حلول متطورة تواكب التحول الرقمي لحماية بيانات المنتسبين.. قمزة المري:

قسم الشبكات جدار الهيئة لصد الهجمات الإلكترونية

- نحن أول جهة تمتلك سحابة تقنية وتكنولوجيا CISCO ACI
- إطلاق مشروع سياسة تأمين المعلومات الوطنية قريبًا

يتولى قسم الشبكات والدعم الفني مسؤولية صد الهجمات الإلكترونية والخروقات الخطرة، وذلك لحماية الأنظمة التقاعدية وضمان سرية بيانات منتسبيها، إذ يوفر القسم حلولًا وتدابيرًا رقمية متطورة تواكب سياسة التحول الرقمي، التي تنتهجها الهيئة العامة للتقاعد والتأمينات الاجتماعية، الرامية إلى أتمتة كافة الخدمات، وفق أحدث المعالجات والبرمجيات الفنية المطبقة على المستوى العالمي، التي تتيح التعامل بصورة استباقية وسريعة مع الهجمات غير المتوقعة، والتنبؤ بها، والسيطرة عليها حال حدوثها؛ للحد من تأثيراتها على دورة العمل.
ويلعب القسم دورًا هامًا في توفير صيانة وقائية للمحافظة على الأجهزة والبرمجيات المستخدمة، كذلك تقع على عاتقه مهمة التحديث والتطوير وحل المشكلات، التي يواجهها المتعاملون مع الحاسوب بكفاءة عالية، وتقديم المساعدة لهم، وتوعيتهم بأمن المعلومات، بالإضافة إلى حفظ وإدارة الوثائق واسترجاعها عند الضرورة، والتأكد من أن جميع أنظمة الهيئة الإلكترونية محدثة.
"التأمينات الاجتماعية"، التقت رئيسته السيدة قمزة علي المري، وأجرت معها حوارًا، سلطت خلاله الضوء على أبرز ما يقدمه القسم من خدمات، والتحديثات التي ينتظرها في الفترة المقبلة، وفي ما يلي نص الحوار كاملًا...

- بداية نود التعرف سريعًا على قسمكم، وما هي المهام التي يؤديها؟

يُطلق مصطلح الدعم الفني غالبًا على التخصص المسؤول عن تقديم الدعم الفني والتقني للموظفين في المسائل التي يجهلونها، وحل كافة المشاكل اليومية سواء كانت في الحاسوب نفسه أو الشبكة وملحقاتها، وأهم ما يمتاز به القسم هو سرعة التدخل في الوقت المناسب كي لا تتعطل دورة العمل.
ويختص القسم بتركيب شبكات الاتصال وتهيئتها للعمل، ومتابعة الأعطال التي تطرأ عليها، والإشراف على الربط الآلي مع الجهات ذات العلاقة، وتطبيق نظام أمني متطور ضد الاختراقات، وحفظ النسخ الاحتياطية، وضبط أنظمة التشغيل لتحسين الأداء، ووضع تعليمات وأسس سلامة الأجهزة.

- ماذا يقصد بالتخزين الاحتياطي للبيانات؟، وما أهميته؟.

هو آلية لحفظ البيانات من الضياع أو التلف عن طريق أخذ نسخ منها دوريًا، لأن البيانات تتغير باستمرار، قد يحذف جزء منها من قبل المستخدمين عن طريق الخطأ، أو بسبب عطل فني يؤدي إلى ضياعها أو التأثير على تكاملها، وهنا تكمن أهميتها بحيث يتم إعادة البيانات إلى وضعها الصحيح، ما يضمن استمرارية العمل في الهيئة، دون ضياع المعلومات أو توقف خدماتها.

- ما هي خططكم عند تعرض بيانات المنتسبين للتلف أو ما شابه ذلك؟.

عند حدوث مثل هذه المشكلة يجب أولًا تحديد سببها، ومن ثم وضع خطة فورية لحلها، للحيلولة دون تعرض البيانات المسترجعة للمشكلة ذاتها، وأخيرًا استعادة نسخة سليمة من أجهزة النسخ الاحتياطي.

- ما البدائل المتاحة حال انقطاع خدمة الإنترنت عن دولة قطر بما فيها الهيئة؟.

صممت البنية التحتية الإلكترونية للهيئة بطريقة مرنة وفعّالة تضمن الوصول إلى جميع خدماتها عن طريق الشبكة الداخلية دون الاعتماد على الشبكة العنقودية "الإنترنت"، باستثناء الجزء الخاص بالمستخدمين الخارجيين، فهو الوحيد الذي يعتمد على ذلك.

