الجمهورية التونسية
رئاسة الحكومة
رئيسة الحكومة

منشور عدد 5

02 سبتمبر 2026

من رئيسة الحكومة
إلى
السيّدات والسّادة الوزراء وكتّاب الدولة والولاّة ورؤساء المؤسسات والمنشآت العمومية

الموضوع: حول تأمين المنظومات الرقمية الوطنية بالهياكل العموميّة.

المراجع: - القانون الأساسي عدد 63 لسنة 2004 المؤرخ في 27 جويلية 2004 المتعلق بحماية المعطيات الشخصية.

- المرسوم عدد 31 لسنة 2020 المؤرخ في 10 جوان 2020 المتعلق بالتبادل الإلكتروني للمعطيات بين الهياكل والمتعاملين معها وفيما بين الهياكل كما تمت المصادقة عليه بالقانون عدد 14 لسنة 2021 المؤرخ في 7 أفريل 2021.
- المرسوم عدد 17 لسنة 2023 المؤرخ في 11 مارس 2023 المتعلق بالسلامة السيبرنية.
- الأمر الحكومي عدد 777 لسنة 2020 المؤرخ في 5 أكتوبر 2020 المتعلق بضبط شروط وصيغ وإجراءات تطبيق أحكام المرسوم عدد 31 لسنة 2020 المتعلق بالتبادل الإلكتروني للمعطيات بين الهياكل والمتعاملين معها وفيما بين الهياكل.
- منشور رئيس الحكومة عدد 24 لسنة 2020 المؤرخ في 5 أفريل 2020 المتعلق بتدعيم إجراءات السلامة المعلوماتية بالهياكل العمومية.

في إطار تعزيز آليات تأمين المنظومات الرقمية الوطنية ضدّ التهديدات والمخاطر السيبرنية المتنامية، لاسيما المتعلّقة بحماية المواقع الإلكترونية الرسمية والمنصّات الإلكترونية للخدمات العمومية، وضمانا لاستمرارية إسداء هذه الخدمات للمواطنين والمؤسسات دون انقطاع، وتبعا للتوصيات والتدابير

الجمهورية التونسية رئاسة الحكومة

التقنية الصّادرة عن الوكالة الوطنية للسلامة السيبرنية والتي تُعمّمها على مسؤولي سلامة نظم المعلومات (RSSI) المعيّنين بالهياكل العمومية، يتعيّن على الهياكل العمومية الالتزام بالإجراءات التالية:

1. بخصوص تأمين المو اقع الإلكترونية الرسمية والمنصّات الإلكترونية للخدمات العمومية:

- إيواء المواقع الإلكترونية الرسمية والمنصّات الإلكترونية للخدمات العمومية حصريّا لدى المركز الوطني للإعلامية، أو المراكز العمومية القطاعية للإعلامية التابعة للهيكل المعني، أو مزوّدي خدمات الأنترنات، أو مسدي خدمات الحوسبة السحابية، أو مشغّلي الشبكات العمومية للاتصالات المرخص لهم من وزارة تكنولوجيات الاتصال طبقا للتشريع الجاري به العمل. وتستثنى من ذلك، الحالات الخصوصية المبرّرة التي تستوجبها مقتضيات الأمن والدفاع الوطنيين.
- اعتماد بروتوكول نقل النص التشعبي الآمن "HTTPS" في كافة صفحات المواقع الإلكترونية الرّسمية ومنصات الخدمات عن بعد، مع توفير شهادات أمان رقميّة معتمدة، وفقا لبروتوكولي طبقة المقابس الآمنة وأمان طبقة النقل "SSL/TLS"، صادرة عن مزّود خدمات مصادقة إلكترونية مرخص له، وفقا للتشريع والتراتيب الجاري بها العمل، مع إلزامية تجديدها بصفة دوريّة، قبل تاريخ انتهاء صلوحيتها.
- تفعيل خدمات التثبّت من الهويّة متعدّدة العوامل"MFA" لجميع مستخدمي المواقع الإلكترونية الرسمية أو المنصات الإلكترونية للخدمات العمومية، لاسيما حسابات المشرفين والمسؤولين عن إدارة هذه المواقع والمنصات والنفاذ إلى واجهاتها الخلفية، مع تسريع إدماج خدمات الهويّة الرقميّة في مختلف المنصات الخدماتية.
- تكليف جهة تدقيق معتمدة من قبل الوكالة الوطنية للسلامة الإلكترونية لإجراء تقييم شامل لسلامة منصات الخدمات أو المواقع المنبثقة عنها، طبقا للتشريع الجاري به العمل، قبل وضعها على ذمّة العموم. ويلتزم الهيكل العمومي المعني، بتطبيق جميع التوصيات المنبثقة عن التقييم، قبل وضع المنصة أو الموقع الإلكتروني حيز الاستغلال، مع موافاة الوكالة الوطنية للسلامة السيبرنية بنسخة من التقرير النهائي للتقييم الشامل، مصادق عليها من الجهة المنجزة للتقييم، ومرفقة بالوثائق الإثباتية لتنفيذ كافّة التوصيات. كما يتعيّن إجراء تقييم شامل بصفة دورية، مرّة واحدة على الأقل سنويّا، وكذلك قبل إطلاق أي إصدار رئيسي جديد للمنصّة أو الموقع الإلكتروني.
- ضمان التحيين المستمّر والصيانة الدورية لمختلف مكونات المواقع الإلكترونية الرسميّة ومنصات الخدمات الالكترونية، قصد الحدّ من المخاطر السيبرنية ومعالجة الثغرات الأمنية المسجّلة بصفة حينية.

