المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

ضمان وحماية الأمن المعلوماتي الوطني

في إطار مواجهة التحديات المتزايدة التي يطرحها الفضاء الرقمي مع ارتفاع الإقبال على شبكة الانترنيت ووسائل الاتصال الحديثة، عملت المملكة المغربية في السنوات الأخيرة على اتخاذ العديد من الإجراءات لتقوية مناعة نظم المعلومات الوطنية أمام المخاطر المحدقة بها والحفاظ على منظومة وطنية متكاملة وفعالة لأمن نظم المعلومات تأخذ بعين الاعتبار السياق الوطني والدولي.

وفي هذا الصدد، تم مؤخرا وضع إطار مؤسساتي للأمن السيبراني بموجب القانون رقم 05.20 المتعلق بالأمن السيبراني، والذي يضم اللجنة الاستراتيجية للأمن السيبراني التي تتولى تحديد التوجهات الاستراتيجية في هذا المجال وحماية المعطيات الرقمية السيادية، فضلا عن ضمان جاهزية واستمرارية نظم معلومات مؤسسات الدولة والبنيات التحتية ذات الأهمية الحيوية. إضافة إلى ذلك، تم إحداث لجنة وطنية لإدارة الأزمات والأحداث السيبرانية الجسيمة تتكلف بضمان تدخل منسق في مجال الوقاية وتدبير الأزمات على إثر وقوع حوادث أمن سيبراني.

كما يضم هذا الإطار أيضا المديرية العامة لأمن نظم المعلومات المكلفة خصوصا بالشق العملياتي من خلال اتخاذ التدابير الهادفة إلى تعزيز حماية وصمود نظم المعلومات الوطنية تنزيلا للاستراتيجية الوطنية للأمن السيبراني.

في هذا السياق وفي إطار سعيها لتطوير القدرات اللازمة لحماية المصالح الحيوية للدولة والاقتصاد الوطني في مجال أمن نظم المعلومات، تحرص المديرية العامة لأمن نظم المعلومات على تقديم المساعدات التقنية اللازمة للبنيات التحتية ذات الأهمية الحيوية، كما تقوم المديرية باستمرار، اعتمادا على كفاءة وخبرة أطرها الداخلية، بعمليات تدقيق وافتحاص أمن نظم معلومات الوزارات والمؤسسات العمومية والهيئات ذات الطابع الاستراتيجي، بغية تقييم نضجها الأمني وقدرتها على الصمود أمام الهجمات السيبرانية. كما تعمل على اقتراح مجموعة من التوصيات الرامية إلى تعزيز أمن وصمود نظم المعلومات على الصعيد الوطني وتتبع تنفيذها وكذا تحسيس الهيئات والمؤسسات المفتحصة حول ضرورة تطبيق الإجراءات الاحترازية والوقائية.

وعلى صعيد آخر، تعمل المديرية العامة من خلال تدخلات مركز اليقظة والرصد والتصدي للهجمات المعلوماتية، على تعزيز عمليات رصد الثغرات التي من شأنها أن تشل الأنظمة أو البنيات التحتية الحساسة بالإضافة الى التصدي للهجمات السيبرانية التي تهدف إلى تغيير المعطيات أو محوها أو سرقة المعلومات الحساسة التي لم يتم تأمينها بشكل صحيح، وكذا التصدي لأي اعتراض يلحق الاتصالات أو تغييرها. ويسهر المركز من جهة أخرى على إدارة حوادث وتهديدات الأمن السيبراني، عن طريق تحليلها بسرعة ودقة بناء على المعرفة المكتسبة من تقنيات كشف الاختراقات وعلى اتخاذ الخطوات اللازمة للتعامل مع الحوادث السيبرانية. ويعتمد المركز لتأمين خدماته على:

- تقديم الاستشارات لمسؤولي أمن نظم المعلومات في الإدارات والهيئات العامة والبنيات التحتية ذات الأهمية الحيوية فيما يتعلق بالثغرات عند ظهور تهديدات جديدة، أو عبر تحديث أنظمة الحماية لاكتشاف ومنع الاختراقات والتأكد من قدرة تلك الأنظمة على اكتشاف التهديدات والتعامل معها بشكل فعال؛

