

اختتام منتدى الحكومة الإلكترونية الثاني برعاية سمو رئيس الوزراء وتنظيم «نوف إكسبو»

«الانباء» الراعي الإعلامي الحصري للمنتدى

9-11 نوفمبر

70٪ من الاختراقات تأتي من داخل المؤسسات.. واستثمارات ضخمة تنفق لتأمين البيانات لمواجهة خطر القرصنة

أمن المعلومات يواجه «خطر الاختراق» من الداخل



تكريم ممثل وزارة المالية أحمد العمار من قبل مجدي صبري



جانب من المشاركين في الجلسة الأولى ويبدو من اليمين د. خضر درة، كريستوف كابلارو ومايكل لوتس وسعد كوكجي (قاسم باشا)

المؤسسات والشركات وهي على النحو التالي: أولاً مركز التحكم بالأجهزة والأنظمة وهو مبني بناء على التطورات والاحتياجات الحديثة لأجهزة البرامج لتلبية متطلبات التطورات العصرية. وأوضح أن نظام السحابة لديه القدرة على استيعاب الكم الهائل من الأجهزة باستخدام أقل قدر ممكن من الطاقة، لافتاً إلى أن أنظمة التبريد الحديثة المتبعة في بناء مركز التحكم تعتمد على التبريد بواسطة المياه لتوفر ذلك كما هائلاً من الطاقة، أما أنظمة المحاكاة فتتطلب كما هائلاً من المعلومات معها لتوفير البيانات المطلوبة والخدمات للمواطنين.

وأشار إلى خطة إدارة الكوارث واستمرارية العمل وهي تعني الإجراءات التي يجب اتخاذها في أوقات الكوارث الخاصة منها والعام، مبيناً أن الكوارث الخاصة يقصد بها انقطاع الاتصالات أو الإنترنت أو الشبكة الإلكترونية أو توقف أحد الخوادم أو البرمجيات عن العمل وذلك لأسباب فنية أو مادية، أما مفهوم الكوارث العامة فيقصد بها الحروب والثورات والاضرابات والكوارث الطبيعية.

المعلومات - توصيف العتاد الصلب Hardware - توصيف شبكات الاتصال - توصيف البرمجيات وقواعد البيانات Software - دراسة طلبات المكتب المساعد Help Desk - وإجراء دراسة ميدانية لاستخدام تكنولوجيا المعلوماتية في المنظمة وتحديد مفهوم ونوعية البيانات التي يتم تداولها. وفيما يتعلق بألية مراقبة وتطبيق المعايير والسياسات المتعلقة بتوريد وتنصيب منظومة متكاملة لمراقبة وقياس أداء آلات ومعدات وبرمجيات تقنية المعلوماتية، وتوريد وتنصيب منظومة متكاملة لتطبيق المعايير وتنفيذ السياسات الخاصة بأمن المعلوماتية.

هيكلي يعتمد المعلومة عنصراً أساسياً في تحسين أدائه وبلوغ أهدافه. وذكر أن بناء استراتيجية أمن المعلومات يتكون من 6 أجزاء ويتم عمله بالتوافق مع المعايير الدولية ISO/IEC 2700x و ITIL و COBIT وهي كما يلي: توصيف البيئة المعلوماتية - التحليل الرباعي لتحديد المخاطر ومواطن الضعف - وضع سياسات البيئة المعلوماتية - وضع معايير وأنماط البيئة المعلوماتية - آلية مراقبة تطبيق المعايير والسياسات، وأخيراً وضع خطة إدارة الكوارث واستمرارية العمل. ووصف د. درة توصيف البيئة المعلوماتية التي توصيف الكادر الوظيفي لمركز نظم