- الاشتراك في خدمات الحماية من هجمات حجب الخدمة الموزّعة "DDoS" المتاحة لدى مزّودي خدمات الاتصالات والأنترنات المرخص لهم وفقا للتشريع الجاري به العمل، بما يضمن استمرارية نفاذ المستخدمين إلى المواقع الإلكترونية الرسمية والمنصات الإلكترونية للخدمات العمومية، والحدّ من مخاطر انقطاعها أو تعطّلها.

2. **بخصوص التراسل الإلكتروني الرسمي:**

- الاعتماد الحصري للبريد الإلكتروني الوطني المعتمد ".tn" في كافّة المعاملات والمراسلات الرّسمية.
- اتخاذ التدابير التقنية والتنظيمية الكفيلة بتحديث قاعدة بيانات حسابات البريد الإلكتروني بصفة دورية، وإيقاف الحسابات غير النشطة أو تلك الخاصة بالموظفين المنتهية خدمتهم.
- تفعيل وظائف تسجيل العمليات وأرشفتها "Logging & Archiving" على مستوى منصّات التراسل الإلكتروني الرسمي.
- منع تداول الوثائق الإدارية الرسمية، أو إرسالها، أو نشرها، أو مشاركتها بأي شكل من الأشكال عبر وسائل وقنوات الاتصال غير الرسمية، ولاسيما تطبيقات الهاتف الجوّال ومنصات التواصل الاجتماعي أو الوسائط المماثلة.

3. **بخصوص الإجراءات التنظيمية لدعم السلامة السيبرنية:**

- الالتزام بإجراء التدقيق الدّوري لسلامة نظم المعلومات، وتطبيق التوصيات المنبثقة عنه طبقا لأحكام الفصلين 6 و8 من المرسوم عدد 17 لسنة 2023 المؤرخ في 11 مارس 2023 المتعلق بالسلامة السيبرنية، مع منح الأولوية القصوى لمنظومات البريد الإلكتروني والمواقع الإلكترونية الرسمية والمنصات الإلكترونية للخدمات العمومية.
- إعلام الوكالة الوطنية للسلامة السيبرنية بصفة حينية بكلّ حادثة أو هجمة سيبرنية، سواء كانت مؤكدة أو محتملة وذلك عبر قنوات الاتصال المعتمدة أو أي وسيلة أخرى تترك أثرا كتابيا.
- منع مشاركة حسابات النّفاذ إلى المنظومات المعلوماتية بين الأعوان، منعا باتّا، مع التأكيد على صبغتها الشخصية الفردية، وعلى ضرورة تحديد صلاحيات النّفاذ بدقّة، وفقا للمهام الوظيفية لكل عون.
- ضرورة التنسيق المُسبق مع وزارة تكنولوجيات الاتصال قبل إقرار أو برمجة أي مشاريع أو دراسات تتعلق بالبنية التحتية للاتصالات، أو المنظومات المعلوماتية الحساسة، أو قواعد البيانات ذات الخصوصية، لاسيما إذا كان تنفيذها سيتّم كليّا أو جزئيّا بالاستعانة بجهات خارجيّة.

- منح أولوية قصوى لحماية المعطيات والبيانات المتعلقة بنظم المعلومات وبالبنى التحتية الرقمية، ومنع إحالتها، أو مشاركتها، أو تمكين الغير منها بأيّ صيغة كانت، إلاّ بعد استيفاء الإجراءات القانونية المستوجبة لضمان السرية والسلامة، وبالتنسيق المسبق مع وزارة تكنولوجيات الاتصال عند الاقتضاء.
- اتخاذ التدابير اللازمة لضمان استمرارية الخدمات، والالتزام بحفظ نسخ احتياطية من قواعد البيانات، وضمان سلامتها وحمايتها من التغيير، أو الإتلاف، أو النفاذ غير المشروع.
- إعداد وتحديث خطتي استمرارية النشاط والتّعافي من الكوارث واختبار نجاعتهما بصفة دورية لضمان استعادة الخدمات والبيانات بأسرع وقت ممكن عند وقوع حادث سيبرني أو عطب جسيم .
- عزل قواعد البيانات الحسّاسة والخدمات الرقمية الداخلية عن شبكات الاتصال الخارجية باعتماد مختلف وسائل الحماية المتاحة طبقا للمعايير الدولية في المجال.

4. الإجراءات المصاحبة:

ضمانا لحُسن تطبيق إجراءات تأمين المنظومات الرّقمية الوطنية، المذكورة أعلاه، يتعيّن على جميع الهياكل العمومية اتخاذ الإجراءات المصاحبة التالية:

- تنظيم دورات تكوينية وحملات تحسيسية دورية لفائدة الإطارات والأعوان في مجال السلامة السيبرنية، وإدراج هذا المحور ضمن مخططات التكوين السنوية للهياكل العمومية .
- الحرص على توفير الموارد البشرية والتقنية والاعتمادات الضرورية لتنفيذ متطلّبات السلامة السيبرنية وضمان استدامة التدابير الوقائية والتصحيحية ذات الصلة .

ونظرا لما يكتسيه الموضوع من أهميّة، يتعيّن على السّيدات والسّادة الوزراء وكتّاب الدولة والولاّة ورؤساء المؤسسات والمنشآت العمومية، الالتزام بمقتضيات هذا المنشور واتخاذ الإجراءات اللاّزمة لتطبيقها بكلّ دقّة وعناية ومتابعة تنفيذها.

رئيسة الحكومة

سارة الزعفراني الزنزري