مرسوم بتحديد إجراءات حماية نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية

تم نسخ المرسوم رقم 2.15.712 صادر في 12 من جمادى الآخرة 1437 (22 مارس 2016) بتحديد إجراءات حماية نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية بمقتضى المادة 45 من المرسوم رقم 2.21.406 بتاريخ 4 ذي الحجة 1442 (15 يوليو 2021) بتطبيق القانون رقم 05.20 المتعلق بالأمن السيبراني، الجريدة الرسمية عدد 7011 بتاريخ 29 ذو الحجة 1442 (9 أغسطس 2021)، ص 5979.

مرسوم رقم 2.15.712 صادر في 12 من جمادى الآخرة 1437 (22 مارس 2016) بتحديد إجراءات حماية نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية[1]

رئيس الحكومة،

بناء على الظهير الشريف رقم 1.12.04 الصادر في 14 من ربيع الأول 1433 (7 فبراير 2012) بتفويض السلطة فيما يتعلق بإدارة الدفاع الوطني؛

وعلى المرسوم رقم 2.11.508 الصادر في 22 من شوال 1432 (21 سبتمبر 2011) بإحداث اللجنة الاستراتيجية لأمن نظم المعلومات ولا سيما المادة الأولى منه؛

وعلى المرسوم رقم 2.82.673 الصادر في 28 من ربيع الأول 1403 (13 يناير 1983) بتنظيم إدارة الدفاع الوطني وإحداث المديرية العامة لأمن نظم المعلومات كما وقع تغييره وتتميمه بالمرسوم رقم 2.11.509 بتاريخ 22 من شوال 1432 (21 سبتمبر 2011) ولا سيما الفصل 4-7 منه؛

وعلى منشور رئيس الحكومة رقم 3/2014 الصادر في 8 جمادى الأولى 1435 (10 مارس 2014) المتعلق بالتوجيهات الوطنية لأمن نظم المعلومات؛

وبعد المداولة في مجلس الحكومة المنعقد بتاريخ 3 ربيع الآخر 1437 (14 يناير 2016)؛

وبعد المداولة في المجلس الوزاري المنعقد بتاريخ 26 من ربيع الآخر 1437 (6 فبراير 2016)،

رسم ما يلي:

المادة الأولى

يقصد في مفهوم هذا المرسوم:

بنيات تحتية ذات أهمية حيوية: التجهيزات والمنشآت والأنظمة الضرورية للحفاظ على استمرارية الوظائف الحيوية للمجتمع والصحة والأمن والسلامة والتقدم الاقتصادي أو الاجتماعي حيث أن أي ضرر أو إتلاف أو ضياع قد يصيبها يترتب عنه خلل في هذه الوظائف.

قطاع الأنشطة ذات الأهمية الحيوية: يتكون من أنشطة تساهم في تحقيق نفس الهدف والتي لها علاقة إما بإنتاج وتوزيع السلع أو الخدمات الضرورية لتلبية الحاجيات الأساسية لعيش المواطنين، أو ممارسة الدولة لصلاحيتها أو سير النشاط الاقتصادي أو الحفاظ على القدرات الأمنية للدولة، على اعتبار أن هذه الأنشطة غير قابلة للاستبدال أو التعويض، أو نظرا للخطر الذي قد تشكله على الساكنة.

1- الجريدة الرسمية عدد 6456 بتاريخ 6 رجب 1437 (14 أبريل 2016)، ص 3175.

معلومة حساسة: كل معلومة من شأن تعريضها لأي مساس أو تسريب أو إتلاف قد يلحق ضررا بالسير العادي أو يشكل خطرا على الرصيد المعلوماتي للبنية التحتية ذات الأهمية الحيوية.

نظام معلومات حساسة لبنية تحتية ذات أهمية حيوية: نظام يعالج معلومات من شأن المساس بسريتها أو بسلامة محتواها أو بتوافرها أن يعرقل استمرارية السير العادي للبنية التحتية ذات الأهمية الحيوية.

السلطة المختصة: السلطة الحكومية المكلفة بإدارة الدفاع الوطني (المديرية العامة لأمن نظم المعلومات).