وذلك عن طريق فصل إدارة الاستثمار المعلوماتي عن إدارة أمن المعلوماتية، وهذا يعني أن إدارة أمن المعلوماتية يجب أن تكون إدارة منفصلة في أي مركز نظم معلومات ويجب ألا تخصص أعمال وأنشطة أمن المعلوماتية إلى الإدارات الاستثمار المعلوماتية مثل إدارة النظم، إدارة قواعد البيانات وإدارة الشبكات أو إدارة الحاسب الآلي والتشغيل بسبب تعارض المصالح والحفاظ على الموضوعية. وتناول د. درة وضع استراتيجية أمن المعلومات وهي وثيقة تتضمن سياسات ومبادئ ومعايير تنظيم عملية استخدام والتعامل مع مصادر البيئة المعلوماتية المختلفة والتصرف فيها ونقلها داخل

المخاطر التي تتعرض إليها المؤسسات والهيئات الحكومية، لافتة إلى أن كل نوعية منها تختلف طريقة مواجهتها بأنظمة الحماية المختلفة. واختراقات المعلومات من جانبه، قال كبير اختصاصيي نظم المعلوماتية خبير أمن المعلومات المركز الوطني لتطوير التعليم د. خضر درة إن 70% من اختراقات المعلومات التي تتعرض لها المؤسسات المالية تأتي من داخل المؤسسات، مبيناً أن هناك استثمارات ضخمة تنفق لتأمين البيانات لمواجهة خطر القرصنة. واستعرض درة كيفية تنظيم وإدارة أمن البيئة المعلوماتية وتوزيع المخاطر

وسيم سليمان: نظام السحابة لديه القدرة على استيعاب الكم الهائل من الأجهزة باستخدام أقل قدر من الطاقة

محمود فاروق ناقشت الجلسة الأولى من اليوم الثالث والأخير من منتدى الحكومة الإلكترونية الثاني: «الاتجاهات المستقبلية لمراكز المعلومات الحكومية» الذي تنظمه شركة «نوف إكسبو» (NoufEXPO) خلال الفترة من 9 إلى 11 نوفمبر الجاري، أحدث أنظمة حماية المعلومات وكيفية التعامل معها خاصة في ظل التطور السريع والهائل في مجال تكنولوجيا المعلومات، كما طرحت الشركات المشاركة في المنتدى عدة أنظمة حديثة تم ابتكارها خصوصاً لمواجهة جميع عمليات الاختراقات التي تتم على المؤسسات المالية الحكومية. وشهدت الجلسة الأولى حضور كل من المدير الإقليمي ورئيس حماية هندسة الحاسب ميشال لوتس والمدير الإقليمي للشرق الأوسط وشمال أفريقيا وليد بدر. وفي بداية الجلسة كشفت شركة جنرال دينامكس فلدرس لأمن المعلومات عن أحدث أنظمة تأمين المعلومات المتمثل في التحقق العميق من المعلومات وتحليلها ومنع تسربها، حيث تناولت الشركة طبيعة المخاطر التي تتعرض إليها المؤسسات والهيئات الحكومية والمالية التي دعت إلى ضرورة ابتكار أنظمة حديثة تواكب التطور السريع في مجال تكنولوجيا المعلومات. وذكرت الشركة أن تلك الأنظمة الإلكترونية الحديثة تهدف إلى إضافة طبقة جديدة من الحماية لأنظمة الحماية التقليدية، مشيرة إلى طبيعة

الكويت مهية للدفاع عن جميع أصولها الإلكترونية

طفرة هائلة.. 135 ألف متصفح إنترنت في الكويت

241 مليار دولار حجم السوق العالمية للحوسبة بحلول 2020

وضعت شركة سيسكو دليلاً عالمياً للحوسبة السحابية، حيث تتنبأ الشركة بأن «الحركة العالمية السنوية للحوسبة السحابية عبر بروتوكول الإنترنت ستصل إلى 1,6 زيتابايت في نهاية 2015 وبأن حركة الحوسبة السحابية عبر بروتوكول الإنترنت ستمثل أكثر من ثلث (34٪) من مجموع حركة مراكز البيانات بحلول 2016. وفيما يتعلق بالإيرادات، فمن المتوقع أن تنمو السوق العالمية للحوسبة السحابية بنسبة 22 في المئة سنوياً لتصل إلى 241 مليار دولار بحلول سنة 2020.

