مؤتمر «سلسلة الابتكار والأمن السيبراني» (النسخة المصرية) [1]

2nd CSIS: Cybersecurity and Innovation Series (Egyptian Edition)

الفترة من ٢٨-٢٩ مارس ٢٠٢٢م بفندق إنتركونتيننتال سميراميس القاهرة

STRATEGIC PARTNER

itida
IT INDUSTRY DEVELOPMENT AGENCY

ORGANISED BY

MARKET SOLUTIONS
EVENTS MANAGEMENT

تنظيم

Market Solutions Events Management

الشريك الاستراتيجي

هيئة صناعة تكنولوجيا المعلومات (ITIDA)

(١) المصدر:
- تقرير من إعداد الأستاذ/ مازن عباس (المسئول الإدارى والتقنى بمركز بحوث القانون والتكنولوجيا) بشأن حضور فعاليات المؤتمر المشار إليه.
- https://msevents.ae/cyber-security-and-innovation-series-egypt-edition-home-page/
- https://www.linkedin.com/company/ms-eventsmea/

مقدمة

نظَّمت MS Events Management والشريك الاستراتيجي هيئة صناعة تكنولوجيا المعلومات (ITIDA) والشركاء المعاونون (الهيئة الوطنية للسلامة المعلوماتية و OIC-CERT) أول مؤتمر مشترك لسلسلة الابتكار والأمن السيبراني (CSIS) وقمة القوى العاملة الرقمية (DWS). والذي عقد حضوريًا بالقاهرة في الفترة من ٢٨-٢٩ مارس ٢٠٢٢م.

وقد استهدف المؤتمر تبادل الرؤى والأفكار الرئيسية في المجالات المتعلقة بالأمن السيبراني، من خلال اتاحة المنصات المتخصصة للمديرين التنفيذيين من مختلف الصناعات للتحدث والمناقشة حول الجهود المبذولة في مجال الأمن السيبراني وعرض أحدث أنظمة ضمان الأمن السيبراني والاستراتيجيات المختلفة لتحقيق أفضل استراتيجية للتحول الرقمي الآمن.

وشارك في المؤتمر عدد كبير من قادة ومسئولي تكنولوجيا المعلومات والتحول الرقمي والأمن السيبراني من مصر وتونس والإمارات العربية المتحدة وماليزيا والهند والصين. وبمشاركة بعض الأساتذة والطلاب الممثلين عن الجامعات المصرية ومن بينهم طلاب الماجستير المهني للتحقيق في الجرائم الإلكترونية بكلية القانون بالجامعة البريطانية في مصر.

وتناول المؤتمر العديد من المحاضرات والنقاشات الهادفة لأن تكون مصر قادرة على الصمود رقميًا عبر الإنترنت بما يواكب رؤية مصر ٢٠٣٠. كما تحدث خبراء أمن المعلومات والفضاء السيبراني عن أهمية وكيفية مواجهة التحديات التي تواجه مختلف القطاعات في بناء نظم أمن معلوماتية يمكنها الصمود في وجه الهجمات السيبرانية الناشئة في مختلف القطاعات المالية والمصرفية والشركات والمؤسسات الحكومية والخاصة والأجهزة الحساسة بالدولة.

كما جرت بعض المناقشات الهامة حول الآليات اللازمة لتوفير سلامة المؤسسات في ظل سارع التقنيات في الفضاء السيبراني مثل الذكاء الاصطناعي والتعلم الآلي

وسلسلة الكتل (بلوك تشين Blockchain) والتشفير والقوانين واللوائح والسياسات الداخلية الخاصة بالأمن السيبراني.