المادة 2: مجال التطبيق

يسري هذا المرسوم على الإدارات والمؤسسات العمومية والمقاولات العمومية والهيئات المتوفرة على اعتماد أو ترخيص مسلم من طرف الدولة لمزاولة نشاط منظم والمعتبرة كبنيات تحتية ذات أهمية حيوية والتي تتوفر على نظم معلومات حساسة ويشار إليها أدناه بعبارة «هيئة».

المادة 3: تحديد قطاعات الأنشطة والبنيات التحتية ذات الأهمية الحيوية

تحدد لائحة قطاعات الأنشطة ذات الأهمية الحيوية والسلطات الحكومية والمؤسسات العمومية والأشخاص الاعتباريين من أشخاص القانون العام، المشرفين على تنسيق القطاعات في ملحق هذا المرسوم.

يتم تحديد البنيات التحتية ذات الأهمية الحيوية المشار إليها في المادة 2 من هذا المرسوم لكل قطاع أنشطة ذات أهمية حيوية من طرف السلطة الحكومية أو المؤسسة العمومية أو الشخص الاعتباري من أشخاص القانون العام المشرف على تنسيق القطاع.

يجب أن تحظى قائمة هذه البنيات التحتية بالسرية وأن يخضع محتواها للمراجعة مرة في السنة على الأقل.

المادة 4: تحديد وجرد نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية

تقوم كل هيئة، اعتمادا على نتائج تحليل المخاطر، بإعداد دليل يتضمن لوائح نظم المعلومات الحساسة كما تم تعريفها في المادة الأولى أعلاه، وتبليغه إلى السلطة المختصة داخل أجل أقصاه 12 شهرا من تاريخ نشر هذا المرسوم في الجريدة الرسمية.

تحدد السلطة المختصة كيفيات تصنيف نظم المعلومات.

يجب على كل هيئة أن تقوم بإبلاغ السلطة المختصة بكل تغيير يطرأ على لائحة نظم معلوماتها الحساسة.

يخضع دليل ولوائح نظم المعلومات الحساسة للبنيات التحتية ذات الأهمية الحيوية للسرية.

يجب على كل هيئة أن تعين مسؤولا عن أمن نظم المعلومات، يشكل نقطة للاتصال مع السلطة المختصة.

المادة 5: تطبيق التوجيهات الوطنية لأمن نظم المعلومات وقواعد الحماية القطاعية

تسهر كل هيئة على مطابقة نظم معلوماتها الحساسة مع القواعد المنصوص عليها في التوجيهات الوطنية لأمن نظم المعلومات ومعايير السلامة المقررة في هذا الشأن من طرف السلطة المختصة والمطبقة على نظم معلومات البنيات التحتية ذات الأهمية الحيوية.

يمكن للسلطة المختصة أن تضع قواعد سلامة خاصة تتعلق بقطاع معين أو نوع من أنشطة الهيئة. وتقوم هذه السلطة بإبلاغ الهيئات المعنية بآجال تطبيقها.

يمكن تمديد تطبيق قواعد السلامة المحددة من طرف السلطة المختصة إلى القطاع الخاص في إطار الاتفاقيات المبرمة مع هذا القطاع.

المادة 6: التبليغ عن حوادث الأمن المعلوماتي ومعالجتها

يجب على كل هيئة أن توفر الوسائل الضرورية للمراقبة والتصدي للهجمات المعلوماتية. وتستغل المعطيات التقنية المحصل عليها بواسطة هذه الوسائل من طرف مركز اليقظة والرصد والتصدي للهجمات المعلوماتية التابع للمديرية العامة لأمن نظم المعلومات، المشار إليه بعده بالمركز.

يجب على كل هيئة إبلاغ المركز، داخل أجل لا يتعدى ثمان وأربعين (48) ساعة، بالمعلومات المتعلقة بالحوادث الجسيمة التي يتعرض لها أمن نظم معلوماتها الحساسة أو السير العادي لهذه النظم. كما يجب عليها إمداد المركز بالمعلومات الإضافية التي يطلبها حول الحادث.

تحدد السلطة المختصة المعلومات التي يجب إبلاغها وكيفيات إرسالها وكذا أنواع الحوادث المعنية.

