وسمعته.
- و- تزويد متلقي الخدمة بتقرير يتضمن الملاحظات المكتشفة وتأثيرها، وأصول المعلومات المرتبطة بها، وتقييم درجة خطورتها، بالإضافة إلى التوصيات المناسبة لمعالجة هذه الملاحظات ونتائج الفحص والأدلة الداعمة.
- ز- عدم تضمين المعلومات الحساسة والسرية في التقارير، أو إخفائها لمنع استغلالها.
- ح- توثيق عملية فحص الاختراقات بما في ذلك توثيق الخطط والمنهجيات والنطاق والآليات المستخدمة، والأدوات والنتائج والأدلة، والاحتفاظ بها وفقاً للأحكام المنصوص عليها في هذه التعليمات.

- المادة ٩- يلتزم مقدم خدمة فحص الاختراقات بإبلاغ المركز عن أي من الحالات التالية: -
- أ- فقدان أي شرط من شروط أو متطلبات الترخيص المنصوص عليها في النظام.
- ب- أي تغيير يطرأ على فريق فحص الاختراقات، ويحظر على أي عضو جديد في فريق الفحص تقديم الخدمة إلا بعد الحصول على شهادة من المركز تخوله ذلك، وتبقى الشهادة مرتبطة بالعضو ولا تتأثر حال انتقاله من أحد مقدمي خدمة فحص الاختراقات إلى آخر.
- ج- أي تغيير يؤثر على قدرة وكفاءة مقدم الخدمة على تقديمها.
- د- الحصول على معلومات أثناء تقديم الخدمة تشير إلى قيام متلقي الخدمة بارتكاب مخالفة لأحكام القانون أو الأنظمة أو التعليمات الصادرة بمقتضاه.

- المادة ١٠- أ- على مقدم الخدمة الاحتفاظ بالمعلومات المتعلقة بخدمة فحص الاختراقات لمدة لا تقل عن (٣) ثلاث سنوات من تاريخ الانتهاء من تقديمها، على أن تتضمن ما يلي:-
- ١- أسماء ومعلومات فريق فحص الاختراقات الذين شاركوا في تقديم كل خدمة فحص الاختراقات.

٢- اسم ومعلومات متلقي الخدمة وتاريخ تقديم الخدمة ومدتها.

٣- التقنيات والأدوات المستخدمة والاختبارات المنفذة.

٤- أي معلومات أخرى يطلبها المركز.

- ب- على الرغم مما ورد في الفقرة (أ) من هذه المادة على مقدم الخدمة الاحتفاظ بالمعلومات المتعلقة بخدمة فحص الاختراقات وفقاً للسياسات والتشريعات ذات العلاقة واتخاذ التدابير اللازمة لحمايتها.





