بسم الله الرحمن الرحيم

معالي المهندس سعيد بن حمود المعولي الموقر

وزير النقل والاتصالات وتقنية المعلومات

راعي أعمال مؤتمر عمان للأمن الإلكتروني

أصحاب السمو والمعالي

المكرمون أعضاء مجلس الدولة

أصحاب السعادة

الحضور الكريم

أُرحبُ بكم أجمل ترحيبٍ في مستهل أعمال مؤتمر عُمان للأمن الإلكتروني في دورته الثانية التي تنعقد تحت عنوان "شراكة من أجل اقتصاد آمن"، والتي يشاركنا فيه كوكبة من الخبراء والمتخصصين في مجال الأمن الإلكتروني وأمن المعلومات، من أجل طرح مختلف الأفكار والرؤى التي تساعدنا على مواصل التقدم بخطى حثيثة نحو

الأهداف التي نصبو إليها، متسلحين في ذلك بالعمل والمعرفة ومتطلبات العصر.

معالي المهندس راعي المؤتمر..
الحضور الكريم..

لقد قطعت بلادنا شوطًا مهمًا على مسار التحول الرقمي وتبني المفاهيم ذات الصلة بالاقتصاد الرقمي، وصولًا إلى إطلاق مجلس الوزراء الموقر للبرنامج الوطني للاقتصاد الرقمي، والذي من خلاله سنتمكن من وضع قدمٍ راسخة في المستقبل الذي سيعتمد اعتمادًا كليًا على "الرقمنة" وستتحول حياتنا من حولنا في جميع تفاصيلها إلى معاملات رقمية، خاصة مع انتشار التطبيقات الداعمة لهذا الاقتصاد الرقمي؛ سواء تقنيات الذكاء الاصطناعي وإنترنت الأشياء و"الفينتِك" والعملات المُشفرة والبلوك تشين أو سلاسل الكتل، وغيرها..

كل ذلك يقودنا إلى مستقبل واعد ينتظرنا، وعلينا أن نستعد له جيدًا وأن نعُد عدتنا من أجل تحقيق أعلى قدر من الاستفادة لنا وللأجيال التي ستأتي من بعدنا.

معالي المهندس وزير النقل والاتصالات وتقنية المعلومات..

ضيوف المؤتمر الأعزاء..

إن الدورة الثانية من مؤتمر عمان للأمن الإلكتروني تنعقد تحت عنوان "شراكة من أجل اقتصاد آمن"، من خلال تعزيز الشراكة بين القطاعين الحكومة والخاص، عبر تأسيس برامج وخطط عمل تستهدف الاستفادة من الأمن الإلكتروني لتمكين التحول الرقمي، وأول ما يُمكن القيام به في هذه الحالة أن تتعرف مختلف المؤسسات بمزيد من التفصيل على مفهوم الأمن الإلكتروني، وأنه لم يعد مجرد وضع برنامج مضاد للفيروسات أو زيادة معدلات الحماية الأمنية عبر البرمجيات التقليدية المتاحة في الأسواق؛ بل إن الأمر يتعدى ذلك بكثير؛ حيث بات الأمن الإلكتروني الركن الأهم في أي منظومة رقمية، ليس فقط لمواجهة الفيروسات والبرمجيات الخبيثة، لكن أيضًا لمجابهة عمليات القرصنة

الممنهجة التي تمارسها عصابات دولية وأجهزة وجواسيس إلكترونيين وغيرهم. وهذا يفرض على المؤسسات تبني أفضل الحلول التقنية للحيلولة دون حدوث أي اختراق للأنظمة الإلكترونية، وضمان أعلى مستويات الأمان الإلكتروني.

وهذا الأمان الإلكتروني، ووفقًا لما نشرته مجلة "هارفارد بزنيس ريفيوز" يسلتزم أولًا: توفير فضاء سيبراني (إلكتروني) آمن من شبكات وأنظمة تشغيل وبرمجيات. وثانيًا: تأسيس قوة ردع إلكترونية لمنع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي. وهذان الإجراءان يسهمان في منع الهجمات السيبرانية وهي أي فعل يتسبب في تقويض القدرات والوظائف الإلكترونية لأي مؤسسة، من خلال استغلال نقطة ضعف معنية تساعد المُهاجم على التحكم في الأنظمة وسرقة البيانات منها وصولًا إلى تدميرها وحذف جميع الملفات.

معالي راعي أعمال المؤتمر..

الضيوف الأعزاء..

الحديث عن الأمن الإلكتروني لم يعد نوعًا من التنظير أو المفاخرة بأنظمة حماية بعينها؛ بل صار إجراءً حتميًا نظرًا لأن هذا الأمن الإلكتروني يوفر للمؤسسات (حكومية وخاصة) والأفراد ومختلف الكيانات، 3 فوائد، أولها السرية، من خلال التحكم في من له صلاحية الولوج إلى البيانات، وثانيها: الحفاظ على سلامة المعلومات والأنظمة الإلكترونية من أي اختراق أو هجمات سيبرانية، وثالثها: الجاهزية، أي أن تكون الخدمات والأنظمة الإلكترونية متاحة وجاهزة وفقًا لحاجة المؤسسة أو الشركة.

