هيئة الاتصالات وتقنية المعلومات
Communications & Information Technology Commission

إجراءات التعامل مع حوادث الأمن السيبراني في قطاع الاتصالات وتقنية المعلومات والبريد

الإصدار: ١,١

التاريخ: نوفمبر ٢٠٢٠م

جدول المحتويات

١. مقدمة

وفقًا لنظام الاتصالات ولائحته التنفيذية وتنظيم هيئة الاتصالات وتقنية المعلومات وما تضمنته من صلاحيات لهيئة الاتصالات وتقنية المعلومات، ومنها تلك المتعلقة بحماية المصلحة العامة ومصالح المستخدمين والمحافظة على سرية الاتصالات وأمن المعلومات، وسعياً من الهيئة إلى رفع مستوى النضج بالأمن السيبراني في قطاع الاتصالات وتقنية المعلومات والبريد في المملكة، ورفع الثقة في مقدمي الخدمات بالقيام بكافة التدابير اللازمة، أعدت الهيئة وثيقة (إجراءات التعامل مع حوادث الأمن السيبراني في قطاع الاتصالات وتقنية المعلومات والبريد)؛ وللتأكيد على تطبيق الإجراءات اللازمة للوقاية والتصدي للأخطار والحوادث الأمنية المتعلقة بالأمن السيبراني.

٢. تعريفات

إن الكلمات والعبارات التي تم تعريفها في نظام الاتصالات ولائحته التنفيذية وأنظمة الهيئة الأخرى سيكون لها نفس المعنى عند استخدامها في هذه الوثيقة والملاحق المرفقة بها، كما يكون للكلمات والتعابير التالية المعاني المقترنة بها ما لم يقتض السياق خلاف ذلك:

الهيئة: هيئة الاتصالات وتقنية المعلومات.

مقدم خدمة: مزود خدمات الاتصالات أو تقنية المعلومات أو البريد في قطاع الاتصالات وتقنية المعلومات والبريد في المملكة العربية السعودية.

جهة الاستجابة: الجهة المقدمة لخدمات الاستجابة لحوادث الأمن السيبراني.

الأمن السيبراني: هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.

حادثة أمن سيبراني: أي انتهاك أو حدث أدى فعلياً إلى اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع لشبكات أو انظمة تقنية المعلومات أو انظمة التقنيات التشغيلية أو أحد مكوناتها من اجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات ويشمل ذلك تسريب البيانات الشخصية أو الحساسة.

تسريب البيانات: الإفصاح عن البيانات، أو الحصول عليها، أو تمكين الوصول لها دون تصريح أو سند نظامي، سواءً بقصد أو بغير قصد.

حادثة حرجة: الحادثة ذات الأثر العالي على المستوى الوطني أو على مستوى القطاع.

التقييم الأولي لحادثة الأمن السيبراني: عملية تحليل سريع للحادثة تهدف إلى التأكد من صحة الحادثة وتحديد نوعها وتصنيفها، وجمع مؤشرات الاختراق الأولية، وتحديد أولي لنطاق التأثر من الحادثة.

الاستجابة لحوادث الأمن السيبراني: عملية التعامل مع الحادثة، خلال الوقت المتوقع، بطريقة منهجية تهدف إلى تقليل مستوى تأثير الحادثة على مقدم الخدمة إلى أقل

مستوى ممكن مع تحديد ومشاركة مؤشرات الاختراق والادلة الرقمية التفصيلية واعداد وايصال التقارير والتوصيات الخاصة بالحادثة.

٣. أحكام عامة

١. يخضع لتطبيق هذه الإجراءات جميع مقدمي خدمات الاتصالات وتقنية المعلومات والبريد في المملكة العربية السعودية.
٢. مقدم الخدمة مسؤول عن اتخاذ كافة التدابير اللازمة لحماية أصوله المعلوماتية، والتحقق بشكل دوري من جاهزيته لمنع وقوع حوادث الأمن السيبراني.
٣. مقدم الخدمة مسؤول عن الاستجابة لحوادث الأمن السيبراني عند وقوعها.
٤. يجب على مقدم الخدمة الالتزام بجميع الإجراءات الواردة في هذه الوثيقة وملحقاتها وفي حال مخالفتها فإنه يتم التعامل مع المخالفات وفق أنظمة الهيئة، ولا يعفي مقدم الخدمة من المسؤولية في حال تعاقده مع أطراف أخرى.
٥. لا تخل هذه الإجراءات بأي إجراءات مضمنه في وثيقة نظامية صادرة من الهيئة أو من الجهات الأخرى ذات العلاقة.