- المادة ١١ أ- على متلقي خدمة فحص الاختراقات الالتزام بما يلي: -
- ١- عدم التعاقد على تقديم الخدمة إلا مع مقدم خدمة فحص الاختراقات مرخص لهذه الغاية وفقاً لأحكام النظام والتعليمات الصادرة بمقتضاه.
 - ٢- التأكد من حصول فريق فحص الاختراقات على شهادات مصدقة من المركز قبل تقديم الخدمة.
 - ٣- تزويد مقدم الخدمة بالمعلومات والمتطلبات التي يحتاج إليها لتقديم الخدمة، وبما يتوافق مع نوع الفحص، بما في ذلك فحص اختبار الصندوق الأسود أو فحص اختبار الصندوق الرمادي أو فحص اختبار الصندوق الأبيض.
 - ٤- إبلاغ المركز عن أي إخلال من مقدم الخدمة بأي من المتطلبات المنصوص عليها في هذه التعليمات.
- ب- لمتلقي الخدمة استشارة المركز فنياً قبل توقيع اتفاقية خدمة مع أي من مقدمي خدمة فحص الاختراقات المرخصين.
- المادة ١٢ - لغايات تنفيذ أحكام هذه التعليمات، يتولى المركز القيام بما يلي: -
- أ- إجراء التدقيق السنوي على مقدمي الخدمة المرخصين للتحقق من امتثالهم لمتطلبات وشروط الترخيص ومعايير الخدمة.
 - ب- نشر وتحديث سجل عام بمقدمي الخدمة المرخصين على مواقعه الإلكترونية ومنصاته الرقمية، على أن يتضمن أسماء مقدمي الخدمة وأرقام تراخيصهم وحالة الترخيص (فعال، أو موقوف، أو ملغى)، وخبراتهم ومعلومات التواصل الخاصة بهم.
 - ج- توثيق أي إجراءات تأديبية أو عقوبات يتم اتخاذها بحق مقدم الخدمة المرخص في السجل العام.
- المادة ١٣ - لرئيس المركز وبناء على تنسيب المديرية المعنية بالترخيص، إيقاف ترخيص مقدم الخدمة أو تعديله أو إلغاؤه قبل انتهاء مدته أو عدم تجديده في أي من الحالات التالية: -
- أ- إذا أفشى أي وثائق أو معلومات أو بيانات سرية اطلع عليها بحكم عمله أو حصل عليها من متلقي الخدمة أو إذا ثبت عدم صحتها.
 - ب- إذا ارتكب أي مخالفة لأحكام القانون أو النظام أو هذه التعليمات ولم يعمل على إزالة المخالفة وأسبابها خلال مدة لا تزيد على (٦٠) ستين يوماً من تاريخ تبلغه بذلك خطياً أو إلكترونياً.
 - ج- إذا ارتكب ثلاث مخالفات خلال السنة من تاريخ ضبط أول مخالفة.
 - د- إذا فقد أي شرط من شروط الترخيص ولم يقم بتصويب أوضاعه خلال المدة المحددة في الفقرة (ب) من هذه المادة.
- هـ- بناء على طلب مقدم الخدمة.
- و- إذا ثبت للمركز عدم التزام مقدم الخدمة بمعايير تقديم خدمة فحص الاختراقات المعمول بها، وذلك بناء على شكوى من متلقي الخدمة.
- ز- إذا صدر بحقه حكم قضائي قطعي يقضي بإيقاف ترخيص مقدم الخدمة أو تعديله أو إلغاؤه.
- ح- إذا اقتضت المصلحة العامة ذلك.





الجريدة الرسمية

المادة ١٤ - أ- تكون مدة الترخيص لخدمة فحص الاختراقات ثلاث سنوات تبدأ من تاريخ إصدار الترخيص وتجدد لمدة مماثلة وفقاً لأحكام النظام.

ب- يحظر على المرخص له تحت طائلة المساءلة القانونية الاستمرار في تقديم خدمته في حال عدم تجديد الترخيص.

المادة ١٥ - كل من يخالف أحكام هذه التعليمات تطبق عليه أحكام المادة (١٦) من القانون، وتعليمات تحديد معايير مخالفات أحكام قانون الأمن السيبراني وضوابطها والإجراءات المستحقة عليها النافذة.

المجلس الوطني للأمن السيبراني





مركز عدالة للمعلومات القانونية
ADALEH Center for Legal Information
Info@Adaleh.Info

نظام ترخيص مقدمي خدمات الأمن السيبراني رقم 76 لسنة 2024
المنشور على الصفحة 6429 من عدد الجريدة الرسمية رقم 5962 بتاريخ 2024/11/17
صادر بموجب الفقرة 2 من المادة 6 من قانون الامن السيبراني رقم 16 لسنة 2019
صادر بموجب المادة 18 من قانون الامن السيبراني رقم 16 لسنة 2019

المادة 15

يصدر المجلس التعليمات اللازمة لتنفيذ أحكام هذا النظام بما في ذلك التعليمات النازمة لكل خدمة من خدمات الأمن السيبراني والإجراءات والمتطلبات اللازمة للعمل بها على أن تتضمن معايير تقديم خدمات الأمن السيبراني والشروط والمؤهلات الواجب توافرها في مقدمي الخدمة.

22/10/2024