يجب على السلطة المختصة، في حالة وقوع حادث جسيم، أن تبعث خلال الشهر الموالي إلى الهيئة المعنية والسلطة الحكومية أو المؤسسة العمومية أو الشخص الاعتباري من أشخاص القانون العام المشرف على تنسيق قطاع الأنشطة ذات الأهمية الحيوية تقريرا تركيبيا يتضمن المعلومات المحصل عليها والتوصيات المستخلصة من هذه المعلومات.

من أجل مواجهة الأزمات الخطيرة التي تهدد أو تمس أمن نظم المعلومات الحساسة، يمكن للسلطة المختصة أن تحدد التدابير التي يتعين على الهيئات تنفيذها.

تحافظ السلطة المختصة على سرية المعلومات المحصل عليها من الهيئات المشار إليها في المادة 2 أعلاه، في إطار تطبيق مقتضيات هذه المادة.

المادة 7: افتحاص أمن نظم المعلومات

تقوم الهيئات المنصوص عليها في المادة 2 أعلاه، طبقا لبرنامج الافتحاص الذي تضعه السلطة المختصة، بإخضاع أنظمة معلوماتها الحساسة لافتحاص تنجزه المديرية العامة لأمن نظم المعلومات أو متعهدون خواص معتمدون من طرف السلطة المختصة.

تحدد بقرار لرئيس الحكومة شروط اعتماد المتعهدين الخواص لافتحاص نظم معلومات الهيئة وكذا كيفيات إجراء الافتحاص.

تقوم السلطة المختصة بتبليغ السلطة الحكومية أو المؤسسة العمومية أو الشخص الاعتباري من أشخاص القانون العام المشرفين، على تنسيق قطاع الأنشطة ذات الأهمية الحيوية برنامج مهمات افتحاص أمن نظم معلومات. ويحدد هذا البرنامج، حسب طبيعة العمليات الواجب اتخاذها، إن كان هذا الافتحاص سينجز من طرف المديرية العامة لأمن نظم المعلومات أو من طرف المتعهدين الخواص المعتمدين من طرف السلطة المختصة.

عند إجراء الافتحاصات من طرف متعهدين خواص معتمدين، تتحمل الهيئات المعنية تكاليف هذه العمليات من ميزانيتها الخاصة وفي جميع الأحوال، تجرى الافتحاصات تحت إشراف السلطة المختصة.

تقوم المديرية العامة لأمن نظم المعلومات أو المتعهد الخاص المعتمد، عند متم كل افتحاص، بإعداد تقرير يتضمن الملاحظات والتوصيات المتعلقة بمستوى أمن نظم معلومات الهيئة المعنية ومدى احترامها لقواعد ومعايير السلامة المنصوص عليها في هذا المرسوم.

في حالة إجراء الافتحاص من طرف متعهد خاص معتمد، تقوم الهيئة المعنية بتبليغ نتائج هذه العملية للمديرية العامة لأمن نظم المعلومات.

تقوم المديرية العامة لأمن نظم المعلومات بتبليغ نتائج تقرير الافتحاص للهيئة المعنية والسلطة الحكومية أو المؤسسة العمومية أو الشخص الاعتباري من أشخاص القانون العام المشرف على قطاع الأنشطة ذات الأهمية الحيوية.

يجب على الهيئات المعنية وضع برنامج عمل لتنفيذ التوصيات الواردة في تقارير الافتحاص وتبليغه للمديرية العامة لأمن نظم المعلومات قصد تتبع تطبيقه.

المادة 8: مخطط ضمان استمرارية واستئناف الأنشطة

يجب على كل هيئة أن تعد مخططا لضمان استمرارية واستئناف الأنشطة يتضمن مجموعة إجراءات وحلول بديلة لتخفيف وقع انقطاعات الأنشطة وضمان السير العادي لهذه الأنشطة وحماية الوظائف المهمة والحساسة من الآثار الناجمة عن اختلالات نظم المعلومات، أو الكوارث، وضمان استئناف عمل هذه الوظائف في أقرب الآجال.

يجب على كل هيئة أن تعد مخططا تقنيا لضمان استمرارية واستئناف الأنشطة متضمنا مجموعة حلول معلوماتية بديلة. ويتعين تجريب هذا المخطط سنويا من أجل تحيينه وفق التطورات الخاصة بالبنية التحتية وكذا تطور المخاطر.