وقد عرض المؤتمر مثال ناجح للبيئة التشريعية الداعمة للتطور التقني من خلال عرض التجربة التشريعية لدولة ماليزيا، حيث قام أحد المتحدثين الأجانب بعرض التطور في التشريعات والقوانين السيبرانية التي اتخذتها ماليزيا نهجًا لها من خلال حفظ الهوية الوطنية وحماية الحدود الرقمية الوطنية والاهتمام بقطاع التعليم ونشر الوعي وتدريب المشرعين على تنفيذ القوانين السيبرانية والمعرفة بالأمن السيبراني وإنشاء سياسة وطنية للتشفير وبناء معامل تحقيق جنائي رقمي معتمدة مما جعل ماليزيا تحتل المرتبة الثانية في أسيا في هذا المجال.

أهداف المؤتمر

من أهم النقاط التي سعى المؤتمر لمناقشتها:

- فهم التنفيذ الفعلي للسياسات والإجراءات في إطار استراتيجية مصر الجديدة لتكنولوجيا المعلومات والاتصالات ٢٠٣٠.
- مناقشة الخطوات التي يتعين على المؤسسات اتخاذها لتظل قادرة على التكيف مع الطبيعة المتغيرة للهجمات السيبرانية.
- التأكد من أن أدوات الأمان قابلة للتكيف لمواكبة المتطلبات المتغيرة باستمرار.
- وضع خطط استباقية لتحديد الانتهاكات المحتملة ومعالجتها والحد منها في النهاية.
- التنفيذ الناجح للتقنيات المتقدمة مثل الذكاء الاصطناعي والتعلم الآلي لتعزيز الإجراءات الأمنية.
- التعرف على تأثير رقمنة سلاسل التوريد على بروتوكولات الأمان في مختلف الصناعات.

- تبادل الأفكار حول أهمية تطبيق أدوات الأمان المناسبة عبر المؤسسة بأكملها.
- التعرف على الثورة الصناعية الخامسة (Industry ٥,٠) واكتشاف كيف تتطور الصناعة لضمان عمل الإنسان والآلة جنبًا إلى جنب لتحسين الكفاءات وتقليل التحديات الأمنية.

محاور المؤتمر

اليوم الأول:

- المحور الأول: أهمية التعاون لتحسين المنعة السيبرانية (Cyber Resilience)[١] داخل وعبر القطاعات وعلى المستوى الإقليمي على السواء.
- المحور الثاني: نهج حماية الفضاء السيبراني الوطني من التهديدات المحتملة ومشاركة الحضور التجربة التونسية وإطار عمل المراقبة وتحليل الأنشطة الخبيثة واستخراج المعرفة اللازمة لتعزيز المستوى الأمني للمؤسسات التونسية.
- المحور الثالث: دمج إطار تنظيمي قوي معمول به لدعم التحول نحو الاقتصاد الرقمي.
- المحور الرابع: ظهور مصر الرقمية الجديدة: أهم تحديات الامتثال التي تواجهها الأسواق.
- المحور الخامس: الذكاء الاصطناعي والتعلم الآلي في عالم الأمن السيبراني: إلى أين نتجه؟
- المحور السادس: النظر إلى الأمن السيبراني على أنه عامل تمكين للتحول الرقمي.
- المحور السابع: الأمن السيبراني في التحول الرقمي.
- المحور الثامن: وضع نموذج لخطة قوية للاستجابة للحوادث لتمكين الفرق وتخفيف الضرر.

(١) قدرة الكيان على الصمود في المواجهة باستمرار على الرغم من الأحداث السلبية الناتجة عن الجرائم الإلكترونية المتغيرة

- المحـور التاسع: تأمـين مؤسستك فـي كل خطوة من سلسلـة التوريد لضمان دفاع إلكتروني أكثر حزمًا.
- المحور العاشر: مواجهة التحديات المرتبطة بسلاسل التوريد المعقدة لتقليل نقاط الضعف.
- المحور الحادي عشر: تعزيز تعاون أفضل للدفاع عن سلاسل التوريد الحديثة من الهجمات الخارجية.
- المحـور الثاني عشر: استخدام قدرة الذكاء الاصطناعي على التعامل مع التعقيد وعدم القـدرة على التنبؤ لحماية أنظمة التكنولوجيـا التشغيلية من أجل تحسين العمليات.