5 توصيات للمنتدى

اختتم منتدى الحكومة الإلكترونية الثاني: «الاتجاهات المستقبلية لمراكز المعلومات الحكومية»، فعالياته أمس، وقدم 5 توصيات هي كالتالي:

- 1- تحديث الهيكال ووضع المعايير الاستراتيجية الفنية والتشغيلية لمراكز المعلومات الحكومية من واقع متطلبات تنفيذ برامج الحكومة الإلكترونية فيما يخص بيئة التشغيل وأجهزة تخزين وحفظ المعلومات على المدى القريب والى المدى البعيد وكذلك أمن المعلومات من كل جوانبه.
- 2- قيام الجهاز المركزي لتكنولوجيا المعلومات بدراسة وتحديد القواسم المشتركة التي تحتاجها مراكز المعلومات الحكومية من خدمات أو تجهيزات آلية ضمن خطة موحدة تمهيداً لتوفيرها من خلال اساليب مبتكرة كالتعاقدات الجماعية.
- 3- ضرورة قيام الجهاز المركزي لتكنولوجيا المعلومات بالتعاون مع الجهات الحكومية للتأكد من فعالية أنظمة أمن المعلومات لديها، وضرورة وضع خطة وطنية لاستمرارية الأعمال ومواجهة الحالات الطارئة والتغطية عند الكوارث.
- 4- متابعة الجهود لنشر الوعي المجتمعي بمخاطر أمن المعلومات باستخدام كل الوسائل الإعلامية والإعلانية المتاحة والتركيز على أهمية تحمل المسؤولية الفردية في حماية الأنظمة والبيانات الشخصية.
- 5- تكثيف الندوات والمؤتمرات وورش العمل الخاصة بتكنولوجيا مراكز المعلومات الحكومية وأطر الحوكمة الخاصة بها وبرامج الحكومة الإلكترونية وأمن المعلومات وذلك بالتنسيق مع الشركات العالمية المتخصصة في هذه المجالات لعرض التجارب التي قامت بها على مستوى العالم.



جانب من الجلسة الثانية ويبدو من اليمين نائلة العوضي وهشام صفر وماك هاري ومايكل لوتس (قاسم باشا)

المنوية لبعض الناقلات للهجمات الإلكترونية خلال 2014 حيث استحوذت لغة الاستعلام الهيكلية SQL على نسبة 35٪ وعمليات الاقتناص أو التصيد على نسبة 30٪ والمطلعين على نسبة 15٪ والهجمات المتقدمة على نسبة 15٪ والشبكات اللاسلكية على نسبة 5٪. وكشف أن الانتهاكات التي بواسطة سحبات الصرف الآلي بلغت نحو 10 مليون دولار خلال 24 ساعة في حوالي 200 إلى 300 مدينة حول العالم.

ولفت إلى أن استعمال الأفراد لخدمات الحوسبة السحابية (بريد الويب، ومواقع الشبكات الاجتماعية، والتجارة الإلكترونية) يمثل اليوم في ظل التطور التكنولوجي الكبير جزءاً من الحياة اليومية للعديد من بلدان العالم مشيراً إلى أن خدمات الحوسبة السحابية تستخدم في أغراض البيع بالجملة أو الأغراض التجارية، وكذلك بالنسبة للاستهلاك الشخصي.

فقط قطاع تكنولوجيا المعلومات. وأشار ماك السى ان اي.بي.ام لديها أكثر من 50 سنة خبرة في مجال بناء وتصميم قاعدة المعلومات وصممت العديد منها داخل المنطقة لاسيما في الإمارات العربية المتحدة حيث قامت ببناء وتصميم قاعدة بيانات لقيادات شركة البترول كذلك في المملكة العربية السعودية.