٤. إجراءات التعامل مع حوادث الأمن السيبراني:

٤,١ إجراءات التعامل مع حوادث الأمن السيبراني من قبل مقدم الخدمة:

يجب على مقدم الخدمة، القيام بالآتي:

١. التسجيل لدى الهيئة وتحديد بيانات التواصل من خلال تعبئة النموذج الموضح بالملحق (أ- نموذج التسجيل لدى الهيئة)، كما يجب تحديث البيانات في حال تم عليها إجراء أي تغيير أو تعديل.
٢. إبلاغ الهيئة فورًا عند وقوع حادثة أمن سيبراني عبر قنوات الاتصال مع الهيئة في حوادث الأمن السيبراني الموضح بالملحق (ب- قنوات الاتصال مع الهيئة في حوادث الأمن السيبراني)، ومن ثم تقديم كل المعلومات الكافية عن الحادثة لفريق الهيئة وتعبئة النموذج الملحق (ج - نموذج الابلاغ عن حادثة الأمن السيبراني).
٣. تحديد ضابط اتصال للإجابة على استفسارات الهيئة وتزويدها بكافة المعلومات المطلوبة –عند الحاجة- طيلة فترة الاستجابة لحادثة الأمن السيبراني.
٤. إجراء التقييم الأولي لحادثة الأمن السيبراني وتزويد الهيئة بنتائجه، وقد تطلب الهيئة من مقدم الخدمة إعادة إجراء التقييم الأولي لحادثة الأمن السيبراني في حال عدم كفاية المعلومات وتحليل المخاطر المترتبة على الحادثة.
٥. تزويد الهيئة بتقرير نهائي عن الحادثة خلال فترة ٢٠ يوم عمل كحد اقصى من انتهاء عملية الاستجابة، كما هو موضح في الملحق (د-التقرير النهائي لحادثة الأمن السيبراني).
٦. الالتزام بالإجراءات التصحيحية المبلغة له من قبل الهيئة خلال المدة الزمنية المحددة.
٧. فيما يخص حادثة الأمن السيبراني، يسمح لمقدم الخدمة التواصل فقط مع الجهات ذات العلاقة.
٨. في حال قامت الهيئة بتكليف جهة استجابة، على مقدم الخدمة التعاون التام وتسهيل أعمال ومهام الهيئة وجهة الاستجابة المكلفة بما فيها السماح لزيارة موقع حادثة الأمن السيبراني والتزويد بالمعلومات والتقارير اللازمة.
٩. إذا دعت الحاجة لذلك، وبعد توجيه الهيئة، يقوم مقدم الخدمة على نفقته الخاصة بإصدار بيان توضيحي عن حادثة الأمن السيبراني.
١٠. إذا كان للحادثة تأثير على جهات أخرى ذات علاقة، مثل مستخدمي خدمات مقدم الخدمة، فيجب على مقدم الخدمة إشعار تلك الجهات بذلك وتزويدهم -في حال دعت

الحاجة- بتقرير موجز عن الحادثة. ويتم إحاطة الهيئة بذلك وتشمل الإحاطة تفاصيل الاشعار.

٤,٢ إجراءات التعامل مع حوادث الأمن السيبراني من قبل جهة الاستجابة:

١. تقوم جهة الاستجابة بالتواصل مع مقدم الخدمة وطلب المعلومات المطلوبة وزيارة موقع الحادثة، وتزويد الهيئة ومقدم الخدمة بالتقارير الدورية أثناء فترة الاستجابة لحوادث الأمن السيبراني، وتقديم التقرير النهائي وفق ما هو بموضح بالملحق (د - التقرير النهائي لحادثة الأمن السيبراني).
٢. تقوم جهة الاستجابة بتزويد الهيئة ومقدم الخدمة بالتقارير الدورية أثناء خدمة الاستجابة والتقرير النهائي للحادثة، كما في ملحق (د - التقرير النهائي لحادثة الأمن السيبراني).

٤,٣ إجراءات التعامل مع حوادث الأمن السيبراني من قبل الهيئة:

١. للهيئة إعادة تقييم حادثة الأمن السيبراني -إذا دعت الحاجة- وتصنيفها بأنها حادثة حرجة مما يستدعي التعامل معها كالتالي:
   ١,١. للهيئة -إذا دعت الحاجة- تكليف جهة استجابة للقيام بالاستجابة لحوادث الأمن السيبراني وإشعار مقدم الخدمة بذلك.
   ١,٢. تقوم الهيئة بتعيين فريق داخلي لمتابعة الحادثة وتنظيم التواصل بين مقدم الخدمة وجهة الاستجابة.
٢. للهيئة -وفق تقديرها المطلق- مشاركة نتائج التقارير الأولية أو النهائية أو جزء منها المعدة من مقدم الخدمة مع الجهات ذات العلاقة مع الحفاظ على خصوصية وسرية المعلومات الواردة في تلك التقارير.
٣. للهيئة القيام بأعمال التفتيش والتحقيق في موقع حادثة الأمن السيبراني، وذلك وفق أنظمة الهيئة.
٤. للهيئة طلب تنفيذ إجراءات تصحيحية من مقدم الخدمة نتيجة لحادثة أمن سيبراني، مع تحديد المدة الزمنية المطلوبة لإتمامها.
٥. للهيئة -وفق تقديرها المطلق- مشاركة الدروس المستفادة من حادثة أمن السيبراني مع الجهات الاخرى في القطاع أو خارجه مع المحافظة على خصوصية ومعلومات مقدم الخدمة.
٦. للهيئة -وفق تقديرها المطلق- أن تصدر بيان توضيحي عن حادثة أمن السيبراني.