- رفع مستوى التوعية من خلال إصدار العديد من المذكرات الإخبارية، والتي بلغ عددها 621 نشرة ومذكرة أمنية من بينها 188 نشرة ذات طبيعة حرجة وذلك خلال سنة 2021؛

- اكتشاف الثغرات التقنية في الوقت المناسب عن طريق المسح الشامل ومعالجتها بشكل فعال، وذلك لمنع إمكانية استغلال هذه الثغرات أثناء الهجمات السيبرانية على الأنظمة الحساسة ومكوناتها التقنية وجميع الخدمات المقدمة خارجيا عن طريق الإنترنت وخاصة المواقع الإلكترونية وتطبيقات الويب وتطبيقات الهواتف الذكية والبريد الإلكتروني والأجهزة المستعملة في الدخول والعمل عن بعد، حيث تم تقييم 54 تطبيقا للويب سنة 2021؛

- إجراء اختبارات الاختراق لتقييم مدى فعالية قدرات الأمن السيبراني، وذلك من خلال محاكاة تقنيات الهجوم السيبراني الفعلية وأساليبه لاكتشاف نقاط الضعف الأمنية الغير معروفة. ويمكن هذا الاختبار أيضا من التأكد من تطبيق التحديثات والإصلاحات اللازمة التي تعالج الثغرات الأمنية حسب مستوى المخاطر المرتبطة بها؛

- جمع سجلات أحداث الامن السيبراني وتحليلها ومراقبتها بطريقة مستمرة من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية، لمنع الاثار السلبية المحتملة أو تقليلها، حيث تم خلال سنة 2021، تسجيل ما مجموعه 577 حادث تم التعامل معها.

ويكثف مركز اليقظة والرصد والتصدي للهجمات المعلوماتية جهوده كما يرفع من درجة يقظته ومستوى جاهزيته عند تصاعد التوترات والتجاذبات الجيوسياسية أو نشوء بعض الأزمات على الصعيد الدولي كما هو حال الحرب الروسية الأوكرانية والتي تؤدي غالبا الى تنامي خطر التهديدات السيبرانية وارتفاع وتيرة الهجمات. ويعتمد المركز في هذا الباب أساسا على علاقات التعاون التي تربطه بنظرائه في الدول الصديقة خصوصا فيما يتعلق بتبادل المعلومات وتقاسم الخبرات.

وموازاة مع ما سبق، تنخرط جميع الأطراف، وخصوصا، مستغلي الشبكات العامة للمواصلات ومزودي خدمات الانترنيت، في تعزيز أمن نظم معلومات الهيئات والبنيات التحتية ذات الأهمية الحيوية ومتعهدي القطاع الخاص والأفراد من خلال الاحتفاظ بالمعطيات التقنية الكفيلة بتحديد حوادث الأمن السيبراني والابلاغ عن أي حادث قد يؤثر على أمن نظم معلومات زبنائهم واتخاذ التدابير الوقائية اللازمة لمنع وتخفيف وقع التهديدات أو المساس بهذه النظم.

أما فيما يتعلق بالرفع من قدرات الموارد البشرية، تعمل المديرية على برمجة دورات تدريبية وتكوينية لفائدة الأطر المتخصصة العاملة في مجال أمن نظم المعلومات في إطار شراكات مع هيئات وطنية ودولية رائدة في هذا المجال. كما تسهر على تنظيم تمارين على المستوى الوطني لتقييم الجاهزية للاستجابة لحوادث الأمن السيبراني وعلى المشاركة في التمارين المنظمة على الصعيد الدولي. وقد بادرت فرق مركز عمليات الأمن التابعة للجنة الاستراتيجية للأمن السيبراني إلى تنظيم تمرينين إلكترونيين سنة 2021، شارك فيهما 60 فريقا.

وارتباطا بدورها التحسيسي، تواصل المديرية العامة لأمن نظم المعلومات تعزيز مجهوداتها المتعلقة بتزويد مسؤولي أمن نظم معلومات الإدارات والمؤسسات العمومية وكذا تلك المتعلقة بمشغلي البنيات التحتية الحيوية الوطنية بالعديد من الارشادات التقنية المتعلقة بالمستجدات في مجال أمن نظم المعلومات.