يجب على كل شخص مكلف بعملية مرتبطة بمخطط ضمان استمرارية واستئناف الأنشطة أن يكون على معرفة بما عليه القيام به في حالة وقوع حادث. كما يتعين عليه استيعاب الغاية المتوخاة وذلك حتى يكون تدخله منسجما مع عمل الهيئة.

المادة 9: إسناد نظم المعلومات لجهة خارجية

يجب على كل هيئة، عند إسناد تدبير نظم معلوماتها الحساسة لجهة خارجية، أن تفرض على هذه الجهة احترام التوجيهات الوطنية لأمن نظم المعلومات وكذا التنظيمات أو المراجع التقنية المتعلقة بأمن نظم المعلومات للبنيات التحتية ذات الأهمية الحيوية.

يتم الإسناد الخارجي لكل خدمة تطبيق تتعلق بنظم معلومات هيئة معينة بمقتضى عقد خاضع للقانون المغربي. ويتضمن هذا العقد وجوبا الالتزام بحماية المعلومة وافتحصاها واستعادتها. ويتم التنصيص بشكل دقيق في العقد المبرم على مقتضيات تتعلق بمتطلبات السلامة ومستوى الخدمة المرغوب فيها.

يعتبر إلزاميا للهيئات إيواء معطياتها الحساسة داخل التراب الوطني.

تحدد السلطة المختصة المرجع التقني المنظم لشروط الأمن والسلامة المتعلقة بالإسناد الخارجي لنظم المعلومات.

المادة 10: مراعاة أمن نظم المعلومات عند عمليات الاقتناء والصيانة

يجب على كل هيئة أن تضمن في ملفات الاستشارة وفي مخططات صيانة نظم المعلومات الحساسة مقتضيات تتعلق بمتطلبات أمن وسلامة هذه النظم.

تحدد السلطة المختصة متطلبات الأمن والسلامة الواجب احترامها من طرف الهيئة عند إعداد مخططات الصيانة وملفات الاستشارة.

المادة 11: مواكبة الهيئة وتقديم المساعدة

تقوم المديرية العامة لأمن نظم المعلومات بمواكبة الهيئات ومساعدتها عند تطبيق مقتضيات هذا المرسوم.

المادة 12: أحكام ختامية

ينشر هذا المرسوم في الجريدة الرسمية.

وحرر بالرباط في 12 من جمادى الآخرة 1437 (22 مارس 2016).

الإمضاء: عبد الإله ابن كيران.

ملحق
لائحة قطاعات الأنشطة ذات الأهمية الحيوية والسلطات الحكومية أو المؤسسات العمومية أو الأشخاص الاعتباريون من أشخاص القانون العام المشرفون على تنسيق هذه القطاعات

القطاعات	السلطات الحكومية أو المؤسسات العمومية أو الأشخاص الاعتباريون من أشخاص القانون العام المشرفون على تنسيق هذه القطاعات
الأمن العمومي	السلطة الحكومية المكلفة بالداخلية
العـدل	السلطة الحكومية المكلفة بالعدل
التشريع	الأمانة العامة للحكومة
قطاع المالية	السلطة الحكومية المكلفة بالمالية
الصناعة	السلطة الحكومية المكلفة بالصناعة
الصحة	السلطة الحكومية المكلفة بالصحة
السمعي البصري والاتصال	السلطة الحكومية المكلفة بالاتصال
إنتاج وتوزيع الطاقة والمعادن	السلطة الحكومية المكلفة بالداخلية السلطة الحكومية المكلفة بالطاقة والمعادن
شبكات النقل	السلطة الحكومية المكلفة بالنقل
التزود وتوزيع الماء	السلطة الحكومية المكلفة بالداخلية السلطة الحكومية المكلفة بالماء
الخدمات البريدية	السلطة الحكومية المكلفة بالبريد
القطاع البنكي	بنك المغرب
المواصلات	الوكالة الوطنية لتقنين المواصلات
قطاع الأسواق المالية	الهيئة المغربية لسوق الرساميل
قطاع التأمينات	هيئة مراقبة التأمينات والاحتياط الاجتماعي