٥. الملاحق

٥,١ ملحق (أ): نموذج التسجيل لدى الهيئة

ملاحظة:

- على جميع الجهات مراعاة أن تصنيف هذا النموذج بعد تعبئته هو مقيد-معلومات سرية.
- يمكن تحميل النماذج من خلال موقع الهيئة على الرابط التالي:

https://www.citc.gov.sa/cybersecurity

هيئة الاتصالات وتقنية المعلومات
Communications & Information Technology Commission

خدمة الإنذار والابلاغ عن حوادث الأمن السيبراني
نموذج التسجيل
(تسجيل جديد / تحديث بيانات)

معلومات الجهة			
اسم الجهة المستفيدة		المدينة	
نوع الطلب	☐ تسجيل جديد ☐ تحديث البيانات	التاريخ	/ / 20م
نوع الجهة	☐ مرخص	نوع الترخيص	
		رقم الترخيص	
	☐ غير مرخص		

معلومات الاتصال للجهة المستفيدة (أمن المعلومات)		
	المدير الإداري	المشرف الإداري
الاسم		
البريد الالكتروني		
الجوال * للاتصال او استلام الرسائل النصية		
هاتف العمل		

	المسؤول الفني	
الاسم		
البريد الالكتروني * يفضل استخدام مجموعة بريدية مثل Soc-group@company.com.sa		
الجوال * للاتصال او استلام الرسائل النصية		
هاتف العمل		

معلومات فنية			
الموقع على الانترنت		العنوان الشبكي للموقع	
مجموعة العناوين الشبكية على الانترنت			
خدمات ISP	هل لدى الجهة رخصة مقدم خدمات انترنت ISP ☐ نعم ☐ لا هل تقدم الجهة عناوين شبكية (IPs) لجهات أخرى ☐ نعم ☐ لا	ASN	

نؤكد على أن جميع البيانات المذكورة صحيحة وتخص المنشأة المذكورة أعلاه في حال طرأ عليها أي تغير لاحقاً نلتزم بتحديث البيانات لدى فريق هيئة الاتصالات وتقنية المعلومات.

المدير الإداري: التوقيع:

٥,٢ ملحق (ب): قنوات الاتصال مع الهيئة في حوادث الأمن السيبراني

قنوات إبلاغ الهيئة	
بريد إلكتروني	incident@citc.gov.sa
رقم الهاتف	011-461-9999

٥,٣ ملحق (ج): نموذج الابلاغ عن حادثة الأمن السيبراني

ملاحظة:

- هذا النموذج يمثل الحد الادنى من المعلومات المطلوبة خلال عملية الابلاغ عن حادثة، وعلى جميع الجهات مراعاة أن تصنيف هذا النموذج بعد تعبئته هو مقيد - معلومات سرية-.
- يمكن تحميل النماذج من خلال موقع الهيئة على الرابط التالي:
  https://www.citc.gov.sa/cybersecurity

هيئة الاتصالات وتقنية المعلومات
Communications & Information Technology Commission

TLP: RED

نموذج الابلاغ عن حادثة الأمن السيبراني

v1.1

بيانات مقدم الخدمة			
اسم مقدم الخدمة			
اسم ضابط الاتصال		المسمى الوظيفي:	
الهاتف			
البريد الإلكتروني			

بيانات الحادثة			
نوع الحادثة:	حجب الخدمة (DoS/DDoS) ☐		
	هجوم او إصابة من برمجيات ضارة ☐		
	هجوم التصيد الالكتروني ☐		
	اختراق موقع الويب أو تشويهه ☐		
	تسريب بيانات شخصية أو حساسة ☐		
	هجوم داخلي ☐		
	اخرى:		
تاريخ الحادثة:		وقت الحادثة:	
هل تم التعامل مع الحادثة؟		وقت التعامل مع الحادثة:	
مستوى تأثير الحادثة:	حرج ☐ عالي ☐ متوسط ☐ منخفض ☐		
نوع التاثير:	مالي ☐		
	حجب الخدمة ☐		
	سمعة الشركة ☐		
	تسريب بيانات: بيانات شخصية ☐ بيانات حساسة ☐ غيرها ☐		
	وصف أنواع البيانات:		
	عدد السجلات المسربة:		
	اخرى:		
جهات اخرى تم ابلاغها؟			
هل يوجد أنظمة متضررة؟ إذا كانت الإجابة نعم، يرجى ذكرها			
وصف الحادثة:			
الإجراءات التي تم اتخاذها:			

٥,٤ ملحق (د): التقرير النهائي لحادثة الأمن السيبراني

يمكن تحميل النماذج من خلال موقع الهيئة على الرابط التالي:

https://www.citc.gov.sa/cybersecurity