قرار من وزير تكنولوجيات الاتصال مؤرخ في 12 سبتمبر 2023 يتعلق بضبط المعايير الفنية للتدقيق في سلامة النظم المعلوماتية وإجراءات متابعة تطبيق التوصيات الواردة في تقرير التدقيق.

إنّ وزير تكنولوجيات الاتصال،

بعد الاطلاع على الدستور،

وعلى مجلة الاتصالات الصادرة بالقانون عدد 1 لسنة 2001 المؤرخ في 15 جانفي 2001 وعلى جميع النصوص التي نقحتها أو تممتها وآخرها القانون عدد 10 لسنة 2013 المؤرخ في 12 أفريل 2013،

وعلى المرسوم عدد 17 لسنة 2023 المؤرخ في 11 مارس 2023 المتعلق بالسلامة السيبرنية،

وعلى الأمر عدد 1248 لسنة 2004 المؤرخ في 25 ماي 2004 المتعلق بضبط التنظيم الإداري والمالي وطرق سير الوكالة الوطنية للسلامة المعلوماتية،

وعلى الأمر عدد 1997 لسنة 2012 المؤرخ في 11 سبتمبر 2012 المتعلق بضبط مشمولات وزارة تكنولوجيا المعلومات والاتصال،

وعلى الأمر عدد 1998 لسنة 2012 المؤرخ في 11 سبتمبر 2012 المتعلق بتنظيم وزارة تكنولوجيا المعلومات والاتصال،

وعلى الأمر الرئاسي عدد 138 لسنة 2021 المؤرخ في 11 أكتوبر 2021 المتعلق بتسمية أعضاء الحكومة،

وعلى الأمر عدد 550 لسنة 2023 المؤرخ في 1 أوت 2023 المتعلق بتعيين رئيس للحكومة.

قرر ما يلي:

الفصل الأول ـ تخضع الهياكل المنصوص عليها بالفصل 6 من المرسوم عدد 17 لسنة 2023 المؤرخ في 11 مارس 2023 المتعلق بالسلامة السيبرنية إلى نظام تدقيق دوري وإجباري من خلال مهمة تقييم ميدانية لسلامة نظمها المعلوماتية.

يتم إجراء التدقيق في سلامة النظم المعلوماتية طبقا للمرجعية المعتمدة من قبل الوكالة الوطنية للسلامة السيبرنية التي تشمل العناصر الأساسية التالية:

- تقييم النواحي الهيكلية والتنظيمية والعملياتية لسلامة النظم المعلوماتية،

- التدقيق التقني في سلامة مكوّنات النظام المعلوماتي واختبار مناعتها من الحوادث السيبرنية،

- تحليل وتقييم المخاطر السيبرنية وتقديم خطة معالجة قصد تفادي أو تقليص الأضرار الناتجة عن الحوادث السيبرنية.

الفصل 2 ـ يسلم الخبير المكلف بالتدقيق للهيكل الذي خضع للتدقيق تقريرا يحمل ختمه وإمضاءه، ينجز وفقا لنموذج تقرير تدقيق توفره الوكالة، يتضمن خاصة ما يلي:

- وصفا شاملا للنظام المعلوماتي مع تقديم التبريرات اللازمة عند إقصاء عدد من مكوناته من مجال التدقيق،

- التثبت من مدى تطبيق التوصيات والحلول التنظيمية والتقنية الخاصة بالسلامة والمقترحة لتجاوز النقائص المسجلة بآخر تدقيق،

- تقييما شاملا لسلامة النظام المعلوماتي وتحليلا دقيقا للنقائص التنظيمية والتقنية المتعلقة بإجراءات وآليات السلامة المعتمدة، وتقييما للمخاطر التي قد تنجر عن استغلال الثغرات المكتشفة،

- الإجراءات والتوصيات والحلول التنظيمية والتقنية للسلامة المقترحة لتجاوز النقائص المسجلة،

- نسخة من محضري إنطلاق وإنتهاء مهمة التدقيق.

الفصل 3 ـ تتولى الوكالة دراسة وإجابة الهيكل بقبول أو رفض تقرير التدقيق، ويمكن للوكالة أن تطلب من الهيكل الذي خضع للتدقيق مدها بمعلومات أو وثائق إضافية كما يمكنها إجراء تثبت ميداني.

الفصل 4 ـ يمكن للوكالة رفض تقرير التدقيق في الحالات التالية:

- عدم مطابقة تقرير التدقيق للنموذج المشار إليه بالفصل 2 من هذا القرار،

- تقييم سلامة النظام المعلوماتي غير دقيق أو غير شامل،

- عدم تضمن تقرير التدقيق التوصيات والحلول الواجب اعتمادها لتجاوز النقائص المسجلة،

- عدم إنجاز مهمة التدقيق طبقا لمرجعية التدقيق المشار إليها بالفصل الأول من هذا القرار.

في حالة رفض تقرير التدقيق، يتعين على الهيكل المعني إعادة إجراء التدقيق وموافاة الوكالة بتقرير جديد في أجل لا يتجاوز شهرين من تاريخ إعلامه بذلك.

الفصل 5 ـ يتعين على الخبير أثناء القيام بالتدقيق إعلام الوكالة فور اكتشافه لمخاطر سيبرنية خطيرة من شأنها أن تهدد سلامة الفضاء السيبراني، ويتعين على الخبير أيضا إعلام الهيكل المعني لاتخاذ إجراءات السلامة المضادة اللازمة.

الفصل 6 ـ ينشر هذا القرار بالرائد الرسمي للجمهورية التونسية.

تونس في 12 سبتمبر 2023.

وزير تكنولوجيات الاتصال

نزار بن ناجي

اطلع عليه

رئيس الحكومة

أحمد الحشاني