- ما هي الآليات المتبعة لتحسين أنظمة التشغيل وتطوير أدائها؟.

مواكبة أحدث التكنولوجيا عند تصميم شبكات المعلومات والخوادم وتحديثها ومتابعة أداء أنظمة التشغيل بشكل مستمر ومتطور مع معالجة الخلل فور ملاحظته، علاوة على ذلك تحديث البرامج أولاً بأول فور صدور التحديثات الجديدة للبرنامج والأجهزة، وهنا لا بد من الإشارة إلى أن الهيئة كانت أول جهة حكومية لديها السحابة الإلكترونية (VMware)، وكان ذلك منذ 2010 – 2011.

- هل لديكم مشروعات مستقبلية لدعم الحلول المعلوماتية؟.

بالتأكيد، لدينا مشاريع خاصة بتطوير شبكة المعلومات والخوادم الافتراضية وفق أحدث التكنولوجيا المطبقة، وتعد الهيئة أول مؤسسة حكومية تطبق تكنولوجيا الـ CISCO ACI بنجاح وبكفاءة عالية، حيث تعد شبكة معلومات البنية التحتية التطبيقية (ACI Networks) من أحدث التكنولوجيا المستخدمة في عالم الشبكات، حيث توفر بيئة متكاملة مع التطبيقات بخلاف المفهوم التقليدي للشبكات.
من أهم ميزات هذا النوع من الشبكات هو سرعة تجهيز البنية التحتية للتطبيقات بفاعلية وتوفير أعلى درجات الأمن على مستوى الشبكة.

- كيف يسهم القسم في حماية بيانات المنتسبين من الاختراق؟.

يطبق القسم أفضل معايير أمن المعلومات لحماية قواعد بيانات المنتسبين من الاختراق، بدءًا بتطبيق التحديثات الأمنية الخاصة بقواعد البيانات وأنظمة التشغيل وبرامج الحماية من التطبيقات الخبيثة (Antivirus)، كذلك تم تركيب نظام الحماية من الاختراق (TrendMicro Tipping Point IPS)، حيث يقوم هذا النظام بمنع محاولات الاختراق في حال حدوثها وتنبيه الفريق المختص لاتخاذ التدابير اللازمة، كما تم تركيب نظام حماية التطبيقات من الاختراق (F5 Web Application Firewall)، ويراقب هذا النظام طبيعة استخدام خدمات الهيئة الإلكترونية على شبكة الويب، ويقوم باكتشاف وإيقاف أي محاولات للاستخدام غير المألوف، قد يهدف لاختراق البيانات.

- واجهت دولة قطر مؤخرًا عددًا من الهجمات الإلكترونية، كيف كانت جاهزيتها لمثل هذه الهجمات؟.

الهيئة أول جهة تطبق أهم نظام في الأمن المعلوماتي من خلال نظام الـ RSA وكان ذلك في 2012، ومن ثم بدأت الجهات الأخرى بتطبيقه، ومنذ ذلك الحين ونحن نطور ونطبق ما هو الجديد في هذا المجال، ويواكب القسم أفضل معايير الاستجابة للحوادث الأمنية وأحدث التقنيات، وهو على تنسيق متبادل مع فريق عمل وزارة الداخلية وفريق Q-cert، اللذان يزودان فريق أمن المعلومات في الهيئة بالاستشارات الأمنية لاتخاذ التدابير والاحتياطات اللازمة.

كما أن الهيئة تطبق السياسات وتتبع الإجراءات الأمنية تبعًا لنظام ISO27001 لأمن المعلومات، والهيئة الآن بصدد إطلاق مشروع سياسة تأمين المعلومات الوطنية NIA، وتسعى إدارة نظم المعلومات جاهدة لتطبيق السياسات والتدابير اللازمة وفق المعايير العالمية.

- كيف يتم توعية موظفي الهيئة بأمن المعلومات؟.

يحصل موظفو الهيئة على أعلى تدريب في مجال أمن المعلومات، حتى يتمكنوا من تمييز الرسائل الضارة، وتبليغ الفريق المختص حال ورود أي بريد إلكتروني مشكوك بأمره، سيما وأن مفهوم أمن المعلومات يبدأ من وعي المستخدم وحسن تصرفه في عدم تصفح الروابط والرسائل غير موثوقة المصدر، حيث تم الاتفاق مؤخرًا مع الجهات المعنية لتدريب الموظفين بهذا الشأن، وهناك تدريب آخر خاص بموظفي قسم الأمن بإدارة نظم المعلومات.