اليوم الثاني:

- المحـور الأول: تمكين المؤسسات من أن تكون أكثر كفاءة من حيث التكلفة والموارد لتحسين العمليات من خلال دمج تكنولوجيا المعلومات والتكنولوجيا التشغيلية.
- المحـور الثاني: ظهور كوفيد ١٩: تطور استراتيجيات الأمن السيبراني في عصر العمل عن بعد.
- المحـور الثالث: كـن استباقيًا وليـس تفاعليًا: التخلص من مشـاكل كلمات مرور المؤسسة.
- المحـور الرابـع: التعامل مـع الأمن السيبراني كقـرار تجاري شامـل للتغلب على المخاطر الأساسية للأمن السيبراني وتحقيق أهداف العمل.
- المحور الخامس: دمج البنية الأمنية التعاونية لضمان الأدوات المناسبة والتدريب والموارد اللازمة لحماية المعلومات.
- المحـور السادس: كيفية عرض الأمـن السيبراني إلى مجلس الإدارة والمستوى C لضمـان الدعـم الفعـال والموارد فـي الحـرب الإلكترونية الخاصـة بك ضد التهديدات.

- المحور السابع: الاستعداد لما لا مفر منه: بناء استراتيجية قوية للأمن السيبراني من أجل إدارة مخاطر مؤسسية ناجحة.

توصيات المؤتمر

- أهمية التعاون المشترك بين الأقسام الداخلية للمؤسسة مثل قسم التحقق من الامتثال والموارد البشرية وإدارة المخاطر وتكنولوجيا المعلومات وعلى رأسهم مجلس الإدارة والتعاون بين القطاعات المختلفة في الدولة مثل القطاع المصرفي والشركات والحكومة كعامل تمكين رئيسي للمنعة السيبرانية.
- يجب السعي وراء التعاون المشترك بهدف الصالح العام وليس لتحقيق حماية فردية فلم يثبت أن فريقًا أو قطاعًا واحدًا استطاع التصدي لهجمات خارجية دون تعاون من قطاعات أخرى.
- يجب على مديرو المؤسسات الفهم الجيد لأهمية الإنفاق والإستثمار في أمن المعلومات وتحقيق بنية رقمية قادرة على التصدي للهجمات السيبرانية.
- الهجمات السيبرانية ونقاط الضعف بالأنظمة الإلكترونية لا يمكن منعها فهذا يعد أمرًا مستحيلًا ولكن يمكن التكيف معها وتقليل خطورتها.
- الاهتمام بالتعليم والتوعية بالأمن السيبراني بداية من طلاب المدارس مما ينشئ جيلًا قويًا بالمستقبل.
- أهمية تنفيذ التشريعات واللوائح الدولية والإقليمية والعالمية وعمل تعديلات على السياسات الداخلية للمؤسسات لبناء بنية تحتية رقمية في إطار التحول الرقمي الذي تشهده مصر والمنطقة.
- أهمية الإلمام بالقوانين واللوائح ذات الصلة مثل قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ وقانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ وقانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣ وقانون البنك المركزي رقم ١٩٤ لسنة ٢٠٢٠ واللائحة الأوروبية لحماية البيانات (GDPR) والقوانين الأمريكية والعربية والأسيوية المعنية بالخصوصية.

- مـن المشاكل والتحديات التي تواجه الأمن السيـبراني فـي مصر هو عدم فعالية الرقابة على تنفيذ بعض القوانين ذات الصلة.
- على كل رؤساء أمن المعلومات وضع استراتيجيات واضحة للأمن السيبراني.
- مـن المهم بنـاء الاستدلال الجنائي الرقمي الخاص بـك دون اللجوء لطرف آخر لعمله لك.

– وانتهـى المؤتمر الذي استمر على مـدار يومين بتسليم جوائز تذكارية لبعض قادة أمـن المعلومات والشـركات تكريمًا لهم على مجهوداتهم المبذولـة فـي الأمن السيبراني فـي مصر والعالم العربي