التصدي للاختراقات

من جانبه طالب كبير مهندسي الأمن الإلكتروني في جينيرال ديناميكس مايكل لوتس ضرورة التصدي للاختراقات الإلكترونية وفحص شبكات المعلومات بصفة دورية للتصدي للاختراقات المتزايدة للبيئة التحتية. كما شدد على عملية تحميل برامج الحماية من الفيروسات ذات الوثوقية، مشيراً إلى أن ناقلات التهديدات الأمنية قابلة للتوسع، واستعرض بعض النسب

قوية في مجال الدفاع على الهجمات الإلكترونية وقادة على الدفاع عن الأصول والمعلومات. **خفض تكلفة الأعمال**

من جانبه قال ماك هاري مسؤول في شركة اي. بي. ام IBM أن مراكز المعلومات اليوم لم تعد مجرد مجموعة من الأصول المادية، مشيراً إلى أن الحوسبة السحابية من شأنها خفض تكلفة الأعمال بشكل كبير من خلال تقديم نموذج الدفع مقابل الاستخدام. وأكد على أن نموذج الحوسبة سيغير استخدام تكنولوجيا المعلومات حول العالم في المستقبل القريب. مشيراً إلى أن هذه المنهجية الجديدة آخذة في التوسع والانتشار كحل متداول بين أصحاب الأعمال منذ أن أبدت نتائج فعالة وإيجابية. وكشف أن للحوسبة السحابية إمكانات عديدة، حيث من شأنها زيادة الإيرادات وتوسيع الأعمال وخلق فرص عمل جديدة تمتد لقطاعات واسعة ليس

بين جميع الجهات الحكومية كما تعمل على إعادة استخدام المصادر المتاحة وتكامل الخدمات وانتشارها وإعادة استخدام المصادر المتاحة واستخدام الخدمات من الأجهزة المتنقلة واستخدام الخدمات الإلكترونية من أي مكان في العالم بكفاءة وأمان. وأشار إلى أن الحوسبة السحابية تعتبر تكنولوجيا تؤدي إلى «تغيير قواعد اللعب وتوفر مزايًا ضخمة للتطور الذي حصل في الفترة الماضية من ناحية أمن المعلومات. وقال أن الكويت تتمتع بنظرة مستقبلية وهذا من شأنه أن يعمل على حماية قواعد معلوماتها الحكومية، وأشار إلى أن الكثير من الشركات في الكويت لديها إمكانات

حجم الخدمات الآلية والمعلوماتية بلغ نحو 1039 خلال 2014 على مستوى الكويت

منى الدغيمى ترأست مراقبة الدعم الفني في الجهاز المركزي لتكنولوجيا المعلومات نائلة العوضي الجلسة الثانية لمنتدى الحكومة الإلكترونية الثاني في اليوم الثالث والختامي، حيث تمحورت الجلسة حول عصر الحوسبة السحابية وتحولت الحكومة الإلكترونية في عصر الحوسبة السحابية دورها في توفير أعلى مستوى من فعالية تكنولوجيا المعلومات والدروس المستفادة من الاختراقات الأمنية والإدارة الفعالة للشبكات ومراكز المعلومات المستقبلية. في البداية استعرض المدير التنفيذي لشركة ديار المتحدة هشام صفر أهمية الحوسبة السحابية في الحكومة الإلكترونية حيث قال إنها تعتبر منهجية تساعد مختلف المنظمات والكيانات على توفير أعلى مستوى من فعالية تكنولوجيا المعلومات مما يمكن هذه المنظمات من حفظ المعلومات وإدارتها وتحليلها حول العالم اعتماداً على نموها المتسارع، مشيراً إلى أنها تعكس نموجاً جديداً لاستهلاك خدمات تكنولوجيا المعلومات وعرضها وسبل توصيلها. كما تتيح قوة معالجة الحوسبة والتخزين ومعدل نقل البيانات واستخدام البرمجيات وتطويرها والاختيار والأمن والهوية كخدمات عبر الإنترنت. وذكر صفر في مداخلته حول الحكومة الإلكترونية في عصر الحوسبة السحابية أن حجم الخدمات الآلية والمعلوماتية بلغ نحو 1039 خلال 2014 على مستوى الكويت فيما بلغ حجم متصفح الإنترنت نحو 135,1 ألف متصفح وفق إحصائية نوفمبر 2014 مقارنة بنحو 13,86 ألف متصفح في 2008. وقال صفر أن الحوسبة السحابية تمكن من التكامل