وفي ظل زيادة الاعتماد على الأنظمة الإلكترونية والتوسع في استخدام التخزين السحابي، بات من الضروري للغاية أن تضع كل مؤسسة القواعد والإجراءات الكفيلة بالحفاظ على سرية البيانات وحمايتها من الهجمات، ولا ينبغي أن تقول شركة إنها لا تخشى الاختراق، فالأمر ليس مرتبطًا فقط بالجوانب المالية؛ بل إن المسألة تتعلق كذلك بالحماية من الابتزاز الإلكتروني، فربما يخترق مهاجم شركة للمقاولات فيستحوذ على أبرز المشاريع المستقبلية التي تنوي الشركة تنفيذها، ثم يعرض

هذه البيانات على شركة منافسة ربما تمارس أسلوبًا غير أخلاقي في العمل، فتتعرض الشركة لخسائر كبيرة، والسبب أنها لم تهتم بأمن المعلومات!

معالي المهندس وزير النقل والاتصالات وتقنية المعلومات..

الحضور الكرام..

واحد من المخاطر التي قد تتعرض لها أنظمة الأمن الإلكتروني، عدم وجود الكفاءات القادرة على تشغيل برمجيات الحماية، وهذا يتطلب على جهات الاختصاص بذل الجهود من أجل طرح تخصصات أكاديمية وتنفيذ دورات تدريبية وتأهيلية للعاملين في مجال الأمن السيبراني.. وإنه لمن المُبشر أننا في سلطنة عُمان أن هذه التخصصات تُقدم في أكبر جامعاتنا، وأخص بالذكر هنا جامعة السلطان قابوس والجامعة الألمانية للتكنولوجيا في عُمان، فكلا هاتين المؤسستين تقدمان محتوى أكاديميًا متقدمًا يسهم في تخريج أجيال من الخبراء والمتخصصين في تكنولوجيا المعلومات والأمن السيبراني والبرمجة بشتى لغاتها وأنواعها. إن أمثال هؤلاء هم جدران الحماية من المخاطر الرقمية التي تتهددنا،

لا سيما ونحن- كما ذكرت- نواصل الخطى الحثيثة نحو التحول الرقمي في شتى مجالات الحياة.
ولذلك أدعو من هذا المنبر إلى زيادة البرامج والتخصصات الأكاديمية ذات الصلة بالأمن السيبراني وتكنولوجيا المعلومات، وعلوم الحاسب، وغيرها.

معالي المهندس راعي أعمال مؤتمر عمان للأمن الإلكتروني..
الجمع الكريم..
من القضايا التي أودُ التطرق إليها في هذا الموضوع، قضية المدفوعات الرقمية، خاصة مع انتشار تقنيات بالغة التقدم، وعلاقة ذلك بالأمن الإلكتروني. فقد كشفت إحصاءات نشرتها شركات الأمن الإلكتروني، أن زيادة الاعتماد على الخدمات المالية والمصرفية الرقمية، تسبب في ارتفاع معدلات الجريمة الرقمية، والهجمات المنظمة على الأنظمة البنكية وأنظمة المدفوعات، وهذا يقودنا إلى ما أشرنا إليه في بداية حديثنا، من حيث أهمية توفير أعلى نُظم الحماية الرقمية للأنظمة والتطبيقات، علاوة على تعزيز وعي المستخدمين، سواء كانوا أفرادًا أو

موظفين يتعاملون مع هذه الأنظمة والتطبيقات، وبناء ثقافة رقمية مجتمعية تساهم في الحد من الهجمات الخبيثة أو هجمات الفدية أو سرقة البيانات وشل الأنظمة الرقمية.

ولا شك أن التوجه نحو بناء منظومة رقمية متكاملة وآمنة سيسهم في تحقيق العديد من الأهداف، سواء ما تتعلق باستمرارية تقديم الخدمات بأعلى معدلات الأمان، أو عبر توفير فرص عمل ووظائف للكفاءات المتخصصة في مثل هذه المجالات.

وفي الختام لا يسعُني إلّا أن أتقدم بخالص الشكر والتقدير إلى معالي المهندس وزير النقل والاتصالات وتقنية المعلومات الموقر، على رعايته الكريمة لأعمال مؤتمر عمان للأمن الإلكتروني في دورته الثانية..

والشكر موصول إلى الإخوة الخبراء والمتخصصين الذين يشاركوننا اليوم بأوراق عمل ونقاشات مهمة..

كما أجزل الشكر إلى شركة عمان داتا بارك الشريك الاستراتيجي لنا في هذا المؤتمر، والشكر كذلك إلى الشركات والمؤسسات الراعية لهذا المؤتمر.

والسلام عليكم ورحمة الله وبركاته،،،