



الرقم : ١٦٣٣ / ١ / ٢٨
التاريخ : ١٤٤٢ / ٦ / ١٣ هـ
الموافق : ٢٠٢١ / ١ / ٢٦ م

تعميم إلى شركات التمويل الأصغر العاملة في المملكة

تحية طيبة وبعد،،،

بالإشارة إلى تعليمات التكيف مع المخاطر السيبرانية رقم (١٩٨٤/١/٢٦) تاريخ ٢٠١٨/٢/٦ وعملاً بأحكام المادة (٤٩) من هذه التعليمات، فإننا إذ نؤكد على ضرورة إخطار البنك المركزي الأردني حال اكتشافكم لأي حدث سيبراني أو أي محاولة للهجوم السيبراني - سواء كانت ناجحة أو تم التصدي لها- لنعلمكم بضرورة تزويدنا بتفاصيل الأحداث السيبرانية وأثارها وإجراءات الاستجابة والإجراءات الوقائية التي تم اتخاذها وبحسب النموذج المرفق وذلك من خلال إرساله للبريد الإلكتروني أدناه:

MFISCB.Supervision@cbj.gov.jo

وبهذا السياق تجدون مرفقاً "دليل تعبئة نموذج الإخطار عن الاحداث السيبرانية" كدليل ارشادي لتعبئة البيانات المطلوبة في ذلك النموذج.

وتفضلوا بقبول فائق الاحترام،،،

المخافظ
د. زياد فريز

نموذج الإخطار عن الأحداث السيبرانية

اسم الشركة	
------------	--

وقت و تاريخ وقوع الحدث	وقت و تاريخ اكتشاف الحدث	وقت و تاريخ تصحيح الحدث

معلومات ضابط الارتباط	
اسم ضابط الارتباط	
رقم الهاتف	
رقم الموبايل	
تفاصيل الحدث	
نوع الحدث	
مكونات البنية التحتية المتأثرة بالحدث	
موقع الحدث	
تصنيف خطورة الحدث	
الأسباب المؤدية لوقوع الحدث	
هل حدث هذا الحدث من قبل؟ (نعم أو لا)	
الجهة أو الدائرة المعنية بإدارة الحدث	
تقييم تأثير الحدث	
تأثير الحدث على عمل الشركة من حيث توافرية الخدمات	
القنوات المتأثرة بالحدث	
تأثير الحدث على أنظمة الشركة وتقنياتها (انقطاع عمل أنظمة حرجية، انقطاع في أي من مكونات البنية التحتية)	
تأثير الحدث على نظام معلومات الشركة (السرية والنزاهة والتوافر)	
تأثير الحدث على الوضع المالي للشركة وموقعها في السوق	
تأثير الحدث على أصحاب المصلحة مثل (عملاء الشركة ، الشركاء، ...)	
إجراءات الاستجابة والتعافي	
إجراءات الاستجابة للحدث	

	إجراءات تصحيحية لمسبب الحدث
	الاجراءات الوقائية
	حالة الحدث (تم إغلاقه ، جاري العمل عليه)

دليل تعبئة نموذج الإخطار عن الأحداث السيرانية

وقت و تاريخ وقوع الحدث	: الوقت والتاريخ الذي وقع به الحدث ويكون على الهيئة (دقيقة : ساعة، يوم/شهر/سنة)
وقت و تاريخ اكتشاف الحدث	: الوقت والتاريخ الذي تم اكتشاف الحدث به ويكون على الهيئة (دقيقة : ساعة، يوم/شهر/سنة)
وقت و تاريخ تصحيح الحدث	: الوقت والتاريخ الذي تم تصحيح المشكلة به أو المتوقع تصحيحها به ويكون على الهيئة (دقيقة : ساعة، يوم/شهر/سنة)

معلومات ضابط الارتباط

اسم ضابط الارتباط	: اسم ضابط الارتباط المخول والمسؤول أمام البنك المركزي عن تزويد البنك المركزي بنموذج الإخطار عن الأحداث السيبرانية (أصيل أو بديل) على أن يكون ممن تم تزويد البنك المركزي بأسمائهم مسبقا
رقم الهاتف	: رقم هاتف الشركة والرقم الفرعي لضابط الارتباط المسمى
رقم الموبايل	: رقم الموبايل لضابط الارتباط المسمى

تفاصيل الحدث

نوع الحدث	: نوع الحدث الذي أثر على الشركة ، وعلى سبيل المثال لا الحصر (Ransomware, Data breach, DDOS,...)
مكونات البنية التحتية المتأثرة بالحدث	: مكونات البنية التحتية الخاصة بالشركة والمتأثرة بالحدث ، وعلى سبيل المثال لا الحصر (Network Level, Hardware Level, Database Level, Server Level, Application Level, OS Level,)

موقع الحدث	: الموقع الفيزيائي المتأثر بالحدث (Main Site, DR Site, HA Site)
تصنيف خطورة الحدث	: تصنيف خطورة الحدث (Crisis, Major, Minor, Negligible)
الأسباب المؤدية لوقوع الحدث	: ذكر السبب في وقوع الحدث في حال معرفة الشركة له، على سبيل المثال (Unpatched Operating Systems,)
هل حدث هذا الحدث من قبل؟	: الإجابة بنعم أو لا بما يخص تكرار الحدث من قبل
الجهة أو الدائرة المعنية بإدارة الحدث	: الدائرة أو الجهة أو الطرف الثالث المسؤول عن متابعة الحدث ومعالجته على سبيل المثال لا الحصر (دائرة تكنولوجيا المعلومات، دائرة أمن المعلومات....)

تأثير الحدث على عمل الشركة من حيث توافرية الخدمات	: هل أدى الحدث السبيرياني في انقطاع أي من خدمات الشركة المقدمة؟ مع ذكرها
القنوات المتأثرة بالحدث	: ما هي القنوات المتأثرة بالحدث السبيرياني؟ على سبيل المثال (Online, Mobile Application,...)
تأثير الحدث على أنظمة الشركة وتقنياتها (انقطاع عمل أنظمة حرجية، انقطاع في أي من مكونات البنية التحتية)	: تأثير الحدث على أنظمة الشركة وشبكاتها وبينتها التحتية والمصنفة كحساسة.

هل تأثر نظام المعلومات في الشركة بالحدث السيبراني من ناحية السرية والنزاهة والتوافر (Confidentiality, Integrity, Availability)؟ وما مدى التأثير؟	تأثير الحدث على نظام معلومات الشركة (السرية والنزاهة والتوافر)
مدى تأثر الشركة بالحدث من الناحية المالية وسمعتها ووجودها في السوق	تأثير الحدث على الوضع المالي للشركة وموقعها في السوق
مدى تأثير الحدث على أصحاب المصالح (Stakeholders)، على سبيل المثال لا الحصر (Customers, Service providers, Business partners,)	تأثير الحدث على أصحاب المصلحة مثل (عملاء الشركة، الشركاء، ...)

ما الإجراءات الاستجابية والتعافي	الإجراءات الاستجابية للحدث
ما الإجراءات التي تم اتباعها فور اكتشاف الحدث للحد من انتشاره وتوسعه وإلحاق المزيد من الضرر؟	إجراءات تصحيحية لمسبب الحدث
ما الإجراءات التي تم اتباعها لاحقاً لاكتشاف الحدث من ناحية تصحيح السبب أو العطل الذي أدى إلى وقوع الحدث؟	الإجراءات الوقائية
هل تم الانتهاء من تصحيح ومعالجة المشكلة؟ أم ما زال العمل مستمر عليها؟	حالة الحدث (تم إغلاقه، جاري العمل عليه)